Die approbierte Originalversion dieser Dissertation ist an der Hauptbibliothek der Technischen Universität Wien aufgestellt (http://www.ub.tuwien.ac.at).

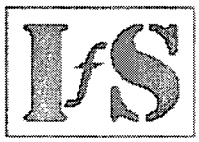
The approved original version of this thesis is available at the main library of the Vienna University of Technology (http://www.ub.tuwien.ac.at/englweb/).

DISSERTATION

SICHERHEITSKONZEPTE FÜR PRIVATE NETZWERKE

ausgeführt zum Zwecke der Erlangung des akademischen Grades eines Doktors der technischen Wissenschaften unter der Leitung von

Univ. Doz. Dipl.-Ing. Dr. techn. Ernst PILLER
Institut für Softwaretechnik und Interaktive Systeme (E188)



Information &
Software Engineering Group

eingereicht an der Technischen Universität Wien
Fakultät für Technische Naturwissenschaften und Informatik
von

Dipl.-Ing. Alexander DUSCH
Matr. Nr.: 9426602
Leibnizgasse 55/16
A-1100 WIEN

Wien, im Oktober 2004

DI Alexander Dusch

Danksagung

Als erstes möchte ich mich bei Herrn Dr. Piller einerseits für die Möglichkeit die Dissertation auch während meiner beruflichen Tätigkeit fertigstellen zu können und andererseits für die genaue Durchsicht der Arbeit und die zahllosen Gespräche bedanken, welche mir wertvolle Anregungen für die kontinuierliche Verbesserung der Arbeit brachten.

Als zweites möchte ich Herrn Prof. Eier für die Zweitbegutachtung und die lebhaften Diskussionen bedanken, die deutlich die Lesbarkeit der Arbeit verbessert haben.

Mein besonderer Dank gilt meiner Frau Edith, die trotz der vielen Zeit in der sich mich entbehren musste immer zu mir gestanden hat.
Ihr möchte ich diese Dissertation widmen.

Kurzzusammenfassung

Diese Dissertation beschäftigt sich mit Konzepten, die es ermöglichen ein privates Netzwerk sowohl gegen Angriffe von außen, als auch von innen zu schützen.
Die Notwendigkeit des Schutzes von Netzen begründet sich vor allem in der rasant wachsenden Internetgesellschaft. Heutzutage besitzt fast jede Firma bereits einen Anschluss an das Internet. Computer haben Einzug in fast jedes Büro erhalten. Die Vernetzung der einzelnen Workstations und Server ist zu einem Muss geworden. Durch diese Entwicklungen ergeben sich eine Vielzahl von neuen Gefahren und Angriffsmöglichkeiten. Der Schutz von sensiblen Daten wird dadurch immer schwieriger, und es müssen Konzepte entwickelt werden, die diese Sicherheitsanforderungen erfüllen können. Ein weiterer Trend ist die Aufsplittung von Firmen in eine Zentrale und diverse Außenstellen im In- und Ausland. Dadurch entsteht natürlich massiver Datenverkehr zwischen den einzelnen Standorten. Dieser Datenverkehr erschwert natürlich die dementsprechende Absicherung. Diese Dissertation soll dementsprechend Konzepte aufzeigen, die es ermöglichen auch in der dezentralisierten Welt, in der wir heute leben, sensible Daten so zu sichern, dass es zumindest sehr erschwert wird, dass diese Daten durch Dritte abgefangen werden.

Abstract

This thesis discusses methods for securing a private network against attacks from inside and outside.
The necessity for securing networks arises from a world where the Internet is growing permanently. Almost every organization in the world owns an Internet connection nowadays. Almost every office is equipped with a lot of computers. Connecting servers with the workstations on the private network has become obligatory. This trend imposes a variety of dangers and possible attacks against the network. Securing confidential data is getting more difficult regarding this specific trend. Concepts have to be developed to implement more secure networks for private organizations. A second trend is the establishment of branch offices all over the world. Massive data throughput emerges from this trend. It is imperative that this data is properly secured against eavesdropping and a variety of attacks. This thesis discusses concepts which make it possible to secure confidential data to that extent, that it is extremly difficult for third parties to obtain this data.

Vorwort

Teil I definiert wichtige Begriffe und beschäftigt sich mit den verschiedenen Bedrohungen, denen Computersysteme heutzutage ausgesetzt sind.

In Teil II werden einige grundlegende Begriffe und Technologien vorgestellt, welche für die Sicherheit relevant sind. Dabei liegt das Hauptaugenmerk auf den Themen Firewall, Verschlüsselung und Authentifikation und Autorisation.

Teil III, beschäftigt sich sodann mit praktischen Möglichkeiten, um private Netzwerke abzusichern. Zusätzlich werden noch einige Punkte aufgezeigt, welche bei zukünftigen Sicherheitskonzepten eine wichtige Rolle spielen werden.

Teil IV, welcher den zentralen Teil dieser Dissertation darstellt, beschäftigt sich mit Lösungsmöglichkeiten für zukünftig zu erwartende Probleme, und deren Lösung. Abschluss der Dissertation bildet eine Zusammenfassung der wichtigsten Sicherheitsthemen und meine persönliche Meinung.

Teil I Einleitung 8

1 Definitionen 8

2 Bedrohungen 8
2.1 Kategorien von Bedrohungen 9
2.2 Arten von Angriffen 10
2.3 Zusammenfassung 13

Teil II Grundlagen der Netzwerksicherheit 14

3 Formale Sicherheitskonzepte 14
3.1 Sicherheitsmodelle 14
3.2 Kryptografie 15
3.3 Authentifikation und Autorisation 17
3.4 Virenschutz 21

4 Protokollspezifische Sicherheitsaspekte 23
4.1 Netzzugangsebene 24
4.2 Netzwerkebene 25
4.3 Transportebene 26
4.4 Anwendungsebene 27
4.5 Verschlüsselungsprotokolle 30
4.6 Sicherheitskriterien bei Multimedia-Protokollen 33

5 Technische Sicherheitskonzepte 36
5.1 Firewalls 36
5.2 Proxy-Server 46
5.3 Content Walls und Content Filtering 47
5.4 Backup & Disaster Recovery 48
5.5 Virtual Private Network (VPN) 51

6 Organisatorische Sicherheitsaspekte 54
6.1 Die Security-Policy und das Security-Wheel 54
6.2 Das Konzept des Patching 56
6.3 Backup & Disaster Recovery 57
6.4 Userspezifische Sicherheitsaspekte 60

Teil III Sicherung eines privaten Netzwerks 62

7 Planung und Implementation von Internet- und Intranet-Sicherheit 62
7.1 Unternehmensrichtlinien für Netzwerksicherheit 62
7.2 Risikoanalyse 62
7.3 Die Erstellung von Sicherheitsrichtlinien 63
7.4 Implementationsplan für eine Internet-Sicherheitsarchitektur 68

8 Betriebssystemsicherheit 69
8.1 Unix/Linux 69
8.2 Windows 70
8.3 Zusammenfassung 71

9 Firewall-Implementation 72
9.1 Firewall-Aufbau 72
9.2 DMZ-Aufbau 73
9.3 Dienste 73
9.4 Minimale Regelbasis 74

10 Sicheheit der von der Firewall erlaubten Dienste 74
10.1 E-Mail Sicherheit 74
10.2 FTP-Sicherheit 75
10.3 HTTP-Sicherheit 75

11 Standortübergreifende Netzwerke 76
11.1 WAN-Verbindungen 76
11.2 RAS-Verbindungen 76
11.3 VPN-Verbindungen 77
11.4 Zusammenfassung 78

12 Wireless LAN (WLAN) Sicherheit 78
12.1 Definition 78
12.2 Funktionsweise 78
12.3 Standard Sicherheits-Mechanismen 79
12.4 Zusammenfassung 80

13 Virenschutzlösungen im Corporate-Bereich 81
13.1 Anforderungen 81
13.2 Implementation 82
13.3 Zusammenfassung 82

14 Intrusion Detection Systeme 83
14.1 Funktionsweise 83
14.2 Grenzen 83
14.3 Zusammenfassung 84

15 Intranetsicherheit 84
15.1 Definition 84
15.2 Anwendungsgebiete 84
15.3 Sicherheitsaspekte 85

Teil IV Die Zukunft der Netzwerksicherheit *86*

16 Trends und zukünftige Entwicklungen 86
16.1 Firewalls und Angriffserkennung auf Basis von künstlicher Intelligenz 86
16.2 Die Post-Firewall-Ära 86
16.3 Zusammenfassung Trends 87

17 Weiterentwicklung und Zukunftsperspektiven 88
17.1 Physische Sicherheit 88
17.2 Weiterentwicklung des SMTP-Protokolls 92
17.3 Entwicklung neuer Netze in der Zukunft 94
17.4 Zukünftige Entwicklung der Chips 95
17.5 Sicherheit durch Zentralisierung 97

18 Expertensysteme für automatische Sicherheitseinstellungen 98
18.1 Einleitung 98
18.2 Anforderungen an „Mobile Security NG“ 98
18.3 Software-Komponenten 99
18.4 Firewall-Software 102
18.5 WLAN-Konfigurationssoftware 102
18.6 Netzwerk- und Modem-Konfigurationssoftware 102
18.7 VPN-Software 108
18.8 OS-Hardening Software 110
18.9 Anti-Virus-Software 113

18.10 Intrusion Detection Software ____ 114
18.11 Content Filtering Software ____ 114
18.12 Architektur von „Mobile Security NG“ ____ 115
18.13 Architektur von „Mobile Security NG Corporate“ ____ 126
18.14 Analyse „Mobile Security NG“ und „Mobile Security NG Corporate“ ____ 128
18.15 Problematik ____ 134
18.16 Pervasive Computing ____ 135
18.17 Telefonanlagen der Zukunft in Verbindung mit „Mobile Security NG Corporate“ ____ 139

19 Zusammenfassung und Ausblick ____ 147

Anhang A: Literaturverzeichnis ____ 148

Anhang B: Abbildungsverzeichnis ____ 151

Anhang C: Liste der wichtigsten Ports ____ 153

Anhang D: Lebenslauf ____ 156

Teil I Einleitung

1 Definitionen

Diese Dissertation beschäftigt sich mit der Sicherheitsproblematik von privaten Netzen. Ein **privates Netzwerk** oder Local Area Network (LAN) bezeichnet dabei ein räumlich abgegrenztes Netzwerk, welches über eine begrenzte Zahl von Teilnehmern verfügt und entweder von Firmen oder staatlichen Organisationen betrieben wird. Unter einem **öffentlichen Netzwerk** oder Wide Area Network (WAN) verstehen wir ein Netzwerk welches sich geographisch weitläufig erstreckt. Dieses Netz wird von den Betreibern allgemein für die Nutzung zur Verfügung gestellt. Ein spezielles öffentliches Netz ist auch das **Internet**. Meist werden private Netzwerke über öffentliche Netze miteinander verbunden, oder nur an öffentliche Netze angebunden. Wenn Informationen in solch einer Umgebung für den Zugriff bereitgestellt werden, müssen sichere Zonen definiert werden. Das Gerät, welches diese Zonen voneinander trennt, wird als **Firewall** bezeichnet. Firewalls können aber auch verwendet werden, um private Netzwerksegmente voneinander zu trennen.
Um Missverständnisse zu vermeiden soll hier noch erklärt werden, dass unter einem **Virtual Private Network** (VPN) ein privates Netz verstanden wird, welches aber nur virtuell über ein öffentliches Netzwerk angeboten wird. Das bedeutet, dass private Netzwerk existiert zwar real, wird aber von Teilnehmern außerhalb des lokalen Netzwerks verwendet.

2 Bedrohungen

Dieses Kapitel befasst sich mit den einzelnen Arten von Bedrohungen und Attacken gegen ein Netzwerk. Es soll aufgezeigt werden, welche Bedrohungen existieren und welchen Stellenwert sie einnehmen. Die Abbildung zeigt die Entwicklung von Vulnerabilities, Sicherheitsvorfällen und den Sicherheitsprdukten mit dem verbreiteten Einsatzzeitraum.

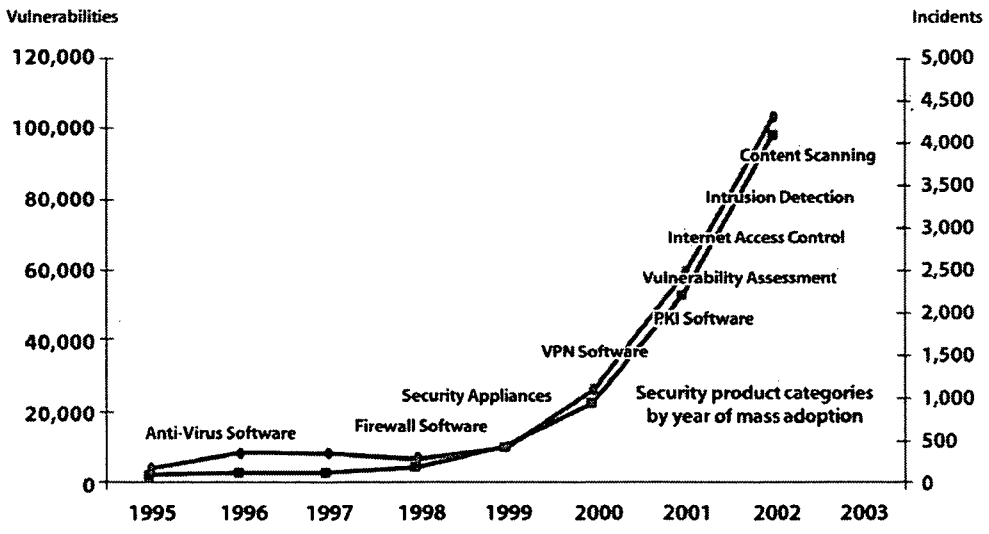


Abbildung 1: Entwicklung [47]

2.1 Kategorien von Bedrohungen

- Unstructured Threats
  Diese kommen vor allem von unerfahrenen Individuen, die sich spezieller vom Internet downloadbarer Tools bedienen. Die meisten werden durch die intellektuelle Herausforderung motiviert, und werden in der Fachsprache als „Script Kiddies" bezeichnet. Diese verursachen eine extreme Bedrohung für Computernetze, da ihnen häufig die Funktionsweisen und Zusammenhänge der verwendeten Tools gar nicht begreiflich sind. Dadurch können Viren oder Trojanische Pferde losgelassen werden, die Firmen viele Millionen Dollar an Kosten verursachen können.

- Structured Threats
  Diese gehen von Individuen aus, die hochmotiviert sind, und auch über die technische Kompetenz verfügen. Diese Personen werden im umgangssprachlichen Gebrauch als Hacker bezeichnet, und werden oft von kriminellen aber auch staatlichen Organisationen angeheuert.

- External Threats
  Diese gehen von Individuen außerhalb der Organisation aus, und sie verwenden das Internet oder Einwahlserver als Medium.

- Internal Threats
  Diese gehen von Individuen aus, welche über autorisierten Zugang verfügen. Einige Studien haben gezeigt, dass dies die häufigste Bedrohung für Netzwerke darstellt.

Folgende Abbildung zeigt die Entwicklung von intelligenten Tools in Zusammenhang mit dem Wissen der Angreifer.

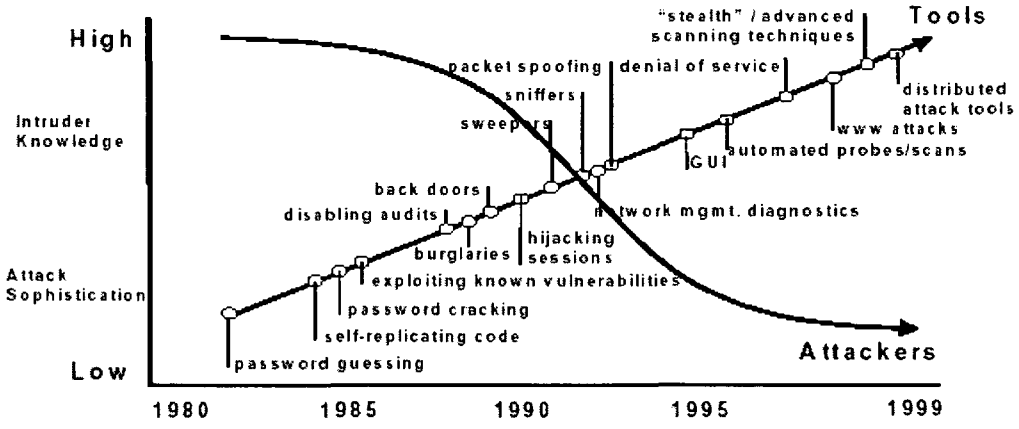


Abbildung 2: Tools und Angreiferwissen

2.2 Arten von Angriffen

2.2.1 Reconnaissance Attacken

Ein Agreifer versucht Systeme, Services und Vulnerabilities zu entdecken und auszunutzen.

Bei dieser Art des Angriffs geht es darum, Netzwerkkomponenten und die darauf laufenden Services zu entdecken. Dadurch können eventuelle Sicherheitslücken entdeckt, und ausgenutzt werden.
Eine Technik, welche für diese Art des Angriffs angewendet wird, ist der sogenannte „ping sweep", bei dem zuerst mithilfe von pings die aktiven IP-Adressen ausgeforscht werden, um dann mithilfe eines Port-Scanners herauszufinden, welche Dienste auf den entdeckten Netzwerkkomponenten aktiv sind.
Diese Art der Attacke wird meist als Basis für die beiden anderen Attacken genutzt.

2.2.2 Access Attacken

Ein Angreifer attackiert Netzwerke oder Systeme um Daten zu gewinnen, Zugriff zu erlangen, oder die persönlichen Benutzerrechte anzuheben.

Unter Access versteht man die Möglichkeit zu haben, von einem Computer, welcher an das Internet angeschlossen ist, Zugriff auf einen anderen, ebenfalls an das Internet angeschlossenen Computer zu haben.
Access Attacken können in drei Ausprägungen auftreten:

- Unauthorized Data Retrieval and Manipulation
  Hierbei geht es um Lesen, Schreiben, Kopieren und Verschieben von Daten, auf die der Eindringling keinen Zugriff hat. Oftmals ist dies sehr einfach, da freigegebene Ordner, oder über NFS exportierte Verzeichnisse unter Unix so definiert sind, dass jeder Lesezugriff oder sogar Lese- und Schreibzugriff auf diesen Freigaben oder NFS-Verzeichnissen hat. Es gibt zwei einfache Möglichkeiten dies zu verhindern. Entweder definiert man Freigaben und NFS-Verzeichnisse so, dass wirklich nur autorisierte User Zugriff auf diese haben, oder man verschlüsselt die Daten.

- Unauthorized System Access
  Hierbei geht es um einen Systemzugriff ohne Autorisierung. Dies kann über eine Vielzahl von Wegen erreicht werden. Sehr oft gibt es Systeme, die nicht passwortgeschützt sind. Hier ist es einfach Zugriff zu erlangen. Manchmal muss aber eventuell ein Script gestartet werden, oder ein Softwaretool verwendet werden, um bestimmte Sicherheitslücken auszunutzen. Bestimmte Schwachstellen im Betriebssystem selbst können ebenfalls für diese Art des Angriffs herangezogen werden.
  Bei diesem Aspekt ist es wichtig, sowohl Passwortrichtlinien durchgängig einzusetzen, als auch jeweils die neuesten Patches anzuwenden, um schon bereits bekannte Sicherheitslücken zu schließen.

- Unauthorized Privilege Escalation
  Dieser Angriff wird von Usern durchgeführt, welche einen sehr niedrigen Zugriffslevel besitzen. Das Ziel liegt darin, diesen eingeschränkten Zugriff mit Tools, wie Packet Sniffern o. ä. zu erweitern, damit Benutzernamen oder Passwörter herausgefunden werden können. Das größte Ziel ist aber, solche Benutzeraccounts zu entdecken, die verwendet werden können, um Zugriff auf weitere Systeme zu erlangen.
  Dies ist sicher eine der am schwierigsten in den Griff zu bekommenden Attacken. Es gibt aber durchaus die Möglichkeit, Benutzerrechte so zu verteilen, dass auf kritische Systeme durch unterprivilegierte User gar kein Zugriff möglich ist. Weiters sollte auch die Passwortrichtlinie so definiert werden, dass selbst dann wenn ein höher privilegierter Zugriff für ein bestimmtes System herausgefunden wurde, dieser User auf den anderen Systemen entweder gar nicht existiert, oder aber ein völlig anderes Passwort besitzt.

2.2.3 Denial of Service (DoS) Attacken

Ein Angreifer attackiert ein Computersystem derart, dass es beschädigt oder zerstört wird, oder damit das System den autorisierten Usern keinen Zugang mehr gewährt.

Unter DoS versteht man, dass ein Angreifer Netzwerke, Systeme oder Services derart überlastet, dass diese entweder nicht mehr funktionstüchtig sind, oder derart verlangsamt werden, sodass sie nicht mehr verwendbar sind. In den meisten Fällen geht dies sehr einfach durch Verwendung eines Hacks, Scripts oder Tools [50]. Ein vorheriger Zugriff auf ein bestimmtes System ist hierbei aber nicht notwendig, allein der Weg zum Ziel muss frei sein. Nachdem diese Art des Angriffs relativ einfach zu realisieren ist und auch völlig anonym durchgeführt werden kann, ist es die meistgefürchtete Attacke im Internet.
An dieser Stelle sei auch noch der Begriff des Distributed Denial of Service (DDoS) erklärt. Hierbei geht der Angriff von mehreren Quellen aus, und es ist deshalb sehr schwierig, einerseits die Quellen ausfindig zu machen und andererseits diese auch zu stoppen.

2.2.4 Spoofing Attacken

Bei dieser Art des Angriffs geht es darum, eine falsche Identität vorzuspiegeln. Ein Beispiel für Spoofing ist das Versenden einer E-Mail mit einer gefälschten Absenderadresse. Weitere Möglichkeiten des Spoofings wären aber auch die Annahme der Identität eines Servers (z.B. DNS-Name oder IP-Adresse), um Anfragen von Clients selbst beantworten zu können. Dabei ist es natürlich leicht möglich, gefälschte Daten an die Clients zu übermitteln. Das Spoofing ist neben den DoS Attacken die häufigste im Internet verbreitete Art der Angriffe.

2.2.5 Würmer

Aufgrund der hochautomatisierten Natur von Würmern verbunden mit einer sehr weiten Verbreitung der Vulnerabilities, welche diese Würmer ausnutzen, erlauben sie eine Vielzahl von Systemen innerhalb von Stunden zu kompromittieren. Ein Beispiel hierfür wäre Code Red, welcher innerhalb von 9 Stunden am 19. Juli 2001 über 250.000 Systeme befiel [46].

2.2.6 Attacken auf das Internet Domain Name System (DNS)

DNS ist ein verteiltes System zur Umwandlung von Domain-Namen in IP-Adressen. Ein Großteil der DNS-Server sind verwundbar gegen Angriffe, die es ermöglichen, dass Domain-Namen auf IP-Adressen des Angreifers umgesetzt werden [46], [49].

2.2.7 Spam und Phishing

Bei Spam und Phishing handelt es sich um Bedrohungen, welche von unerwünschten Mails augehen. Spam unterscheidet sich vom Phishing aber dahingehend, dass diese E-Mails meist keinen Schaden verursachen, sondern es sich nur um unerwünschte Mails mit Werbeinhalten oder dergleichen handelt. Zum Problem wird Spam nur dann, wenn dadurch die E-Mail-Kommunikation durch Überlastung des Mail-Servers, unterbrochen wird. Wirksamen Schutz hierfür bietet meist nur ein Spam-Filter, welcher entweder in den Mail-Server integriert, oder davor geschaltet wird. Diese Filter blockieren Mails mit bestimmten Inhalten oder aufgrund von Absender-Blacklists.
Beim Phishing werden E-Mails als seriöse Nachrichten von Kreditinstituten getarnt und fordern den Empfänger auf, z.B. seine persönlichen Daten, Passwörter oder PIN-Codes zu aktualisieren. Mithilfe dieser erhaltenen Daten können die Betrüger dann Konten plündern [71]. Auch um dem in den letzten Monaten verstärkt auftretenden Phishing-Mails entgegenzuwirken, haben sich Spam-Filter bewährt. Die Problematiken, welche sich durch Spam-Filter ergeben, sollen im folgenden erläutert werden. Einerseits besteht die Möglichkeit, einen zentralen Spam-Filter einzusetzen. Dies bietet den Vorteil, dass Mitarbeiter sich nicht um Konfiguration und Wartung kümmern müssen. Problematisch ist aber hingegen, dass bei dieser Variante die Möglichkeit besteht, dass Mails blockiert werden, die als geschäftkritisch eingestuft werden müssen. Jeder noch so gute Spam-Filter ist nicht in der Lage, für jedes Mail 100%-ig zu bestimmen, ob es sich dabei um Spam handelt oder nicht. Zwar gibt es einerseits die Möglichkeit, dass jedes als Spam eingestufte Mail vom Administrator überprüft wird, was aber vom Datenschutzaspekt als bedenklich anzusehen ist, und andererseits können diese Mails natürlich automatisch an den Absender retourniert werden, was aber ebenfalls Probleme mit sich bringen kann. Eine zweite Variante wäre, dass auf den Desktops Spam-Filter installiert werden. Hierbei muss aber der Mitarbeiter die Konfiguration und Wartung des Filters übernehmen, was ebenfalls als problematisch anzusehen ist.
Welche Möglichkeit auch immer eingesetzt wird, es ist trotz dessen immer die beste Strategie, seine Mitarbeiter durch Schulungen oder Hinweise auf diese Gefahren hinzuweisen, und Ihnen aufzuzeigen, wie mit der jeweiligen Situation umgegangen werden muss.
Schwieriger wird die Situation im rein privaten Bereich. Hier ist es viel schwieriger die Menschen über derartige Dinge zu informieren. Medien und Politik sind an dieser Stelle gefragt, die Bevölkerung so schnell wie möglich zu informieren. Auch Provider könnten in diesen Informationsprozess integriert werden, da sie den direktesten Zugang zum Anwender haben.
In der Zukunft soll mithilfe der Mail-Server-Authentifizierung erreicht werden, dass die Identifikation des tatsächlichen Absenders einer Mail möglich wird [71]. Derzeit arbeiten mehrere Anbieter, unter Ihnen auch Microsoft, an jeweiligen Lösungen, welche beinhalten, dass die IP-Adressen der Absender in einem speziellen Format im DNS publiziert werden müssen. Bis diese Produkte aber Serienreife besitzen müssen erst einheitliche Standards definiert werden, sodass dabei noch einige Zeit vergehen wird.

2.2.8 Dialer

Bei Dialern handelt es sich um Programme, welche es dem Anwender erleichtern sollen, eine Online-Verbindung einzurichten. Die seriöse Variante wird meist von Providern zur Verfügung gestellt, damit auch unerfahrene Anwender auf möglichst einfache Weise eine Internetverbindung einrichten können. Die unseriösen Dialer installieren sich entweder über einen getarnten Link, oder vollautomatisch über ActiveX. Bei dieser Art der Dialer werden Mehrwertnummern (0900) verwendet, um sich ins Internet einzuwählen. Nach der Installation wird dann immer automatisch über diese Dialer-Verbindung der Internet-Zugang hergestellt.

Die Kosten werden über die normale Telefonrechnung abgebucht. Problemtisch werden Dialer meist nur im Privatbereich, wo viele Anwender sich noch über Modem oder ISDN ins Internet einwählen. Breitbandverbindungen sind durch diese Art der Bedrohung nicht betroffen, wodurch die meisten Firmen auch keine Probleme mit Dialern bekommen.
Der beste Schutz vor Dialern ergibt sich durch die Sperrung sämtlicher Mehrwertnummern, was bei der Österreichischen Telekom einfach möglich ist. Nichtsdestotrotz spielt genau wie bei Spam und Phishing die Information der Nutzer eine tragende Rolle. Da die vollautomatische Installation derzeit nur per ActiveX möglich ist, kann entweder ein anderer Browser als der Internet Explorer verwendet werden, oder eine Erhöhung der Sicherheitsstufe im Internet Explorer den gewünschten Erfolg bringen.

2.2.9 Adware, Spyware und Browser Hijacking

Ein weiterer relativ neuer Trend sind Adware, Spyware und Browser Hijacking. Dabei handelt es sich um spezielle Software, welche durch den Besuch von bestimmten Web-Seiten automatisch installiert werden. So kann es passieren, dass plötzlich Browser-Fenster mit Werbung (Adware), Programme automatisch installiert werden, und plötzlich im Tray auftauchen, dubiose Links in den Favoriten erscheinen, man immer auf andere Start-Seiten umgeleitet wird und degleichen (Browser Hijacking), und Programme, die den Computer ausspionieren, und Daten für Dritte sammeln (Spyware). Zusammengefasst werden die drei Begriffe meist unter dem Synonym der Malware [72]. Im Corporate Bereich haben sich hierfür Web-Filter bewährt, welche solche Seiten prinzipiell sperren. Für den Privatbereich gibt es diverse Freeware-Programme, um diese Arten von Software wieder zu entfernen. Die Problematik dabei ist, dass es dann meist schon zu spät und sogar das Betriebssystem soweit beschädigt ist, dass eine Neuinstallation unumgänglich ist. Sinnvoll wäre es deshalb, die Erkennung dieser Bedrohungen in Virenschutzsoftware zu integrieren.

2.2.10 Weitere Formen von Attacken

Zusätzlich existieren eine Vielzahl von anderen Angriffsmethoden, wie z.B. der Versand von falschen Microsoft-Patches per E-Mail oder Angriffe gegen ungeschützte Internet-Router und dergleichen [46]. Außerdem steigt die Geschwindigkeit, mit der bestimmte Vulnerabilities publik werden. Damit entstehen permanent neue Angriffsmöglichkeiten, und es wird immer schwerer rasch genug auf die neue Situation zu reagieren.

2.3 Zusammenfassung

Die oben genannten Attacken geben einen guten Überblick, mit welchen Sicherheitsproblemen bei einem privaten Netzwerk, welches an das Internet angebunden ist, zu rechnen ist. Gegen sämtliche Angriffe, gibt es Möglichkeiten vorzubeugen. Diese Möglichkeiten sollen im weiteren beleuchtet werden und vor allem speziell im Bezug auf private Netzwerke untersucht werden.
Wichtig ist dabei, die einzelnen Arten von Bedrohungen zu kennen, und Vorbeugungen dagegen anwenden zu können. Wer nun aber meint, dass er mit der Absicherung des Netzwerks nach außen auf der sicheren Seite ist, hat aber weit gefehlt. Studien [5] haben gezeigt, dass über 60% der Angriffe von innerhalb einer Organisation ausgehen. Auch die Absicherung gegen Attacken von innen ist ein zentraler Bestandteil dieser Dissertation.

Teil II Grundlagen der Netzwerksicherheit

Heutzutage besteht das Internet aus zehntausenden Netzwerken, welche untereinander verbunden sind. Netzwerksicherheit ist essentiell in dieser Umgebung, da jedes Firmennetzwerk von jedem beliebigen Rechner auf der ganzen Welt erreichbar ist. Dadurch wird dieses Netzwerk angreifbar gegen Attacken, die von Personen ausgehen, die dadurch keinen physischen Zugang benötigen.
Neue Studien haben gezeigt, dass 70% der befragten Firmen bereits Opfer einer Netzwerkattacke wurden, und dass 60% der Vorfälle von innerhalb der Organisation kamen [1].

3 Formale Sicherheitskonzepte

3.1 Sicherheitsmodelle

Der folgende Abschnitt befasst sich mit praktischen Sicherheitsmodellen. Neben diesen praktischen Modellen existieren noch eine Vielzahl von formalen Modellen, wie z.B. das Harrison-Ruzzo-Ullman Modell, das Bell-LaPadula Modell [9] [10], das Biba Modell [11], das Lattice-Modell des Informationsflusses [12] [13] oder das Chinese-Wall Modell [14]. Hierbei sei auf die vielfältige Literatur verwiesen, da es sich hierbei um formale Modelle handelt, die in der Praxis an hochkomplexen Systemen extrem schwer nachprüfbar sind [8].

3.1.1 Keine Sicherheit

Der einfachste Ansatz besteht darin, sich um Schutzmaßnahmen nicht weiter zu kümmern und nur mit den Sicherheitsvorkehrungen zu arbeiten, die ein Hersteller standardmäßig bereitstellt. Es ist sicherlich jedem klar, dass dieses Modell für private Netzwerke absolut indiskutabel ist.

3.1.2 Sicherheit durch Verschleierung (security through obscurity)

Bei diesem Modell geht man davon aus, dass ein System geschützt ist, weil (angeblich) niemand von ihm weiß. Diese Methode funktioniert aber nur über kurze Zeiträume, da es für Angreifer nur eine Frage der Zeit ist, bis sie, unter Umständen auch nur zufällig, das System entdecken.

3.1.3 Sicherheit einzelner Rechner

Dies ist das wahrscheinlich am häufigsten verwendete Sicherheitsmodell. Hierbei geht es darum, jede einzelne Maschine so sicher wie möglich zu machen. Dieses Modell eignet sich aber nur für kleinere Netzwerke, da der Aufwand, jeden einzelnen Rechner immer am neuesten Stand der Sicherheit zu halten sonst viel zu hoch wäre.

3.1.4 Netzsicherheit

Bei diesem Modell werden die Computer nicht einzeln gesichert, sondern man konzentriert sich darauf, den Netzzugang sowie die angebotenen Dienste zu kontrollieren. Konzepte, die bei diesem Modell Anwendung finden, beinhalten Firewalls, strenge Authentifizierungsverfahren sowie Verschlüsselungsverfahren.

3.1.5 Zusammenfassung Sicherheitsmodelle

Kein Sicherheitsmodell kann alle Probleme lösen, aber nur durch Verbindung des Modells der Sicherheit einzelner Rechner mit dem Modell der Netzsicherheit, kann man eine Vielzahl von Angriffen vermeiden. Alle Angriffe werden niemals abgewehrt werden können. Wichtig ist es aber, dass wenn dieser Fall eintritt, es nicht zur Katastrophe kommt, sondern es sich nur um einen unangenehmen Vorfall handelt. Deshalb muss Sicherheit von Grund auf geplant und implementiert werden.

3.2 Kryptografie

3.2.1 Einleitung

In diesem Abschnitt sollen zu Anfang einige Definitionen gegeben werden, danach werden Verfahren vorgestellt, welche zur sicheren Übertragung von Daten auf dem Weg über das Netzwerk, verwendet werden können. Die Vertraulichkeit von Daten kann nur durch Verschlüsselung sichergestellt werden. Dieser Abschnitt konzentriert sich hierbei nur allgemein auf symmetrische und asymmetrische Verfahren.

3.2.2 Definitionen

Unter der Kryptografie versteht man die Lehre von den Methoden zur Ver- und Entschlüsselung von Nachrichten zum Zweck der Geheimhaltung von Informationen gegenüber Dritten (Angreifern) [5].
Die Kryptoanalyse ist die Wissenschaft von den Methoden zur Entschlüsselung von Nachrichten, ohne Zugriff auf den verwendeten Schlüssel zu haben [5]. In der Praxis sind Kryptoanalyse und Kryptografie eng miteinander verbunden, da zur Entwicklung sicherer kryptografischer Verfahren stets auch die kritische Beurteilung der Verfahren gehört, wozu man sich der Methoden der Kryptoanalyse bedient.
Diese beiden Teilgebiete werden unter dem Oberbegriff der Kryptologie zusammengefasst. Mit dem zunehmenden Einsatz kryptografischer Verfahren in offenen Netzen und der damit verbundenen politischen Debatte um die einführung einer Kryptoregulierung oder eines Verbots des Einsatzes kryptografischer Verfahren, gewinnen zunehmend Techniken der Steganografie an Bedeutung. Unter Steganografie fasst man Methoden zusammen, die darauf abzielen, bereits die Existenz einer Nachricht zu verbergen und nicht nur den Informationsgehalt einer Nachricht zu verschleiern [5].

3.2.3 Symmetrische Verfahren

Verschlüsselungsverfahren, die für die Verschlüsselung von Daten den gleichen Schlüssel verwenden, wie für die Entschlüsselung, werden als symmetrische oder Private-Key-Verfahren bezeichnet [3].

Einer der bekanntesten symmetrischen Verschlüsselungsverfahren ist der DES-Algorithmus (Data Encryption Standard) [41], der heutzutage hauptsächlich als Triple-DES Verwendung findet. Neben diesem Verfahren existieren auch RC-4 [41] und der International Data Encryption Algorithm (IDEA) [41].

3.2.3.1 Nachteile von symmetrischen Verschlüsselungsverfahren

Der wohl schwerwiegendste Nachteil bei symmetrischen Verschlüsselungsverfahren ist, dass beide Kommunikationspartner über den gleichen Schlüssel verfügen müssen. Das größte Problem dabei ist aber die sichere Übermittlung des Schlüssels vom einen Kommunikationspartner zum anderen. Die Schlüsselverteilung muss deshalb besonders sicher sein. Im Extremfall muss der Schlüssel eventuell sogar persönlich oder per Kurier übermittelt werden. Das Sicherheitsrisiko besteht darin, dass die Schlüssel, die geheim gehalten werden müssen, durch Nachlässigkeit, Vorsatz, oder Zufall in falsche Hände geraten können [3].

3.2.3.2 Vorteile von symmetrischen Verschlüsselungsverfahren

Der Vorteil von symmetrischen Verschlüsselungssystemen ist, dass sie sehr schnell sind. Derzeit gibt es bereits Hardware-Lösungen, die bis zu 1 GBit/s und Software-Lösungen, die bis zu mehreren MBit/s verschlüsseln [3].

3.2.4 Asymmetrische Verfahren

Das klassische Problem der Kryptographie ist die Schlüsselverteilung. Um dies zu vereinfachen, wurden so genannte asymmetrische Verfahren entwickelt, die mit öffentlichen Schlüsseln arbeiten, den public keys. Diese Verfahren arbeiten mit zwei verschiedenen Schlüsseln. Der Vorteil daran ist, dass mit dem einen Schlüssel die Verschlüsselung durchgeführt werden kann, und mit dem anderen Schlüssel eine Entschlüsselung möglich ist. Selbst wenn einer der beiden Schlüssel bekannt ist, kann der andere nicht daraus berechnet werden. Aus diesem Grund kann der eine Schlüssel veröffentlicht werden, und dieser wird als öffentlicher Schlüssel bezeichnet. Der andere Schlüssel muss geheim gehalten werden, und wird als geheimer Schlüssel bezeichnet [3].

Die bekanntesten Algorithmen sind hierbei der RSA-Algorithmus [41] und der sehr weit verbreitete Diffie-Hellman-Algorithmus [41].

3.2.4.1 Nachteile von asymmetrischen Verschlüsselungsverfahren

Sämtliche Public-Key-Verfahren entstammen der Komplexitätstheorie und sind daher sehr rechenintensiv und nicht für die Verschlüsselung von großen Datenmengen geeignet.

3.2.4.2 Vorteile von asymmetrischen Verschlüsselungsverfahren

Mit Hilfe von Public-Key-Verfahren sind ein einfaches Key-Management (Schlüsselverteilung) und die Digitale Signatur möglich.

3.2.5 Zusammenfassung Kryptografie

Durch eine einfache Gegenüberstellung der Verfahren, sind die Stärken und Schwächen sehr leicht erkennbar. Der wohl ausschlaggebenste Punkt ist die Geschwindigkeit der Verfahren. Diese Eigenschaft kann man sich aber zunutze machen. So ist es z.B. möglich, ein asymmetrisches Verfahren dazu zu benutzen, um den Schlüssel bzw. einen Basiswert für den Schlüssel eines symmetrischen Verfahrens auszutauschen. Dadurch ist die Datenmenge bei der asymmetrischen Verschlüsselung äußerst klein, was keine Einbussen in der Performance verursacht und erst wenn dann die echten Daten ausgetauscht werden, kommt das sehr schnelle symmetrische Verfahren zum Zuge. Dies gewährt optimale Sicherheit, und nutzt die jeweiligen Vorteile der einzelnen Verfahren ideal aus.

3.3 Authentifikation und Autorisation

3.3.1 Schutzziele

Informationen bzw. Daten sind die zu schützenden Güter informationssicherer bzw. datensicherer Systeme. Der Zugriff auf diese ist zu beschränken und zu kontrollieren, so dass nur dazu autorisierten Subjekten ein Zugriff gewährt wird. Die Schutzziele, die diese Anforderungen präzisieren, sind die Eigenschaft der Datenintegrität [40] und der Informationsvertraulichkeit [40]. Zugreifende Subjekte müssen eindeutig identifiziert und ihre Identität muss verifiziert sein. Die entsprechende Eigenschaft nennt man die Authentizität [40] von Subjekten. Ist ein Subjekt authentifiziert und berechtigt, also autorisiert, einen Zugriff auf ein Objekt durchzuführen, dann sollte das System gewährleisten, dass dieser Zugriff auch möglich ist. Man spricht in diesem Fall von der Eigenschaft der Verfügbarkeit [40]. Hat ein Subjekt einen Zugriff, bzw. eine Aktion durchgeführt, so ist es vielfach notwendig, dass auch im Nachhinein die Urheberschaft des Zugriffs bzw. der Aktion eindeutig dem entsprechenden Subjekt zuordenbar ist. Man spricht hier von der Verbindlichkeits- oder Zuordenbarkeitseigenschaft des Systems [5].

3.3.2 Definitionen

Unter der Authentizität eines Objekts bzw. Subjekts verstehen wir die Echtheit und Glaubwürdigkeit des Objekts bzw. Subjekts, die anhand seiner eindeutigen Identität und seiner charakterisierenden Eigenschaften überprüfbar ist [5].

Ein System gewährleistet Datenintegrität, wenn es Subjekten nicht möglich ist, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren [5] [8].

Ein System gewährleistet die Informationsvertraulichkeit, wenn keine unautorisierte Informationsgewinnung möglich ist [5].

Ein System gewährleistet die Verfügbarkeit, wenn authentifizierte Subjekte in der Wahrnehmung ihrer Berechtigungen nicht unautorisiert beeinträchtigt werden können [5] [8].

Ein System gewährleistet die Verbindlichkeit bzw. Zuordenbarkeit einer Menge von Aktionen, wenn es nicht möglich ist, dass ein Subjekt im Nachhinein die Durchführung einer solchen Aktion abstreiten kann [5].

Unter der Anonymisierung versteht man das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können [5] [8].

Eine schwächere Form der Anonymisierung stellt die Pseudomisierung dar. Dabei handelt es sich um das verändern personenbezogener Daten durch eine Zuordnungsvorschrift derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Kenntnis oder Nutzung der Zuordnungsvorschrift nicht mehr einer natürlichen Person zugeordnet werden können [5] [8].

3.3.3 Überblick

Wie aus obigen Definitionen ersichtlich, ist es bei der Authentifikation sehr wichtig, dass die behauptete Identität eindeutig überprüfbar ist. Deshalb sind Mechanismen notwendig, die eine hohe Fälschungssicherheit der Identität garantieren, bzw. Maskierungsversuche abzuwehren vermögen. Dieser Abschnitt befasst sich mit Methoden zur Authentifikation von Subjekten. Zuerst soll aber der Begriff des Subjekts noch präzisiert werden. Unter einem Subjekt verstehen wir Prozesse und Benutzer, aber auch Hardwarekomponenten wie z.B. PCs. Ein Beispiel hierfür wäre eine Windows NT oder 2000 Domäne, in der sowohl jeder Benutzer, als auch jeder PC in der Domäne eindeutig definiert wird. Dadurch kann sich nur ein Domänen-User bzw. kann sich ein User nur von einem PC aus anmelden, der Mitglied einer Domäne ist. Selbiges gilt auch für die Prozesse, die unter einem bestimmten Account laufen, und deshalb genau diese Berechtigungen besitzen. Man spricht in so einem Fall von einer so genannten Client-Server-Architektur. Hierbei bieten die Server, wie z.B. Druckserver, Fileserver oder Datenbankserver, Dienste an, die Clients über das Kommunikationsnetz nutzen können. Der Zugriff erfolgt aber nur wenn die Abwicklung der Authentifikationsprotokolle zwischen Client und Server erfolgreich war.
Derzeit werden in der Praxis Maßnahmen, die auf Kenntnis eines spezifischen Wissens, auf einem persönlichen Besitz oder auf biometrischen Merkmalen basieren, unterschieden [15]. Hierbei spielt es keine Rolle, ob diese Techniken in offenen, geschlossenen, zentralen oder verteilten Systemen eingesetzt werden. Anzumerken ist aber jedenfalls, dass in verteilten, bzw. vernetzten Systemen die Übertragung der eingegebenen Merkmale gegen unerlaubten Zugriff gesichert werden muss.

3.3.4 Passwörter

Eine Art von Verfahren der Authentifikation durch Wissen, sind die Passwortverfahren. Hierbei authentifiziert sich ein Subjekt an einem System durch den Austausch eines Geheimnisses. Geheimnis ist deshalb hier allgemein gewählt, da ein Passwortsystem nicht zwingend auf numerische bzw. alphanumerische Zeichenketten beschränkt ist. Passwortbasierte Authentifikationssysteme sind bei heutigen Betriebssystemen wie Windows NT/2000 oder Unix/Linux integriert. Essentiell ist dabei, dass die Passwörter derart verwaltet werden, dass kein unautorisierter Zugriff möglich ist. Heutige Betriebssysteme verwenden kryptografische Verfahren um Passwörter zu verschlüsseln, und diese zusammen mit Informationen über den Benutzer abzuspeichern. Diese Passwortdatei muss natürlich durch entsprechende Berechtigungen vor unautorisiertem Zugriff geschützt werden. Als zusätzliche Sicherheitsmaßnahme werden zur Verschlüsselung Einweg-Funktionen verwendet. Das bedeutet, dass verschlüsselte Passwörter nicht mehr entschlüsselt werden können. Sicherheitsprobleme treten aber bei der Windows 9X-Serie bzw. älteren Unix-Systemen auf, da die Passwortdateien dort für jedermann zugänglich sind. So kann ein Angreifer entweder mittels eines Tools oder durch Ausprobieren, wahrscheinliche Passwörter durch die Betriebssystemfunktionen verschlüsseln, und diesen verschlüsselten Text dann mit der Passwortdatei vergleichen. Diese Art des Angriffs wird als Password Cracking bezeichnet. Wenn von Betriebssystemseite eine sichere Passwortverwaltung gewährleistet wird, bleiben noch die Wahl des Passwortes bzw. der Umgang mit diesem außerhalb des technischen Systems ein Schwachpunkt. Hierbei sind vor allem die Passwortauswahl, die Möglichkeit der Eingabebeobachtung, sowie das Notieren mögliche Angriffspunkte.

3.3.4.1 Anforderungen an Passwörter

Wie schon im vorigen Abschnitt erläutert, ist es besonders wichtig im Umgang mit Passwörtern bestimmte Richtlinien zu beachten. Um also ein Mindestmaß an Sicherheit zu gewährleisten, sollten die Passwortauthentifikationssysteme folgende Anforderungen erfüllen [5]:

- Jedes Passwort sollte eine Mindestlänge von 8 Zeichen aufweisen, und keinesfalls ein Wort sein, welches aus dem Wörterbuch entstammt. Diese Policy kann vielfach auf Betriebssystemebene gesetzt werden.
- Bei dem Passwort sollte es sich auch keinesfalls um einen Eigennamen, oder irgendeinen Wert handeln, der mit der Person in Bezug gesetzt werden kann. Darunter fallen Geburtsdaten, Postleitzahlen, Telefonnummern oder ähnliches.
- Passwörter sollten neben Großbuchstaben, Kleinbuchstaben und Zahlen auch Sonderzeichen enthalten. Windows 2000 bietet hier beispielsweise die Möglichkeit, dass Passwort auf bestimmte Komplexitätskriterien hin zu überprüfen.
- Passwörter sollten keinesfalls auch Zeichenfolgen bestehen, die auf der Tastatur nebeneinander liegen.
- Passwörter sollten in regelmäßigen Abständen geändert werden. Besonders sinnvoll ist hierbei die automatische Aufforderung des Betriebssystems in regelmäßigen Intervallen. Ferner sollte das Betriebssystem hierbei die Verwendung der letzten 5 Passwörter verwehren (Passworthistorie).
- Nach einer gewissen Anzahl von Fehlversuchen sollte das Betriebssystem den Benutzeraccount sperren.

3.3.4.2 Challenge-Response-Verfahren

Beim Challenge-Response-Verfahren handelt es sich prinzipiell nur um eine Erweiterung der herkömmlichen Passwortverfahren. Zusätzlich zur Benutzerkennung werden dem Benutzer eine Folge von Fragen präsentiert, wobei nach richtiger Beantwortung aller Fragen, der Zugang zum System gewährt wird. Hierzu wird nicht nur ein geheimes Passwort mit dem System vereinbart, sondern zusätzlich eine Folge von Frage/Antwort-Paaren.
Dieses Verfahren wird aber heutzutage nur verwendet, um bestimmte Geräte zu authentifizieren. So prüfen beispielsweise manche Drucker, ob die eingesetzte Tonerkassette von einem zertifizierten Hersteller stammt.

3.3.5 Zusammenfassung Authentifikation und Autorisation

Neben den oben beschriebenen Authentifikationsverfahren gibt es noch eine Vielzahl von anderen Techniken, wie Chipkarten, biometrische Methoden, Kerberos, RADIUS [42], RPC und Microsoft Passport. Eine detaillierte Erläuterung würde den Rahmen dieser Dissertation sprengen, und es sei hier auf die einschlägige Fachliteratur verwiesen.
Die meiner Meinung nach kritischste Komponente ist in allen Authentifikationssystemen eindeutig der Benutzer. Die meisten Fehler, welche im Umgang mit Passwörtern geschehen sind zwar durch entsprechende Betriebssystemvorkehrungen und Benutzerrrichtlinien abfangbar, aber die kritische Komponente bleibt im Endeffekt doch der Mensch. Selbst noch so strenge Organisationsrichtlinien, welche die Weitergabe oder das Notieren von Passwörtern verbieten, können den Faktor Mensch hierbei ausschalten. Deshalb ist es extrem wichtig den Benutzern auch die Bedeutung von Sicherheit zu erklären, und ihre Sensibilität in diesem Bereich zu schärfen. Diesem Thema widmet sich ausführlich das Kapitel über die User-Schulung.
Man sollte aber nicht aus den Augen verlieren, dass sämtliche sich heute im Einsatz befindlichen Betriebssysteme, und dies betrifft sowohl Unix- als auch Windows-Systeme, auf der klassischen Benutzerkennung in Kombination mit einem Passwort aufgebaut sind. Hier wären die Hersteller aufgefordert, bereits entwickelte Verfahren, wie z.B. Einmal-Passworte [6] oder Zero-Knowledge-Verfahren [7], in Systeme zu implementieren. Auch Chipkarten oder biometrische Methoden wären sicher für bestimmte Anwendungen sinnvoll einsetzbar.

3.4 Virenschutz

3.4.1 Computeranomalien / Arten von bedrohlichen Programmen

Neben dem Virus im eigentlichen Sinn gibt es eine Vielzahl von bedrohlichen Programmen, die an dieser Stelle erklärt werden sollen. Es handelt sich hierbei um ablauffähige Computerprogramme oder um Programmteile, die zum Zweck einer Softwaremanipulation entworfen und in Umlauf gebracht wurden.

- Bug: Dabei handelt es sich um einen Programmfehler, d.h. eine Differenz zwischen der gewünschten Logik des Programms und einer Realisierung.
- Trojanisches Pferd (trojan horse): Ein Trojanisches Pferd ist ein Programm, dessen implementierte Ist-Funktionalität nicht mit der angegebenen Soll-Funktionalität übereinstimmt. Es erfüllt zwar diese Soll-Funktionalität, besitzt jedoch eine darüber hinausgehende, beabsichtigte zusätzliche, aber verborgene Funktionalität [5].
- Wurm (worm): Ein Wurm ist ein ablauffähiges Programm mit der Fähigkeit zur Reproduktion. Ein Wurm-Programm besteht in der Regel aus mehreren Programmteilen, den Wurm-Segmenten. Die Vervielfältigung erfolgt selbstständig unter Kommunikation mit anderen Wurm-Segmenten.
- Logische Bombe (logic bomb): ist ein lauffähiges Programm, das solange die gewünschte Funktion korrekt ausführt, bis eine vorgegebene Bedingung des Manipulanten erfüllt ist.
- Hintertür (backdoor): erlaubt die Realisierung eines nicht autorisierten Zugangs zu einem EDV System.
- Schläfer (sleeper): Teile innerhalb eines Programms, die erst zu einem späteren Zeitpunkt wirksam werden.
- Krebs (cancer): Modifiziert vorhandene Programme oder Datenbestände.

3.4.2 Viren

Ein Computervirus ist eine Befehlsfolge, die ein Wirtsprogramm zur Ausführung benötigt. Viren sind zur Reproduktion fähig. Dazu wird bei der Ausführung des Virus eine Kopie (Reproduktion) oder eine modifizierte Version des Virus in einen Speicherbereich, der diese Befehlssequenz noch nicht enthält, geschrieben (Infektion). Zusätzlich zur Fähigkeit zur Reproduktion enthalten Viren in der Regel einen Schadensteil. Dieser kann unbedingt oder bedingt durch einen Auslöser aktiviert werden [5].

3.4.2.1 Ablauf der Infektion mit einem Virus

Als erstes muss ein Opfer gefunden werden. Danach muss der Virus feststellen, ob das gefundene Programm bereits mit diesem Virus infiziert wurde. Falls ja, dann muss ein neues Opfer gefunden werden. Sind aber die Infektionsbedingungen erfüllt, dann wird eine Kopie des Virus in das Opfer eingebracht. Danach erfolgt eine mögliche Suche nach weiteren Opfern und deren Infektion. Zusätzlich kann, wenn eine erforderliche Bedingung (Erreichen eines best. Datums etc.) erfüllt ist eine bestimmte Aktion ausgeführt werden. Danach nimmt das Wirtsprogramm seine normale Tätigkeit wieder auf, falls dies noch möglich ist.

3.4.2.2 Virusarten

- Parasitärer Virus: Dies ist die meist verbreitete Art von Viren. Er verbreitet sich durch Anhängen an Programme.
- Speicherresidenter Virus: Dieser Virus hält sich im Speicher und infiziert Programme, welche gestartet werden.
- Stealth Virus: Dieser versteckt sich vor Virenschutzprogrammen, z.B. durch Verschlüsselung.
- Polymorpher Virus: Dieser Virus verändert sich selbst bei jeder Infektion, und ist dadurch von Virenschutzprogrammen schwerer aufzufinden.
- Makrovirus: Virus geschrieben als Excel- oder Wordmakro.

3.4.2.3 Sicherheitsvorkehrungen

- Disketten mit Schreibschutz versehen, ein Virus kann im Normalfall den Schreibschutz einer Diskette nicht umgehen, da dies hardware- und nicht softwaremäßig gesteuert wird.
- keine Installation von Raubkopien oder Shareware, da die Gefahr einer Virenverseuchung hierbei sehr hoch ist.
- Fremde Disketten vor Benutzung auf Viren scannen.
- Schreibrechte auf Programme einschränken.
- Berechnung von digitalen Fingerabrücken von Programmen.
- Computer gegenüber unbefugten Personen sichern.
- Überprüfung der Dateigröße von wichtigen Systemdateien
- Passwörter benutzen, und diese regelmäßig ändern
- Makrovirusschutz in Office-Programmen aktivieren

Der beste Schutz ist aber sicherlich die Installation einer Virenschutzsoftware, von denen dutzende am Markt heutzutage erhältlich sind. In Kapitel 13 werden Vorgehensweisen beschrieben, die für einen optimalen Virenschutz erforderlich sind.

3.4.2.4 Anzeichen für einen Virenbefall

- unerklärliche und häufige Fehlermeldungen vom Betriebssystem
- Längere Zugriffszeiten
- plötzlich gelöschter Bildschirm
- Anzeige von unerwarteten Texten oder Bildern
- Eigenartige und ungewöhnliche grafische Effekte am Bildschirm
- Akustische Effekte, die üblicherweise nicht auftreten
- Veränderte Länge von Dateien
- Veränderte Datumsangaben bei Dateien
- Verschwinden von Dateien

3.4.2.5 Verhaltensmaßnahmen bei Virenbefall

- Gerät vom Netzwerk isolieren
- Dateien auf Vireninfektion testen
- Infizierte Dateien mit Virenschutzprogramm „entseuchen“
- Wenn kein Virenschutzprogramm installiert wurde, oder eine Entfernung fehlschlägt, müssen alle Festplatten formatiert werden, und eine Neuinstallation von sauberen Disketten oder CD-ROMs vorgenommen werden. Dabei müssen fehlende Daten durch Backups ersetzt werden.

4 Protokollspezifische Sicherheitsaspekte

Nachdem für das TCP/IP-Protokoll nicht alle Schichten so eindeutig trennbar sind, wie dies im OSI-Referenzmodell propagiert wird, wird hier ein vereinfachtes 4-Schichten Modell wie in [2] und [3] verwendet.

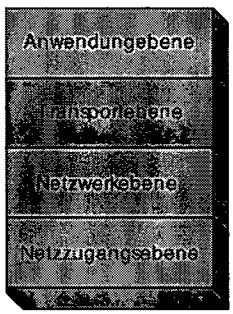


Abbildung 3: 4-Schichten Modell

Das TCP/IP-Schichtenmodell besteht dabei aus folgenden vier Layern:

- Netzzugangsebene: Diese enthält Routinen für den Zugriff auf physikalische Netze. Dieser Layer entspricht dabei Layer 1 und 2 aus dem OSI-Referenzmodell.
- Netzwerkebene: Diese definiert den Aufbau von Datagrammen und routet Daten. Dieser Layer entspricht dabei Layer 3 aus dem OSI-Referenzmodell.
- Transportebene: Diese stellt Ende-zu-Ende Datendienste zur Verfügung. Dieser Layer entspricht dabei Layer 4 aus dem OSI-Referenzmodell.
- Anwendungsebene: Diese enthält Anwendungen und Prozesse, die auf das Netz zugreifen. Dieser Layer entspricht dabei Layer 5 bis 7 aus dem OSI-Referenzmodell.

Diese vier Layer sollen untersucht werden, inwiefern sie sich für sicherheitsrelevante Anwendungen eignen.

4.1 Netzzugangsebene

Diese Ebene dient rein für den physikalischen Zugriff auf das Netzwerk. Es kann sich hierbei um Ethernet, Token Ring, ATM (Asynchronous Transfer Mode) und dergleichen handeln.

4.1.1 Sicherheit

Vom Sicherheitsaspekt betrachtet, gibt es derzeit nur zwei Möglichkeiten, sicherheitstechnische Verbesserungen zu machen. Im Zusammenhang mit Firewalls, kann hier Paketfilterung anhand der MAC-Adresse (Media Access Control) durchgeführt werden. Dies ist aber nur für ein lokales Netzwerk von praktischer Bedeutung. Im Bereich der Netzwerkinfrastruktur kann man durch Austausch der Hubs gegen Switches eine bessere Segmentierung erreichen.

4.1.2 Filtermöglichkeiten

Mithilfe der Paketfilterung anhand der MAC-Adresse kann verhindert werden, dass Endgeräte an eine freie Dose angehängt werden, um z.B. den Paketverkehr abzuhören. Wichtig ist dabei aber eine genaue Dokumentation, damit es nicht vorkommt, dass etwaige, berechtigte Netzwerkstationen z.B. bei Tausch der Netzwerkkarte plötzlich nicht mehr berechtigt sind.

4.1.3 Probleme

Da es bei den meisten Netzwerkkarten relativ einfach ist, die MAC-Adresse zu ändern, bietet dies natürlich keinen vollkommenen Schutz. Für WAN-Verbindungen, die durch eine Firewall vom internen LAN getrennt sind, ist es meist nicht sinnvoll, eine Filterung auf MAC-Basis durchzuführen, da die Pakete immer die MAC-Adresse des nächsten Internet-Routers enthalten, und so eine Filterung nicht durchführbar ist [2].
Ein weiterer Nachteil ist, dass diese Protokolle keine Unterstützung für Verschlüsselung bieten.

4.1.4 Zusammenfassung Netzzugangsebene

Wie man sieht, bietet die physikalische Ebene derzeit nur äußerst schwache Unterstützung der Sicherheit. Hierbei gibt es definitiv Handlungsbedarf, denn Sicherheit muss auf allen Ebenen ein wichtiges Thema sein. Vorstellbar wären in diesem Zusammenhang, dass die Daten auf physikalischer Ebene verschlüsselt werden. Dies würde den Vorteil bieten, dass etwaige Verschlüsselungsalgorithmen direkt in den Hardwarekomponenten implementiert werden könnten. Dies bietet einerseits einen erhöhten Schutz vor Manipulation, da keine Software diese Verschlüsselung steuert, und andererseits könnten hier durchaus asymmetrische und symmetrische Verfahren kombiniert eingesetzt werden. Im Detail ist damit gemeint, dass ein öffentlicher Schlüssel der von einem der beiden Kommunikationspartner stammt, an den anderen Kommunikationspartner gesendet wird. Dieser benutzt den öffentlichen Schlüssel, um den privaten Schlüssel des symmetrischen Verfahrens zu verschlüsseln, und dem Partner zu übertragen. Der Sender kann nun mit seinem privaten Schlüssel des asymmetrischen Verschlüsselungssystems, den Schlüssel des symmetrischen Verfahrens decodieren. Danach kann die Kommunikation mit dem symmetrischen Verfahren vollständig verschlüsselt werden. Der einzige Punkt, der hierbei weiterhin offen bleibt, ist die sichere Übertragung des öffentlichen Schlüssels. Der Vorteil dieser Technologie ist, dass die Generierung von symmetrischen Schlüsseln durch Zufallsgenerator direkt in der Hardware erfolgen könnte. Ein weiterer entscheidender Vorteil wäre, dass der private Schlüssel des asymmetrischen Verfahrens direkt in der Hardware (analog wie bei einer Chipkarte) unauslesbar gespeichert werden könnte.

4.2 Netzwerkebene

Dies ist die Ebene des IP-Protokolls [77].

4.2.1 Sicherheit

Auf dieser Ebene gibt es bereits verschiedene Ansatzpunkte, um die Sicherheit zu erhöhen. Einerseits ist es die Ebene, auf der IPSec zum tragen kommt, andererseits können hier Paketfilterregeln von Firewalls greifen. Bei IPSec handelt es sich um ein Protokoll, welches zur Verschlüsselung, und damit zum sicheren Datenaustausch zwischen Netzwerkkomponenten verwendet wird. Nähere Erläuterungen zu IPSec sind im Abschnitt 4.5.1 zu finden.

4.2.2 Filtermöglichkeiten

Für Firewalls sind die IP-Quelladresse, die IP-Zieladresse und der IP-Protokolltyp von besonderer Bedeutung. Anhand dieser Informationen können Regeln erstellt werden, die angeben, ob bestimmte Pakete durchgelassen werden oder nicht. Diese Filterregeln können sowohl Quelladresse oder Zieladresse als auch den Protokolltyp betreffen. Da dies die primäre Eigenschaft einer Firewall darstellt, ist diese Ebene neben der Transportebene die wichtigste Ebene.

4.2.3 Probleme

Das größte Problem im Hinblick auf die Sicherheit, ist die so genannte IP-Fragmentierung. Dabei werden große Pakete in Fragmente aufgeteilt [77]. Bei einigen Firewalltypen wird nur das erste Fragment einer Filterung zugeführt. Alle weiteren Fragmente werden durchgelassen. Dies bringt das Problem mit sich, dass die restlichen Fragmente noch einige Zeit im Speicher des Zielrechners behalten werden. Dies ist ein Angriffspunkt für Denial-of-Service-Attacken. Eine weitere Angriffsmöglichkeit bietet sich durch die künstliche Erstellung sich überlappender Fragmente. Da dies im Normalfall nie passiert, reagieren verschiedene Betriebssysteme unterschiedlich auf diese Anomalie. In den schlimmsten Fällen kann es zu einem Absturz kommen.
Bei IPSec ist das Problem vorhanden, dass dieses Protokoll eigentlich für IPv6 entwickelt wurde. Für IPv4 gibt es zwar schon einige Implementationen, IPSec befindet sich aber noch im Standardisierungsprozess [2]. IPSec-Pakete können zwar von Firewalls gefiltert werden, aber der Paketinhalt kann weder inspiziert noch verändert werden.

4.2.4 Zusammenfassung Netzwerkebene

Besonders wichtig ist es, sich auf der IP-Ebene mit der Fragmentierung auseinanderzusetzen und Konzepte gegen die möglichen Angriffe zu erstellen. Besonders die gewählte Firewall sollte dahingehend überprüft werden, dass eingehende Fragmente vor der Filterung oder Weiterleitung erst zusammengesetzt werden. Dadurch können oben erwähnte DoS-Attacken bereits an der Firewall ausgeschaltet werden. Bei IPSec ist sicher noch das Ende der Standardisierung, bzw. eine flächendeckende Einführung von IPv6 abzuwarten. Erst dann können Aussagen gemacht werden, inwiefern IPSec angewendet werden kann, um die Sicherheit tatsächlich zu verbessern.

4.3 Transportebene

Dies ist die Ebene des TCP- [80], UDP- [81] und ICMP-Protokolls [82].

4.3.1 Das TCP-Protokoll

Die primär wichtige Eigenschaft des TCP-Protokolls ist die zur Verfügungstellung von so genannten Ports, damit die Applikationen zweier Netzwerkstationen miteinander kommunizieren können. TCP stellt also eine zuverlässige, bidirektionale Verbindung zwischen zwei Endpunkten zur Verfügung.

4.3.2 Das UDP-Protokoll

UDP unterscheidet sich von TCP dahingehend, dass es keine Zuverlässigkeitsgarantien für Auslieferung, Reihenfolge und Schutz vor Doppelungen gibt. Deshalb benötigt UDP auch keine Mechanismen, um diese Garantien einzuhalten. Jedes UDP-Paket ist unabhängig und UDP-Pakete gehören nicht zu einer virtuellen Verbindung, wie TCP-Pakete.

4.3.3 Das ICMP-Protokoll

ICMP wird für IP-Status- und Kontrollmeldungen verwendet.
Anders als TCP oder UDP besitzt ICMP keine Quell- oder Zielports, und es gibt keine anderen Protokolle, die auf ihm aufbauen. Stattdessen gibt es eine Anzahl definierter ICMP-Meldungstypen. Diese Typen bestimmen, wie der Rest des ICMP-Pakets interpretiert wird.

4.3.4 Sicherheit

Wie bei der Netzwerkebene kommen bei TCP und UDP die Paketfilterregeln der Firewalls zum Einsatz, wobei der Port dabei die wesentliche Rolle spielt. Die Filter unterscheiden sich aber bei TCP und UDP dahingehend, dass UDP-Pakete keine Flags und Sequenznummern im Header besitzen.

4.3.5 Filtermöglichkeiten

Hierbei ist es möglich nach TCP-Quellport bzw. UDP-Quellport, oder TCP-Zielport bzw. UDP-Zielport zu filtern. Dies wird oft in Verbindung mit IP-Adress-Filterung angewendet.

4.3.6 Probleme

Nachdem es bei UDP kein Pendant, des von TCP bekannten ACK-Flags gibt, ist es bei UDP nicht möglich festzustellen, ob das Paket das erste Paket eines externen Clients an einen internen Server oder die Antwort eines externen Servers auf eine Anfrage eines internen Clients ist.

4.3.7 Zusammenfassung Transportebene

Wie bereits oben angesprochen, kommunizieren Anwendungen, die mit dem TCP- bzw. UDP-Protokoll arbeiten über Ports miteinander. Jeder Port steht dabei für eine ganz spezielle Anwendung. Der große Vorteil, der sich daraus ergibt, ist die Möglichkeit mithilfe einer Firewall nur ganz bestimmte Anwendungen überhaupt freizugeben. Alle Anwendungen, die nicht benötigt werden, bzw. die ein besonderes Sicherheitsrisiko darstellen, können somit vollkommen blockiert werden.

4.4 Anwendungsebene

Auf dieser Ebene gibt es eine Vielzahl von verschiedenen Protokollen. Diese Arbeit konzentriert sich auf einige wichtige TCP-basierende Anwendungen. Ich greife an dieser Stelle die Protokolle HTTP [86], SMTP [84], FTP [83] und Telnet [85] heraus, da dies die meist verwendeten Anwendungsprotokolle darstellt.

4.4.1 Telnet

Bei Telnet handelt es sich um ein schon eher veraltetes Protokoll. Dabei wird von einem Client eine Terminalsitzung zu einem Server auf Port 23 hergestellt. Danach erfolgt eine Login-Prozedur, bei der ein Benutzername und ein Passwort angegeben werden muss [3].

4.4.1.1 Sicherheit

Bei der Authentifikation über den Telnet-Dienst wird das Passwort im Klartext übertragen. Verfügt ein Angreifer über einen Packet-Sniffer, so kann er sowohl Benutzername als auch Passwort problemlos auslesen. Deshalb ist dieser Dienst als sehr unsicher zu bezeichnen.

4.4.1.2 Filtermöglichkeiten

Telnet-Pakete zu filtern ist relativ einfach, da nur TCP-Pakete überprüft werden müssen, die den Zielport 23 haben.

4.4.1.3 Zusammenfassung Telnet

Der Telnet-Dienst sollte auf jeder Firewall deaktiviert werden. Durch die unsichere Übertragung des Passworts, stellt dieser Dienst ein großes Sicherheitsproblem dar. Sinnvoller ist es hier Secure Shell (SSH) zu verwenden, um eine sichere Verbindung zu gewährleisten. Für rein interne Verbindungen, die nicht über die Firewall laufen, ist es noch vertretbar diesen Dienst zu verwenden. Hier besteht aber weiterhin die Gefahr, dass ein User versuchen wird, sich auf diesem Weg Zugang z.B. mithilfe eines Packet-Sniffers zu verschaffen.

4.4.2 FTP

Das File Transfer Protocol (FTP) ermöglicht den Austausch und die Übertragung von beliebigen Dateien zwischen entfernten Rechnersystemen. Der Client baut hierbei von einem beliebigen Port oberhalb 1024 eine Verbindung zu Port 21 des Servers auf (Kommandokanal). Die Daten werden von Port 20 des Servers zu einem beliebigen Port oberhalb 1024 des Clients transferiert (Datenkanal) [3].

4.4.2.1 Sicherheit

Die Sicherheitslücke entsteht hierbei durch den beliebigen Client-Port für die Daten. Der Angreifer kann sich dadurch selbst als Server ausgeben, oder eigene Daten in die Kommunikation mit dem Server einfügen. Damit bekommt er die Möglichkeit, gefährliche Programme wie z.B. Viren oder Trojanische Pferde in das Rechnersystem einzuschleusen, die anschließend Daten ausspionieren oder zerstören können. Abhilfe schafft hierbei die passive Methode, bei der der Client die TCP-Verbindung aufbaut, und damit der Verbindungsaufbau nicht aus dem unsicheren Netzwerk erfolgt.

4.4.2.2 Filtermöglichkeiten

Wird die passive Methode verwendet, so ist eine Filterung relativ unproblematisch, da die Serverports 20 und 21 ja bekannt sind. Es empfiehlt sich aber zusätzlich FTP-Zugänge über einen Proxy laufen zu lassen, damit Zugriffe einerseits protokolliert werden können, und andererseits die Anzahl der möglichen Kommandos, und der übertragbaren Dateien eingeschränkt wird.

4.4.2.3 Zusammenfassung Telnet

Bei passiven FTP-Verbindungen spricht eigentlich nichts gegen die Verwendung über eine Firewall. Ein Proxy-Server sollte aber dennoch zusätzlich Verwendung finden, damit die Verbindungen einerseits nicht direkt in das Internet gehen, und andererseits um Protokollierung und Befehlseinschränkungen aktivieren zu können.

4.4.3 SMTP

Das Simple Mail Transfer Protocol (SMTP) ist ein einfaches Protokoll für die Übertragung von E-Mails durch das Internet oder Intranet. Das E-Mail-System besteht aus zwei Komponenten, dem Message Transfer Agent (MTA) und dem User Agent (UA). Der MTA hat die Aufgabe, die Nachrichten weiterzuleiten, und läuft auf Port 25. Der UA entspricht der E-Mail-Software auf Benutzerseite.

4.4.3.1 Sicherheit

Die Übertragung der Nachrichten mittels SMTP erfolgt im Klartext. Desweiteren ist eine Überprüfung der Absenderadresse nicht möglich. Deshalb kann der Absender relativ einfach gefälscht werden. Es ist zwar möglich, mithilfe der Header der E-Mail auf den wirklichen Absender zu schließen, dies kann einem normalen User aber keinesfalls zugetraut werden. Sinnvoller ist die Einführung von digitalen Signaturen und Verschlüsselung der Nachrichten. Damit kann die Herkunft eindeutig und unverfälschbar gesichert werden.

4.4.3.2 Filtermöglichkeiten

Da der SMTP-Server sich auf Port 25 befindet, wäre es relativ einfach, nach diesem Port zu filtern. Dies wird in den meisten Fällen aber völlig sinnlos sein, da E-Mails sowohl über die Firewall in das Internet gelangen sollen, als auch umgekehrt. Man sollte aber den E-Mail-Server mit einer Virenschutzsoftware ausstatten, damit zumindest E-Mail-Viren sowohl aus eingehenden und ausgehenden Mails herausgefiltert werden.

4.4.3.3 Zusammenfassung SMTP

Wie man sieht, macht es wenig Sinn, SMTP zu verhindern. Trotz der immer wieder auftretenden Sicherheitslücken und der Möglichkeit der Fälschung von Absenderadressen, kann es sich eine Organisation nur dann erlauben, diesen Port zu sperren, wenn kein Mail-Verkehr vonnöten ist. In der heutigen Zeit ist dieser Ansatz aber absolut unpraktikabel. Deshalb sollte man nur einen Virenschutz implementieren, und eventuell einen Content-Filter für E-Mails definieren, damit E-Mails mit potentiell bedenklichem Inhalt weder versandt noch empfangen werden können.

4.4.4 HTTP

Das HyperText Transfer Protocol (HTTP) dient zur Übertragung von Webseiten oder Dateien, welche über multimedialen Inhalt verfügen können. Das Protokoll arbeitet dabei Session-orientiert, das bedeutet, dass nach Übertragung aller für eine Webseite notwendigen Dateien die Verbindung wieder abgebaut wird. HTTP benutzt Port 80 auf der Serverseite.

4.4.4.1 Sicherheit

Das größte Sicherheitsproblem im Zusammenhang mit HTTP, sind aktive Elemente in Webseiten, Wie Java-Applets, ActiveX-Controls oder JavaScript-Befehle. Diese werden erst am Client ausgeführt, und können dort unter Umständen auf Systemressourcen zugreifen, und damit Dateien oder Verzeichnisse manipulieren oder sogar löschen.

4.4.4.2 Filtermöglichkeiten

Wie auch bei allen anderen Protokollen der Anwendungsschicht, die hier vorgestellt wurden, ist eine Filterung aufgrund des Zielports einfach möglich. Hier hängt es nun wieder vom Unternehmen ab, wie dies gehandhabt wird. Viele Unternehmen verzichten auf die totale Filterung von Webseiten. Stattdessen wird ein Proxy eingesetzt, der eine Authentifizierung erfordert. So können nur berechtigte Personen das Internet nutzen. Zusätzlich zu diesem Mechanismus haben sich auch aufgrund von gesetzlichen Bestimmungen Content-Filter-Systeme bewährt, die Webseiten mit bestimmten kriminellen oder obszönen Inhalten herausfiltern, und es den Nutzern unmöglich machen diese Seiten aufzurufen.

4.4.4.3 Zusammenfassung HTTP

Wie man sieht, stellt das HTTP-Protokoll selbst keine wirkliche Sicherheitslücke dar. Die Problematik besteht einerseits in Webseiten mit aktiven Inhalten, die enormen Schaden an den Clients verursachen können, sowie Seiten mit illegalen Inhalten, die wenn sie von Mitarbeitern aufgerufen werden zu einer deutlichen Imageschädigung des Unternehmens oder sogar rechtlichen Konsequenzen für das Unternehmen führen können. Deshalb sei an dieser Stelle darauf hingewiesen, dass einerseits der Virenschutz in einem Unternehmen oberste Priorität haben sollte, und andererseits auch die Internetnutzer auf die potentiellen Gefahren im Umgang mit Webseiten geschult werden müssen. Aus diesen Sicherheitsgründen das Internet unternehmensweit zu verbieten macht definitiv wenig Sinn, da es für den Aufbau von Wissen und den Informationsaustausch eine sehr wertvolle Quelle darstellt.

4.5 Verschlüsselungsprotokolle

4.5.1 IPSec

IPSec wird derzeit nur für spezielle Anwendungen eingesetzt. Die wichtigste Anwendung ist der Aufbau von VPN-Tunnels über WANs oder das Internet. Im folgenden werden die wichtigsten Merkmale charakterisiert.
Bei IPSec handelt es sich um eine Sicherheitsarchitektur für IPv4 und IPv6 [43]. Dabei definiert IPSec Sicherheitsdienste auf Schicht 3 des ISO-OSI-Referenzmodells, um einen vertraulichen und authentifizierten Transport von IP-Paketen zu ermöglichen. Die Implementierung von IPSec ist in IPv6 verpflichtend, und deshalb im Protokolldesign bereits implementiert. Nachdem es sich um ein Schicht 3 Protokoll handelt, werden sichere Kommunikationskanäle zwischen Endsystemen, zwischen Endsystemen und Gateways, sowie zwischen Gateways aufgebaut. Mit IPSec hat man die Möglichkeit, Kommunikation sowohl innerhalb eines LAN, als auch über WANs oder das Internet, entsprechend abzusichern. Ein typisches Einsatzszenario für IPSec ist ein Unternehmensnetz, das aus mehreren einzelnen LANs besteht, die räumlich verteilt und über das Internet angebunden sind. Dies können z.B. Tochterunternehmen oder auch Filialen sein.

4.5.1.1 Funktionsweise

IPSec besteht aus den folgenden drei Protokollen:

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)
- Internet Security Association Key Management Protocol (ISAKMP)

Das AH-Protokoll unterstützt sowohl die Nachrichtenintegrität, als auch die Authentifizierung des Datenursprungs. Das ESP-Protokoll ermöglicht Vertraulichkeit und begrenzten Schutz vor Analysen des Verkehrsaufkommens. Das ISAKMP-Protokoll dient für den Austausch der kryptographischen Schlüssel für das AH- und ESP-Protokoll. Da eine genauere Erläuterung von IPSec an dieser Stelle zu weit führen würde, sei für weitere Informationen auf die Literatur verwiesen.

4.5.1.2 Sicherheit

IPSec bietet einerseits die Möglichkeit der Zugriffskontrolle, wobei eine sichere Kommunikation nur dann aufgebaut wird, wenn das Aushandeln der Sicherheitsparameter erfolgreich durchgeführt wird. Der Datenursprung des Pakets ist immer eindeutig, und kann daher immer als authentisch angesehen werden. Die Nachrichten erfüllen auch die Forderung nach Integrität, sodass ein verändertes Paket keinesfalls akzeptiert wird. Die Pakete sind auch vor Wiedereinspielung geschützt, und damit wird sichergestellt, dass bei erneutem Senden eines Paketes dieses nicht akzeptiert wird. Ebenfalls erfüllt IPSec auch die Forderung der Vertraulichkeit, da abgefangene Daten nicht gelesen werden können. IPSec eignet sich aus diesen Gründen, wie schon bereits zuvor erwähnt, hervorragend für den Aufbau von VPNs (Virtual Private Network).

4.5.1.3 Grenzen

Einerseits ist die Implementierung in IPv4 noch weiterhin im Standardisierungsprozess, aber es besitzt bereits eine hohe Stabilität. Erst in IPv6 wird aber die volle Funktionalität zur Verfügung stehen. Auch lässt sich IPSec mit Network Adress Translation nicht verwenden, da der Header auch mitverschlüsselt wird, und daher die Quelladresse des Pakets nicht verändert werden kann.

4.5.2 Secure Socket Layer (SSL)

Das Secure Socket Layer Protokoll setzt auf der Transportebene des ISO-OSI-Referenzmodells auf. SSL wurde von der Firma Netscape zum Aufbau von sicheren HTTP-Verbindungen entwickelt. Mit der Version 3.0 hat sich mittlerweile ein Internetstandard für sichere HTTP-Verbindungen entwickelt, der von allen gängigen WWW-Browsern unterstützt wird. SSL kann aber nicht nur für sichere HTTP-Verbindungen verwendet werden, da es der Anwendungsebene generische TCP/IP-basierte Dienste anbieten kann, und somit sichere FTP, E-Mail oder auch Telnet-Verbindungen aufgebaut werden können.

4.5.2.1 Funktionsweise

Bei SSL handelt es sich um ein Verfahren, bei dem sowohl mit symmetrischer als auch asymmetrischer Verschlüsselung gearbeitet wird. Es ist aber kein wirkliches Hybridverfahren, wie in [4] behauptet wird. Es wird nämlich nicht der Schlüssel für das symmetrische Verfahren durch das asymmetrische Verfahren ausgetauscht, sondern nur eine Basisinformation, anhand derer sowohl Server als auch Client ihre symmetrischen Schlüssel berechnen. Ein weiterer wichtiger Aspekt ist, dass Client und Server die jeweils verwendeten Verschlüsselungsverfahren mithilfe eines Handshake-Prokolls aushandeln. Um die Integrität der Nachrichten sicherzustellen wird zusätzlich noch ein Message Authentication Code (MAC) [5] verwendet. Ein MAC bezeichnet in diesem Kontext den Hash-Wert einer Einwegfunktion [41]. Unter einem Hash-Wert versteht man dabei die spezielle Bildung einer Quersumme von umfangreichen Informationen, die dabei sicherstellt, dass zu verschiedenen Informationen niemals der gleiche Hash-Wert existieren darf, und dass die Funktion nicht umkehrbar ist. Bei diesem Protokoll hat man den Vorteil, dass für die Nutzdaten schnelle symmetrische Verfahren angewendet werden können, und für den Nachrichtenaustausch die langsamen asymmetrischen Verfahren, die aber wichtig sind, damit Rückschlüsse oder eventuell sogar Berechnungen des symmetrischen Schlüssels unmöglich gemacht, bzw. sehr erschwert werden.

4.5.2.2 Sicherheit

Die Sicherheit des Protokolls steht und fällt mit den verwendeten kryptografischen Verfahren, welche während des Handshake ausgemacht werden. Dies betrifft besonders die internationalen SSL-Versionen, da hier aufgrund der US-Exportbeschränkungen nur symmetrische Verfahren mit 40-Bit und asymmetrische Verfahren mit 512-Bit zur Verschlüsselung herangezogen werden.

4.5.2.3 Grenzen

Nachdem SSL auf dem TCP-Protokoll aufsetzt, bietet es nur für verbindungsorientierte Dienste Vertraulichkeit und Integrität an. UDP-basierende Dienste können deshalb mit SSL nicht geschützt werden. Der zweite große Problempunkt liegt im Aushandeln der Verschlüsselung. Hier wäre es von Vorteil, wenn beim Client fehlende Verschlüsselungsverfahren, die aber von der Priorität her höhere Sicherheit bäten, automatisch nachinstalliert werden würden. Traditionell wird es außerdem für eine einseitige Authentifizierung für Web-Server verwendet, und nicht für Userauthentifikation [27].

4.5.3 Transport Layer Security (TLS)

Beim TLS-Protokoll handelt es sich um eine Erweiterung des SSL-Protokolls.

4.5.3.1 Funktionsweise

In der Funktionsweise unterscheidet sich TLS von SSL nur dahingehend, dass TLS das kryptografisch sichere HMAC-Verfahren zur Berechnung der MAC-Werte verwendet.

4.5.3.2 Sicherheit

TLS verwendet ein modifiziertes Schlüsselerzeugungsverfahren, wodurch eine stärkere Robustheit gegen Angriffe auf Hashfunktionen erreicht wird. Weiters wurde auch die Menge der Alert-Nachrichten erhöht, um auf zusätzliche Fehler oder sogar Angriffe dementsprechend reagieren zu können.

4.5.3.3 Grenzen

TLS basiert genau wie SSL auf dem TCP-Protokoll, sodass für UDP-basierte Dienste keine Sicherheit zur Verfügung gestellt werden kann. Zusätzlich gilt dasselbe, wie für SSL im Bezug auf die Authentifizierung [27].

4.6 Sicherheitskriterien bei Multimedia-Protokollen

Dies beinhaltet Protokolle, die für den Echtzeitdatenaustausch entwickelt wurden. Dazu gehören Internet-Telefonie, Video-Konferenz-Systeme und Systeme zur gemeinsamen Nutzung von Anwendungen. Diese Datentypen erfordern in der Regel eine höhere Bandbreite als einfacher Text und haben größeren Einfluss auf die Sicherheit.
Sämtliche Multimedia-Protokolle weisen einige gemeinsame Eigenschaften auf. Einerseits benutzen sie normalerweise mehr als einen Port. Es werden nämlich für die verschiedenen Datenströme getrennte Verbindungen benötigt. Dies begründet sich vor allem darin, dass man versucht, die Effektivität der Netzwerkressourcen zu maximieren. Normalerweise gibt es somit eine Trennung von Audio- und Videodaten, oftmals sogar noch eine zusätzliche Aufsplittung in eingehende und ausgehende Datenströme. Für die Signalisierung wird außerdem noch eine zusätzliche Verbindung benötigt. Die Daten werden dabei über UDP übertragen, und die Signalisierung wird dagegen über TCP übertragen. Dies hat seine Ursache darin, dass der Payload mit maximaler Geschwindigkeit übertragen werden muss. Es spielt dabei nur eine untergeordnete Rolle, ob einzelne Pakete verloren gehen. Wichtiger ist, dass die angekommenen Pakete sofort verarbeitet werden. Die Signalisierung benötigt aber unbedingt Garantien für die Übertragung. Dies begründet sich durch die Notwendigkeit, dass Signalisierungsnachrichten keinesfalls verloren gehen dürfen.
Daraus lässt sich leicht erkennen, dass Multimedia-Protokolle die Anforderungen an eine Firewall sehr in die Höhe schrauben. Neben den verschiedenen Kanälen, den verschiedenen Protokollen und der Bidirektionalität wird die Sache noch dadurch kompliziert, dass sie zusätzlich eine hohe Leistung erfordern.

Im Folgenden werden die wichtigsten Multimedia-Protokolle auf ihre Tauglichkeit im Zusammenhang mit Firewalls untersucht.

4.6.1 H.323

Bei H.323 handelt es sich um ein binäres Protokoll, welches zur Übertragung von Audio- und Videodatensignalisierung eingesetzt wird. Das Protokoll enthält zusätzlich noch einige niedere Protokolle, welche z.B. für die Codierung des Payloads eingesetzt werden. Wir betrachten aber im Folgenden nur H.323 selbst.
Im H.323 Standard sind keine Sicherheitsvorkehrungen definiert. Damit sind weder Signalisierung noch Payload direkt geschützt. Hier besteht sicher noch Handlungsbedarf, denn vor allem durch Verschlüsselung könnte hier eine Verbesserung erzielt werden.

4.6.1.1 Paketfiltereigenschaften

Bei H.323 werden sowohl UDP- als auch TCP-basierte Verbindungen zum internen Netz aufgebaut. Dabei benötigt jeder Datenstrom sowohl einen dynamisch allokierten TCP-Port für den Kontrollkanal sowie einen dynamisch allokierten Port für den Datenkanal. Weiters werden Audio- und Videodaten separat übertragen, und für jede Richtung wird zusätzlich ein eigener Kanal aufgebaut.
Wie man sieht, kann eine zustandslose Firewall keinerlei Filterung durchführen, da die Ports dynamisch vergeben werden. Bei einer dynamischen Firewall kann zumindest das Aushandeln der Ports protokolliert werden. Da aber H.323-Daten nicht den Charakteristika der UDP-Antwortnachrichten entsprechen, und IP-Adressen an nicht festgelegten Stellen in den Paketen aufscheinen, kann eine herkömmliche Firewall H.323 nicht sinnvoll filtern. Hierbei sind spezielle Firewalls notwendig, die über einen H.323-spezifischen Anwendungsfilter verfügen. Liegt keine Firewall mit diesem spezifischen Filter vor, empfiehlt es sich, sämtliche H.323-Verbindungen nach außen hin zu blockieren.

4.6.2 RTP und RTCP

Das Real Time Transport Protocol (RTP) [78] und das Real Time Control Protocol (RTCP) [79] sind IETF-Standards zur Übertragung von Echtzeitdaten. Bei diesen Echtzeitdaten handelt es sich hauptsächlich um Audio und Video. Meist werden die beiden Protokolle zusammen mit H.323 eingesetzt.

4.6.2.1 Paketfiltereigenschaften von RTP und RTCP

RTP und RTCP verwenden in TCP/IP basierenden Netzen als zugrunde liegendes Protokoll UDP. Dabei können sie prinzipiell jedes Paar von UDP-Ports benutzen. In den meisten Fällen, sofern nicht anderweitig verwendet, wird aber von RTP erwartet, einen geradzahligen Port zu verwenden. In diesem Fall verwendet RTCP die nächsthöhere Portnummer. Falls RTP aber einen ungeradzahligen Port verwendet, benutzt RTCP die nächstniedrigere Portnummer. Dadurch werden immer zwei aufeinanderfolgende Ports verwendet, was natürlich für die Paketfilterung bedeutet, dass die Erkennung relativ einfach von statten geht. Standardmäßig verwendet RTP Port 5004 und RTCP Port 5005, oder 24032 bzw. 24033 [2].
RTP und RTCP werden normalerweise nicht unabhängig von anderen Protokollen eingesetzt. Die beiden Protokolle selbst beinhalten keine Risiken, es hängt nur vom Einsatz des restlichen Pakets ab, wie mit den Protokollen verfahren werden muss.

4.6.3 NetMeeting

NetMeeting baut auf H.323 auf, verwendet aber noch einige zusätzliche Protokolle. Neben den bereits oben erwähnten Sicherheitsproblemen mit H.323 ergeben sich zusätzlich die von Microsoft typischen Implementierungsfehler, die unter gewissen Umständen zu Pufferüberläufen führen können. Zusätzlich können vom User bestimmte Features von NetMeeting wie die gemeinsame Verwendung von Anwendungen oder Dateiübertragungen aktiviert oder deaktiviert werden. Dies stellt vor allem innerhalb der Organisation ein nicht unbeträchtliches Sicherheitsrisiko dar. Für Administratoren ist es dadurch besonders schwierig diese Probleme zu kontrollieren. Es empfiehlt sich daher innerhalb der Organisation NetMeeting zu deaktivieren, bzw. zu deinstallieren.

4.6.3.1 Paketfiltereigenschaften von NetMeeting

Wie bereits oben erwähnt, basiert NetMeeting auf H.323. Zusätzlich wird von Netmeeting auf TCP-Port 1731 eine Audio-Verbindung zur Verbindungsüberwachung, ein LDAP-basierender Suchdienst namens Internet Locator Service (ILS) an TCP-Port 389, und ein proprietärer Suchdienst namens User Location Service (ULS) an TCP-Port 522 eingesetzt [2].
Aufgrund der bereits dargestellten Sicherheitsproblematik ist von der Verwendung von NetMeeting sowohl innerhalb der Organisation als auch über die Firewall dringend abzuraten.

4.6.4 Multicast und das Multicast Backbone

Bei Multicast geht es darum, bestimmte Pakete an eine Gruppe von Empfängern zu versenden. Dafür werden spezielle IP-Adressbereiche verwendet [2]. Meist wird Multicast für die Multimedia-Übertragung verwendet, um so z.B. die Daten einer Videokonferenz an alle Teilnehmer zu senden. Multicast-Pakete können nur von Routern weitergeleitet werden, die multicastingfähig sind. Sind keine solchen Router vorhanden, kann ein Multicast-Paket in ein Unicast-Paket gekapselt werden, und so bis zum nächsten multicastfähigen Router getunnelt werden. Im Internet existiert der sogenannte MBONE (Multicast Backbone), welcher aus einem Geflecht von multicastfähigen Routern besteht [2].

4.6.4.1 Paketfiltereigenschaften von IP-Multicasting

Die meisten multicastfähigen Router akzeptieren keine Unicast-Pakete im Tunnel. Darauf sollte besonderes Augenmerk gelegt werden, da so keine Unicast-Pakete eingeschleust werden können, die einen eventuellen Angriff darstellen. Weiters müssen alle Pakete, die eine Multicast-Quelladresse enthalten blockiert werden, da es solche Pakete gar nicht gibt. Es existieren nämlich nur Multicast-Zieladressen. Außerdem sollte jeder Multicast-Verkehr blockiert werden, außer UDP.
Wenn Multicast aber in einer Organisation kein Thema ist, sollte jeglicher Multicast-Verkehr blockiert werden. Dadurch können eventuelle Sicherheitsprobleme bereits von vornherein eliminiert werden.

4.6.5 SIP

4.6.6 Zusammenfassung Anwendungsebene

Wie man sieht, spielen die Protokolle der Anwendungsebene eine zentrale Rolle in der modernen Komunikationswelt. Definitiv ist klar, dass jedes Protokoll, welches ich durch eine Firewall zulasse, ein potentielles Sicherheitsrisiko darstellt. Auch hier muss aber die Frage nach Kosten/Nutzen gestellt werden. Die erlaubten Protokolle müssen jedenfalls mit den verantwortlichen Managern eindeutig definiert werden. Damit dann diese Protokolle aber nicht zur Sicherheitslücke werden, muss speziell an den verwendeten Servern auf größtmögliche Sorgfalt beim Einspielen von Patches zur Schließung von Sicherheitslücken geachtet werden. Damit kann das Risiko gering gehalten werden, und der Nutzen für das Unternehmen gleichzeitig enorm wachsen.

5 Technische Sicherheitskonzepte

5.1 Firewalls

Die Abbildung zeigt einen simplen Firewall-Aufbau.

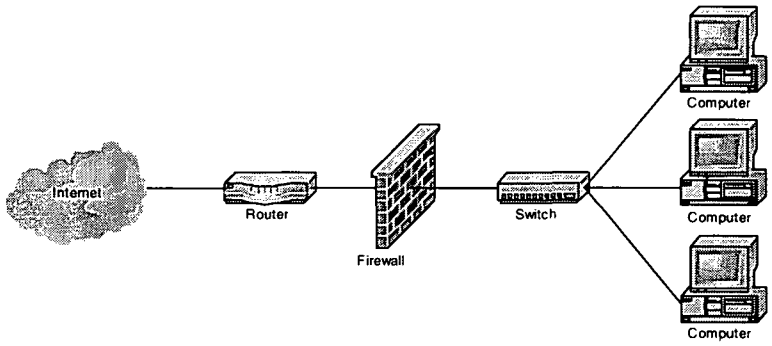


Abbildung 4: Simpler Firewall-Aufbau

5.1.1 Firewall-Aufbau

Prinzipiell gibt es zwei Möglichkeiten eine Firewall zu implementieren. Wenn die Firewall mit zwei Interfaces aufgebaut wird, hat man keine Möglichkeit Informationen für Dritte zur Verfügung zu stellen, da man in diesem Fall einen Zugriff von außen auf das interne LAN erlauben müsste, was vom Sicherheitsaspekt gesehen fatal wäre. Deshalb wird meist die Variante mit drei Interfaces implementiert. Dies bietet den Vorteil, sowohl Informationen für außen zur Verfügung stellen zu können, als auch Proxy-Systeme oder Content Filter in einem gesicherten Rahmen platzieren zu können.
Wenn eine Firewall mit drei Interfaces aufgebaut wird, werden dadurch drei Netzwerke kreiert:

- Inside – Als Inside bezeichnet man die vertraute Zone des Netzwerks. Die Bestandteile auf dieser Seite sind die Komponenten des privaten Firmennetzes. Für die einzelnen Bestandteile existiert eine einheitliche Security Policy gegenüber dem äußeren Netzwerk.
- Outside – Als Outside bezeichnet man die nicht vertraute Zone des Netzwerks. Die Firewall sichert die Bestandteile auf der Inside und der einer eventuell vorhandenen DMZ gegenüber der Outside.
- DMZ (Demilitarized Zone) – Die DMZ ist ein isoliertes Netzwerk, welches normalerweise für User von außen zugänglich ist. Die Firewall muss so konfiguriert werden, dass von außen bzw. von innen ein Zugriff auf die DMZ möglich ist. Die Erstellung einer solchen DMZ ermöglicht es einer Organisation, Information in einer sicheren und kontrollierten Umgebung für User von außen zur Verfügung zu stellen. Dies ermöglicht Usern den Zugriff von außen, ohne das ein Zugang zur Inside möglich ist. Die Abbildung zeigt einen Firewall-Aufbau mit DMZ.

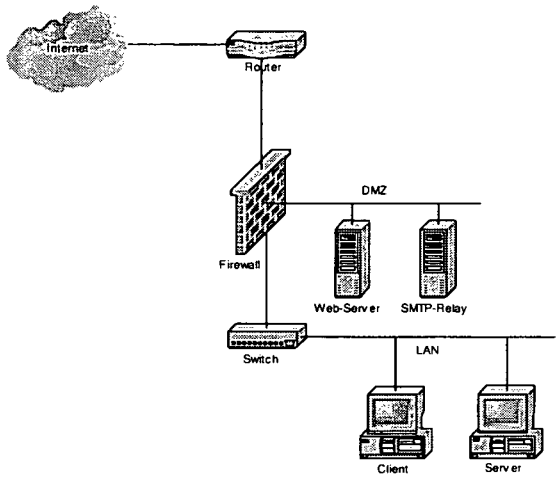


Abbildung 5: Firewall-Aufbau mit DMZ

Die Hosts oder Server, welche sich in der DMZ befinden, bezeichnet man üblicherweise als Bastion Hosts. Ein Bastion Host, ist ein System, welches sowohl vom Betriebssystem als auch den betriebssystemspezifischen Patches auf dem neuesten Stand ist. Dies bringt den Vorteil, dass schon bekannte Sicherheitslücken im Betriebsystem zumindest bis zu einem gewissen Grad ausgemerzt sind. Weiters laufen auf dem Bastion Host nur diejenigen Services, die für seine Aufgaben unbedingt notwendig sind. Alle anderen Services werden deaktiviert, oder entfernt.

Eine Firewall muss folgende Funktionen erfüllen:
- Kein Zugriff von Außen nach Innen
- Limitierter Zugriff von Außen auf die DMZ
- Voller Zugriff von Innen nach Außen

Sinnvoll ist es außerdem, einen SMTP-Server in der DMZ zu platzieren, da ein direkter SMTP-Zugang von außen auf einen SMTP-Server, der im Inneren liegt ein nicht zu unterschätzendes Risiko darstellt. Zusätzlich werden auch Proxy-Systeme meist in der DMZ implementiert.
Ein in diesem Zusammenhang weiterer Aspekt ist auch die Filterung von URLs, um den Internet-Usern den Zugriff auf bestimmte Seiten zu verweigern. Solch ein System sollte ebenfalls in der DMZ platziert werden.

5.1.2 Firewall-Architekturen

In diesem Kapitel werden verschiedene Firewall-Architekturen mit ihren Vor- und Nachteilen vorgestellt. Weiters wird definiert, für welche Anwendungszwecke diese sich eignen und für welche nicht. Hierbei sollte bedacht werden, dass die Single-Box-Architekturen und die Architektur mit überwachten Hosts nur einen Einstieg in die Thematik darstellen sollen. In heutigen Firewall-Systemen, die Höchstmass an Sicherheit gewährleisten sollen, spielen sie nur mehr eine untergeordnete Rolle.

5.1.2.1 Single-Box-Architekturen

Die Single-Box-Architektur [2] beschreibt den einfachsten Aufbau einer Firewall, wobei ein einziges Gerät als Firewall fungiert. Diese Architektur kann auf dreierlei Arten realisiert werden, welche in den folgenden drei Abschnitten genau beleuchtet werden.

5.1.2.1.1 Überwachungsrouter

Bei dieser Architektur wird einfach ein Router zwischen internem Netzwerk und dem Internet platziert. Dies ist definitiv das preiswerteste System, da in jedem Fall ein Router zwischen Internet und LAN benötigt wird. Auf dem Router kann zwar die Paketfilterung aktiviert werden, aber diese ist bei den meisten Routerprodukten sehr einfach gehalten. Man ist sowohl von der Anzahl der Regeln die definiert werden können, als auch von der Flexibilität der Filterregeln stark eingeschränkt. Es können natürlich bestimmte Ports gesperrt werden, man hat aber nicht die Möglichkeit einerseits ein Protokoll auf bestimmte Operationen einzuschränken, und andererseits ist es auch nicht möglich festzustellen, ob ein Paket, welches an einem bestimmten Port ankommt zu dem definierten Protokoll gehört. Ein weiteres Problem ist, dass sobald der Router überwunden wurde, es praktisch keinen Schutz mehr für das LAN gibt.

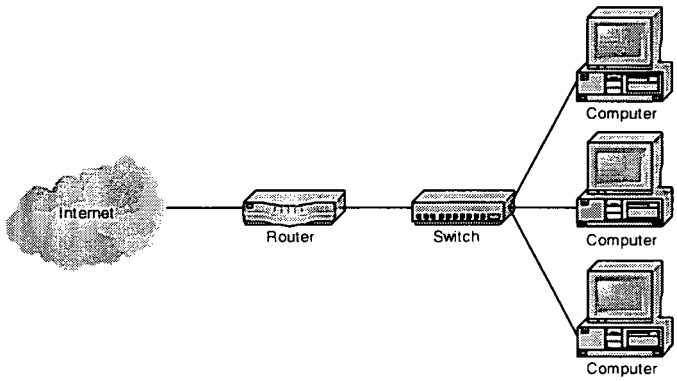


Abbildung 6: Überwachungsrouter

5.1.2.1.1.1 Einsatzmöglichkeiten

Ein Überwachungsrouter ist dann eine geeignete Firewall, wenn:

- das interne Netz über einen sehr hohen Grad an Rechnersicherheit verfügt
- die Anzahl der verwendeten Protokolle sehr begrenzt ist
- die verwendeten Protokolle eine einfache Struktur aufweisen
- maximale Leistung gefordert wird

Meiner Meinung nach ist dieser Ansatz nicht mehr zeitgemäß. Einerseits können keine dynamischen Filter angewendet werden, und andererseits ist man von den verwendbaren Protokollen sehr eingeschränkt. Damit ist die Sicherheit keinesfalls gewährleistet. Außer als interne Firewall sollte der Überwachungsrouter keinesfalls eingesetzt werden.

5.1.2.1.2 Dual-Homed-Host

Bei einem Dual-Homed-Host handelt es sich um einen Rechner der mit zwei Netzwerkinterfaces ausgestattet ist. Ein Interface dient dabei zur Verbindung mit dem Internet, das andere stellt die Verbindung zum LAN her. Hierbei können Zugriffe sowohl vom Internet ins interne Netzwerk, als auch umgekehrt realisiert werden. Eine direkte Kommunikation zwischen zwei Netzwerkpartnern, wobei sich der eine innerhalb, und der andere außerhalb des LAN befindet, ist aber nicht möglich. Ein wesentlicher Unterschied zum Überwachungsrouter, ist die geringere Leistungsfähigkeit, aber auch dass Services direkt am Dual-Homed-Host angeboten werden können. Die zweite Eigenschaft stellt natürlich eine große Sicherheitsproblematik dar, da mit der Anzahl der Dienste auch die Anzahl der Angriffsmöglichkeiten steigt.

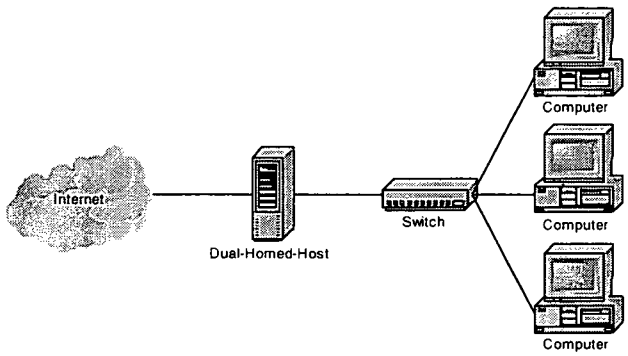


Abbildung 7: Dual-Homed-Host

5.1.2.1.2.1 Einsatzmöglichkeiten

Ein Dual-Homed-Host ist dann eine geeignete Firewall, wenn:

- es nur wenig Verkehr ins Internet gibt
- die geschäftliche Tätigkeit durch den Internetausfall nicht beeinträchtigt wird
- den Benutzern im Internet keine sicherheitskritischen Dienste zur Verfügung gestellt werden
- keine geheimen Daten im internen LAN existieren

Dual-Homed-Hosts sollten meiner Meinung nach nicht verwendet werden. Dies hat einige gewichtige Gründe. Einerseits ist ein Rechner schon vom Betriebssystem wesentlich leichter angreifbar, als ein Router, andererseits bietet er keinen wirklichen Vorteil, verglichen mit dem Überwachungsrouter. Es wäre zwar möglich auf dem Host selbst Services anzubieten, dies sollte aber aus Sicherheitgründen vermieden werden. Weiters ist die schwache Peformance ein weiterer Grund, welcher gegen so ein System spricht. Einzig und allein von den Kosten ergibt sich ein Vorteil, da hoch entwickelte Routerhardware um ein Vielfaches teurer ist, als ein einzelner Rechner mit zwei Netzwerkinterfaces. Wie auch beim Überwachungsrouter ist höchstens ein Einsatz als interne Firewall denkbar.

5.1.2.1.3 Multipurpose-Rechner

Hierbei sind Geräte gemeint, die einerseits einen Paketfilter zur Verfügung stellen, als auch als Proxy fungieren. Unter einem Proxy verstehen wir eine Software, die Dienste aus dem internen Netzwerk in das externe Netzwerk weiterleitet. Somit können Internetzugänge vermittelt implementiert werden.

5.1.2.1.3.1 Einsatzmöglichkeiten

Ein Multipurpose-Rechner ist dann eine geeignete Firewall, wenn:

- das zu schützende Netzwerk klein ist
- keine Dienste für das Internet zur Verfügung gestellt werden

Wie bereits erwähnt, steigt mit der Anzahl der Services die Angriffsmöglichkeit. Dies macht sich besonders deutlich, wenn nur ein einziger Rechner diese Services hostet. Deshalb sei an dieser Stelle wieder einmal von solch einer Architektur abgeraten. Diese Architekturen sind höchstens für den Heimbereich gedacht, aber sicher für Firmennetze keinesfalls brauchbar.

5.1.2.1.4 Vorteile

Ein Vorteil der Single-Box-Architektur besteht darin, dass man sich nur auf eine Stelle konzentrieren, und diese richtig konfigurieren muss. Es handelt sich zwar um keine besonders umfassende Verteidigung, aber es ist immer eindeutig definiert, wo die schwächste Stelle ist, und wie schwach diese ist. Bei mehrschichtigen Modellen nimmt die Komplexität exponentiell mit der Anzahl der Komponenten zu. Ein weiterer Vorteil besteht darin, dass diese Architektur sehr preiswert, leicht verständlich und dem Management gegenüber einfach zu erklären ist. Einzig und allein für relativ kleine Standorte mit sehr geringen Sicherheitsanforderungen bzw. für den Privatbereich stellt diese Architektur eine sehr gute und vor allem preiswerte Lösung dar.

5.1.2.1.5 Nachteile

Selbstverständlich beinhaltet eine derart einfach gestaltete Architektur eine Vielzahl von Nachteilen, die sorgfältig in Betracht gezogen werden müssen, um vor einer Fehlentscheidung zu schützen.
Die Sicherheit hängt in diesem Fall völlig an einer einzigen Stelle, und bietet daher keine umfassende Verteidigung. Dies kann im schlimmsten Fall bedeuten, dass eine Fehlkonfiguration zur Katastrophe führt. Bei mehrschichtigen Systemen ist diese Gefahr geringer, da eine eventuelle Fehlkonfiguration in einer der Komponenten durch eine andere Komponente kompensiert werden kann. Weiters kann durch einen Ausfall in einem Szenario ohne redundante Komponenten den Ausfall des gesamten Netzverkehrs bedeuten, da die Firewall unter Umständen auch für den Datenaustausch zwischen mehreren Standorten, und nicht nur allein für eine Internetverbindung genutzt werden kann. Auch ein alleiniger Ausfall des Internet kann für eine Organisation erhebliche Verluste mit sich ziehen.

5.1.2.1.6 Zusammenfassung

In den letzten Abschnitten wurde ziemlich deutlich, dass diese Art der Architektur mehr Nachteile mit sich bringt, als Vorteile daraus zu ziehen wären. Einzig der Überwachungsrouter hat eine gewisse Daseinsberechtigung, da er von allen 3 Varianten die sicherste darstellt. Für den Firmenbereich ist aber keine der obigen Subarchitekturen geeignet, da vom Sicherheitsstandpunkt keine geeigneten Maßnahmen gesetzt werden.

5.1.2.2 Architekturen mit überwachten Hosts

Bei dieser Art der Architektur verwendet man einen Rechner, der im Gegensatz zum Dual-Homed-Host, nur an das interne Netzwerk angeschlossen ist. Dadurch ist es für Clients nicht möglich Verbindungen zum Internet über den Router direkt aufzubauen. Jedweder Verkehr muss durch den überwachten Host gehen, der auch als Bastion Host bezeichnet wird [2]. Somit können erlaubte Dienste am Bastion Host definiert werden, wobei dieser dann für diese Dienste als Proxy fungiert. Wichtig dabei ist aber, dass der Bastion Host gut abgesichert ist.

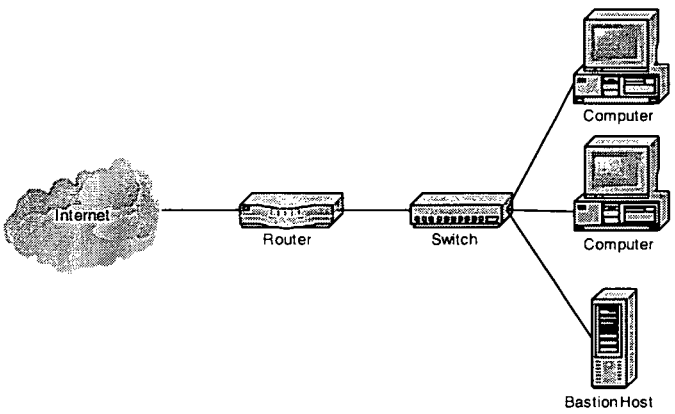


Abbildung 8: Architektur mit überwachtem Host

5.1.2.2.1 Vorteile

Ein wichtiger Vorteil ist die Trennung zwischen Paketfilter und Proxy. Der Bastion Host fungiert als Proxy und der Router als Paketfilter. Weiters ist es natürlich viel einfacher, einen Router abzusichern, deshalb ist auch hierbei die Trennung von Vorteil. Deshalb ist gegenüber einer Dual-Homed-Host-Architektur diese klar im Vorteil. Sollte sich also die Wahl zwischen Dual-Homed-Host-Architektur oder dieser Architektur stellen, ist diese Architektur jedenfalls vorzuziehen.

5.1.2.2.2 Nachteile

Der Hauptnachteil besteht darin, dass wenn ein Angreifer schafft in den Bastion Host einzudringen, dass ihm das gesamte interne Netzwerk offen steht. Auch in dem Fall, wo der Router überwunden werden sollte, steht dem Angreifer das Netz völlig schutzlos gegenüber.

5.1.2.2.3 Zusammenfassung

Wie man aus den Nachteilen erkennen kann, ist die Architektur mit überwachtem Host genauso unbrauchbar, wie die Single-Box-Architekturen, um ein Firmennetz abzusichern. Deshalb werden wir uns im nächsten Kapitel den Architekturen mit überwachtem Teilnetz widmen, die sich heutzutage als Standard durchgesetzt haben.

5.1.2.3 Architekturen mit überwachtem Teilnetz

Dies ist eine Erweiterung, der im vorigen Abschnitt vorgestellten Architektur. Hierbei wird ein zusätzliches Netzwerk, das so genannte Grenznetzwerk, als Erweiterung eingeführt. Durch dieses Grenznetzwerk wird das Internet vom internen Netzwerk abgeschottet.
Nun stellt sich die Frage, wozu der Aufwand gut sein soll. Natürlicherweise sind die Bastion Hosts die verwundbarsten Maschinen im Netzwerk. Bei diesen Rechnern ist die Wahrscheinlichkeit eines Angriffs definitiv am höchsten. Bei der Architektur mit überwachtem Host steht dem Angreifer das gesamte Netzwerk zur Verfügung, sobald der Bastion Host geknackt wurde. Durch die Isolierung des Bastion Host in einem Grenznetzwerk, können die Auswirkungen so eines Einbruchs extrem minimiert werden. Der Angreifer hat nämlich nicht automatisch den vollen Zugang zum internen LAN, sobald der Bastion Host geknackt wurde. Typischerweise wird ein äußerer Router verwendet, der das Internet und das Grenznetzwerk, in dem sich der Bastion Host befindet voneinander trennt. Ein weiterer Router, der als interner Router bezeichnet wird, trennt das Grenznetzwerk vom internen LAN. Ein Angreifer, der den äußeren Router überwindet, kann er zwar versuchen den Bastion Host anzugreifen, aber selbst wenn dieser erfolgreich überwunden wird, muss er immer noch den internen Router knacken, um in das LAN eindringen zu können. Durch diese mehrschichtige Architektur erzielt man demnach eine wesentlich höhere Sicherheit, als bei den zuvor vorgestellten Architekturen.

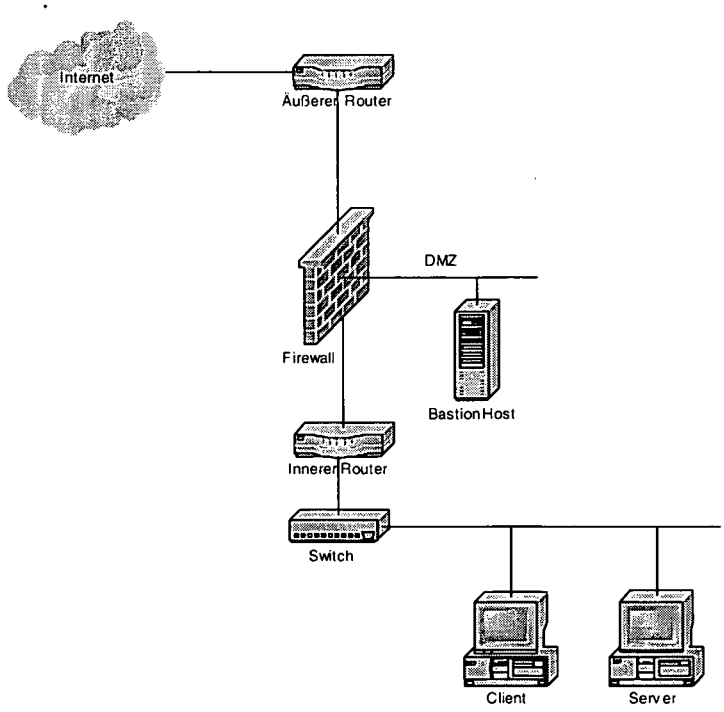


Abbildung 9: Architektur mit überwachtem Teilnetz

5.1.2.3.1 Das Grenznetzwerk

Das Grenznetzwerk, das oft auch als Demilitarized Zone (DMZ) bezeichnet wird, stellt ein Schutznetzwerk zwischen dem äußeren Netzwerk und dem inneren Netzwerk dar. Damit ein Einbruch erfolgreich ist, muss sowohl der äußere Router, als auch der innere Router geknackt werden. Ein weiterer Vorteil ist, dass bei Einbruch in die DMZ, der interne Netzwerkverkehr nicht abgehört werden kann.

5.1.2.3.2 Der Bastion Host

Der Bastion Host verfügt nur über eine Verbindung zur DMZ. Dadurch kann er für eingehenden E-Mail-Verkehr, WWW-Dienste oder anonyme FTP-Dienste eingesetzt werden. Zusätzlich kann am Bastion Host auch ein Proxy implementiert werden, damit es den Clients nicht möglich ist, direkte Verbindungen zum Internet aufzubauen. Dadurch ist die Hauptaufgabe des Bastion Host der Proxy-Betrieb für verschiedene, von der Sicherheitspolitik abhängige Dienste.

5.1.2.3.3 Der innere Router

Der innere Router schützt das interne Netzwerk sowohl vor dem Internet, als auch vor dem Grenznetzwerk. Der interne Router hat somit die Aufgabe, den größten Teil der Paketfilterung durchzuführen. Er erlaubt somit ausgewählten Diensten, den Zugriff vom internen LAN ins Internet. Sinnvollerweise erlaubt man es den internen Client nur über den Bastion Host, der dabei als Proxy fungiert, Verbindungen ins Internet aufzubauen. Direkte Verbindungen von internen Client ins Internet sollten soweit als möglich vermieden werden. Weiters sollte die Anzahl der Proxy-Dienste beschränkt sein, damit es Angreifern erschwert wird, falls diese den Bastion Host knacken, auch ins interne LAN einzudringen. Die wichtigsten Dienste beinhalten dabei SMTP, damit E-Mails aus dem Internet an den internen Mail-Server weitergeleitet werden können, und umgekehrt; FTP und HTTP um den Zugriff auf öffentliche Webseiten und FTP-Server zu gestatten. Ist es auch notwendig, DNS-Abfragen von internen Clients durchzuführen, kann auch dieser Dienst erlaubt werden.

5.1.2.3.4 Der äußere Router

Der äußere Router hat vor allem die Aufgabe, das Grenznetzwerk vor dem Internet zu schützen. Dabei können dieselben Regeln wie auf dem internen Router verwendet werden. Zusätzlich müssen alle Pakete, welche aus dem Internet stammen und mit einer gefälschten Absenderadresse versehen sind blockiert werden. Diese Pakete geben nämlich vor, vom internen Netzwerk zu kommen, sie kommen aber in Wirklichkeit aus dem Internet. Ebenfalls müssen von ihm auch die Quelladressen überprüft werden, und ungültige Quelladressen sofort blockiert werden. Dies ist nämlich ein Hinweis darauf, dass jemand im internen Netzwerk versucht Quelladressen zu fälschen.

5.1.2.3.5 Zusammenfassung

Die Architektur mit überwachtem Teilnetz stellt derzeit die sicherste Variante von allen Firewall-Architekturen dar. Sie ist für jede Art von Anwendungsbereich geeignet. Wie schon in Abschnitt 6.1 angesprochen, ist eine Sicherheitspolitik nur dann effektiv, wenn sie permanent getestet und verbessert wird. Eine Firewall einmal einzurichten, und dann zu vergessen, ist sicher einer der größten Fehler, welche gemacht werden. Oft spielen auch mangelnde Investitionen oder inkompetente EDV-Administratoren eine entscheidende Rolle. Firewalls sind sicher kein Allheilmittel für alle Sicherheitsprobleme, bilden aber das Fundament jeder vernünftigen Sicherheitspolitik.

5.1.3 Network Adress Translation

Network Adress Translation (NAT) verbirgt das gesamte interne Netz hinter einigen wenigen offiziellen IP-Adressen, um möglichst wenig Information über das interne Netz bekannt zu geben [80]. Dabei verwendet man für das interne LAN vorzugsweise IP-Adressen aus [87], die nicht im Internet geroutet werden, und daher nicht direkt erreichbar sind. Die Aufgabe der Übersetzung kann entweder eine Firewall, oder ein Router übernehmen. Die Geräte arbeiten dabei auf Basis der IP-Datenpakete, und ändern beim Transport der Pakete in beide Richtungen jeweils die Absender- und Empfängeradressen sowie die zugehörigen Ports. Der Vorteil dieser Technik ist einerseits, dass der Aufbau des internen Netzwerks beliebig ist, und dass nur wenige öffentliche IP-Adressen benötigt werden. Das bedeutet, dass alle Rechner, die von außen nicht erreicht werden müssen hinter einer offiziellen IP-Adresse versteckt werden können. Man spricht dann von dynamischen NAT. Rechner, die von außen erreicht werden müssen, wie z.B. Mail-Server, WWW-Server und Proxies müssen eine eindeutige statische externe IP-Adresse besitzen. Hierbei kann statisches NAT eingesetzt werden, falls diese Rechner nur im internen LAN hängen, und kein externes Interface besitzen. Die Firewall oder der Router tauschen dann bei externen Verbindungen die internen IP-Adressen gegen die externen aus.

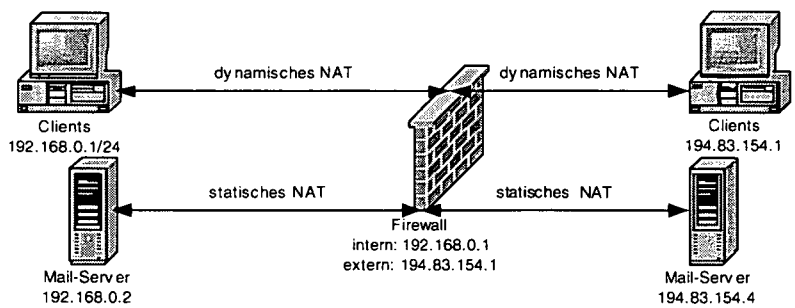


Abbildung 10: Ablauf NAT

5.1.4 Stärken von Firewalls

5.1.4.1 Eine Firewall ist ein Schwerpunkt der Sicherheitsmaßnahmen

Die Firewall agiert in diesem Sinn als Kontrollpunkt, den sowohl eingehende als auch ausgehende Daten passieren müssen. Der Vorteil besteht darin, dass Sicherheitsmaßnahmen an einem Punkt konzentriert werden, und nicht über das Netzwerk verteilt sind. Dadurch können diese zielgerichtet eingesetzt werden.

5.1.4.2 Eine Firewall kann die Security Policy durchsetzen

Ein sehr wichtiger Aspekt ist die Anwendung der Security Policy, da hierbei nur bestimmte Dienste von der Firewall akzeptiert werden. So können potentiell unsichere Dienste gesperrt werden. Diese Policys können dabei sehr komplex definiert werden, und auch nur für bestimmte User oder Computer, Dienste zur Verfügung stellen.

5.1.4.3 Eine Firewall muss effektiv alle Internet-Aktivitäten protokollieren

Da der gesamte externe Datenverkehr die Firewall passieren muss, eignet sich diese hervorragend, Informationen über die System- und Netzwerkbenutzung zu sammeln. Dies schließt natürlich auch den Missbrauch mit ein.

5.1.4.4 Eine Firewall verkleinert die Angriffsfläche

Dieser Aspekt ist nur dann von Relevanz, wenn das interne Netzwerk durch eine Firewall in mehrere Bereiche aufgegliedert wird. Der große Vorteil daran ist die erhöhte Sicherheit, denn selbst wenn ein Angreifer die äußere Firewall überwindet, muss er noch eine zweite Firewall überwinden um in den nächsten internen Bereich vorzudringen. So können z.B. besonders kritische Teilnetze noch zusätzlich gesichert werden.

5.1.5 Schwächen von Firewalls

5.1.5.1 Eine Firewall kann nicht vor bösartigen Insidern schützen

Eine Firewall kann zwar verhindern, dass vertrauliche Informationen über das Netzwerk nach außen geschmuggelt werden, sie kann aber nicht verhindern, dass Daten über Datenträger oder auf Papier entwendet werden, dass Hard- und Software beschädigt werden, oder subtile Änderungen an Programmen vorgenommen werden. Dies fällt dann in den Themenbereich der Rechnersicherheit und der Benutzerschulung, die noch an anderer Stelle genau erläutert werden.

5.1.5.2 Eine Firewall kann nicht vor Verbindungen schützen, die nicht durch sie hindurchgehen

Eine Firewall kann selbstverständlich nur den Verkehr kontrollieren, welcher durch die Firewall hindurchgeht. Oft gibt es aber neben den externen Zugängen, welche durch die Firewall hindurchführen, auch noch Möglichkeiten für Einwählverbindungen, welche z.B. durch RAS-Server (Remote Access Service) realisiert werden. Gegen Angriffe, welche durch diesen Zugang durchgeführt werden, kann eine Firewall natürlich nicht schützen.

5.1.5.3 Eine Firewall kann nicht vor vollkommen neuen Gefahren schützen

Eine Firewall dient dazu, vor bekannten Gefahren zu schützen. Fast täglich werden aber neue Angriffsmöglichkeiten entdeckt. Darum muss aber auch die Firewall immer auf dem neuesten Stand gebracht werden. Eine prinzipiell gute Vorgehensweise ist z.B. nur gewisse vertrauenswürdige Dienste von vornherein zuzulassen. Sobald neue Dienste entstehen, werden diese automatisch abgelehnt. Weiters muss aber ständig geprüft werden, ob nicht neue Angriffstechniken gegen vertrauenswürdige Dienste entwickelt wurden. Eine ständige Betreuung sowie die Auseinandersetzung mit sicherheitsrelevanten Themen sind bei der Betreuung einer Firewall unabdingbar.

5.1.5.4 Eine Firewall bietet keinen vollständigen Schutz vor Viren

Eine Firewall ist keinesfalls dazu geeignet ein Netzwerk vor Viren zu schützen. Dies ist dadurch bedingt, dass eine Firewall normalerweise auf Paketebene prüft. Selten wird es vorkommen, dass ein Virus nur in einem einzelnen Paket ankommt. Deshalb ist es wichtig neben der Sicherheit durch Firewalls zusätzlich auf Virenschutz auf den einzelnen Clients und Servern Wert zu legen. Ein zusätzlicher Schutz, um z.B. eingehende E-Mails auf Viren zu überprüfen, wäre eine Koppelung der Firewall mit einem SMTP-Proxy, welcher alle eingehenden und eventuell auch ausgehenden E-Mails auf Viren überprüft.

5.1.5.5 Eine Firewall kann sich nicht selbst richtig einrichten

Jede Firewall benötigt ein Maximum an Konfigurationsarbeit, um größtmögliche Sicherheit zu gewährleisten. Dies begründet sich vor allem daraus, dass jedes Netzwerk anders aufgebaut ist, und dass auch die Anforderungen an die Firewall relativ unterschiedlich sein können. Eine korrekte und vor allem genau geplante Konfiguration ist deshalb unerlässlich. Eine fehlkonfigurierte Firewall bietet nur die Illusion der Sicherheit. Die große Gefahr besteht dann darin, dass dadurch das Risiko im Endeffekt nur noch größer wird.

5.2 Proxy-Server

5.2.1 Einleitung

Ein Proxy ist eine Software, die als Vermittler zwischen Client und dem Internet fungieren. Bei Proxies erfolgt jede Verbindung aus dem internen Netzwerk zunächst ausschließlich zum Proxy, der dann die gewünschte Verbindung zum Internet für den internen Client aufbaut. Bei der Realisierung von Proxies wird zwischen Application Level und Circuit Level Proxies unterschieden.

5.2.2 Application Level Proxies

Application Level Proxies sind für bestimmte Dienste und Anwendungen implementiert. Sie verstehen also Kommandos der Anwendungsprotokolle und können diese analysieren und kontrollieren. Meist ist es aber notwendig, die Anwendungssoftware auf den Proxy-Betrieb einzustellen, und die Verbindung zum Internet wird erst nach erfolgreicher Authentifizierung am Proxy, hergestellt. Beispiele für solche Application Level Proxies sind Proxies für HTTP, FTP, SMTP und Telnet.

5.2.3 Circuit Level Proxies

Bei den Circuit Level Proxies handelt es sich um generische Proxies, welche für eine Vielzahl von Diensten mit verschiedenen Protokollen implementiert werden können, für die keine Application Level Proxies zur Verfügung stehen. Diese arbeiten meist mit so genannten Port-Relays, die es ermöglichen von vielen Clients aus dem internen Netzwerk auf einen bestimmten Port eines bestimmten Servers aus dem Internet kommunizieren zu können.

5.2.4 Sicherheit

Proxies bieten eine elegante Möglichkeit, Clients vor direkten Verbindungen mit dem Internet zu schützen. Dadurch ist es auch nicht notwendig, ein aufwendiges NAT einzurichten, da nur die externe Adresse des Proxies bei Verbindungsaufbau ins Internet gesendet wird. Zusätzlich können durch Proxies Beschränkungen definiert werden, sodass nicht jeder Benutzer die gleichen Verbindungsmöglichkeiten erhält, und für bestimmte Benutzer kein Zugriff gewährt wird.

5.2.5 Zusammenfassung

Proxies bieten einerseits die Möglichkeit Internetverbindungen zu beschränken und zu vermitteln, und andererseits die Möglichkeit sämtliche Zugriffe zu protokollieren. Es empfiehlt sich daher, wo es möglich und sinnvoll ist, Proxies einzusetzen. Dies ergibt sich einerseits aus der Vereinfachung der Firewall-Regeln, da nicht eine Vielzahl von NAT-Einträgen vonnöten sind, welche die Übersichtlichkeit vermindert, und die Fehleranfälligkeit erhöht. Andererseits können Beschränkungen definiert werden, wobei dies natürlich auch die Sicherheit erhöhen kann, da wirklich nur Benutzer auf bestimmte Ressourcen Zugriff erhalten, die diese unbedingt benötigen.

5.3 Content Walls und Content Filtering

5.3.1 Einleitung

Hierbei handelt es sich um Systeme, die einerseits Web-Seiten mit bestimmten, definierbaren Inhaltskriterien herausfiltern können (URL-Blocker), und andererseits gibt es auch die Möglichkeit, aktive Inhalte von Web-Seiten oder E-Mails zu entfernen, um die Risiken eines Viren- oder Wurmbefalls zu minimieren.

5.3.2 Sicherheit

Die Sicherheit erhöht sich vor allem dadurch, dass potentiell gefährliche Scripts aus Web-Seiten und E-Mails zentral entfernt werden können, sodass diese gar nicht das interne LAN erreichen. Ein Nachteil ergibt sich dadurch höchstens, dass bestimmte Web-Seiten diese Scripts unbedingt benötigen, um korrekt zu funktionieren. Man sollte deshalb eine Menge von vertrauenswürdigen Seiten definieren, um den Anwendern nicht die benötigte Funktionalität zu entziehen.

5.3.3 Zusammenfassung

Für Unternehmen bieten diese Systeme den großen Vorteil, dass Internet-Seiten mit kriminellem oder pornographischem Inhalt automatisch blockiert werden können. Damit kommen Abteilungsleiter und Verantwortliche nicht in die Verlegenheit, mit Strafandrohungen konfrontiert zu werden. Der weitere Vorteil ist sicher die Möglichkeit zur Entfernung von aktiven Inhalten, um Datenverlust im internen Netzwerk vorzubeugen.

5.4 Backup & Disaster Recovery

5.4.1 Einleitung

Soll ein vernetztes System zuverlässig und möglichst störungsfrei arbeiten, so stellt sich alsbald die Frage: Was passiert, wenn es zu Datenverlust kommen sollte? Dabei spielt es eher eine untergeordnete Rolle, aus welchem Grund es zu diesem Datenverlust kam. Es ist vielmehr wichtig, die korrekten Daten innerhalb eines möglichst kurzen Zeitraumes wieder verfügbar zu machen. Unternehmen sind also von ihren elektronisch gespeicherten Daten in einem großen Maße abhängig [25]. Es muss sichergestellt werden, dass die Daten sowohl korrekt, als auch verfügbar sind. Deshalb muss sich das Management bewusst sein, dass ein Disaster jederzeit eintreffen kann. Viele Firmen verzichten aber aufgrund der scheinbaren Kosteneinsparung auf Maßnahmen, die im Katastrophenfall ein Wiederanlaufen der EDV innerhalb kurzer Zeit ermöglichen würden. Viele Studien zeigen aber, dass nach ca. 15 Tagen ohne EDV die Geschäftstätigkeit kritisch eingeschränkt ist und die Chance zur Wiederbelebung bei nur 25% liegt [25]. Dieses Kapitel gibt einen Überblick über die Problematik, und beschäftigt sich danach mit den technischen Vorgehensweisen. Kapitel 6.3 erläutert danach die organisatorischen Rahmenbedingungen, wie Katastrophenpläne und dergleichen.

5.4.2 Ursachen

Über die Ursachen solcher Störungen herrscht im allgemeinen Einigkeit. Es sind in erster Linie Kompatibilitätsprobleme auf Hardware- und Softwareseite, welche die Erblast einer über die Jahre hinweg ungeplant und wild gewachsenen IT-Landschaft darstellen. Zusätzlich spielen auch Bedienungs- und Konfigurationsfehler neben dem Ausfall von Hard- und Softwarekomponenten eine wichtige Rolle. Aufgrund dieser Störfaktoren sichern sich Unternehmen meist nur durch Einzelmaßnahmen gegen Risiken im IT-Betrieb ab. Dabei handelt es sich meist um Backups, Spiegelserver und Viruskontrollen, die ganz oben auf der Maßnahmenhitliste stehen. Diese ermöglichen aber nur den Status quo nach einem IT-Zusammenbruch wieder herzustellen. Hier sind umfassende Wartungs- und Sicherheitskonzepte gefragt, welche in den nächsten Abschnitten näher beleuchtet werden sollen.

5.4.3 Definitionen

In diesem Abschnitt sollen einige Definitionen gegeben werden, die in Zusammenhang mit Backup & Disaster Recovery eine zentrale Rolle spielen:

Notfall: Nicht jeder Teil- oder Gesamtausfall des Systems stellt einen Notfall dar. Oftmals lassen sich Ausfälle des IT-Systems durch geplante Maßnahmen, z.B. Ersatzbeschaffungen auch in kurzer Zeit beheben. Der Notfall tritt erst dann ein, wenn ein Zustand erreicht wird, bei dem innerhalb der geforderten Zeit eine Wiederherstellung der Verfügbarkeit nicht möglich ist und sich daraus ein sehr hoher Schaden ergibt. Schon bei Eintritt eines Ereignisses, in dessen Folge der Notfall entstehen könnte, sind die erforderlichen Maßnahmen zu ergreifen, die zu einer Schadensreduzierung führen [25].

Ausfallzeit (downtime): Ausfallzeit beschreibt die Dauer der Nichtverfügbarkeit eines Computersystems, einschließlich der Software und der Zusatzgeräte. Im Ergebnis der Ausfallzeit entsteht ein Produktivitätsverlust.

5.4.4 Schutzmaßnahmen

In diesem Abschnitt werden technische Möglichkeiten erläutert, um für bestimmte Ausfallsituationen schnellstmöglich reagieren zu können, bzw. Automatismen, die keinerlei Eingriff erfordern.

5.4.4.1 RAID-Systeme (Redundant Array of Independent Disks)

RAID-Systeme können im Falle eines Festplattenausfalls Ausfallzeiten verhindern. In der Praxis sinnvoll sind aber nur RAID-1-Systeme (Spiegelung), z.B. für Systempartitionen und RAID-5-Systeme (Stripe-Sets), z.B. für Datenbanken einsetzbar. RAID-0 Systeme bieten aufgrund der nicht vorhandenen Ausfallsicherheit keine Alternative zu RAID-1 und RAID-5 Systemen. Man darf aber niemals vergessen, dass sowohl bei RAID-1 als auch RAID-5 maximal eine Platte ausfallen darf. Sollte dieser Fall eintreten, so haben sich Spares als sehr nützlich erwiesen, um bis zum Eintreffen der Ersatzplatte die Möglichkeit eines zweiten Plattenausfalls nicht im Disaster enden zu lassen.

5.4.4.2 Cluster-Systeme

Cluster-Systeme bieten im Fall eines kompletten Serverausfalls einen hohen Grad an Sicherheit, da hierbei ein Ersatzserver die Aufgaben des ausgefallenen Servers übernimmt. Viele Unternehmen scheuen aber den Einsatz redundanter Server, vor allem aus Kostengründen. Hierbei sollte mithilfe eines Kostenvergleichs festgestellt werden, welche Alternative im Endeffekt wirklich günstiger ausfällt.

5.4.4.3 USV & Notstromgeneratoren

Im Falle eines Stromausfalles haben USVs (Unterbrechungsfreie Stromversorgung) und Notstromgeneratoren einen sehr hohen Wert. Man darf dabei aber nicht vergessen, dass USVs meist nur über einen kurzen Zeitraum die kritischen Komponenten am Leben erhalten können, meist nur für ein paar Minuten, um ein ordnungsgemäßes Herunterfahren der Systeme zu gewährleisten. Dauert der Stromausfall länger, so sind Notstromgeneratoren unerlässlich. USVs basieren auf Akkumulatoren, und sollten regelmäßig auf Funktionstüchtigkeit getestet werden, damit im Notfall diese auch wirklich funktionieren. Der Einsatz von Notstromgeneratoren ist aus Kostengründen meist nur dort sinnvoll, wo mit häufigen und länger andauernden Stromausfällen zu rechnen ist. Für alle anderen Bereiche ist eine USV meist ausreichend.
Neben diesen beiden Geräten für den Notstrom sollte auch ein Überspannungsschutz nicht vergessen werden.

5.4.4.4 Redundanz von Netzwerkkomponenten

Redundanz empfiehlt sich vor allem bei aktiven Netzwerkkomponenten, sodass im Falle eines Ausfalls nicht das gesamte Netzwerk lahm gelegt wird. Hier stellt sich genau, wie bei Cluster-Systemen wieder die Kostenfrage. Die Entscheidung sollte hierbei aber genauso aufgrund einer Kosten-Nutzen-Analyse basieren, und nicht rein budgetär abgetan werden.

5.4.4.5 Software-Updates & Patches

Dies betrifft vor allem Fehlverhalten von Software und Betriebssystemen, die zu einem Datenverlust führen können. Das Konzept wird in Abschnitt 6.2 genau erläutert.

5.4.4.6 Backups

Eine der wohl wichtigsten technischen Schutzmaßnahmen sind Backups. Darunter versteht man das Sichern von wichtigen Daten oder kompletten Systemen auf speziellen Speichermedien. Je nach Datenvolumen kommen verschiedene Backup-Medien zum Einsatz. Für kleine Datenmengen sind Datenträger, wie DVD-RW, CD-RW, ZIP, Jaz und dergleichen geeignet. Handelt es sich um Datenmengen mit einigen hundert Gigabyte oder mehr, empfehlen sich diverse Bandmedien, wie DLT, SDLT und dergleichen. Bei Bandmedien gibt es je nach Datenvolumen skalierbare Tape-Libraries, welche die Sicherung von mehreren Servern gleichzeitig ermöglichen. Dabei sollte aber nie vergessen werden, dass einerseits eine Auslagerung der Medien an einen anderen Standort (besonders im Brandfall oder bei Naturkatastrophen) extreme Bedeutung beigemessen werden muss. Andererseits muss ein Backupplan entwickelt werden, der im Einklang mit der Datenänderung und der Zunahme des Datenvolumens steht. Diesem Thema widmet sich Abschnitt 3.2.2 im Detail. Zusätzlich ist es extrem wichtig, die Medien regelmäßig auf Funktionstüchtigkeit zu überprüfen, damit nicht erst im Ernstfall festgestellt wird, dass ein Recovery eigentlich gar nicht möglich ist, weil die Daten auf den Medien nicht mehr lesbar sind.

5.4.4.7 Sonstiges

Zu diesem Gebiet sind Disaster zuzuordnen, wie Sabotage und Vandalismus, Diebstahl von Systemkomponenten und Daten und Naturkatastrophen. Den ersten beiden kann nur durch verstärkte Sicherheitsmaßnahmen und Zutrittskontrollen, sowie durch ein gutes Betriebsklima begegnet werden. Vor allem Notebooks und Flachbildschirme erfreuen sich bei Diebstahl höchster Beliebtheit. Hierbei muss aber auch das Verantwortungsbewusstsein der Anwender geschärft werden, damit dem vorgebeugt werden kann. Gegen Naturkatastrophen jeglicher Art kann nur ein allgemeiner Katastrophenschutz Abhilfe bieten.

5.4.5 Zusammenfassung

Wie man aus den vorangegangenen Abschnitten sieht, kann mithilfe von technischen Maßnahmen eine Vielzahl von Katastrophen teils sogar automatisiert abgeholfen werden. Oft mangelt es dem Unternehmen aber an Investitionsbereitschaft, oder es wird von höheren Stellen eine Kostensenkung gefordert. Dabei ziehen meist solche technischen Maßnahmen den Kürzeren, da sie einfach „zu teuer" sind.
Dem kann ich aber definitiv nicht zustimmen. Man muss einfach die Relation zwischen dem Stillstand oder Totalausfall eines EDV-Systems und den damit verbundenen Kosten bis zum Wiederanlaufen und den Kosten von Schutzmaßnahmen, beachten. Dabei wird sich in 90% aller Fälle zeigen, dass ein Ausfall wesentlich höhere Kosten verursachen würde, als eine Investition in Schutzmaßnahmen. Ein weiterer Grund, neben den Kosten, ist dass das Management das Risiko eines Ausfalls weit unterschätzt.
Abschließend ist noch zu erwähnen, dass mit technischen Mitteln aber nur ein Teil der Schutzmaßnahmen abgedeckt ist. Ohne einen sinnvollen Katastrophenplan sind auch die tollsten technischen Spielereien wirkungslos.

5.5 Virtual Private Network (VPN)

5.5.1 Definition

Unter einem virtuellen privaten Netz verstehen wir eine Netzinfrastruktur, bei der Komponenten eines privaten Netzes über ein öffentliches Netz wie dem Internet miteinander kommunizieren, wobei sie die Illusion besitzen, das Netz zu ihrer alleinigen Verfügung zu haben. Das wichtigste dabei ist, dass die Daten verschlüsselt werden.

5.5.2 Überblick

Bei VPN wird eine Tunneltechnik verwendet, so dass es dem User gegenüber so erscheint, als ob er direkt im privaten Netzwerk arbeiten würde (**Abbildung 11**). Ein VPN hat also die Aufgabe, die Benutzer des privaten Netzes zu authentifizieren, die Vertraulichkeit der übertragenen Daten zu gewährleisten, und das Schlüsselmanagement sowie die Verschlüsselung abzuwickeln.

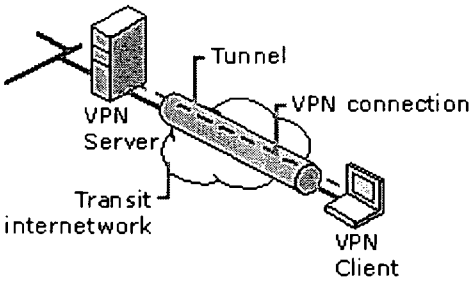


Abbildung 11: VPN-Verbindung

5.5.3 Anwendungsbereiche

Der wichtigste Anwendungsbereich für VPNs ist sicherlich bei geografisch weit verteilten Organisationen zu sehen. Hierdurch kann von verschiedenen Standorten mittels VPN-Clients eine Verbindung zum Unternehmensnetzwerk hergestellt werden. So können zentral gespeicherte Daten, sowie Datenbanken und deren Anwendungen einer Vielzahl von geografisch verteilten Nutzern zur Verfügung gestellt werden. Hierbei können vorhandene WANs genutzt werden. Hierbei bekommt natürlich auch die Telearbeit einen weiteren Schritt nach vorne, da vom Standpunkt der Sicherheit aus gesehen, VPNs eine ideale Lösung darstellen. Natürlich besteht weiterhin die Möglichkeit RAS-Server zu verwenden, doch hier spielt auch das Bandbreitenproblem eine immer größere Rolle. Firmen besitzen oft Internetzugänge mit einer Bandbreite von mehreren MegaBit, und schon aus dieser Überlegung heraus bieten VPNs wesentlich flexiblere und kostengünstigere Verbindungslösungen an. Neben den externen Zugängen kann ein VPN natürlich auch für Intranets eine interessante Lösung anbieten. Dies ist vor allem dann der Fall, wenn Server im internen Netz existieren, auf denen besonders sensible Daten gespeichert sind. Hier können dann nur mit VPN-Clients ausgestattete Teilnehmer nach der korrekten Identifikation am VPN-Server auf die Daten auch zugreifen.

5.5.4 Tunneling

Damit eine logische Verbindung zwischen privaten Netzwerkkomponenten aufgebaut werden kann, wird eine Technik eingesetzt, die als Tunneling bezeichnet wird. Beim Tunneling werden die Pakete bzw. Frames durch einen zusätzlichen Header gekapselt. Dieser Header enthält alle Routinginformationen, die notwendig sind, dass die gekapselten Daten dem Empfänger am Tunnelende zugestellt werden können. Dort werden die Daten dann entpackt, und über das private Netz an den eigentlichen Empfänger weitergeleitet.

5.5.4.1 Layer-2 Tunneling Protokolle

Die bekanntesten Tunneling-Protokolle auf Layer-2 des ISO-OSI-Referenzmodells sind das Point-to-Point-Tunneling Protocol (PPTP) und das Layer-2 Tunneling Protokoll (L2TP) [5]. Bei PPTP wird ein PPP-Datenframe verschlüsselt. Danach wird ein IP-Header hinzugefügt, und dieses in ein IP-Datagramm gekapselt. Danach wird das Paket über das IP-Protokoll zum Tunnelendpunkt gesendet.
L2TP ist im Gegensatz zu PPTP kein auf IP zugeschnittenes Protokoll. PPP-Frames werden durch einen zusätzlichen Header gekapselt, sodass das Paket über ein beliebiges paketvermittelndes Protokoll wie IP, ATM oder X.25 weitergeleitet werden kann. Ein weiterer Vorteil gegenüber PPTP ist die Möglichkeit mehrere Tunnels zwischen zwei Endpunkten aufzubauen.

Heutzutage ist sicher L2TP dem PPTP vorzuziehen, da hierbei die Infrastruktur auch über IP-Router aufgebaut werden kann. Dies hat vor allem den Vorteil, dass der Client von jedem beliebigen Punkt auf der Welt, sofern ein Internetzugang existiert, diese kostengünstige Variante zu verwenden. PPTP und Telefonleitungen oder Wählverbindungen haben somit ausgedient.

5.5.4.2 Layer-3 Tunneling Protokolle

Das bekannteste Layer-3 Tunneling Protokoll ist IPSec, welches in Abschnitt 4.5.1 detailliert erklärt wurde.

5.5.5 Zusammenfassung und Ausblick

VPN hat und wird auch weiterhin sehr große Bedeutung haben. Der Trend geht weiterhin in die Richtung, von weit verteilten Organisationen, aber zentralen Rechenzentren. Eine Anbindung über VPN stellt eine wesentlich kostengünstigere und sicherere Möglichkeit dar, die Anbindung zu realisieren. Auch das Thema der Telearbeit wird immer bedeutender. Dadurch ergibt sich ein weiterer Einsatzpunkt für VPNs. Auch die immer kostengünstiger werdenden Internetzugänge bewegen immer mehr Leute in die Richtung, auch öfters von zuhause aus zu arbeiten. Den Organisationen kommt dies natürlich auch entgegen, da sie sich immer horrenderen Büromieten ausgesetzt sehen. Der zentrale Aspekt, wie bei allen sicherheitskritischen Kommunikationsformen liegt aber der genauen Planung und detaillierten und immer wieder überprüften und verbesserten Security-Policy.

6 Organisatorische Sicherheitsaspekte

6.1 Die Security-Policy und das Security-Wheel

Netzwerksicherheit ist immer ein kontinuierlicher Prozess. Dies ist aufgrund der raschen Weiterentwicklung der Computertechnologie notwendig. Wenn die potentiellen Gefahren bekannt sind, ist es möglich sowohl für Teilsysteme als auch für ein ganzes System eine Security Policy zu implementieren.
Unter einer Security Policy versteht man folgendes: Eine Security Policy ist eine formale Menge von Regeln, die Personen, welche auf Informationen und Technologien einer Organisation Zugriff haben, einhalten müssen [75]. Etwas deutlicher wird es in [64] definiert: A network security policy defines the organisation's expectations of proper computer and network use and the procedures to prevent and respond to security incidents. A network security policy is the foundation of security because it outlines what assets are worth protecting and what actions or inactions threaten the assets. The policy will weigh possible threats against the value of personal productivity and efficiency and identify the different corporate assets which need different levels of protection. Without a network security policy, a proper security framework cannot be established. Employees cannot refer to any established standards and security controls would be circumvented for the sake of increasing efficiency.

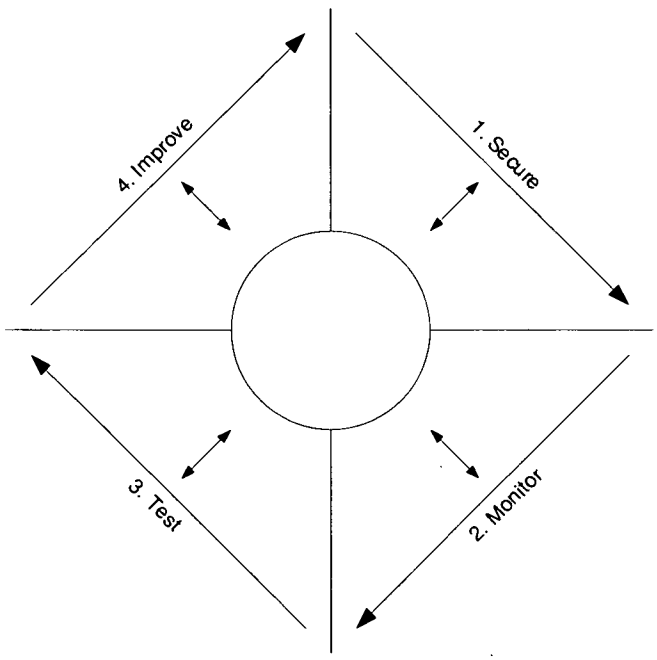


Abbildung 12: Das Security Wheel

Um eine Security Policy zu definieren, müssen folgende Tasks durchgeführt werden:

- Sicherheitsziele müssen definiert werden. Es muss festgestellt werden, was geschützt und wie es geschützt werden soll. Wenn man die Schwachstellen in einem Netzwerk kennt, und weiß wie diese ausgenutzt werden können, ist das ein Schritt in Richtung Verbesserung dieser Schwachstellen.
- Dokumentation der zu schützenden Ressourcen. Hierbei muss Wissen vorhanden sein, wie Systeme im Normalfall funktionieren, wie einzelne Netzwerkkomponenten arbeiten, und wie die Daten fließen.
- Identifikation der Netzwerkinfrastruktur mithilfe von Karten und Bestandsverwaltung. Hierbei muss die physische Sicherheit des Netzwerks in Betracht gezogen werden, denn wenn ein System physisch von jedem User erreichbar ist, könnten diese das ausnutzen.

Wie bereits erwähnt, ist eine Security Policy nur dann effektiv, wenn sie laufend überarbeitet und verbessert wird. Eine Möglichkeit dies graphisch darzustellen ist das Security Wheel. Ein analoges System ist die SKiP-Methode (Security Knowledge in Practice) [54]. Da beide Systeme dasselbe darstellen, wird hier nur das Security Wheel beschrieben, da es meiner Meinung nach anschaulicher ist. Dieses Security Wheel besteht aus vier Schritten, die immer wieder durchlaufen werden müssen:

6.1.1 Schritt 1: Secure the System

Ziel dieses Schrittes ist die Implementation von Geräten oder Systemen, welche Sicherheit gewährleisten und unautorisierten Zugang verhindern:

- Identification Authentication Systems, wie z.B. One-Time Passwords (OTP), gewähren nur authentifizierten und autorisierten Usern Zugriff.
- Encryption: Durch Verschlüsselung des Datenverkehrs kann ungewolltes Auslesen von Informationen verhindert werden. Dadurch kann die Vertraulichkeit der Daten gewährleistet werden. Derzeit wird im Internet als Standard IP Security (IPSec) verwendet [76].
- Firewalls können bestimmten Datenverkehr und spezielle Services zulassen oder verweigern.
- Vulnerability Patching ist der Vorgang, Updates oder Patches anzuwenden, damit dadurch schon bekannte Sicherheitslücken geschlossen werden. Dabei muss auch darauf geachtet werden, dass Services, welche nicht benötigt werden deaktiviert bzw. entfernt werden. Durch die Verringerung der bestehenden Services wird es für einen Angreifer wesentlich schwieriger in das System einzudringen.
- Physical Security ist ein sehr wichtiger, aber oft vernachlässigter Aspekt der Systemsicherheit. Wenn es nämlich jemandem möglich ist, mit der Hardware davon zu spazieren, dann sind alle anderen Sicherheitsvorkehrungen sinnlos. Ein weiterer wichtiger Aspekt ist, dass die Möglichkeit Geräte im System zu installieren, um Daten abzuhören, oder abzufangen, nicht möglich ist.

6.1.2 Schritt 2: Monitor

Hierbei wird das Netzwerk auf Verstöße und Attacken gegen die Security Policy der Firma überwacht. Die Angriffe können sowohl von innerhalb durch einen unzufriedenen Mitarbeiter, als auch von außen durch Hacker initiiert werden. Hier können Real-Time Intrusion Detection Systems unbefugten Zugang entdecken und verhindern. Logging ist ein sehr wichtiger Aspekt des Monitoring. Durch Überwachung der Datenströme mithilfe von Logs können bereits versuchte Angriffe entdeckt werden. Wenn nämlich der Angreifer das Netzwerk bereits lahm gelegt hat, ist es schon zu spät.

6.1.3 Schritt 3: Test

Das Testen der sicherheitsrelevanten Komponenten ist eine absolute Notwendigkeit. Selbst das ausgefeilteste Sicherheitssystem ist wertlos, wenn es entweder falsch konfiguriert ist, oder nicht richtig funktioniert.

6.1.4 Schritt 4: Improve

Es ist absolut imperativ, dass die Security Policy ständig verbessert wird. Die Informationen die in der Monitor- und Testphase müssen analysiert und gesammelt werden, um Verbesserungen durchführen zu können.

Nachdem Sicherheitslücken und Risiken täglich erstellt und gefunden werden, ist es wichtig alle vier Schritte kontinuierlich und wiederholt zu durchlaufen. Nur so kann verhindert werden, dass eine veraltete Security Policy zu einer nicht zu unterschätzenden Gefahr werden kann.

6.2 Das Konzept des Patching

Darunter verstehen wir das Updaten von Systemen mit Patches, welche entweder Fehler beheben, oder Sicherheitslücken schließen. Besonders bei Microsoft-Produkten gibt es fast wöchentlich einen Patch, welcher eine gerade entdeckte Sicherheitslücke schließt. Aber auch bei Linux-Systemen steigt die Anzahl der Patches rapide an. Das Konzept des Patching ist notwendig, um Betriebssysteme und Software immer auf dem neuesten Stand zu halten. Besonderes Augenmerk sollte dabei auf sicherheitskritische Systeme gelegt werden. Bevor solche Patches eingespielt werden, sollte aber jedenfalls in einer Testumgebung überprüft werden, inwiefern der Patch einerseits eine bestehende Sicherheitslücke schließt und andererseits, ob durch den Patch selbst nicht eine weitere Sicherheitslücke geöffnet wird, welche unter Umständen um ein Vielfaches gefährlicher ist, als jene, welche versucht wurde zu schließen. Gewarnt sei an dieser Stelle auch vor Patches, die Probleme beseitigen sollen, welche gar nicht auftreten, oder Teilkomponenten betreffen, die gar nicht in Verwendung sind. Auch hier sei vor einem Einspielen definitiv abgeraten. Ein deutlicher Unterschied sei hier auch zwischen Patches und echten Upgrades aufgeführt. Bei einem Upgrade wird meist ein ganzes System oder ein bestimmtes Softwarepaket auf eine neue Version umgestellt. Dabei ist mit noch größerer Sorgfalt vorzugehen, als bei einem Patch, da die Auswirkungen im Fehlerfall um ein Vielfaches höher sein können, als bei reinen Patches.

6.3 Backup & Disaster Recovery

Dieser Abschnitt beschäftigt sich mit der Erstellung eines Katastrophenplans und den dafür notwendigen Schritten.

6.3.1 Einleitung

Das wichtigste, was erkannt werden muss, ist dass es nicht „den" Katastrophenplan, der universell einsetzbar ist, gibt. Dies begründet sich vor allem durch den Wandel in der Netzwerkwelt. In Zeiten, wo sämtliche Anwendungen auf zentralisierten HOST-Rechnern zur Verfügung gestellt wurden, gab es eine eindeutige Organisation der Abläufe. Dadurch war es den Herstellern möglich universelle Katastrophenpläne zu verkaufen [25]. Dies hat sich aber zu hochgradig vernetzten, und heterogenen Computersystemen gewandelt. Dadurch erhält jedes Netzwerk eine individuelle Note, vor allem dann wenn Administratoren nur kleine Teile des Gesamtnetzwerks betreuen. Auch Benutzer haben vielfach die Möglichkeit, eigene Software auf ihren Arbeitsplätzen zu installieren. Solche Dinge sind aber nur sehr schwer zu erfassen, vor allem wenn Administratoren keine Kenntnis über diese Vorgänge besitzen. So kann ein Ausfall so eines PCs zu immensem Datenverlust führen. Durch diese kurze Ausführung sieht man bereits, dass für jedes Netzwerk bzw. jede Organisation der Katastrophenplan unterschiedliche Ausprägungen annehmen kann. Die folgenden Abschnitte sollen erläutern, wie anhand allgemein gültiger Verfahren, ein maßgeschneiderter Katastrophenplan entwickelt werden kann. Zusätzlich spielen im Katastrophenplan aber noch zwei Einflussfaktoren eine wesentliche Rolle. So muss eindeutig klar sein, welche Komponente im Katastrophenfall, welche Kosten verursacht. Desweiteren muss auch für jede Komponente definiert werde, welcher maximale Ausfallszeitraum gewährt wird.

6.3.2 Der Katastrophenplan

6.3.2.1 Klärung der Zuständigkeiten

Die Klärung der Zuständigkeiten ist der erste wichtige Schritt in die Richtung zur Entwicklung eines Katastrophenplans. Hierbei muss eindeutig definiert werden, wer für was zuständig ist. Wichtig ist, dass ein Projektleiter eingesetzt wird, der weit reichende Vollmachten im Bezug auf die Durchführung des Projekts bekommt. Weiters hat es sich als sinnvoll erwiesen, dass die einzelnen Fachabteilung in den Prozess eingebunden, und sogar zur Zusammenarbeit verpflichtet werden. Eine weniger rigorose Herangehensweise hat meist den Nachteil, das Projekt nicht innerhalb einer akzeptablen Zeitspanne abschließen zu können [25].

6.3.2.2 Der Aktionsplan

Der Aktionsplan umfasst alle notwendigen Schritte zu Erstellungs-, Test- und Überarbeitungsabläufen des Notfallplans.

- Übernahme des Auftrags zur Schaffung eines Notfallplanes
- Durchführung einer Informationssammlung zu den Geschäftsabläufen innerhalb des Unternehmens
- Durchführung einer Informationssammlung in Bezug auf die vorhandene Infrastruktur im Unternehmen
- Auswertung des gesammelten Datenmaterials mit dem Ziel der Erstellung einer Risikoanalyse der die Geschäftsabläufe unterstützenden Systeme
- Entwurf von Strategien für Wiederanlaufpläne
- Entwicklung von Vorbeugemaßnahmen zur Unterstützung der Havarievermeidung
- Organisation eines weit reichenden Datensicherungssystems
- Definition und Organisation eines Trainingsprogramms hinsichtlich der Havariebekämpfung
- Überprüfung der Notfallpläne durch gezielte Tests
- Plan zur Aufrechterhaltung der Aktualität der Notfallpläne

6.3.2.3 Zusammenstellung des Projektteams

Jedem Mitglied des Projektteams muss anfangs eine genau definierte Rolle zugewiesen werden. Die untenstehende Auflistung enthält alle Schlüsselpositionen, die aber je nach Unternehmensgröße eventuell erweitert, oder mehrere Rollen auf ein Teammitglied übertragen werden.

- Projektmanager
  Der Projektmanager hat die Verantwortung für das Gesamtprojekt. Er ist für die Einhaltung des Zeitplans, Abstimmung der Vorgehensweise mit dem Management und eine fristgerechte Fertigstellung verantwortlich.
  Die Person muss über gute Führungseigenschaften, Kontakt zum Management und Erfahrung aus vorangegangenen Projekten besitzen.

- Netzwerkadministrator
  Der Netzwerkadministrator übernimmt alle mit dem Netzwerk zusammenhängenden Aufgaben, Installationen und Tests.
  Diese Person muss Erfahrungen im Client/Server-Betrieb haben, und die verwendeten Kommunikationsprotokolle kennen.

- Datenbankadministrator
  Der Datenbankadministrator übernimmt alle mit der Datenbank zusammenhängenden Aufgaben, Installationen und Tests.
  Diese Person muss über Erfahrungen im Umgang mit Datenbanksystemen verfügen.

- Leiter des Benutzerservices
  Der Leiter des Benutzerservices hat den besten Kontakt zu den Benutzern der EDV-Systeme. Aus diesem Bezug kann man wertvolle Anregungen und praktische Erfahrungen erhalten.
  Die Person, die diese Rolle ausfüllen soll, muss Kenntnisse von den Abläufen der Arbeit des Benutzerservices haben und die Forderungen der Benutzer kennen.

- Consultant
  Consultants werden zu Unterstützung der eigenen EDV-Kräfte eingesetzt, da sie Erfahrungen aus ähnlichen Projekten mitbringen.
  Der Consultant ist sicherlich nicht unbedingt notwendig, kann aber durch seine Erfahrung wertvollen Input liefern. Vor allem wenn noch keine Erfahrung im Hinblick auf Notfallpläne bestehen, sollte auf seine Unterstützung keinesfalls verzichtet werden.

6.3.2.4 Voraussetzungen für ein erfolgreiches Projektteam

Für die erfolgreiche Projektdurchführung, sind folgende Voraussetzungen notwendig:

- Zustimmung und Unterstützung durch das Management
  Das Projekt muss die Unterstützung des Managements haben. Dies ist besonders entscheidend in kritischen Situationen und für die Priorisierung der Abläufe.

- Das Projekt hat bei den Teammitgliedern hohe Priorität
  Jedes Teammitglied muss diesem Projekt auf seiner persönlichen Prioritätenliste einen oberen Platz einräumen. Der Erfolg des Projektes hängt in hohem Maße von der Bereitschaft der einzelnen Teammitglieder zur Teamarbeit ab.

- Offene Kommunikation
  Eine gut organisierte Kommunikation während des gesamten Projektes sorgt für eine offene Atmosphäre innerhalb des Teams. Jedes Mitglied ist über die Fortschritte und Ergebnisse aktuell informiert.

- Einbeziehung der späteren Benutzer
  Frühzeitig müssen die Benutzer in das Projekt einbezogen werden. Sie müssen aufgefordert werden, ihre Bemerkungen und Vorschläge dem Projektteam zur Verfügung zu stellen. Dies vermindert mit Sicherheit bestehende Vorbehalte und Widerstände.

6.3.3 Zusammenfassung

Man sieht, dass die Ausarbeitung eines solchen Notfalls- oder Katastrophenplans nicht innerhalb kürzester Zeit erfolgen kann. Dies ist sicher auch nicht sinnvoll, da der Plan im Ernstfall ja eine Anleitung darstellen soll, wie die Systeme raschest wieder lauffähig gemacht werden können. Deshalb sollte die Ausarbeitung dieses Plans eine sehr hohe Priorität in EDV-unterstützten Organisationen einnehmen. Denn kommt es wirklich zur Katastrophe, und es gibt keinen Katastrophenplan, oder schlimmer noch, nicht einmal funktionierende Datensicherungen, dann ist eine Firmenpleite nicht ausgeschlossen. Diese Bedrohung muss dem Management aber deutlich gemacht werden, damit die Bereitschaft für eventuelle Investitionen in diesem Bereich gesichert ist.

6.4 Userspezifische Sicherheitsaspekte

6.4.1 Einleitung

Neben den oben genannten Sicherheitsaspekten im organisatorischen Bereich, spielt auch die Einbindung der Benutzer in das Sicherheitskonzept eine zentrale Rolle. Diese müssen auf die Wichtigkeit und auf bestimmte Verhaltensmaßnahmen aufmerksam gemacht werden, um auch von dieser Seite ein Maximum an Sicherheit zu gewährleisten.

6.4.2 Benutzerrechte und Pflichten

Die sinnvollste Herangehensweise ist die Aufstellung von Rechten und Pflichten der Benutzer. Dabei darf dies aber keinesfalls über den Köpfen der Anwender entschieden werden, sondern muss in Zusammenarbeit mit den Nutzern entwickelt werden, damit diese von der Wichtigkeit der Maßnahmen überzeugt werden. Besonders schwierig gestaltet sich dieser Prozess in Organisationen, wo eine komplett neue Regelung eingeführt wird, da eine gewisse Gewohnheit der Anwender existiert, die schwer zu durchbrechen ist.

6.4.3 Benutzungsrichtlinien

Nachdem ein sinnvoller Entwurf durchgeführt wurde, ist es sinnvoll eine Reihe von Benutzungsrichtlinien zu definieren. Diese müssen sowohl vom Betriebsrat als auch von Juristen auf ihre Anwendbarkeit geprüft werden. Außerdem müssen sie von jedem Mitarbeiter, der einen PC zur Verfügung hat, unterzeichnet werden.
Folgende Richtlinien sollen einen Anhaltspunkt darstellen:

- Das Senden und Empfangen von privaten E-Mails ist in vertretbarem Ausmaß erlaubt.
- Mails, deren Inhalt für mehrere Mitarbeiter der Firma interessant sein könnte, müssen an entsprechenden Stellen gespeichert werden, und dürfen nicht ausschließlich in der Mailbox am Mail-Server liegen.
- Wenn man mehr als einen Arbeitstag außerhalb des Büros ist, muss eine entsprechende Abwesenheitsnotiz aktiviert werden, welche dem Absender der E-Mail automatisch mitteilt, wann man wieder erreichbar ist und wer die Vertreter sind.
- Bei ausgehender Mail muss klar erkenntlich sein, ob es sich um eine private oder Firmen-Mail handelt.
- Die Verwendung des Internet für private Zwecke ist / ist nicht / ist nur außerhalb der Arbeitszeit erlaubt.
- Jeder Zugriff auf das Internet wird mitprotokolliert.
- Ausschließlich die EDV-Abteilung darf Software installieren
- Das Betrachten von illegalen oder sexuell anstößigen Internet-Inhalten ist verboten.
- Kostenpflichtige Internet-Dienste dürfen nicht genutzt werden, außer sie stehen in Zusammenhang mit der Arbeitstätigkeit und sind offiziell genehmigt.
- Finanztransaktionen dürfen nicht für private Zwecke durchgeführt werden.
- Persönliche Daten, wie z.B. Name, Adresse, E-Mail usw. sollen im Internet so wenig wie möglich bekannt gegeben werden.
- Das Herunterladen und Speichern von urheberrechtlich geschützten Daten ist verboten.
- Passwörter dürfen niemals bekannt gegeben werden.
- Wenn der Arbeitsplatz verlassen wird, muss der Bildschirm gesperrt werden, bzw. müssen Bildschirmschoner mit Kennwortschutz zusätzlich verwendet werden.
- Man hat sich an die Netiquette zu halten.

- Nationale gesetzliche Bestimmungen sind selbstverständlich gültig.
- Zur Verwendung des Internet darf ausschließlich der offizielle Zugang über die Firewall benutzt werden. Der Einsatz von Modems, ISDN-Karten, Routern oder sonstigem Telekommunikationsequipment außer jenen Geräten, die von der EDV-Abteilung installiert wurden, ist verboten.
- Es sind starke Passwörter zu verwenden, die nicht an offensichtlichen Stellen aufgeschrieben werden dürfen.
- Definition der möglichen Konsequenzen bei Nichteinhaltung der Richtlinien.

6.4.4 Social Engineering

Beim Social Engineering geht es darum, vertrauliche Informationen durch Vorgabe einer falschen Identität zu erhalten. Dabei geht es um Passwörter, Namen von Mitarbeitern und andere vertrauliche Daten. Hierbei muss bei den Benutzern ein Bewusstsein geschaffen werden, dass so etwas existiert, und im Verdachtsfall sofort eine Vertrauensperson im Unternehmen kontaktiert werden muss.

6.4.5 Zusammenfassung

Man sieht, dass neben allen technischen und organisatorischen Sicherheitsaspekten, die Benutzer niemals vergessen werden dürfen. Bei Ihnen muss ein Bewusstsein geschaffen werden, und die Folgen eines möglichen Fehlverhaltens aufgezeigt werden. Nur auf diese Art und Weise kann verhindert werden, dass Anwender und Mitarbeiter gegen die gängigen Sicherheitskonzepte des Unternehmens arbeiten, und damit eine erfolgreiche Sicherheitspolitik untergraben. Selbstverständlich hängt es stark von der herrschenden Unternehmenskultur ab, inwiefern die Mitarbeiter bereit sind, sich mit diesen Sicherheitskonzepten anzufreunden, deshalb muss ein Klima des Vertrauens und der Transparenz geschaffen werden, damit sich die einzelnen Individuen nicht übergangen fühlen. Nur so kann die Sicherheit auch auf dieser Ebene erfolgreich implementiert werden.

Teil III Sicherung eines privaten Netzwerks

7 Planung und Implementation von Internet- und Intranet-Sicherheit

Will man eine Sicherheitsarchitektur aufbauen, ist der erste Schritt in diese Richtung die Formulierung von Unternehmensrichtlinien für die Datensicherheit. Mit dieser Grundlage kann dann ein Implementationsplan erstellt und umgesetzt werden. In den Unternehmensrichtlinien werden die Anforderungen des Unternehmens an die ordnungsgemäße Benutzung von Computer-Systemen und Datennetzen dargestellt. Maßnahmen zur Verhinderung von Verletzungen dieser Vorschriften, sowie Schritte als Reaktion auf Verstöße dagegen werden definiert. Grundvoraussetzungen für die Sicherheitsrichtlinien sind, dass sie nicht gegen geltendes Recht, sowie gegen andere, bereits bestehende Unternehmensrichtlinien bzw. Betriebsvereinbarungen verstoßen.

7.1 Unternehmensrichtlinien für Netzwerksicherheit

Der Ausgangspunkt für die Erstellung der Unternehmensrichtlinien sollte eine allgemeine Definition der Aufgabe der Datennetze und der Computer-Systeme darstellen. Dabei wird festgelegt, welche Dienste zur Verfügung gestellt werden, und welche Verfügbarkeits- und Sicherheitsanforderungen an die einzelnen Informationstechnologien zu erfüllen sind. Vor allem bei Banken und Versicherungen spielt Netzwerksicherheit eine wesentlich größere Rolle als in anderen Unternehmen. Die Art der Sicherheits- und Verfügbarkeitsanforderungen hängt somit stark von der jeweiligen Organisation ab. Ein weiteres Kriterium ist, dass die aufgestellten Sicherheitsrichtlinien sowohl technisch als auch ökonomisch sinnvoll umgesetzt werden können und damit eine Durchsetzung gegenüber der Geschäftsleitung sichergestellt ist. Die Erarbeitung sollte daher gemeinsam durch EDV-Personal und das Management durchgeführt werden.

7.2 Risikoanalyse

Damit sichergestellt ist, dass die in den Unternehmensrichtlinien definierten Maßnahmen zur Gewährleistung der Netzwerksicherheit in einem adäquaten Verhältnis zu den tatsächlichen Gegebenheiten stehen, sollte zunächst eine möglichst detaillierte Risikoanalyse durchgeführt werden. Dabei muss definiert werden, was geschützt wird, vor wem es geschützt wird, und wie es geschützt wird [16]. Aus dieser Grundlage kann eine passende Sicherheitsstrategie erarbeitet werden. Sowohl eine Unter- als auch eine Überbewertung der einzelnen Sicherheitsaspekte kann im schlimmsten Fall zu beträchtlichen finanziellen Verlusten für das Unternehmen führen. Deshalb gilt folgende einfache Grundregel: Der Aufwand für den Schutz eines Systems sollte den Wert desselben nicht übersteigen [16]. Treten Fehler bei der Überprüfung der zu schützenden Objekte in dieser frühen Phase auf, werden diese erst später im Gesamtkonzept als schwere Sicherheitslücken erkennbar.

Folgende Kategorien sollten in der Auflistung der zu schützenden Objekte jedenfalls inkludiert werden:

- Hardware
- Software
- Daten
- Personen
- Dokumentation
- Zubehör

Nachdem die zu schützenden Objekte definiert wurden, können Szenarien ausgearbeitet werden, welche Anschläge auf das Unternehmen und die möglichen Auswirkungen beinhalten:

- Eindringen von nichtautorisierten Personen
- Beeinträchtigung und Störung des Netzbetriebes
- Verlust von vertraulichen Informationen

Mithilfe der Ergebnisse der Risikoanalyse können sodann die Sicherheitsrichtlinien definiert werden.

7.3 Die Erstellung von Sicherheitsrichtlinien

7.3.1 Sicherheitsrichtlinien für Personen

In den Sicherheitsrichtlinien für Personen sind die Rechte und Pflichten aller Benutzergruppen des Datennetzes zusammengefasst. Allgemein kann man folgende Benutzergruppen definieren:

- Mitarbeiter
- Gäste, Aushilfen
- Systemadministratoren
- Service-Personal und externe Berater

Neben diesen allgemeinen Benutzergruppen existieren aber noch eine Vielzahl von Untergruppen, besonders bei den Mitarbeitern. Diese haben meist noch viel differenziertere Rechte und Pflichten. Folgende Unterteilung soll eine beispielhafte Trennung darstellen:

- Vorstände
- Prokuristen
- Abteilungsleiter/Gruppenleiter
- Buchhaltung
- Personalwesen
- Weitere abteilungsspezifische Trennungen

Dies soll aber nur eine mögliche Gruppierung darstellen. In den meisten Organisationen wird noch eine viel feingranularere Unterteilung nötig sein.

Richtlinien, welche alle Mitarbeiter betreffen, sind in der Regel unter dem Begriff „Allgemeine Nutzungsbestimmungen für EDV-Systeme und Datennetze" zusammengefasst. Folgende Punkte sollten dabei beinhaltet sein [16]:

- Wer ist berechtigt, welche Systeme bzw. Dienste zu nutzen?
- Was wird unter zulässiger Nutzung der Systeme bzw. Dienste verstanden?
  Verbot von Einbruch in Fremdsystemen
  Verbot der Enttarnung von Passwörtern
  Verbot von Datenmanipulation an fremden Dateien
  Verbot von Teilung des eigenen Accounts mit weiteren Personen/Mitarbeitern
  Verbot der Vervielfältigung von Software, die dem Kopierschutz unterliegt
- Wer ist berechtigt, für Benutzer einen Systemzugang (Benutzer-Account) einzurichten?
- Welchen Pflichten sind die Benutzer der EDV-Anlagen unterworfen?
  Geheimhaltung der Benutzerpasswörter
  Regelmäßige Änderung der Passwörter
  Durchführung von Sicherheitskopien der eigenen Daten
  Geheimhaltung von vertraulichen Daten
  Befolgung der Richtlinien für die Nutzung von Systemressourcen (Speicherplatz, Nutzung rechenintensiver Applikationen, etc.)
  Richtlinien für die Internet-Nutzung
  Richtlinien für die Nutzung der EDV-Systeme für private Zwecke
  Überwachung des eigenen Account hin auf unautorisierte Nutzung
  Meldung von verdächtigen Vorgängen, Entdeckung von Viren etc.

Besonderes Augenmerk sollte auch auf das Sicherheitsrisiko Systemverwaltung gelegt werden. Dieser Personenkreis besitzt meist uneingeschränkte Rechte im Bezug auf die EDV-Infrastruktur. Oft wird aber aus den Augen verloren, dass diese dadurch eine der potentiell größten Gefahren für die Sicherheit der EDV-Anlagen darstellen. Deshalb müssen diese Personen einerseits sorgfältig ausgewählt werden und andererseits müssen die Rechte und Pflichten der Systemverwalter genau definiert werden.
Einige der Problembereiche beinhalten [16]:

- Wer ist berechtigt, Systemverwalter-Rechte (Superuser-Zugang) zu erhalten?
  Wer vergibt diese Rechte?
  Nach welchen Kriterien erfolgt die Zuteilung der Benutzerrechte (Grundregel: Es werden jedem Benutzer nur so viele Rechte zugeteilt, wie zur Erfüllung seiner Aufgaben notwendig ist)?
- In welchem Ausmaß ist der Systemverwalter berechtigt, Benutzerdaten zur Problemdiagnose zu analysieren?
- Hat der Systemverwalter das Recht, einzelne Systeme oder das Netzwerk als gesamtes zu überwachen?

Essentiell ist dabei, dass der betroffene Personenkreis eingehend geschult wird, und dass die Einhaltung regelmäßig überwacht wird. Maßnahmen zur Aus- und Weiterbildung der Mitarbeiter in Bezug auf Daten- und Netzwerksicherheit sowie die Durchführung von Kontrollen (Sicherheits-Audits) sollten daher ebenfalls fester Bestandteil einer umfassenden Sicherheitsstrategie sein.

7.3.2 Sicherheitsrichtlinien für Hardware-Komponenten

Einen weiteren zentralen Punkt der Sicherheit stellen die Hardwarekomponenten der Datennetze dar. Die besten Sicherheitsvorkehrungen sind nämlich völlig nutzlos, wenn die Hardwarekomponenten der Datennetze nicht ausreichend geschützt sind. Die Richtlinien zum Schutz von EDV-Systemen bestehen aus den Bereichen [16]:

- Sicherheitsvorkehrungen für die einzelnen Hardware-Elemente (Server, Router, Terminals, Verteilerschränke, etc.)
- Sicherheitsvorkehrungen für das Gesamtunternehmen (Brandmeldesysteme, Klimatisierungsanlagen, etc.)

Sämtliche kritischen EDV-Systeme, wie Server, Router, Root-Terminals usw. sollten grundsätzlich in klimatisierten Computerräumen installiert sein. Der Zugang zu diesen Räumen sollte nur durch persönliche Identifikation (Magnetkarten, Zugangs-Code, etc.) ermöglicht werden. Zusätzlich sollte natürlich die Anzahl der Personen mit Zutrittsberechtigung auf ein Minimum beschränkt sein. Zu diesen sicherheitskritischen Bereichen zählen aber auch die Verteilerschränke. Oftmals sind diese für jedermann frei zugänglich an einem zentralen Ort installiert.

Folgende Maßnahmen zur Gewährleistung der Sicherheit von Hardware-Komponenten sollte unbedingt berücksichtigt werden [16]:

- Physische Zugangskontrollen zu kritischen Komponenten (Server, Root-Terminals, Router, Switches, Verteilerschränke, Modems, Firewall-Komponenten, etc.)
- Physische Sicherheit von Remote-Terminals
- Diebstahlschutz von PCs, Terminals
- Definition von Bereichen mit Rauch- bzw. Essverbot
- Komponenten für Überspannungsschutz
- Komponenten zur unterbrechungsfreien Stromversorgung
- Lagerung von Sicherungskopien
- Lagerung von vertraulichen Daten
- Regelungen für den Werksschutz
- Besucherkontrolle

7.3.3 Sicherheitsrichtlinien für Software

Ein weiterer wichtiger Bestandteil einer gesamtheitlichen Sicherheitsstrategie, ist die Kontrolle, der unternehmensintern eingesetzten Software-Applikationen. Individuell konfigurierte PCs mit selbst installierter Software stellen vielfach einen Angriffspunkt für Trojaner oder Viren dar. Deshalb sollte es nur autorisierten Personen der Systemverwaltung möglich sein, Software zu installieren und Änderungen an ihrer Konfiguration durchzuführen. Eine genaue Dokumentation ist ebenfalls von höchster Wichtigkeit. Durch eine systematische Backup-Strategie ist zusätzlich für eine Sicherung der benutzerbezogenen Daten zu sorgen.

7.3.4 Sicherheitsrichtlinien für vertrauliche Daten

Bevor für einen Benutzer der Zugang zu einem bestimmten Dienst eingerichtet wird, muss definiert werden, ob dabei vertrauliche Daten anfallen können. Vertrauliche Daten sollten jedenfalls nur auf solchen Systemen gespeichert werden, wo diese auch dementsprechend abgesichert sind. Die Benutzer müssen informiert werden, welche Daten als vertraulich anzusehen sind, und wie mit diesen Daten zu verfahren ist. Folgende Punkte müssen dabei festgelegt werden [16]:

- Welche Daten sind als vertraulich bzw. geheim anzusehen?
- Welche Geheimhaltungsstufen sind definiert?
- Welche Benutzer haben Zugang zu solchen Daten?
- Welche Dienste erzeugen bzw. vermitteln Zugriff zu vertraulichen Daten?
- Auf welchen Systemen können solche Daten gespeichert werden?
- Welchen Zugangskontrollen sind diese Systeme unterworfen?
- Wie werden vertrauliche Daten über Datenleitungen übertragen (Verschlüsselung?)?
- Wie werden Sicherungskopien von vertraulichen Daten aufbewahrt?
- Wie werden Ausdrucke von vertraulichen Daten aufbewahrt bzw. entsorgt?

7.3.5 Sicherheitsrichtlinien für externe Datenverbindungen

Diese Sicherheitsrichtlinie ist sicher diejenige, welche am schwierigsten zu realisieren ist, vor allem da die Netzwerksicherheit dabei keinesfalls gefährdet werden darf. Besonders eine Anbindung an das Internet kann bei fehlerhafter Planung zur Kompromittierung der Netzwerksicherheit führen.
Folgende Prämissen sind dabei zu beachten [16]:

- Die Sicherheit und Integrität des internen Unternehmensnetzwerkes muss gewährleistet sein.
- Das Risiko des Zugriffs von nichtautorisierten Personen über die externen Datenverbindungen muss minimiert werden.
- Die Benutzung der externen Dienste durch Mitarbeiter soll in geringstmöglichem Ausmaß durch Sicherheitsmaßnahmen eingeschränkt werden.

Dem letzten Punkt kann ich allerdings nicht ganz zustimmen, da ein völlig freier Zugriff auf sämtliche Internetdienste zur Förderung von kriminellen Aktivitäten beiträgt. Vor allem für Webseiten sollte daher ein Content-Filter-System verwendet werden, das es sonst jedermann möglich ist, auch Seiten mit kriminellem Inhalt anzeigen zu lassen, wie z.B. Kinderpornographie, Rechtsradikalismus und ähnliches. Dies könnte sonst für das Unternehmen schwerwiegende rechtliche Schritte nach sich ziehen. Handelt es sich aber bei den externen Verbindungen um reine Anbindungen von Außenstellen oder Tochtergesellschaften, die nur Zugriff auf Daten und Datenbankdienste organisationsweit erlauben, sind die Verbindungen selbstverständlich dahingehend nicht einzuschränken. Zusätzlich zu den oben angeführten Punkten ist eine detaillierte Liste der zur Verfügung gestellten Dienste und für diese zugelassene Benutzergruppen zu erstellen. Anhand dieser Vorgaben kann ein Implementationsplan für ein Firewall-System erstellt werden.

Folgende Auflistung soll ein Beispiel für diese Sicherheitsrichtlinien darstellen [16]:

- Alle Internetdienste, die nicht ausdrücklich zugelassen sind, sind zu blockieren.
- Registrierte und autorisierte Benutzer haben Zugang zu den Internetdiensten WWW, FTP, E-Mail.
- Nicht registrierte und nicht autorisierte Benutzer haben keinen Zugang zum Internet. Das Zugriffsmanagement erfolgt über ein dediziertes Firewall-System.
- Eine direkte Verbindung des internen Unternehmensnetzwerkes mit dem Internet ist zu blockieren. Jede Internetverbindung hat über das unternehmenseigene Firewall-System zu erfolgen.
- Überwachungs- und Meldesysteme zur Erkennung von Verletzungen bzw. versuchten Verletzungen der Sicherheitsvorschriften (Angriffe von außen, Konfigurationsänderungen, Verletzung der Datenintegrität, etc.) sind auf dem Firewall-System zu installieren.

7.3.6 Vorgehensweise bei Verstößen gegen die Sicherheitsvorschriften

Die durchzuführenden Maßnahmen bei Verstößen sind grundsätzlich auch bereits im Vorfeld zu definieren. Prinzipiell sind zwei Strategien dafür geeignet [16]:

- Sicherung und Betriebsfortführung
- Überführung und Bestrafung

In den meisten Fällen wird sicher eine Kombination der beiden Verfahren die sinnvollste Entscheidung darstellen. Die erste Strategie beschreibt dabei die Absicherung der Sicherheitslücken, um möglichst rasch wieder zum Normalbetrieb zurückkehren zu können. Bei der zweiten Strategie wird versucht, weitere Sicherheitsverletzungen bewusst in Kauf zu nehmen, um den Täter überführen zu können. Dies ist aber definitiv die riskantere Strategie, da sie voraussetzt, dass neben erfahrenen Systemspezialisten für die Suche, das Risiko in Kauf genommen wird, dass weitere Sicherheitsverletzungen auftreten, und damit eventueller Datenverlust möglich ist.
Folgende Punkte sollten bei Einsatz der Strategie „Sicherung und Betriebsfortführung" beachtet werden [16]:

- Daten und Computer-Systeme sind nicht ausreichend geschützt.
- Weitere Sicherheitsverletzungen stellen ein unkalkulierbares Risiko dar.
- Die Bereitschaft, den Aufwand für eine Strafverfolgung der Täter zu betreiben, ist nicht vorhanden.
- Die genaue Zusammensetzung der Benutzergruppen ist nicht bekannt.
- Die Benutzer besitzen geringe EDV-Kenntnisse.

Folgende Punkte sollten bei Einsatz der Strategie „Überführung und Bestrafung" beachtet werden [16]:

- Daten und Computer-Systeme sind ausreichend geschützt.
- Sicherungskopien (Backups) für alle betroffenen Bereiche sind verfügbar.
- Das Risiko von Schäden durch weitere, bewusst in Kauf genommene Sicherheitsverletzungen zur Überführung der Täter steht in vernünftiger Relation zu Schäden durch mögliche zukünftige Verstöße.
- Die Angriffe treten häufig und in massiver Form auf, das Unternehmen selbst stellt ein attraktives Ziel für Angreifer dar und ist häufig Ziel von Sicherheitsverletzungen.
- Erfahrene Netzwerkverwalter sowie ausreichende Überwachungswerkzeuge stehen zur Verfügung.
- Die Geschäftsleitung unterstützt die Verfolgung und Bestrafung der Täter.

Ein großer Teil der Verstöße gegen Sicherheitsvorschriften erfolgt nachweislich entweder unwissentlich oder aus Nachlässigkeit durch Mitarbeiter des eigenen Unternehmens. Eine strafrechtliche Verfolgung kommt in diesen Fällen normalerweise nicht in betracht. Alternativ sollten deshalb für diesen Bereich der Sicherheitsvorfälle spezielle Schulungen bzw. in schweren Fällen eventuelle disziplinäre Maßnahmen vorgesehen werden.

7.4 Implementationsplan für eine Internet-Sicherheitsarchitektur

Aufbauend auf den Unternehmensrichtlinien für Netzwerksicherheit kann alsdann mit der Realisierung der Sicherheitsarchitektur begonnen werden. Dafür müssen die Vorgaben der Unternehmensrichtlinien zunächst in einem detaillierten, funktionellen Entwurf umgesetzt werden. In der darauf folgenden Implementationsphase, wird diese funktionelle Architektur installiert, getestet und sodann in Betrieb genommen. Unter Umständen ergeben sich daraus technische Neuerungen, Organisationsänderungen oder bauliche Maßnahmen. Natürlich ist zur Erreichung eines angemessenen Sicherheitsniveaus von der Geschäftsleitung ein kontinuierlicher Sicherheits-Management-Prozess zu initiieren.

7.4.1 Entwurf einer funktionellen Internet-Sicherheitsarchitektur

Ausgehend von der vorhandenen EDV Infrastruktur

- Betriebssysteme
- Netzwerktopologie
- Netzwerkprotokolle/Netzwerkbetriebssysteme
- externe Datenleitungen/Kommunikationsprotokolle

kann für jeden der geforderten Dienste eine technische Lösung erarbeitet werden. Betrachtet man dann die Gesamtheit der technischen Lösungen, kann eine geeignete Firewall-Architektur ausgewählt werden. Zusätzlich muss auch noch eine Detailspezifikation für die Sicherheitsarchitektur entwickelt werden. Aufgrund der Detailspezifikation, kann eine Produktauswahl gemacht werden und nach einer sorgfältigen Risikoanalyse der Firewall-Konfiguration schließlich der endgültige Aufbau des Schutzsystems festgelegt werden.

7.4.2 Implementation des Firewall-Systems

Die Erstinstallation des Firewall-Systems erfolgt zunächst getrennt vom Unternehmensnetzwerk. Dabei kann schon in dieser Testumgebung z.B. das Security-Wheel (s. Abschnitt 6.1) verwendet werden, um Verbesserungen zu erzielen. Erst nach vollständigen Tests und Verbesserungen kann eine vollständige Dokumentation und ein Einsatz im Produktionsbetrieb durchgeführt werden.

7.4.3 Einführung von Betriebsprozessen

Neben der Implementation des Firewall-Systems ist es genauso essentiell zuverlässige Betriebsprozesse für das Sicherheitssystem einzuführen. Grundlage dafür ist die Dokumentation der Sicherheitsarchitektur, bestehend aus, Systemdokumentation, Betriebsdokumentation und Log-Buch [16].

Die Systemdokumentation beinhaltet folgende wichtige Punkte:

- Netzwerk-Konfiguration
- Firewall-Konfiguration
- Konfiguration der Internet-Dienste
- Dokumentation der installierten Überwachungs- und Meldesysteme

Die Betriebsdokumentation enthält wichtige Anleitungen für den Betrieb des Firewall-Systems:

- Durchführung von Backups
- Durchführung von Wartungen (Hard- und Software)
- Auswertung und Interpretation der Überwachungs- und Meldesysteme
- Anleitung für System-Shutdown/Systemstart
- Verhalten bei Eintritt von Betriebsproblemen
- Verhalten bei Eintritt eines Sicherheitsvorfalles

In das Logbuch werden alle Tätigkeiten des Systemadministrators sowie die Auswertung der im Einsatz befindlichen Überwachungs- und Meldesysteme eingetragen.

8 Betriebssystemsicherheit

In diesem Kapitel sollen Betriebssysteme untersucht werden, inwiefern sie bestimmten Sicherheitsanforderungen genügen, und wo etwaige Schwachstellen zu finden sind.

8.1 Unix/Linux

Bereits im Jahr 1969 begannen die ersten Entwicklungen der Vorläufer, der uns heute bekannten Unix-Versionen [16]. Dadurch waren die ersten Hacker hauptsächlich damit beschäftigt, sich in diese Systeme einzuhacken. Mit der frei verfügbaren Unix-Variante Linux, stieg aber in den letzten Jahren die Anzahl der Internet- und Intranet-Server mit Linux. Da Linux nur ein weiterer Dialekt von Unix ist, gelten dafür die gleichen Überlegungen und Grundsätze, wie für alle anderen Unix-Derivate. Die Beliebtheit von Unix/Linux begründet sich in der unübertroffenen Einsetzbarkeit. Besonders die Linux-Derivate bieten eine Vielzahl von verschiedenen Einsatzmöglichkeiten bei minimalen Kosten. So verfügen die meisten Linux-Varianten üb Webserver, Mailserver, FTP-Server, SQL-Server, DNS, DHCP, ... Bei Microsoft-Produkten ist meist für jede einzelne Funktionalität extra zu bezahlen. Es sei an dieser Stelle aber auch darauf hingewiesen, dass bei Linux nur ein eingeschränkter Support zur Verfügung steht. Dies begründet sich dadurch, dass vielleicht ein exotisches Paket eingesetzt wird, welches vielleicht einmal in drei Jahren ein Update erhält. Deshalb sollte beim Einsatz von diversen Funktionalitäten auch darauf geachtet werden, dass Updates und Bugfixes in regelmäßigen Abständen erscheinen.

8.1.1 Server

Das Betriebssystem Unix/Linux eignet sich besonders für den Serverbetrieb. Vor allem die frei verfügbaren Linux-Varianten stellen eine interessante Wahl dar. Wichtig ist nur zu beachten, dass egal für welchen Anwendungszweck, nur jene Dienste jeweils aktiviert werden, die unbedingt benötigt werden. Dies impliziert auch, dass bei der Installation vorsichtig vorgegangen werden muss, damit unnötige Pakete erst gar nicht installiert werden. Es ist oft sinnvoller, mit einem Minimalsystem anzufangen, und etwaige benötigte Pakete erst bei Bedarf zu installieren. Zusätzlich ist es wichtig, alle Informationsquellen, die zur Verfügung stehen zu nutzen, um sich über Updates bzw. Sicherheitslücken zu informieren. Die Maschine sollte weiters für eine gewisse Zeit in einer Testumgebung laufen, damit sämtliche Funktionalität ausführlich getestet werden kann. Danach sollte der eigentliche produktive Einsatz erst erfolgen.

8.1.2 Client

Für den Client stellt sich nicht so sehr die Frage nach der Sicherheit. Hier ist das Hauptproblem im Zusammenhang mit den Unix-Betriebssystemen die Benutzerunfreundlichkeit. Für einen normalen User ist trotz der schon sehr verbesserten X-Windows-Oberflächen, wie KDE oder Gnome[1], eine Verwendung nicht wirklich zumutbar. Weiters ergibt sich auch die Problematik der Kompatibilität mit der bereits eingesetzten Software. Viele Unternehmen setzen deshalb im Client-Bereich weiterhin auf Windows. Ich persönlich finde das auch aufgrund der angeführten Problematik als sinnvoll.

8.1.3 Firewall/Bastion Host

Dies ist der wohl sicherheitskritischste Bereich. Nach wohlüberlegter Absicherung, arbeiten Unix-Systeme wesentlich zuverlässiger, als vergleichbare Windows-Varianten. Deshalb ist es empfehlenswert, in den sensiblen Bereichen, auf Unix-Systeme zu bauen.

8.2 Windows

Von Windows existieren mittlerweile eine Vielzahl von Versionen, angefangen mit Windows 3.x, über Windows 9X und ME, und Windows NT, 2000, XP und 2003, die vor allem für Netzwerke entwickelt wurden, und deshalb auch davon Server-Versionen existieren. Dieser Abschnitt beschäftigt sich mit der Netzwerkbetriebssystem-Serie. Die anderen Versionen eignen sich für Unternehmensnetzwerke keinesfalls, da sie sowohl von der Sicherheit, als auch von der universellen Einsetzbarkeit in Netzwerken zu wenig Unterstützung bieten.

[1] KDE und Gnome sind graphische Oberflächen für Unix/Linux-Systeme

8.2.1 Server

Die gängigen Versionen für den Server-Bereich sind derzeit NT 4.0 Server, 2000 Server und Server 2003. Firmennetzwerke bauen meist auf Windows auf, da hiermit Domänen erstellt werden können, und damit die Verwaltung des Netzwerks vereinheitlicht werden kann. Unternehmen entscheiden sich meist für Microsoft-Produkte, da diese von der Wartung durch die Administratoren wesentlich einfacher zu verwalten sind. Gegen den Einsatz spricht im Prinzip nichts, sofern auf die Server kein externer Zugriff möglich ist, nur sollte wie schon bereits früher erwähnt, der jeweilige Server nur mit denjenigen Programmen und Diensten ausgestattet werden, die auch unbedingt notwendig sind. Zusätzlich gelten dieselben Vorgehensweisen, wie auch bei Unix-Systemen.

8.2.2 Client

Die gängigen Versionen für den Client-Bereich sind derzeit NT 4.0 Workstation, 2000 Professional und XP Professional. Aus der Benutzersicht ist natürlich Windows der eindeutige Favorit. Dies begründet sich vor allem durch den ausgeprägten Bedienkomfort, wobei auch gesagt werden muss, dass bei jedem Umstieg auf eine neue Version der User sich mit diversen Bedienungsänderungen herumschlagen muss. Viele Unternehmen wählen aufgrund des Bedienungskomforts und der universellen Programmkompatibilität meist Windows-Betriebssysteme für Ihre Anwender. Meist bleiben Unternehmen bei Windows, wenn es bereits eingesetzt wird. Ein Umstieg auf eine der zahlreichen Unix-Varianten ist meist zu kostspielig, bzw. existieren für diese Systeme unter Umständen nicht alle Programme, die derzeit in der Organisation eingesetzt werden.

8.2.3 Firewall/Bastion Host

Wie bereits in Abschnitt 8.1.3 erwähnt, ist ein Einsatz von Windows im Firewall- und Bastion Host-Bereich aus Sicherheitsgründen keinesfalls zu empfehlen.

8.3 Zusammenfassung

Abschließen kann man sagen, dass der Einsatz eines Betriebssystems im Server- oder Client-Bereich hauptsächlich von der Unternehmensphilosophie abhängig ist. Bei beiden Betriebssystemen hängt die Sicherheit sowohl von der Wartung, als auch von der Konfiguration der Systeme ab. Meiner Meinung nach ist es in sicherheitskritischen Bereichen, wie bei Firewalls oder Bastion Hosts, sinnvoller, Unix-Varianten einzusetzen, da diese wesentlich zuverlässiger arbeiten, Sicherheitsprobleme offen dokumentiert sind, und Sicherheitslücken in wesentlich geringerem Maße auftreten und auch vom Schweregrad nicht annähernd so fatal sind. Eine weitere Begründung liegt darin, dass Sicherheitslücken von Microsoft oft verschwiegen, oder geheim gehalten werden [16]. Bei den Unix-Systemen wird wesentlich offener mit den Sicherheitsproblemen umgegangen, und daher kann schneller auf bestimmte Situationen reagiert werden.

9 Firewall-Implementation

Wie in Kapitel 5.1.2 bereits diskutiert, bietet allein die Architektur mit überwachtem Teilnetz die Sicherheitsanforderungen, die für ein privates Netzwerk relevant sind. Dieser Abschnitt beschreibt eine mögliche Standard-Implementation für ein Maximum an Sicherheit.

9.1 Firewall-Aufbau

Abbildung 13 zeigt den optimalen Aufbau einer Firewall für ein sicheres privates Netzwerk.

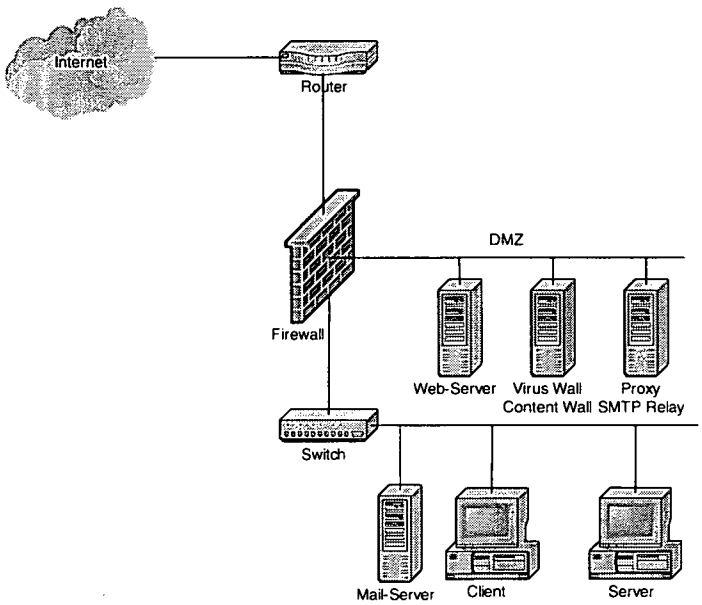


Abbildung 13: Firewall-Aufbau

Die Firewall besitzt in diesem Fall die geforderten drei Interfaces, um zwischen internem Netz und externem Netz ein Zwischennetzwerk zu kreieren.
Die Firewall besitzt dabei folgende IP-Adressen:

- Interne Adresse
- Externe Adresse
- DMZ-Adresse

Der Proxy und der Web-Server besitzen dabei folgende IP-Adressen:

- Externe Adresse
- DMZ-Adresse

Der Mail-Server besitzt dabei folgende IP-Adressen:

- Interne Adresse
- Externe Adresse

Die interne IP-Adresse des Mail-Servers wird dabei durch ein statisches NAT (Kapitel 5.1.3) auf die externe Adresse gemappt.
Die internen und DMZ IP-Adressen können dabei frei gewählt werden, und sollten aus [87] stammen, da diese über das Internet nicht geroutet werden. Dies bietet einerseits den Vorteil der Kostenersparnis, da nicht für jede Netzwerkstation eine externe IP-Adresse angefordert werden muss, und andererseits wird das interne LAN hinter wenigen offiziellen IP-Adressen versteckt. Somit ist der Aufbau des LAN für Angreifer von außen nicht nachvollziehbar.

9.2 DMZ-Aufbau

In der DMZ befinden sich drei Server. Wie in Kapitel 8 diskutiert, sollten sowohl die Firewall als auch die Bastion Hosts in der DMZ als Unix/Linux-Systeme implementiert werden.
Der Web-Server dient in dieser Konfiguration nur für die externe Homepage der Organisation. Die Virus Wall/Content Wall überprüft eingehende E-Mails auf Viren und aktive Inhalte, welche dabei entfernt werden. Ist eine Entfernung nicht möglich, so wird die E-Mail gelöscht. Weiters ist die Virus Wall/Content Wall dafür verantwortlich, Web-Seiten die über den Proxy angefordert werden, und über kriminelle oder obszöne Inhalte verfügen, sowie Web-Seiten mit aktiven Inhalten zu blockieren. Nur diejenigen Web-Seiten mit aktiven Inhalten, die für die Arbeitstätigkeit der Mitarbeiter notwendig sind, werden zugelassen. Der Proxy-Server dient zur Vermittlung der Client-Anfragen, sodass diese keine direkte Verbindung in das Internet aufbauen können. Weiters sind am Proxy diejenigen Teilnehmer des internen LAN definiert, welche die Berechtigung auf Internetdienste haben. Weiters dient der Proxy auch als SMTP-Reay, wobei eingehende E-Mails zuerst an die Virus Wall/Content Wall zur Überprüfung weitergeleitet werden, und erst danach zum internen Mail-Server. Ausgehende E-Mails werden ebenfalls vor der Weiterleitung ins Internet an die Virus Wall/Content Wall gesendet.

9.3 Dienste

Die nachfolgenden Dienste müssen auf den einzelnen Systemen implementiert werden.

Web-Server:
- HTTP/HTTPS-Service
- SQL-Service, falls Web-Seite Datenbank benötigt

Virus Wall/Content Wall:
- SMTP-Service
- Content Filtering System für Web-Seiten und E-Mails
- Virenschutzsoftware

Proxy-Server:
- Proxy-Software für HTTP/HTTPS und FTP

Das bedeutet, dass nur die Dienste HTTP, HTTPS, FTP und SMTP erlaubt sind.
Alle anderen Anfragen werden blockiert.

9.4 Minimale Regelbasis

Dieses Kapitel soll den Aufbau einer minimalen Regelbasis zeigen, um die oben angeführten Dienste zu erlauben.

Source	Destination	Service	Action
Firewall	Any	Any	Accept
Proxy Web-Server Virus Wall/Content Wall	DMZ	Any	Accept
Mail-Server	Proxy	SMTP	Accept
LAN	Proxy	HTTP HTTPS FTP	Accept
Internet	Web-Server	HTTP HTTPS FTP	Accept
Any	Any	Any	Log & Drop

Hierbei hat die Firewall auf alle Dienste und sämtliche Destinationen Zugriff. Die Server in der DMZ haben aus Sicherheitsgründen wiederum nur Zugriff auf die DMZ. Damit wird gewährleistet, falls es einen Einbruch in die DMZ gibt, dass das interne LAN weiterhin geschützt bleibt. Der interne Mail-Server darf nur den SMTP-Dienst des Proxy benutzen. Die Clients im LAN können nur über den Proxy Verbindungen ins Internet aufbauen, und dies auch nur für HTTP, HTTPS und FTP. Aus dem Internet sind nur Zugriffe über HTTP, HTTPS und FTP auf den Web-Server möglich. Sämtliche anderen Verbindungsversuche werden einerseits protokolliert und andererseits blockiert.

10 Sicheheit der von der Firewall erlaubten Dienste

10.1 E-Mail Sicherheit

Diese Kapitel beschreibt, wie der E-Mail-Verkehr abgesichert werden kann.

10.1.1 Interne E-Mails

Bei internen E-Mails ist es meist nicht notwendig Sicherheitsvorkehrungen zu treffen. Will man aber auf 100%-ige Sicherheit bauen, so gelten dieselben Kriterien wie für externe E-Mails (siehe unten).

10.1.2 Externe E-Mails

Externe E-Mails sind vor dem Abhören keineswegs geschützt. Jeder kann prinzipiell die Nachrichten abfangen und lesen. Zusätzlich ist es möglich den Absender zu verfälschen.

10.1.2.1 Verschlüsselung

Um dieser Sicherheitslücke Herr zu werden, können asymmetrische Verschlüsselungsverfahren verwendet werden. Das verbreitetste Programm zu diesem Zweck ist Pretty Good Privacy (PGP). Diese Software integriert sich in bestehende E-Mail-Software, und ermöglicht es die Nachrichten sowohl zu verschlüsseln als auch mit einer digitalen Signatur zu versehen. Hierbei ergibt sich meist nur die Problematik des Schlüsselmanagements, denn sowohl Sender als auch Empfänger müssen über dieselbe Software verfügen, damit ein Ver- und Entschlüsseln möglich ist. Der Vorteil an dieser Methode ist einerseits die eindeutige Nachvollziehbarkeit des Absenders und die sichere Integrität der Nachricht selbst.
Eine zweite etwas weniger sichere Methode ist die Verwendung von SSL für den Abruf bzw. den Versand von Mails. Hierbei wird zwischen Client und Server eine sichere Verbindung aufgebaut, sodass keiner die Nachrichten zwischen Client und Server abfangen kann. Der weitere Versandweg erfolgt wiederum unverschlüsselt. Meiner Meinung nach macht dies höchstens für interne E-Mails Sinn, damit diese bei Versand und Abruf nicht von anderen Mitarbeitern abgehört werden können.
Externem Mail-Verkehr sollte auf jeden Fall verschlüsselt werden, besonders dann, wenn sensible Daten übertragen werden. PGP und verwandte Produkte bietet hierfür eine optimale Basis.

10.1.2.2 Viren, Würmer und aktive Inhalte

Neben dem Abhören existieren weiters Bedrohungen, die sich im Inhalt der Nachricht verbergen. Dies können Viren, Würmer und aktive Inhalte sein. Um diese Bedrohung abzuwenden hilft meist nur die Verwendung von Virenschutzsoftware (s. Kapitel 13). Zusätzlich sollte genau wie bei Web-Seiten ein Content-Filter implementiert werden, der es ermöglicht aktive Inhalte aus E-Mails zu entfernen.

10.1.2.3 Spam

Bei Spam handelt es sich um Werbe- und sonstige Junk-E-Mails. Abhilfe gegen die Überflutung mit Spam ermöglicht eine Spam-Filter Software. So können einerseits bereits bekannte Spam-Absender blockiert werden, und andererseits sind diese Systeme selbstlernend und erkennen einen Großteil des Spam automatisch, ohne dass ein administrativer Eingriff notwendig wäre.

10.2 FTP-Sicherheit

Um die FTP-Sicherheit zu erhöhen, sind zwei wichtige Kriterien zu erfüllen. Einerseits muss der FTP-Server sofort nach Bekanntwerden einer Sicherheitslücke auf den neuesten Stand gebracht werden. Auch die Proxy-Software sollte auf dahingehende Beeinträchtigung überprüft werden. Andererseits darf der Proxy nur passive FTP-Verbindungen durch die Firewall schleusen (s. Kapitel 4.4.2)

10.3 HTTP-Sicherheit

Genau wie bei FTP muss hierbei einerseits durch Patches sichergestellt werden, dass Sicherheitslücken schnellstmöglich geschlossen werden. Andererseits empfiehlt es sich, wo nur möglich SSL einzusetzen, um die Möglichkeit des Abhörens der Verbindung auf ein Minimum zu reduzieren.

11 Standortübergreifende Netzwerke

Die meisten Firmen und größeren Organisationen sind über mehrere Standorte verteilt. Durch den immer größer werdenden Druck nach Kommunikation haben sich diverse Möglichkeiten etabliert, Verbindungen zwischen den einzelnen Standorten einzurichten. Die Problematik ergibt sich aber dadurch, dass dabei Daten über öffentliche Netze transportiert werden müssen, und sich dadurch natürlich ein erhöhter Sicherheitsbedarf ergibt.

11.1 WAN-Verbindungen

Die älteste Variante zur Vernetzung von räumlich verteilten Intranets ist die WAN-Verbindung. Dabei wird eine Verbindung über dezidierte Standleitungen oder Wählverbindungen etabliert.

11.1.1 Vorteile

Der Vorteil bei richtiger Wahl der WAN-Verbindung, ist die garantierte Bandbreite. Dadurch entstehen auch bei hohem Verkehrsaufkommen keine Engpässe. Ein weiterer Vorteil ist die einfache Möglichkeit der Verschlüsselung, indem an beiden Enden der WAN-Leitung Verschlüsselungsboxen installiert werden.

11.1.2 Nachteile

Diese Art der Verbindung ist sowohl kostenintensiv, als auch unflexibel, da die Abrechnung meist auf Leitungs- bzw. Zeitbasis erfolgt. Auch bei wenig Datenaufkommen ist für solche Leitungen der volle Preis zu bezahlen. Auch eine Umlegung der Leitung ist meist nur mit sehr hohem administrativem Aufwand möglich, vor allem dann, wenn Ländergrenzen dabei überschritten werden.

11.1.3 Zusammenfassung WAN-Verbindungen

WAN-Verbindungen empfehlen sich dort, wo der Kostenaufwand für Firewalls höher als die Miete der Standleitung betragen würde. Auch wenn eine garantierte Bandbreite gefordert wird, ist dies über Standleitungen problemlos möglich. Vom Standpunkt der Sicherheit betrachtet, ergibt sich mit den Verschlüsselungsboxen eine interessante Variante für die sichere Verbindung von mehreren Standorten.

11.2 RAS-Verbindungen

Als RAS (Remote Access Service) werden Dienste bezeichnet, die einen Zugang von außen über Modem bzw. ISDN-Anlage ermöglichen. Das Bindeglied stellt meist ein RAS-Server dar. Dadurch können Außendienstmitarbeiter oder Telearbeiter von zuhause auf das Firmen-LAN zugreifen. Da diese Zugänge immer über öffentliche Netze laufen, sind außer einem Rückrufmechanismus strenge Verfahren zur Authentifizierung und Verschlüsselung erforderlich.

11.2.1 Vorteile

RAS-Verbindungen sind bei räumlicher Nähe zum Firmen-Netzwerk eine sehr kostengünstige Alternative, vor allem, wenn der RAS-Server über einen Rückrufmechanismus gesteuert wird. Dies ermutigt oft auch Mitarbeiter, welche normalerweise nicht von zuhause aus arbeiten, diese Möglichkeit zu nutzen.

11.2.2 Nachteile

Wenn der Arbeitsplatz weit vom Firmennetzwerk entfernt ist, rentiert sich RAS aufgrund der hohen Telefongebühren sicherlich nicht.

11.2.3 Zusammenfassung RAS-Verbindungen

RAS ist dann sinnvoll einsetzbar, wenn eine räumliche Nähe besteht und wenn der RAS-Server nur per Rückruf und mit starker Verschlüsselung mit einem Anrufer kommuniziert. Ansonsten stellt sich RAS als extrem gefährlich dar, vor allem wenn Anrufer sich direkt ohne Rückruf einwählen können.

11.3 VPN-Verbindungen

Virtuelle Private Netzwerke bieten sich dann an, wenn zwischen den zu koppelnden Netzen oder Arbeitsplätzen große Entfernungen überbrückt werden müssen, und die Kosten einer WAN-Verbindung, die eines normalen Internet-Anschlusses bei weitem übersteigen.

11.3.1 Vorteile

Diese Verbindung kann praktisch überall verwendet werden, wo ein Internetanschluss vorhanden ist. Der große Vorteil ergibt sich dadurch, dass Internetverbindungen meist wesentlich kostengünstiger als Standleitungen oder Wählverbindungen sind.

11.3.2 Nachteile

Durch die Verwendung des Internet als Medium ergeben sich hier im Gegensatz zu RAS- und WAN-Verbindungen, die Gefahr des Mitlesens von Paketen, unberechtigte Anmeldung an einem Server oder Blockade der Kommunikation durch eine Denial-of-Service-Attacke.

11.3.3 Zusammenfassung VPN-Verbindungen

VPN ist dort sinnvoll, wo Internetanschlüsse bereits existieren. Wichtig ist dabei aber, dass die Daten über IPSec verschlüsselt werden, um ein Ausspionieren zu erschweren, bzw. unmöglich zu machen. Von allen drei Verbindungsarten, ist diese sicher die modernste. Wichtig ist nur eine sorgfältige Planung, um Sicherheitsrisiken so weit wie möglich ausschließen zu können.

11.4 Zusammenfassung

Die Verbindung von mehreren Standorten erfordert immer sorgfältige Planung. Für Organisationen zählen nicht nur Sicherheitsaspekte, sondern es spielen auch Kosten immer eine wichtige Rolle. Deshalb entfernt man sich von WAN-Verbindungen und RAS-Systemen mit Rückruffunktion immer weiter. VPNs bieten für die Firma die kostengünstigste Alternative, da ein Internetzugang an den meisten Standorten bereits vorhanden ist. Ein negativer Effekt ist aber, dass Mitarbeiter oft Ihren Internetzugang selbst bezahlen müssen, um auch von zuhause aus arbeiten zu können. Viele Firmen sehen dies als Angebot, meiner Meinung nach ist das aber Missbrauch von neuen Technologien. Erklärt sich ein Mitarbeiter bereit von zuhause in seiner Freizeit zu arbeiten, ist das Minimum ein Kostenersatz seiner Verbindung.

12 Wireless LAN (WLAN) Sicherheit

12.1 Definition

Unter einem WLAN versteht man die drahtlose Verbindung von Netzwerkteilnehmern nach dem 802.11b Standard [88].

12.2 Funktionsweise

Ein Wireless LAN kann in zwei Operationsmodi betrieben werden [65]. Einerseits ist dies der ad-hoc Modus. Hierbei können Clients, welche sich in der Transmissionsreichweite (Zelle) befinden miteinander kommunizieren. Will der Client auch mit Systemen kommunizieren, welche sich außerhalb der Zelle befinden, muss ein Mitglied der Zelle als Gateway fungieren, und das Routing übernehmen.

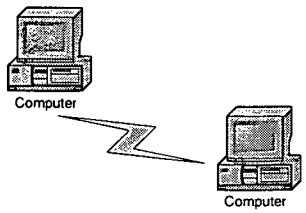


Abbildung 14: Ad-hoc Modus

Der zweite Modus ist der Infrastruktur-Modus. Hierbei sendet jeder Client seine Pakete an eine zentrale Station, welche als Access Point (AP) bezeichnet wird. Der Access Point agiert dabei als Router, welcher die Pakete entweder in das kabelvernetzte LAN, oder in das WLAN weiterleitet.

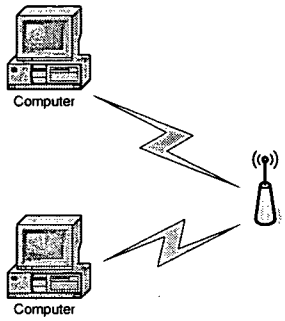


Abbildung 15: Infrastrukutr-Modus

Bevor eine Kommunikation beginnen kann, muss zwischen Client und Access Point eine Relation aufgebaut werden, die als Association bezeichnet wird. Erst wenn diese Association etabliert ist, können zwei Teilnehmer Daten austauschen. Im Infrastruktur-Modus müssen die Clients eine Association mit einem Access Point herstellen. Dies ist ein Zwei-Stufen-Prozess, der drei States umfasst:
1. Unauthenticated and unassociated,
2. Authenticated and unassociated, und
3. Authenticated and associated.
Der Übergang zwischen den einzelnen States erfolgt durch den Austausch von sogenannten Management Frames.
Im Folgenden sei nun der Ablauf einer Association erläutert.
Sämtliche Access Points senden ein Beacon Management Frame in fixen Intervallen aus. Um mit einem Access Point zu assoziieren, hört der Client auf die Beacon Messages, um einen Access Point in der Nähe zu identifizieren. Die Netzwerknamen, auch Service Set Identifiers (SSID) genannt, welche in dem Beacon Frame enthalten sind, werden dem User präsentiert, um ein Netzwerk auszuwählen. Ein Client kann auch ein Probe Request aussenden, um so ein Netzwerk mit einer bestimmten SSID zu finden. Nachdem ein Access Point identifiziert wurde, tauschen Client und Access Point eine Anzahl von Management Frames zur Authentifizierung aus. Die zwei standardisierten Authentifikationsmechanismen werden in 12.3 beschrieben. Nach erfolgreicher Authentifizierung, geht der Client in den zweiten State über. Um den dritten Zustand zu erreichen, sendet der Client ein Association Request, und der Access Point antwortet mit einem Association Response Frame. Danach ist der Client in das WLAN integriet, und kann nun mit allen Teilnehmern kommunizieren.kk

12.3 Standard Sicherheits-Mechanismen

Der 802.11-Standard definiert einige Sicherheitsmechanismen, um WLANs in einer sicheren Umgebung anzubieten.

12.3.1 Wired Equivalent Privacy Protocol

Das Wired Equivalent Privacy Protocol (WEP) wurde designed, um vertraulichen Netzwerkverkehr in WLANs zu ermöglichen. Eine detaillierte Erläuterung des WEP-Protokolls würde den Rahmen dieser Dissertation sprengen. Die zwei Arbeiten [66], [67] zeigen aber sehr eindrucksvoll, dass das WEP-Protokoll nur sehr wenig Sicherheit bietet, und deshalb als Sicherheitsmaßnahme als unbrauchbar einzustufen ist.

12.3.2 Open System Authentication

Open System Authentication ist das Default-authentifikatiosprotokoll in WLANs. Das Problem bei diesem Protokoll liegt darin, dass jeder authentifiziert wird, der authentifikation anfordert. Experimente [65] haben gezeigt, dass Management Frames sogar dann, wenn WEP aktiviert wird, im Klartext übermittelt werden.

12.3.3 Access Control Lists

Ein weiterer Mechanismus, der zwar von vielen Herstellern implementiert wird, aber kein Teil des Standards ist, sind Access Control Lists. Dabei wird die MAC-Adresse des Clients am Access Point mit einer Liste von erlaubten MAC-Adressen verglichen. Ist die Adresse in der Liste, so wird Zugriff gewährt, andernfalls nicht.

12.4 Zusammenfassung

Betrachtet man die Sicherheit von Seiten der Access Control Lists, so kann wie auch schon in 4.1.3 beschrieben, dies keinesfalls als sicher bezeichnet werden. Einerseits können MAC-Adressen sehr leicht mit einem Sniffer abgefangen werden, da diese immer im Klartext übermittelt werden müssen, und andererseits ist dann die MAC-Adresse sehr leicht auf eine der herausgefundenen Adressen änderbar [68]. Selbst WEP und ganz zu schweigen von Open System Authentication, bieten keine ausreichenden Schutzmaßnahmen vor potentiellen Angriffen [69]. Deshalb sollte im Firmenbereich auf den Einsatz von WLANs komplett verzichtet werden. Firmen, wie BlueSocket und Vernier Networks, arbeiten bereits an Produkten, die die Integration von IPSec und VPNs ermöglichen. Diese sind aber von der Marktreife noch weit entfernt [70]. Erst wenn sichere Protokolle gefunden werden, die es einem Angreifer unmöglich machen, oder zumindest sehr erschweren in das WLAN einzudringen, oder Produkte Marktreife erlangen, die eine Integration von firewalls, IPSec, VPN und IDS in WLANs ermöglichen, können Firmen den Einsatz von WLANs in betracht ziehen.

13 Virenschutzlösungen im Corporate-Bereich

Folgende Abbildung verdeutlicht die Notwendigkeiten eines umfassenden Virenschutzes innerhalb einer Organisation.

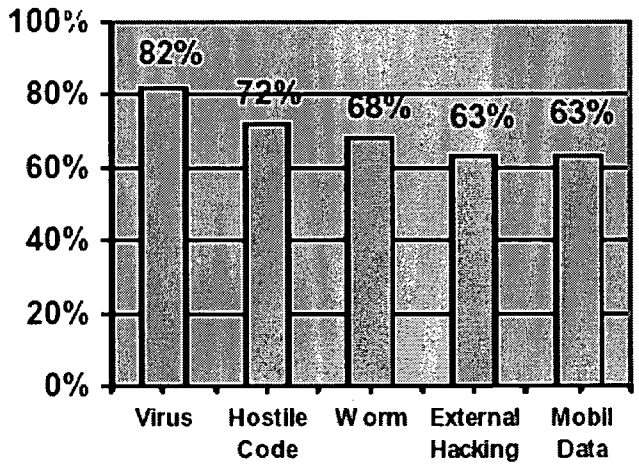


Abbildung 16: Sicherheitsvorfälle in Prozent 2002 [51]

Für den Corporate-Bereich ergeben sich aber ganz andere Anforderungen, wie im Privatbereich. Dieser Abschnitt soll die Anforderungen und eine sinnvolle Implementation veranschaulichen.

13.1 Anforderungen

Für den Unternehmensbereich lassen sich folgende Anforderungen definieren:

- Zentrale Verwaltung und Wartung
- Automatische Virendefinitionsupdates
- Zentrales Ausrollen der Virenschutzsoftware
- Umfassende zentrale Konfiguration des Client-Verhaltens
- Software für Server, Clients, E-Mail-Server, SMTP-Gateways und Firewalls

Für Administratoren und Systemverwalter muss die Virenschutzsoftware zusätzlich zum selbstverständlichen Virenschutz Funktionalitäten anbieten, die die Verwaltung und Wartung möglichst einfach gestalten. Für sämtliche Server und Clients, auf denen die Software installiert wurde, sollte das Management über eine zentrale Konsole erfolgen. Diese Konsole muss dem Systemverwalter eine Ansicht zur Verfügung stellen, wo alle Server und Clients ersichtlich sind, der Status der Virendefinitionen, etwaige Vireninfektionen, oder auch Benachrichtigungen über die Entfernung oder Isolation eines Virus angezeigt werden. Die Virendefinitionen müssen nach Konfiguration der Update-Funktion in regelmäßigen Zeitintervallen automatisch aktualisiert werden. Weiters muss es dem Administrator ermöglicht werden, neue Server oder hinzugekommene Clients mittels Remote-Installation mit der erforderlichen Virenschutzsoftware auszustatten. Als letzter wichtiger Punkt wäre wünschenswert, wenn die Software ermöglicht Clients so zu konfigurieren, dass die Virenschutzsoftware weder deaktiviert, noch entfernt werden kann. Desweiteren muss die Software auch auf speziellen Anwendungsservern, wie z.B. Mail-Servern einsetzbar sein. Dort ist wichtig, dass alle E-Mails vor der Zustellung automatisch auf Viren überprüft werden. Diese Notwendigkeit verdeutlicht folgende Abbildung.

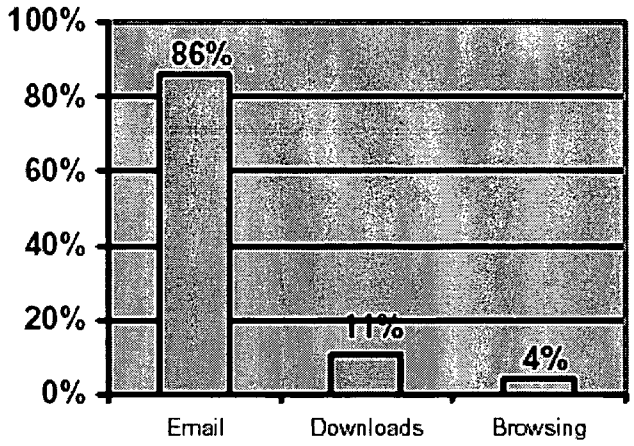


Abbildung 17: Virusinfektionen nach Quelle [51]

Sind all diese Anforderungen erfüllt, ist das Produkt geeignet, im Unternehmensbereich eingesetzt zu werden.

13.2 Implementation

Bevor die Virenschutzlösung im Unternehmen ausgerollt wird, sollte erst ein detaillierter Plan erstellt werden, wie die Vorgehensweise ist. Dafür spielen folgende Punkte eine wichtige Rolle:

- Abrufen der Virendefinitionen auf Clients und Servern vom Internet oder von einem zentralen Update-Server
- Einsatz von Produkten verschiedener Hersteller

Prinzipiell ist es sinnvoll, nachdem meist nicht alle Clients über einen Internet-Zugang verfügen, einen dezidierten Server als Update-Server zur Verfügung zu stellen. In diesem Fall ist es ausreichend, wenn dieser Server über einen Internetzugang verfügt, und dann die Updates von allen anderen Clients und Servern von diesem Update-Server abgerufen werden. Vorrausetzung ist natürlich, dass die Software das auch unterstützt.
Der zweite Punkt kann auch eine ganz bedeutende Rolle spielen, denn es kann natürlich passieren, dass ein Hersteller bei der Aktualisierung der Updates nicht gar so schnell reagiert wie ein anderer, und dadurch der Virenschutz kurzfristig unzureichend wird. Hierbei hat es sich in der Praxis als sinnvoll erwiesen, dass Proxy-Server, oder SMTP-Gateways, die sich meist in der DMZ befinden, mit einer Software eines anderen Herstellers ausgestattet werden, als alle anderen Clients und Server. Somit besteht ein mehrschichtiger Schutz, der sehr zum Vorteil der Virensicherheit beiträgt.

13.3 Zusammenfassung

Ohne eine umfassende Virenschutzlösung sind Unternehmen heutzutage äußerst angreifbar. Viele Beispiele in der unmittelbaren Vergangenheit haben gezeigt, dass Milliardenverluste durch Vireninfektionen, Würmer oder Trojanische Pferde verursacht werden können. Deshalb ist es essentiell, dass Virenschutz ein zentrales Thema jedes Sicherheitsbeauftragten zu sein hat. Nur eine gezielte Virenschutzpolitik zusammen mit regelmäßigen Virendefinitionsupdates und konsequente Updates bei Sicherheitslücken in Betriebssystemen und Software, mindern die Auswirkungen einer unternehmensweit möglichen Vireninfektion.

14 Intrusion Detection Systeme

Bei Intrusion Detection Systemen handelt es sich um spezielle Software, die entwickelt wurde, um herauszufinden, ob jemand in ein Unternehmensnetzwerk eingebrochen ist. Die Bandbreite reicht hier von relativ einfachen, passiven Systemen, welche nur Protokolldateien analysieren, bis hin zu Systemen mit künstlicher Intelligenz, welche an verschiedenen Orten im Netzwerk positioniert werden, und permanent den Verkehr analysieren.

14.1 Funktionsweise

Bei der Intrusion Detection werden prinzipiell zwei Techniken angewendet. Die einen Systeme wissen welches Verhalten schlecht ist, und geben somit Alarm, wenn dieses auftritt [48]. Die anderen Systeme wissen welches Verhalten gut ist, und schlagen Alarm, wenn etwas anderes auftritt [48]. Dabei sind Systeme mächtiger, aber auch schwieriger zu implementieren, die gutartiges Verhalten erkennen. Systeme, die schlechtes Verhalten erkennen können verwenden Angriffssignaturen. Dies sind Informationen darüber, wie bestimmte Angriffe aussehen. Systeme, die gutes Verhalten erkennen, verwenden Benutzungsprofile. Dies sind Informationen darüber, was normalerweise passiert. Diese müssen aber oftmals eine Lernphase unterlaufen, in der sie den Netzwerkverkehr analysieren, und daraus in weiterer Folge ableiten können, was als Angriff zu werten ist, und was nicht. Es können aber auch Techniken verwendet werden, die fast alle Versuche vereiteln, Angriffe zu verbergen. Die beste und verbreitetste dieser Techniken ist der Honigtopf, der verlockende Köder, hinter dem sich nichts als eine Falle verbirgt. Wenn zum Beispiel eine Maschine in das Grenznetz eingebunden wird, die für keinen einzigen Dienst benutzt wird, dann ist sichergestellt, dass jeder Verbindungsversuch zu dieser Maschine einen Angriff darstellt.

14.2 Grenzen

Wie jedes System gibt es natürlich auch bei der Intrusion Detection gewisse Probleme, egal welche der Techniken verwendet wird. Im ersten Fall kann das System nur Angriffe erkennen, für die es auch Angriffssignaturen besitzt. Läuft ein Angriff nicht nach dem Schema einer der Signaturen, wird er nicht erkannt. Selbstverständlich werden permanent Updates der Angriffsmuster veröffentlicht, sie hinken aber natürlich den Angriffstaktiken selbst hinterher. Im zweiten Fall gibt es das Problem mit den Fehlalarmen. Dies sind Fälle, in denen das System einen Angriff vermutet, aber keine durchgeführt wird. Dies ergibt sich vor allem daraus, dass die Systemnutzung mit der Zeit alteriert. Bei guten Systemen liegt zwar die Fehlerrate im bereich von 1 bis 3 Prozent, was im Fall von Netzwerken, 1 bis 3 Prozent der Pakete bedeutet. Da viele Standorte Millionen eingehender Pakete pro Tag aufbringen, kann diese angeblich geringe Fehlerrate schnell in tausenden von Fehlalarmen pro Tag resultieren. Dies ist natürlich völlig inakzeptabel.

14.3 Zusammenfassung

Wie viel ein Intrusion Detection System für eine Organisation bringt, hängt vor allem davon ab, wie viel Zeit, Geld und Entwicklungsaufwand in das System investiert wird. Es handelt sich zwar um eine sehr effektive Technik, aber es nicht trivial sie zum Laufen zu bringen. Außerdem ist der Wartungsaufwand enorm. Völlig unnötig ist ein Intrusion Detection System dann, wenn nicht genügend Personal für Wartung und Auswertung der Alarme zur Verfügung stellt. Die derzeit günstigste Alternative ist sicherlich der Honigtopf, welcher aber die Einschränkung hat, nur von außen als ein interessantes Ziel gesehen zu werden.

15 Intranetsicherheit

Das Intranet hat in Firmen in den letzten Jahren immer mehr an Bedeutung bekommen. Durch dieses wurde es möglich Informationen schnell und kostengünstig an die Mitarbeiter zu verteilen. Auch die Kosten für Druck von diversen Listen und Informationsblätter kann so erheblich gesenkt werden. Einzig und allein die Bereitschaft der Mitarbeiter, dieses neue Kommunikationsmedium anzuwenden, ist Vorraussetzung für eine erfolgreiche und kostensparende Implementierung.

15.1 Definition

Unter einem Intranet versteht man ein Konzept für die firmeninterne Kommunikation. Das Intranet selbst wird durch folgende Aspekte definiert [26]:

- Die Basistechnologie ist Internet-Technologie
- Das Intranet ist deutlich vom Internet getrennt
- Das Intranet und seine Dienste werden von einer geschlossenen Benutzergruppe verwendet
- Dem Intranet stehen meist bedeutend höhere Bandbreiten zur Verfügung
- Es gibt eindeutige Verantwortlichkeiten – das gesamte Intranet gehört einer Organisation

15.2 Anwendungsgebiete

Im folgenden seien die wichtigsten Anwendungsgebiete des Intranet beschrieben.

15.2.1 Interne E-Mail

Eine zentrale Komponente des Intranet ist die Bereitstellung der Möglichkeit interne E-Mail-Nachrichten zu versenden. Wird das Medium sinnvoll in den Kommunikationsablauf integriert, so ist sowohl eine Papier-, als auch Zeitersparnis zu verbuchen.

15.2.2 Interne Newsgroups und Foren

Dies kann einerseits als Plattform für Diskussionen über aktuelle Projekte verwendet werden, als auch als Forum für Hilfestellungen des Benutzersupports. So können Lösungen für häufig auftretende Fehler und Probleme einmal beantwortet werden, und im Forum für jedermann ersichtlich abrufbar sein. Damit erübrigen sich dutzende von Telefonanrufen mit immer denselben Fragestellungen. Das Forum kann alsdann auch für andere Problemstellungen, die nicht unbedingt mit dem Benutzersupport in Zusammenhang stehen eingesetzt werden. So können Mitarbeiter Erfahrungen austauschen, und damit die Kommunikation zwischen Abteilungen verbessert oder angeregt werden.

15.2.3 Interner Informationsserver

Dies ist einer der zentralsten Aufgaben eines Intranet. Über WWW und FTP werden den Benutzern allgemeine Informationen zur Verfügung gestellt, die ansonsten entweder durch Papier oder per E-Mail verteilt wurden. So ist es sinnvoll, für die diversen Bereiche, wie Geschäftleitung, Betriebsrat oder auch Firmenfußballverein einen eignen Bereich am Informations-Server einzurichten. Die Gesamtstruktur als auch die Qualität der Beiträge sollte von einer zentralen Stelle überprüft und definiert werden. Auch die Aufbereitung der einzelnen Information für das WWW sollte zentral von erfahrenen Web-Designern durchgeführt werden.
Dabei darf nicht vergessen werden, dass bezüglich der Informationen die Bringschuld zu einer Holschuld wird. Darum sollten wichtige Verlautbarungen weiterhin per E-Mail ausgesandt und mit einem Verweis auf die entsprechende Webseite am Informationsserver versehen werden.

15.2.4 WWW als Interface zu internen Applikationen

Dies stellt eine weitere Ausbaustufe dar. Hierbei werden alle internen Applikationen, bei denen es möglich ist, mit Webinterfaces versehen. Man hat dadurch den Vorteil, dass auf den Client außer einem Internetbrowser keine zusätzliche Software installiert werden muss. Dadurch kann größtmögliche Plattformunabhängigkeit gewährleistet werden, und der administrative Aufwand sinkt, da das Interface für die Clients nur mehr an zentraler Stelle angepasst werden muss.

15.3 Sicherheitsaspekte

Beim Intranet sind grundsätzlich schwächere Sicherheitskriterien anzuwenden, als beim Internet. Dennoch sollte das Angriffspotential für Intranet-Server nicht unterschätzt werden. Wie schon bereits zu Anfang erwähnt, geht ein großer Anteil der Angriffe von innerhalb des Unternehmens aus. Deshalb sollte ein Intranet-Server ebenfalls gegen Missbrauch geschützt werden. Einerseits ist ein ausgefeiltes Berechtigungssystem vonnöten, sodass nicht jeder beliebige Mitarbeiter Informationen veröffentlichen oder verfälschen kann. Zusätzlich sollte der Server mit aktuellen Sicherheitsupdates ausgestattet werden, und der Zugriff für administrative Dienste, wie Secure Shell (SSH) oder Telnet nur für autorisierte administrative Workstations zugelassen werden. So ist einerseits gewährleistet, dass auf den Informationsseiten selbst nur berechtigte Personen Veränderungen durchführen dürfen, und dass Anwender nur diejenigen Dienste verwenden können, die sie auch wirklich benötigen. In den meisten Fällen wird dies nur der HTTP-Server und eventuell der SMTP-Dienst sein.

Teil IV Die Zukunft der Netzwerksicherheit

16 Trends und zukünftige Entwicklungen

Die neuen und immer umfangreicher werdenden Anwendungen, und die damit im Zusammenhang stehenden immer komplexer werdenden Protokolle in einer zunehmend vernetzten Umwelt werden in Zukunft zu weiter wachsenden Sicherheitsproblemen. Sowohl die immer schneller werdenden lokalen Netzwerkverbindungen, wie FastEthernet oder Gigabit-Ethernet, aber auch die Weitverkehrsnetze mit immer höheren Bandbreiten stellen bereits heute hohe Anforderungen an die Netzwerksicherheit der nächsten Generation. Auch die Konvergenz von Daten und Sprache stellen völlig neue Anforderungen an die Netzwerksicherheit. Daraus ergeben sich völlig neuartige Sicherheitssysteme, die auf Basis von völlig neuen Technologien arbeiten müssen.

16.1 Firewalls und Angriffserkennung auf Basis von künstlicher Intelligenz

Seit einiger Zeit schon versucht die Grundlagenforschung Expertensysteme in die Architektur von Firewall-Systemen miteinzubinden. Ständig veränderte Angriffsmethoden und permanent auftretende Sicherheitslücken erfordern es, mit intelligenten Systemen dem Kontra zu bieten. So wird beispielsweise versucht mit selbstlernenden Strukturen wie neuronalen Netzen oder Entscheidungsbäumen, dem Herr zu werden. Diese befinden sich aber noch im Experimentalstadium, und selbst wenn diese Marktreife erhalten, werden ebenso intelligente expertensystembasierte Angriffsprogramme nicht lange auf sich warten lassen.

16.2 Die Post-Firewall-Ära

In welchem Ausmaß Firewall-Systeme auch in Zukunft als zentrale, für ein gesamtes Netzwerk zuständige Einheit realisiert werden müssen, lässt sich heute noch nicht abschätzen. Aufgrund der zunehmenden Leistungsfähigkeit von Prozessoren und Computersystemen, rücken Systeme in greifbare Nähe, welche sich selbst mithilfe von leistungsfähigen Authentifikations- und Verschlüsselungsmechanismen schützen können. Jedes System kann sodann Daten einzig und allein über sichere Kanäle mit authentifizierten Kommunikationspartnern austauschen. Diese Leistungsfähigkeit wird heutige Systeme weit übertreffen. Man sollte dem aber nicht allzu optimistisch gegenüber treten, und glauben, dass damit sämtliche Sicherheitsprobleme gelöst werden können. Die höhere Leistungsfähigkeit der Hard- und Software kann nämlich auch auf der Seite des Angreifers eingesetzt werden, was den Leistungsvorsprung wieder gegen Null konvergieren lässt.
Ein gewaltiger Boom ist auch im Bereich der Intrusion Detection Systeme zu erwarten. Dabei können Agenten auf jedem Rechner eingesetzt werden, die Angriffsversuche sofort an eine Alarmzentrale melden, und somit Angreifer frühzeitig erwischt werden können.
Ein weiterer Entwicklungszweig ist die Schaffung von integrierten Systemen. Heutzutage tauschen Sicherheitskomponenten, wie Firewalls, VPN-Gateways, Virenschutzlösungen, usw. Informationen mühsam über CVP (Content Vectoring Protocol) aus. Dies wird bei integrierten Systemen nicht mehr notwendig sein. Es sei aber auch dazu gesagt, dass viele Firmen bereits an solchen Lösungen arbeiten, die Versuche bisher aber recht erfolglos verliefen.

16.3 Zusammenfassung Trends

Wie man sieht arbeiten viele Firmen, die sich mit Netzwerksicherheit beschäftigen an immer ausgefeilteren Lösungen. Man darf aber dabei niemals vergessen, dass es kein perfektes und auch kein 100% sicheres System geben kann. Genauso entwickeln auch Angreifer immer ausgefeiltere Techniken und Programme, die es sogar absoluten Laien ermöglichen in ein sicheres System einzudringen. Daraus ergibt sich, dass das Thema der Sicherheit immer Wettlauf sein wird, in dem es aber keinen Sieger geben wird, denn auch wenn einer den anderen überholt, wird er selbst sofort wieder überholt. Daraus ergibt sich ein Kreislauf, dessen Ende und vor allem dessen Folgen derzeit noch nicht absehbar sind.

17 Weiterentwicklung und Zukunftsperspektiven

17.1 Physische Sicherheit

17.1.1 Verbesserte Zutrittssysteme

Im Bezug auf physische Sicherheit und Zutrittssysteme gibt es in Firmen oftmals nur wenig Absicherung. Verbesserungsmöglichkeiten sollen in diesem Abschnitt erläutert werden. Ein erster Schritt könnte eine Eingangszutrittskontrolle darstellen. Diese könnte durch Chip-Tokens (Abbildung 18), bzw. biometrischen Methoden (Abbildung 19) aktiviert werden. Unter Chip-Tokens werden alle Geräte oder Dinge bezeichnet, welche über einen integrierten, berührungslosen Chip verfügen. Diese Zutrittssysteme sollten an sämtlichen Firmeneingängen positioniert werden. Ein Mitarbeiter muss sich somit zuerst am Eingang mithilfe des Chips authentifizieren. Erst wenn diese Authentifizierung erfolgt, wird der normale User-Account, mit dem sich der User am PC anmeldet freigeschaltet. Dieser Account besteht aus einer normalen User/Passwort-Kombination. Der Authentifizierungs-Server besitzt eine Datenbank, die die Zuordnung zwischen Chip-Token und Benutzername enthält. Nach der Authentifizierung am Eingang erkennt der Server, welcher Mitarbeiter das Haus betreten hat, und aktiviert den zugehörigen Benutzer-Account. Der Benutzer-Account sollte aber nur für eine gewisse Zeit, innerhalb derer sich der Mitarbeiter am PC anmelden muss, aktiviert bleiben. Dies ist abhängig von der Größe des Firmengeländes, aber ein Referenzwert von ca. 30 Minuten kann trotzdem angenommen werden. Meldet sich der Mitarbeiter nicht innerhalb dieses Zeitfensters am PC an, so wird der Benutzer-Account wieder gesperrt, und erst eine neuerliche Authentifizierung im Eingangsbereich mithilfe des Chips hebt diese Sperre wieder auf. Der Server verwaltet hierbei die Zeitfenster, die in Abhängigkeit der Entfernung des Arbeitsplatzes vom Eingangsbereich für jede Person individuell festgelegt werden kann. Eine Alternative wäre die definitive Sperre bei Überschreitung des Zeitfensters. In diesem Fall kann nur ein Administrator, nachdem er sich von der Authenzität des Mitarbeiters überzeugt hat, den Account wieder reaktivieren. Um eine zusätzliche Verbesserung der Sicherheit bei den PCs zu erreichen, könnten Chip-Tokens in Form eines USB-Gerätes eingesetzt werden. Diese müssen vor dem Starten des Gerätes in einen USB-Slot eingesetzt werden, damit der PC überhaupt aktiviert werden kann. Die Authentifizierung sowohl im Eingangsbereich als auch durch Benutzer/Kennwort-Kombination würde trotzdem erhalten bleiben.
Wählt man statt des Chip-Tokens für den Eingangsbereich eine biometrische Methode, wie z.B. Fingerabdruck-Scan oder Iris-Scan, kann die Implementierung wie oben beschrieben ebenfalls übernommen werden.
Verlässt der Mitarbeiter das Haus, so muss er im Eingangsbereich die Prozedur wiederholen. Dadurch erkennt der Server, dass sich der Mitarbeiter nicht mehr im Haus befindet, und sperrt somit den Benutzer-Account umgehend. Dabei spielt es keine Rolle, ob es sich um einen Aussen-Termin, die Mittagspause, oder das Arbeitsende handelt. Jedes Mal, wenn das Haus verlassen wird, ist diese Authentifizierung obligatorisch.
Bei dieser Implementation ist es wichtig, dass die Benutzer die Notwendigkeit des Systems verinnerlichen und akzeptieren. Zusätzlich sollten Richtlinien eingeführt werden, die Verstöße gegen das System abdecken. Es ist aber zu erwarten, dass bei diesem System wesentlich sorgfältiger mit den Anmelde-Tokens umgegangen wird. Wenn es sich nur um ein passwortbehaftetes System handelt, werden diese meist trotz entsprechender Richtlinien an andere Mitarbeiter weitergegeben. Bei Chip-Tokens wie z.B. in Schlüsselanhänger oder Uhren sinkt die Gefahr der Weitergabe dramatisch, da in diesem Fall eine eindeutige Nachvollziehbarkeit möglich ist, was bei Passwörtern allein noch mit der Begründung abgeschoben werden kann, dass ein anderer Mitarbeiter das Passwort gehackt oder erraten

hat. Bei biometrischen Eingangsauthentifizierungssystemen wird dieses Gefahrenpotential komplett ausgeschaltet.
Ein weiterer Vorteil dieser Methode ist, dass Kennwortrichtlinien wesentlich lockerer definiert werden können, da die große Authentifizierung bereits am Eingang erfolgt. So können längere Kennwortänderungsintervalle und kürze Passwörter implementiert werden. Dies kommt dadurch natürlich auch den Benutzern entgegen, wodurch ebenfalls die Akzeptanz steigen wird.
Einzig und allein bei Laptops im Außeneinsatz ergibt sich eine etwaige Änderung. Hierbei ist es vorteilhaft, wenn die bereits oben angesprochene USB-Variante in Kombination mit dem Laptop eingesetzt werden muss, um eine Verbindung mit dem Firmennetzwerk zu erlauben. Zusätzlich muss gewährleistet werden, dass der Datenaustausch verschlüsselt erfolgt. Dabei können Hybrid-Verfahren zum Aufbau einer sicheren Kommunikation eingesetzt werden. Zusätzlich muss die Festplatte der Laptops verschlüsselt werden, damit bei Diebstahl keine Firmendaten in die falschen Hände geraten. Diese Verschlüsselung passiert vorzugsweise hardwaremäßig. Zur Aktivierung des Laptops sollte zusätzlich ein Hardware-PIN notwendig sein, der vor Start des BIOS eingegeben werden muss, damit der Laptop überhaupt bootet. Ein zweiter PIN ermöglicht dann erst den Zugriff auf die verschlüsselte Festplatte.

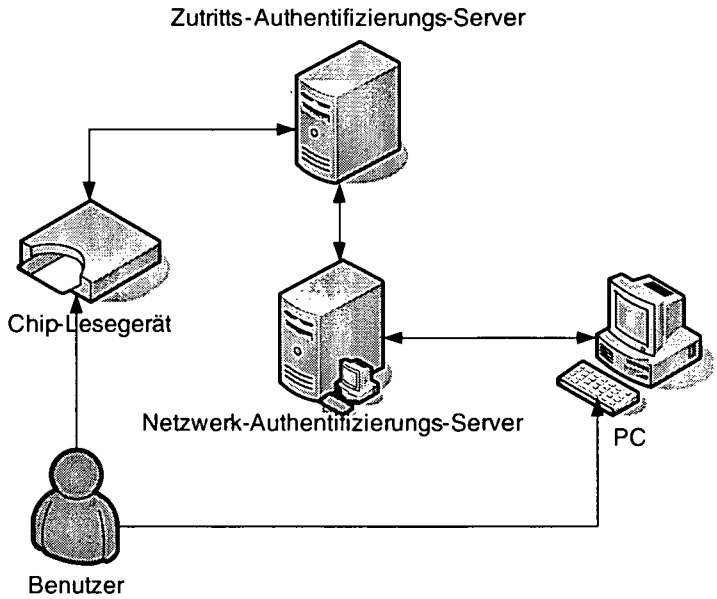


Abbildung 18: Modell Zutrittssystem mit Chip

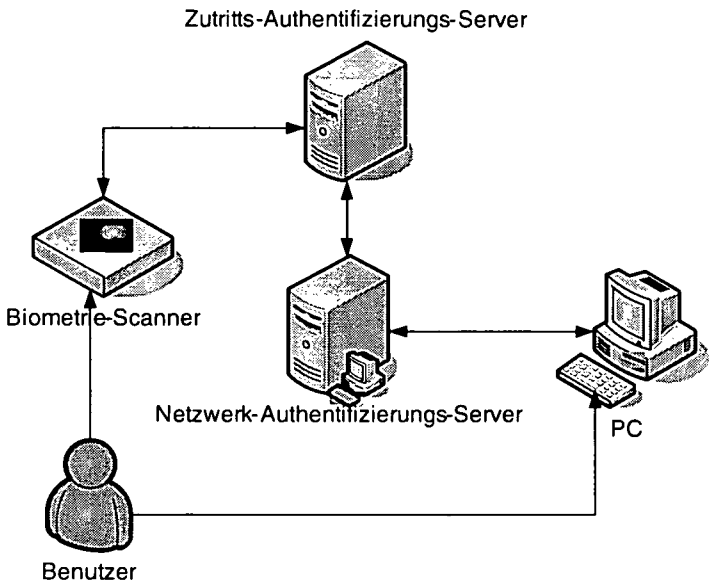


Abbildung 19: Modell Zutrittssystem mit Biometrie

17.1.1.1 Design der Authentifizierungs-Software

Das Design und die Implementation einer solchen Software gestaltet sich nicht sonderlich schwierig. Je nachdem welches Authentifizierungs-System an den PCs verwendet wird muss in der Software eine Schnittstelle existieren, welche Benutzer-Accounts aktivieren, bzw. deaktivieren kann. Die Software sollte dabei für die gebräuchlichsten Netzwerkbetriebssysteme, wie Windows NT und Active Directory, Novell und UNIX-Systeme Schnittstellen anbieten. Damit kann die Software auch in heterogenen Umgebungen universell eingesetzt werden. Umgekehrt muss natürlich auch eine Schnittstelle zum Eingangsauthentifikationssystem integriert sein. Hierbei wäre noch zu evaluieren, welche die gebräuchlichsten Systeme in diesem Bereich darstellen. Weiters muss die Software über eine Datenbank verfügen. Diese Datenbank enthält die Zuordnung zwischen Chip-Tokens bzw. biometrischen Merkmalen und dem Netzwerk-Benutzer-Account. Weiters muss in der Software ein Timer integriert werden, welcher für jeden Benutzer individuell oder wahlweise auch global gesetzt werden kann.
Eine Erweiterung dieser Software, wäre die Anbindung an SAP-Systeme, Großrechner und dergleichen. Hierbei werden die entsprechenden Benutzer-Accounts auf den einzelnen Systemen ebenfalls erst nach erfolgreicher Eingangsauthentifizierung aktiviert.

17.1.1.1.1 Architektur der Authentifizierungs-Software

Die Software besteht aus folgenden Komponenten, welche in Abbildung 20 und Abbildung 21 dargestellt wird:

- Chip-Komponente: Diese Komponente liest die Daten, welche vom Chip-Lesegerät empfangen werden.

Oder

- Biometrie-Komponente: Diese Komponente liest die Daten, welche vom Biometrie-Lesegerät empfangen werden.
- Datenbank-Komponente: Diese Komponente stellt die Verbindung mit der Datenbank her.
- Netzwerk-Authentifizierungs-Komponente: Diese Komponente kommuniziert mit dem Netzwerk-Authentifizierungs-Server und aktiviert oder deaktiviert dort Benutzeraccounts.

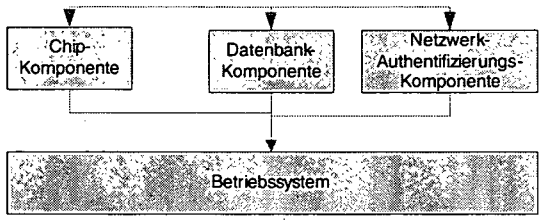


Abbildung 20: Architektur mit Chip

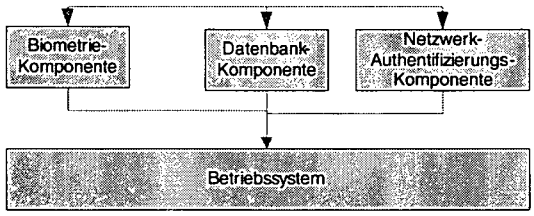


Abbildung 21: Architektur mit Biometrie

17.1.1.1.1.1 Schnittstellen

Die Software stellt folgende Schnittstellen zur Verfügung:

- Chip-Datenbank-Schnittstelle: Diese Schnittstelle dient für die Kommunikation zwischen Datenbank und den empfangenen Chip-Daten.

Oder

- Biometrie-Datenbank-Schnittstelle: Diese Schnittstelle dient für die Kommunikation zwischen Datenbank und den empfangenen Biometrie-Daten.
- Datenbank-Netzwerk-Authentifizierungs-Schnittstelle: Diese Schnittstelle stellt den Konnex zwischen Chip- bzw. Biometrie-Daten und den Netzwerk-Anmeldedaten her.

Zusätzlich besitzen sämtliche Komponenten eine Schnittstelle zum Betriebssystem. Besonders interessant ist jene zwischen der Netzwerk-Authentifizierungs-Komponente und dem Betriebssystem. Diese ist nämlich für die Aktivierung und Deaktivierung der Benutzeraccounts zuständig und muss, da es eine Vielzahl von gebräuchlichen Betriebssystemen gibt, diese auch unterstützen.

17.1.2 Verbesserung der LAN-Sicherheit

Auch für die Verbesserung der LAN-Sicherheit gibt es zwei praktikable Ansätze. Diese sollen im Folgenden dargestellt werden.

17.1.2.1 Hardware-Crypto-Einheiten

Bei diesem Ansatz sollten sämtliche Netzwerkkomponenten, wie Netzwerkkarten, Hubs, Switches und dergleichen mit Hardware-Crypto-Einheiten ausgestattet werden. Somit wird sichergestellt, dass über jedes Kabel nur verschlüsselte Daten ausgetauscht werden können. Damit haben Paket-Sniffer keine Chance mehr kompromittierende Daten zu erfassen.
In den Hardware-Crypto-Einheiten können Hybrid-Verfahren zum Aufbau einer sicheren Kommunikation eingesetzt werden. Dies bietet den Vorteil, dass zum Schlüsselaustausch

langsame asymmetrische Verfahren zum Einsatz kommen, und danach die Daten mit schnellen symmetrischen Verfahren ver- und entschlüsselt werden können. Wichtig ist hierbei aber eine Standardisierung um die Interoperabilität der einzelnen Geräte untereinander sicherzustellen. Dies ist sicher einer der am schwierigsten in den Griff zu bekommenden Probleme. Selbst heutzutage verwenden verschiedene Hersteller gänzlich verschiedene, wenn nicht gar proprietäre Protokolle um Daten mit anderen Geräten auszutauschen. Erst wenn eine Standardisierung sich durchsetzt, werden Firmen auf solche Lösungen zurückgreifen. Dabei müssen einerseits die Protokolle, als auch die Verschlüsselungsverfahren selbst im Standardisierungsprozess berücksichtigt werden.

17.1.2.2 Segmentierung durch Firewalls

Neben diesen Verschlüsselungssystemen sollten zusätzlich interne Firewalls im LAN platziert werden, um besonders sensible Bereiche vom restlichen Netzwerk abzuschirmen. Dabei sind die Policys auch im Hinblick auf Würmer, Viren und dergleichen derartig anzupassen, dass nur die für die entsprechenden Anwendungen notwendigen Ports verfügbar sind. Dies bietet auch den Vorteil, dass selbst wenn ein Angreifer die externe Firewall überwunden hat, die Chancen gering sind, dass auch die interne Firewall geknackt werden kann, da hier nur wenige unbedingt notwendige Protokolle durchgeschleust werden, und damit etwaige Sicherheitslücken wesentlich geringer sind, als bei externen Firewalls, welche eine Vielzahl von Protokollen erlauben muss.

17.2 Weiterentwicklung des SMTP-Protokolls

Das größte Problem, das sich derzeit beim SMTP-Protokoll zeigt, ist, dass es derzeit auf der Server-Seite keine Möglichkeit gibt den Absender zu authentifizieren. In der heutigen Zeit, wo Würmer und Viren in großen Mengen über das Medium E-Mail in private Netze eindringen, wird es notwendig, den Absender eindeutig identifizieren zu können. Derzeit gibt es zwar schon Lösungen, die auf Client-Seite eingesetzt werden können (z.B. PGP). Hierbei ist einerseits der Anwender der Schwachpunkt, und andererseits müssen beide Kommunikationspartner über die gleiche Software verfügen. Dies sind beides Schwachpunkte, welche durch eine serverseitige Realisierung ausgemerzt werden könnten.

17.2.1 Anforderungen an einen sicheren SMTP-Server

Die erste Anforderung wäre ein sicheres SMTP-Protokoll, welches Mails nur über SSL-Verbindungen annimmt. Dieses so genannte SSMTP gibt es bereits. Dies allein ist aber nicht ausreichend. Geht man von dem Konzept der digitalen Signatur aus, so wäre es möglich, dass der Server die Signatur jedes E-Mails überprüft, und mithilfe von zentralen Zertifizierungsstellen die Authenzität des Absenders überprüft. Dies bäte den Vorteil, dass jeder Mail-Empfänger immer sicher sein kann, dass das Mail wirklich von dem „angeblichen" Absender stammt. Der Benutzer muss in diesem Fall weder spezielle Software installieren, noch sich mit der Konfiguration und Bedienung der Software auseinandersetzen.

17.2.2 Ablauf der Authentifizierung

Wird ein E-Mail versandt, und wird dieses vom SMTP-Server empfangen, überprüft dieser bei einer zentralen Zertifikatsstelle die Authenzität des Absenders. Ist die Bestätigung positiv, wird das Mail zugestellt (Abbildung 22). Für den Umgang mit nicht authentifizierten Mails beschreibt das nächste Kapitel einige Möglichkeiten und Verfahrensweisen.

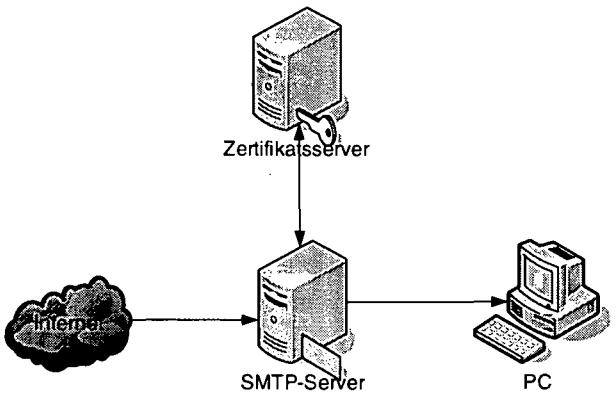


Abbildung 22: Sicherer SMTP-Server

17.2.3 Verfahrensweisen im Umgang mit nicht authentifizierten Mails

Kann der Absender der Mail nicht eindeutig identifiziert werden, gibt es verschiedene Möglichkeiten, wie mit diesen Mails verfahren wird. Die erste Möglichkeit ist, dass solche Mails prinzipiell blockiert werden, und der Absender eine Verständigung bekommt, dass nur signierte Mails angenommen werden. Die zweite Möglichkeit besteht darin, dass solche E-Mails in einer zentralen Quarantäne aufbewahrt werden, und dass von Seiten des Virenschutzes mindestens zwei Updates der Virendefinitionsdateien abgewartet werden, und die Mails sodann mit diesen neuen Definitionen erneut überprüft werden. Ist der Zeitrahmen abgelaufen, und wurden keine Viren gefunden, so wird das Mail an den Empfänger zugestellt. Dadurch ergeben sich zwar Verzögerungen, aber es werden nicht prinzipiell alle unauthentifizierten Mails abgeblockt, vor allem deshalb, da am Anfang der Einführung solcher Technologien nicht damit gerechnet werden kann, dass jeder Absender auch über ein zentrales Zertifikat verfügt. Hier ist vor allem auch der Gesetzgeber gefragt, sicherzustellen, dass es eine eindeutige Regelung bezüglich der Authenzität von E-Mails gibt. Eine weitere Möglichkeit ist, dass unauthentifizierte Mails zuerst von einem Administrator manuell auf Inhalt und Viren überprüft wird. Hier ergibt sich aber sicherlich ein Konflikt mit dem Datenschutz. Deshalb ist diese Möglichkeit zu verwerfen. Die letzte und wohl strengste Alternative ist, dass unauthentifizierte Mails gelöscht werden, und auch der Absender bekommt keine Benachrichtigung, dass sein Mail nicht akzeptiert wurde. Diese Variante ist sicherlich die restriktivste. Eine Anwendung empfiehlt sich jedenfalls erst dann, wenn jeder über ein zentrales Zertifikat verfügt.

17.3 Entwicklung neuer Netze in der Zukunft

Für die privaten Netzwerke heutzutage gibt es bereits viele Lösungen, welche die Sicherheit optimieren oder zumindest versuchen diese zu verbessern. Technologien, wie Firewalls, Intrusion Detection Systeme, Virenschutzlösungen und dergleichen bieten bei richtigem Einsatz und korrekter Konfiguration einen guten Schutz für verkabelte Netzwerke. Die Netzwerke der Zukunft werden sich aber von denen heutzutage grundlegend unterscheiden. Die Kommunikation wird immer mehr in Richtung drahtlos gehen, was bedeutet, dass der Traffic über Funkverbindungen extrem ansteigen wird. Die Technologien die heute im Einsatz sind können aber meist die Anforderungen solcher drahtloser Netze nicht mehr erfüllen.

17.3.1 Problematik

Durch die fortschreitende „Vermobilisierung" entsteht der Bedarf der mobilen Anwender jederzeit und von überall auf die Firmendaten zugreifen zu können. Betrachtet man nun die mobilen Netzwerke von heute, wie GSM und WLAN, so stellt sich die Frage, wie diese Netzwerke sicherer gemacht werden können. Bereits bestehende Lösungen lassen sich nicht so einfach von verkabelten Netzen auf Funk-Verbindungen übertragen, da diese ein höheres Potential an potentiellen Angriffsmöglichkeiten bieten. Besonders die Gefahr des Abhörens kommt hier sehr stark zum Tragen, da das Medium Luft dafür geradezu prädestiniert ist. Hier sind intelligente Verschlüsselungsverfahren gefragt, die nicht so einfach geknackt werden können. Andererseits müssen selbstverständlich auch die Anwender für die Gefahrenpotentiale sensibilisiert werden.

17.3.2 Lösungsmöglichkeiten

Einerseits kann dies erreicht werden durch „Mobile Security NG", welches im nächsten Anschnitt diskutiert wird. Andererseits wird es auch einen Boom bei Virtuellen privaten Netzen geben. Keine Firma kann es erlauben, dass Daten, welche über Funk übertragen werden einfach abgehört werden können, besonders dann nicht wenn es sich um sensible Firmendaten handelt. Der Einsatz von VPN für mobile Geräte jeglicher Art hat deshalb absolute Priorität. Es muss sich natürlich nicht unbedingt definitiv um ein VPN handeln, wie wir es heute verstehen. Es geht prinzipiell nur darum, dass Daten vom mobilen Gerät bis zum Gateway in das Firmen-LAN verschlüsselt übertragen werden. Dabei ist natürlich darauf zu achten, dass die Verschlüsselung selbst nicht knackbar ist, und die verwendeten Protokolle permanent verifiziert und weiterentwickelt werden, damit ein Hacken somit unmöglich wird, bzw. zumindest sehr erschwert wird.

17.3.3 Zusammenfassung

Wie man sieht, gibt es in der Zukunft gänzlich andere Anforderungen an die Sicherheit von Systemen. Besonders der mobile Bereich muss besser geschützt werden, als dies derzeit der Fall ist. Verkabelte LANs werden zwar weiterhin bestehen und auch weiterhin enorm wichtig sein, aber hier werden die Anforderungen sich nur durch den Einsatz von Voice over IP ändern. Hierbei müssen sowohl Firewalls als auch Intrusion Detection Systeme dahingehend angepasst werden, dass auch dieser Traffic überwacht werden kann. Auch bei den Virenschutzlösungen könnte es einige Veränderungen durch Voice over IP geben, da dies neue Möglichkeiten für Angriffe durch Würmer oder Viren mit sich bringen könnte. Definitiv kann gesagt werden, dass das Hauptaugenmerk auf der sicheren Übertragung von mobiler Kommunikation liegen wird.

17.4 Zukünftige Entwicklung der Chips

Bereits heutzutage werden Chips in vielen Bereichen eingesetzt. Von der Bankomatkarte über Zutrittssysteme bis zum Handy sind Chips bereits zu finden. Für die Zukunft kann erwartet werden, dass der Einsatz von Chips weiter ausgedehnt werden wird. Die große Vision ist, dass sich berührungslose Chips in allen Alltagsdingen enthalten sein werden. Dies betrifft sowohl banale Supermarktartikel, Kleidung, elektronische Geräte, Einrichtungsgegenstände, Bücher usw. Dieser abschnitt gibt nur einen kurzen Überblick. Eine detaillierte Erläuterung wird im Kapitel 18.16 dargestellt.

17.4.1 Problematik

Der Einsatz von Chips in allen nur erdenklichen Alltagsgegenständen wirft aber auch große Probleme auf. Ein großes Problem bei dieser Entwicklung ergibt sich durch die mögliche Kommunikation der Chips untereinander. So ist es durchaus vorstellbar, dass zum Beispiel bei Betreten eines Modehauses, alle Chips in meinen Kleidungsstücken abgefragt werden. So lässt sich für das Modehaus feststellen, welche Marken ich trage, wie alt die Kleidungsstücke sind, welche Farben die Kleidungsstücke haben usw. und der Verkäufer kann mit diesen Informationen versorgt werden. Nach dem Einkauf, können gekaufte Kleidungsstücke automatisch zu meinen Kundendaten ergänzt werden, was wiederum diverse marketingtechnische Vorteile für das Modehaus bringt. Anhand dieses Beispiels lässt sich sehr gut erkennen, wo hier die Problematik liegt. Für das Marketing handelt es sich um die Erfüllung eines Traumes, aber für den Einzelnen bedeutet dies einen starken Einschnitt in die Privatsphäre. Sind Informationen auf den Chips nicht so geschützt, dass diese nicht beliebig ausgelesen werden können, so ergibt sich die an dem Beispiel dargestellte Problematik. In Firmen wäre es durchaus vorstellbar, wenn ich einen Raum betrete, dass der Chip meines Firmenausweises abgefragt wird, welche Temperatur ich bevorzuge, ob ich ein Anhänger von geöffneten Fenstern bin usw. Dies ist zwar einerseits sehr komfortabel und praktisch, so dass wen ich einen Raum betrete dieser raschestmöglich meinen Bedürfnissen entsprechend temperiert wird. Hier ergibt sich aber noch stärker, als in dem ersten Beispiel die Problematik der Anonymisierung. Es ist zwar definitiv sinnvoll, dass eine Zuordnung zwischen Informationen, die auf dem Chip gespeichert sind existieren, und meiner Person existieren, dass aber besonders aus Log-Files nicht ersichtlich ist, dass genau ich mich zu einer bestimmten Zeit in einem bestimmten Raum aufgehalten habe. Hier ist eine Anonymisierung sehr wichtig, da dies sonst sehr leicht von der Geschäftsleitung für eine totale Überwachung der Mitarbeiter ausgenutzt werden könnte. Die Aufhebung dieser Anonymisierung sollte nur durch den Betriebsrat möglich sein, und auch nur dann, wenn gegen einen bestimmten Mitarbeiter ein plausibler Verdacht z.B. auf Diebstahl besteht.

17.4.2 Lösungsmöglichkeiten

In diesem Bereich Lösungen zu finden, gestaltet sich als relativ schwierig, da sowohl die an den Entwicklungen beteiligten Firmen als auch Konsumentenschützer in den Prozess eingebunden werden müssen. Auch der Staat trägt in dieser Hinsicht eine große Verantwortung, und muss mit gesetzlichen Regelungen Rahmenbedingungen schaffen, sodass die totale Überwachung nicht einmal zur Wirklichkeit wird. Eine denkbare Möglichkeit wäre, wenn man das Beispiel der Fernwartung eines elektronischen Gerätes betrachtet, dass einerseits durch den Service-Techniker zwar das genaue Modell identifizierbar ist, aber nicht die weltweit eindeutige Kennung des Gerätes ersichtlich ist. Besonders bei elektronischen Geräten ist es wichtig, dass Diagnose- und Fehlerprotokolle nur für den Techniker selbst abrufbar sind, und auch Updates zur Fehlerbeseitigung nur durch autorisierte Personen erfolgen kann. Dafür sind einerseits Authentifizierungsmaßnahmen notwendig, die nicht beeinflussbar sind, wie z.B. durch Chip-Karten und andererseits muss die Kommunikation mit strengen kryptographischen Verfahren, wie z.B. IPSec gesichert werden, damit ein Abhören unmöglich wird.

17.4.3 Zusammenfassung

Besonders das Thema der Chip-Integration in alle Alltagsgegenstände gehört zu einem der zentralen Problempunkte in der Zukunft. Diese Entwicklung kann bei mangelhafter Steuerung zu einer Welt der totalen Überwachung führen. Andererseits eröffnet diese Entwicklung gänzlich neue Angriffsmöglichkeiten. Nicht allein der Computer wird zum Ziel von Angriffen, sondern auch alle anderen Gegenstände, welche über integrierte Chips verfügen. So könnte ein mit Viren oder Würmern infizierter Kühlschrank mit integriertem Chip auch andere elektronische Haushaltsgeräte mit infizieren. Dadurch könnten Brände, Wasserschäden und dergleichen auch in Wohnhäusern allein durch Viren und Würmer rapide zunehmen. Man kann aber keinerseits so blauäugig sein, und darauf vertrauen, dass Menschen vernünftig genug sind, solche Angriffe nicht zu initiieren. Durch Tools, welche vom Internet herunter geladen werden können, ist es sogar Laien möglich Viren und Würmer selbst zu erstellen, wobei meist das Gefahrenpotential für den Laien unabschätzbar ist. Dadurch wird das Unwissen zur Hauptgefahr in der Zukunft. Auch das Thema der Anonymisierung wird in einer solchen Welt zu einem zentralen Thema, wobei Regulierungen dazu rasch greifen müssen, um etwaigen Missbrauch schnellstmöglich zu unterbinden. Zusätzlich muss auf der technischen Seite noch viel passieren, denn auch für Firmen werden miteinander kommunizierende Chips zu einem schwer kontrollierbaren Gefahrenpotential. Dazu müssen Informationen auf den Chips speziell geschützt werden, damit diese nicht von jedermann ausgelesen werden können. Andererseits muss aber auch die Kommunikation einerseits der Chips untereinander als auch andererseits mit externen Teilnehmern mit starker Verschlüsselung implementiert werden, damit Hacker sich in diese Kommunikationsprozesse nicht einschleusen können.

17.5 Sicherheit durch Zentralisierung

Durch den historisch bedingten dezentralen Aufbau des Internet sind viele Sicherheitsprobleme erst entstanden. Durch die prinzipiell mögliche Kommunikation von jedem mit jedem sind Systeme erst angreifbar geworden. Zwar bieten Firewalls, Intrusion Detection Systeme und Virenschutzlösungen mehr Sicherheit, doch lösen sie beim Problem der Dezentralisierung nicht die Ursachen.

17.5.1 Problematik

Die Problematik entsteht durch jede Verbindung zum Internet, welche nicht hinter einer Firewall initiiert wird. Dies sind z.B. alle Internetverbindungen von privaten Zugängen. Sobald die Verbindung besteht, ist das Endgerät von jedem beliebigen anderen Endgerät erreichbar. Dieser Abschnitt soll zeigen, wie mit einer vorsichtigen Zentralisierung diese Problematik entscheidend verbessert werden kann.

17.5.2 Lösungsmöglichkeiten

Eine Variante hierfür wäre der so genannte „Secure Provider". Seine Aufgaben sollen im Folgenden diskutiert werden.
Das Prinzip dieses Ansatzes ist, dass der Provider in diesem Fall nicht jegliche Kommunikation zwischen Kunde und dem Internet zulässt. Hierfür wird beim Aufbau der Verbindung eine VPN-Verbindung zwischen Kunde und Provider hergestellt. Jegliche Kommunikation kann dann nur mehr über diese VPN-Verbindung laufen. Der Provider selbst verfügt einerseits über eine Firewall, die so konfiguriert ist, dass der Kunde nur bestimmte, als sicher anzusehende Dienste nutzen kann. Dies könnten z.B. E-Mail, Web und FTP sein. Alle anderen Verbindungsversuche werden blockiert. Zusätzlich muss der Provider über ein Intrusion Detection System verfügen, sodass jeglicher Einbruchsversuch in das Netzwerk des Providers erkannt und blockiert wird. Weiters muss der Provider über ein zumindest zweistufiges Virenschutzsystem verfügen, bei dem aber unbedingt zwei verschiedene Produkte von verschiedenen Herstellern eingesetzt werden müssen. Weiters müssen sämtliche eingehenden und ausgehenden E-Mails auf Viren überprüft werden. Optional kann der Provider auch einen Content Filter einsetzen, um so Webseiten mit potentiell kriminellen oder anstößigen Inhalten automatisch zu blockieren.

17.5.3 Zusammenfassung

Besonders durch eine Zertifizierung, die es Providern ermöglicht, als sicher eingestuft zu werden, bieten auch dem Kunden den Vorteil, dass er sicher sein kann, dass sein Endgerät nicht permanent Angriffen aus dem Internet ausgesetzt ist. Der Nachteil der sich aber durch einen „Secure Provider" ergibt ist, dass nicht sämtliche Dienste des Internet genutzt werden können. Hier liegt die Entscheidung aber beim Kunden, ob der Sicherheitsgewinn diesen Nachteil aufwiegen kann, oder nicht. Prinzipiell bietet dieser Ansatz den Vorteil, dass Firmen, welche über Heimarbeitsplätze verfügen, dem Mitarbeiter einen Zugang über solch einen „Secure Provider" zur Verfügung stellen können, um somit auch dem Sicherheitsproblem der dezentralen Arbeitsplätze Herr werden zu können.

18 Expertensysteme für automatische Sicherheitseinstellungen

18.1 Einleitung

Durch die steigende Mobilität von Mitarbeitern, und dem dadurch vermehrten Einsatz von Laptops, PDAs und Handys, ergeben sich andere Sicherheitsanforderungen, wie in abgeschirmten lokalen Netzwerken. Die klassischen lokalen Netze verfügen normalerweise über eine oder mehrere Firewalls, die sämtliche Verbindungen nach außen kontrollieren. Diese werden zentral verwaltet und durch Administratoren gewartet und mithilfe von Updates auf dem neuesten Stand gehalten, um bekannt gewordene Sicherheitslücken raschestmöglich zu schließen. Anders verhält es sich mit Mitarbeitern, welche im Außeneinsatz sind und trotzdem einen Zugang zum Firmennetz benötigen. Für diese Geräte soll eine Architektur für eine Sicherheitssoftware diskutiert werden, die es ermöglicht die Geräte mit nur wenigen Eingriffen des Anwenders selbst auf ein Höchstmaß an Sicherheit einzustellen. Die Software, welche in Kleinbetrieben eingesetzt werden kann, soll im weiteren „Mobile Security NG" bezeichnet werden. NG steht hierbei für „Next Generation". Für große Firmen ergibt sich eine etwas andere Architektur. Diese soll ebenfalls diskutiert werden, und die Unterschiede herausgearbeitet werden. Die Software welche hier zur Anwendung kommen soll, wird als „Mobile Security NG Corporate" bezeichnet.

18.2 Anforderungen an „Mobile Security NG"

In diesem Abschnitt sollen die Anforderungen an diese Sicherheitssoftware beschrieben werden.
Die wohl wichtigsten Anforderungen sind einerseits, dass die Software nur ein Mindestmaß an Konfiguration des Anwenders verlangt, und andererseits, dass sie ein Höchstmaß an Sicherheit gewährleistet. Dies begründet sich vor allem darin, dass die meisten Anwender nicht das Wissen besitzen, solche Konfigurationen durchzuführen. Ein intelligenter Automatismus ist deshalb unbedingt notwendig.

Die Software soll hierbei folgende Komponenten untersuchen und optimieren:
Hardware:
- Netzwerkkarten
- WLAN-Karten
- Modems und ISDN-Karten
- Interne Handykarten
- Infrarotschnittstellen

Software:
- Betriebssystemsicherheit
- Virenschutz
- Firewallfunktionalität
- Intrusion Detection

18.3 Software-Komponenten

Die Software besteht aus folgenden Komponenten:

- Firewall-Software: Diese Software-Komponente schützt den Client vor Angriffen aus dem Internet.
- WLAN-Konfigurationssoftware: Diese Software-Komponente konfiguriert das WLAN für maximale Sicherheit.
- Netzwerk- und Modem-Konfigurationssoftware: Diese Software-Komponente konfiguriert sämtliche kabelbasierenden Netzwerkkomponenten.
- VPN-Software: Diese Software-Komponente stellt eine Verbindung zur Firmen-Firewall her.
- OS-Hardening Software: Diese Software-Komponente überprüft das Betriebssystem auf bekannte Sicherheitslücken und installiert bei Bedarf die notwendigen Patches.
- Anti-Virus-Software: Diese Software-Komponente überwacht den Computer in Echtzeit auf mögliche Infektionen durch Viren, Würmer, Trojanische Pferde, und dergleichen.
- Intrusion Detection: Diese Software-Komponente überwacht den Client anhand bekannter Angriffs-Signaturen auf mögliche Angriffe.
- Content Filtering: Diese Software-Komponente blockiert Web-Seiten mit kriminellen oder pornographischen Inhalten.

18.3.1 Software-Architektur

Abbildung 23 zeigt die Architektur von „Mobile Security NG".

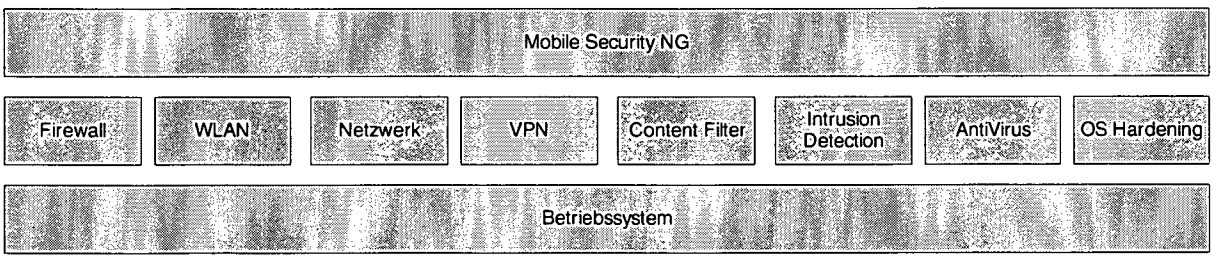


Abbildung 23: Software-Architektur

„Mobile Security NG" integriert somit die oben abgebildeten Software-Komponenten. Dabei existieren sowohl zwischen den einzelnen Teilkomponenten Schnittstellen für die Kommunikation untereinander als auch zwischen Betriebssystem und jeder einzelnen Teilkomponente. Dies ist notwendig, damit die einzelnen Komponenten gemeinsam auf Bedrohungen reagieren können, und damit Veränderungen auf Betriebssystemebene durchgeführt werden können.

18.3.1.1 Schnittstellen

Um ein sicherheitstechnisch adäquates System zu erzeugen, müssen die einzelnen Komponenten miteinander über Schnittstellen kommunizieren können (Abbildung 24). Dieser Abschnitt zeigt, zwischen welchen Komponenten Schnittstellen existieren, und warum diese wichtig sind.

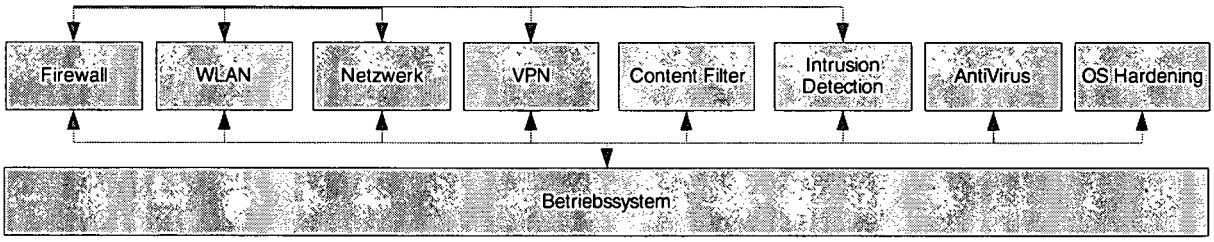


Abbildung 24: Schnittstellen

18.3.1.1.1 Firewall-WLAN und Firewall-Netzwerk Schnittstelle

Diese beiden Schnittstellen verbinden die Firewall mit den aktiven Netzwerkkomponenten des Systems. Damit wird sichergestellt, dass einerseits alle ein- und ausgehenden Pakete von der Firewall erfasst werden und überprüft werden können und andererseits die Firewall im Fall eines Angriffes die WLAN- und Netzwerk-Software zur Umkonfiguration anstoßen kann.

18.3.1.1.2 Firewall-VPN Schnittstelle

Diese Schnittstelle ermöglicht die dynamische Rekonfiguration der Firewallregeln bei Auf- und Abbau von VPN-Verbindungen. Somit wird gewährleiste, dass nur für den jeweiligen Nutzungsfall die richtigen Ports geöffnet werden.

18.3.1.1.3 Firewall-Intrusion Detection Schnittstelle

Diese Schnittstelle ermöglicht die dynamische Rekonfiguration der Firewallregeln bei erkannten Angriffen. Sowohl die Intrusion Detection Software als auch die Firewall können diesen Prozess anstoßen. Die Firewall kann einerseits Pakete an die Intrusion Detection übergeben, sodass diese die Pakete auf etwaige Angriffsmuster überprüfen kann. Umgekehrt kann die Intrusion Detection, welche einen Angriff erkennt, die Firewall dazu anstoßen dynamisch ihre Regelbasis dem Angriff entgegenwirkend zu ändern.

18.3.1.1.4 Betriebssystem-Schnittstellen

18.3.1.1.4.1 Firewall

Diese Schnittstelle bindet die Firewall direkt in das Betriebssystem ein. Somit ist es nicht möglich, Pakete an der Firewall vorbei in das Betriebssystem einzuschleusen. Zusätzlich ermöglicht diese starke Koppelung die dynamische Rekonfiguration der Firewall-Regeln, ohne dabei die Verbindung zu unterbrechen und die direkte Bindung der Firewall auf die Netzwerkkomponenten.

18.3.1.1.4.2 WLAN

Diese Schnittstelle überwacht und verwaltet die im Betriebssystem definierten Drahtlosverbindungen. Dabei werden mögliche falsche Konfigurationen, welche sicherheitsproblematisch sind automatisch geändert.

18.3.1.1.4.3 Netzwerk

Diese Schnittstelle überwacht und verwaltet die im Betriebssystem definierten Netzwerkverbindungen. Dabei werden genau wie bei der WLAN Schnittstelle mögliche falsche Konfigurationen, welche sicherheitsproblematisch sind automatisch geändert.

18.3.1.1.4.4 VPN

Diese Schnittstelle übernimmt den Aufbau und die Verschlüsselung der VPN-Verbindungen.

18.3.1.1.4.5 Content Filter

Diese Schnittstelle überwacht Web-Seiten-Aufrufe, um diese bei inadäquatem Inhalt zu blockieren. Zusätzlich überwacht sie die Installation von ActiveX-Komponenten.

18.3.1.1.4.6 Intrusion Detection

Diese Schnittstelle überwacht Angriffe auf Betriebssystemebene. Sollte ein Angriff durch die Firewall ohne Entdeckung durchgehen, versucht die Intrusion Detection diese Attacke auf Betriebssystemebene zu unterbinden.

18.3.1.1.4.7 AntiVirus

Diese Schnittstelle kommuniziert sowohl mit dem Dateisystem als auch dem Hauptspeicher auf Betriebssystemebene, um Bedrohungen in Echtzeit zu finden und zu eliminieren.

18.3.1.1.4.8 OS Hardening

Diese Schnittstelle überprüft, wenn es sich um ein Windows-System handelt mittels des Microsoft Baseline Security Analyzers und der Windows-Update Funktion auf Updates und gleicht diese mit denen des Security Update Servers ab. Handelt es sich nicht um ein Microsoft-Betriebssystem, werden die Hersteller-Seiten nach Updates durchsucht. Jedenfalls werden nur solche Updates eingespielt, welche am Security Update Server zur Verfügung stehen. Die Untersuchung dient lediglich der Protokollierung. Diese Protokollierung verwendet der Hersteller um den Prozess der Updatefreigabe zu beschleunigen und zu verbessern. Zusätzlich werden auch freigegebene Programm-Updates und Software-Aktualisierungen eingespielt.

18.4 Firewall-Software

Handelt es sich bei dem Client um ein Windows-Betriebssystem, so wird die Internetverbindungsfirewall automatisch deaktiviert (Abbildung 25). Ist bereits eine andere Firewall-Software auf dem Client installiert, so wird der Benutzer darauf aufmerksam gemacht, dass bereits eine Firewall-Software installiert ist, und es wird empfohlen, diese zu entfernen und stattdessen die Firewall-Software von „Mobile Security NG“ zu installieren. Standardmäßig ist die Firewall mit einer Regelbasis ausgestattet, die nur HTTP und die Protokolle für die E-Mail Kommunikation erlauben.

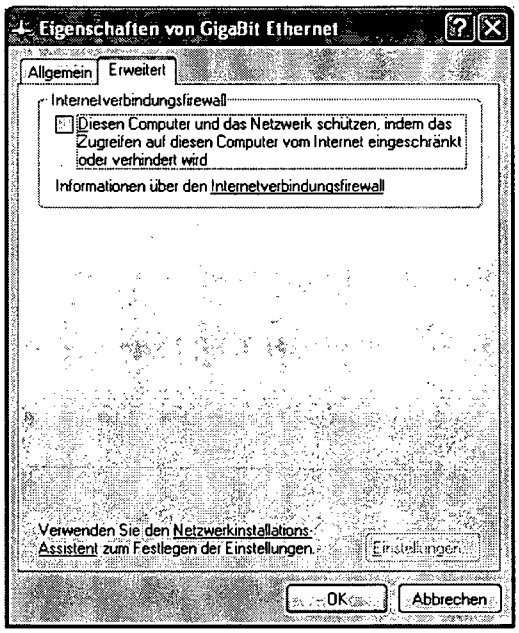


Abbildung 25: Internetverbindungsfirewall

18.5 WLAN-Konfigurationssoftware

Nachdem bei sämtlichen WLAN-Karten, diese einerseits vom Hersteller, und andererseits vom Betriebssystem her mit dem niedrigsten Sicherheitsniveau installiert wird, greift an dieser Stelle die WLAN-Konfigurationssoftware. Diese stellt sicher, dass einerseits die ID der WLAN-Karte auf einen Nicht-Standard-Wert gesetzt wird, und andererseits, dass WEP aktiviert wird. Wie schon in Kapitel 12 gezeigt, ist WEP zwar problematisch, doch solange keine anderen Ansätze existieren, ist dies immer noch wesentlich sicherer, als ohne dieses Protokoll zu fahren.

18.6 Netzwerk- und Modem-Konfigurationssoftware

Diese Software konfiguriert einerseits die kabelbehafteten Netzwerkkomponenten bereits bei der Installation, um die Sicherheit zu erhöhen. Andererseits verfügt die Software über eine Echtzeitkomponente, die das Netzwerk permanent den Gegebenheiten anpasst.

18.6.1 Vorabkonfiguration

Bei der Vorabkonfiguration der Netzwerkkarten werden als erstes der „Client für Microsoft-Netzwerke“ und die „Datei- und Druckerfreigabe für Microsoft-Netzwerke“ deaktiviert. Da diese beiden Dienste nur bei einer Verbindung mit dem Firmen-LAN notwendig sind, und bei reinen Internetverbindungen ein Sicherheitsrisiko darstellen, werden die beiden Dienste standardmäßig deaktiviert (Abbildung 26). Die Sicherheitsproblematik der beiden Dienste besteht darin, dass es bei Aktivierung möglich ist, vom Internet auf den Computer insbesondere auf die Festplatten zugreifen zu können.

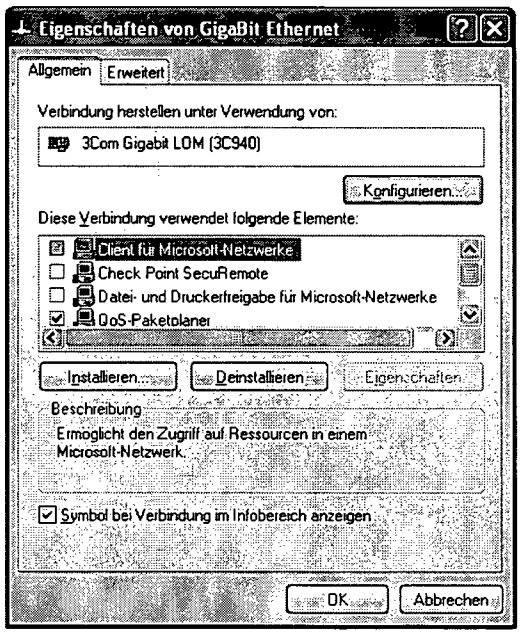


Abbildung 26: Netzwerkkarten-Konfiguration

Bei der Vorabkonfiguration der Modems werden ebenfalls der „Client für Microsoft-Netzwerke“ und die „Datei- und Druckerfreigabe für Microsoft-Netzwerke“ deaktiviert (Abbildung 27).

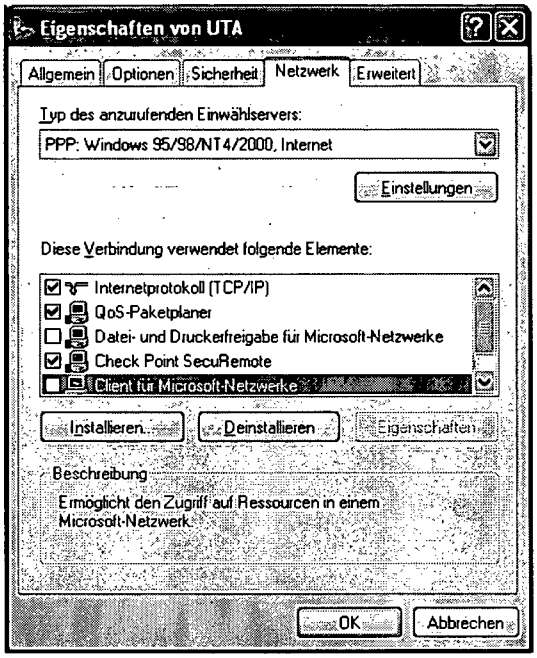


Abbildung 27: Modem-Konfiguration

Zusätzlich dazu wird die Konfiguration dahingehend geändert, dass nur verschlüsselte Kennwörter zugelassen werden (Abbildung 28).

Abbildung 28: Kennwort-Konfiguration

18.6.1.1 Ablauf Vorabkonfiguration

Abbildung 29 zeigt den im vorigen Abschnitt beschriebenen Ablauf der Vorabkonfiguration.

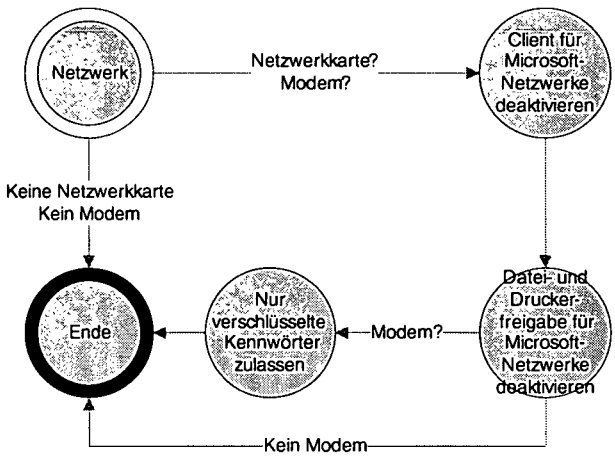


Abbildung 29: Ablauf Vorabkonfiguration

Die Netzwerkkomponente kann dabei folgende vier Zustände annehmen:

- Client für Microsoft-Netzwerke deaktivieren: In diesem Zustand wird auf allen Netzwerk- und DFÜ-Adaptern dieser Dienst deaktiviert.
- Datei- und Druckerfreigabe für Microsoft-Netzwerke deaktivieren: In diesem Zustand wird auf allen Netzwerk- und DFÜ-Adaptern dieser Dienst deaktiviert.
- Nur verschlüsselte Kennwörter zulassen: In diesem Zustand wird auf allen DFÜ-Adaptern diese Option aktiviert.
- Ende: Endzustand. Alle Konfigurationen wurden erfolgreich durchgeführt.

Wird mindestens eine Netzwerkkarte oder ein DFÜ-Adapter oder beides erkannt, werden die einzelnen Zustände linear durchlaufen. Dabei wird in jedem Zustand für alle vorhandenen Adapter die jeweilige Konfiguration durchgeführt, bevor in den nächsten Zustand gewechselt wird. Der Endzustand wird entweder erreicht, wenn alle Konfigurationen erfolgreich durchgeführt wurden, oder keine Netzwerkarten oder DFÜ-Adapter erkannt wurden. Der Endzustand ist ebenfalls vom dritten Zustand erreichbar, falls kein Modem vorhanden sein sollte.

18.6.2 Echtzeitkonfiguration

Bei der Echtzeitkonfiguration, wird die Netzwerkkarte bzw. das Modem bei bereits bestehender Internetverbindung umkonfiguriert. Dies kann einerseits dadurch bedingt sein, dass ein Angriffsversuch gestartet wurde, der entweder von der Intrusion Detection Komponente erkannt wurde, falls der Einbruch erfolgreich verlaufen ist, oder von der Firewall Attacken festgestellt wurden, wodurch es notwendig ist, Maßnahmen zu treffen. Die erste Maßnahme, die die Software trifft, ist die Anforderung einer neuen IP-Adresse am DHCP-Server des Providers. Dadurch kann es passieren, dass die Verbindung zwar kurzfristig getrennt wird, aber eine mögliche Kompromittierung wird somit verhindert. Ist diese Maßnahme nicht erfolgreich, oder verfügt die Internetverbindung über eine fixe IP-Adresse, erhält der Benutzer eine Warnmeldung (Abbildung 30). Danach wird die Verbindung für 10 Minuten getrennt, danach erfolgt automatisch ein neuer Verbindungsversuch.

Abbildung 30: Einbruchsversuch

Erfolgen nach erneuter Verbindung weitere Einbruchsversuche, oder glücken diese, wird eine E-Mail mit Informationen den Einbruch betreffend an den Hersteller der Software versandt, und die Internetverbindung deaktiviert (Abbildung 31). Eine Reaktivierung der Internetverbindung ist nur durch einen Freischaltcode möglich, der vom Hersteller aber erst dann zur Verfügung gestellt wird, wenn das Sicherheitsproblem behoben wurde. Je nach Art des Sicherheitsproblems setzt der Hersteller die entsprechenden Maßnahmen und kontaktiert danach den Anwender.

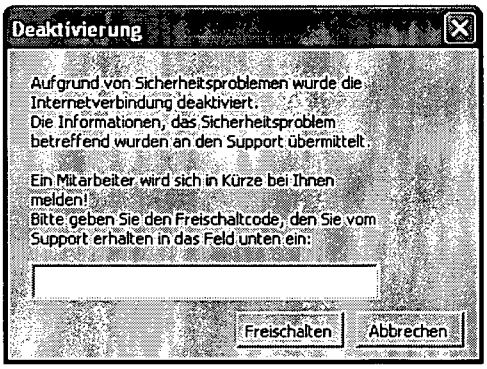


Abbildung 31: Deaktivierung der Internetverbindung

18.6.2.1 Ablauf Echtzeitkonfiguration

Abbildung 32 zeigt den im vorigen Abschnitt beschriebenen Ablauf der Echtzeitkonfiguration.

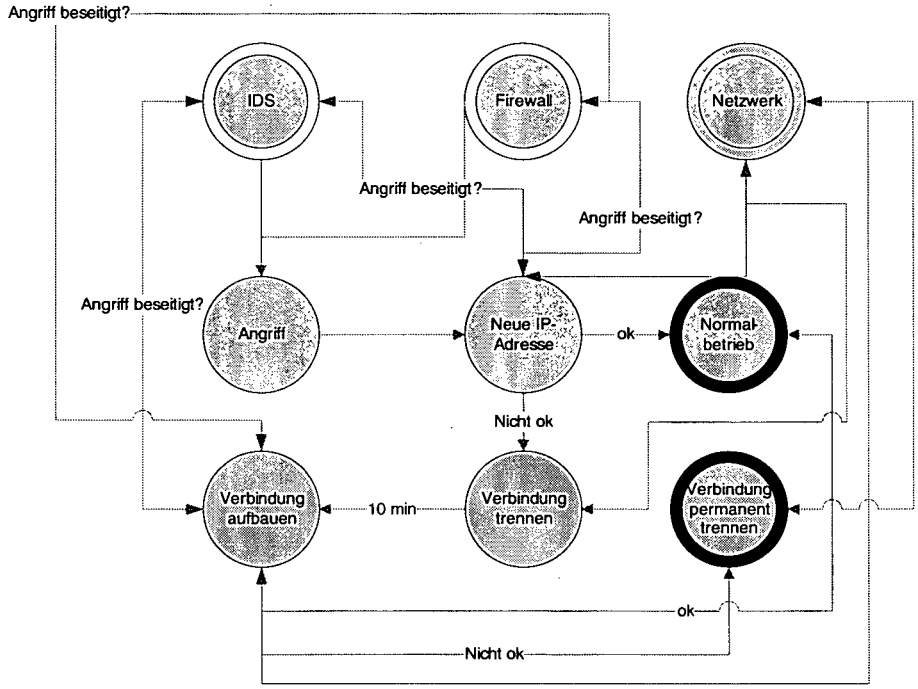


Abbildung 32: Ablauf Echtzeitkonfiguration

Die Intrusion Detection Komponente, die Netzwerkkomponente und die Firewallkomponente können dabei folgende sechs Zustände annehmen:

- Angriff: ein Angriff wurde von der Firewall oder der Intrusion Detection erkannt.
- Neue IP-Adresse: Hierbei wird versucht, eine neue IP-Adresse zu erhalten, um somit die Angriffe auf die alte IP-Adresse zu unterbinden.
- Verbindung aufbauen: Die Netzwerkkomponente stößt einen erneuten Verbindungsaufbau an.
- Verbindung trennen: Die Netzwerkkomponente stößt einen Verbindungsabbau an.
- Normalbetrieb: Endzustand. Ist der Angriff beseitigt, gehen alle Komponenten wieder in den Normalbetrieb über.
- Verbindung permanent trennen: Endzustand. Der Angriff konnte nicht beseitigt werden, die Verbindung ist nicht mehr aufbaubar.

Wird von der Firewall oder der Intrusion Detection ein Angriff erkannt, wird zuerst versucht, eine neue IP-Adresse zu erhalten. Ist dies erfolgreich, und ist der Angriff damit beseitigt, wird in den Normalbetrieb gewechselt. Ist dies nicht erfolgreich, so wird die Verbindung für zehn Minuten getrennt. Danach wird die Verbindung wieder aufgebaut, und festgestellt, ob der Angriff damit beseitigt ist. Ist dies erfolgreich, und ist der Angriff damit beseitigt, wird in den Normalbetrieb gewechselt. Ist dies nicht erfolgreich, so wird die Verbindung permanent getrennt. Ein neuerlicher Verbindungsaufbau ohne Freischaltung des herstellers ist nicht mehr möglich.

18.7 VPN-Software

Dabei handelt es sich um eine Standard-VPN-Software, die es ermöglicht mit den verschiedensten Firewalls sichere Tunnel aufzubauen, wobei die Daten über IPSec verschlüsselt übertragen werden. Die VPN-Software steht auch in enger Verbindung mit der Firewall-Software, um sicherzustellen, dass bei Aufbau des Tunnels zum Firmen-LAN, nur diejenigen Ports geöffnet werden, welche zur VPN-Kommunikation benötigt werden. Versucht nun der Anwender eine Kommunikation mit dem Internet herzustellen, z.B. mit einem Browser, so wird der Browser in Echtzeit so umkonfiguriert, dass dieser den internen Proxy-Server der Firma verwendet. Damit wird wiederum sichergestellt, dass im VPN-Modus keine direkte Kommunikation mit dem Internet möglich ist. Gibt es keinen Proxy-Server, der die Anforderung verarbeiten kann, so erhält der Benutzer eine Warnung, dass im VPN-Modus keine direkte Kommunikation mit dem Internet möglich ist (Abbildung 33). Er kann dann wählen, ob er die VPN-Verbindung trennen möchte oder nicht.

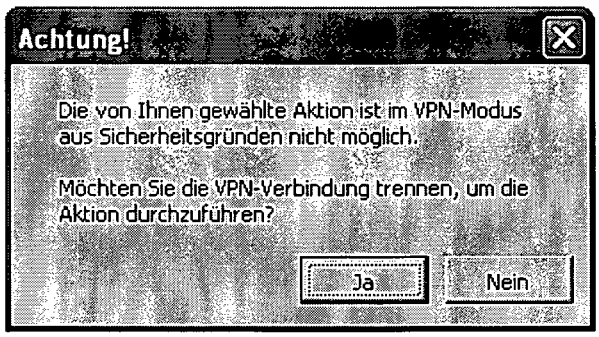


Abbildung 33: VPN-Software

Beantwortet der Benutzer diese Frage mit „Nein“ bleibt die Firewallkonfiguration erhalten, dass nur VPN-Traffic durch die Firewall-Software gestattet wird (Abbildung 34).

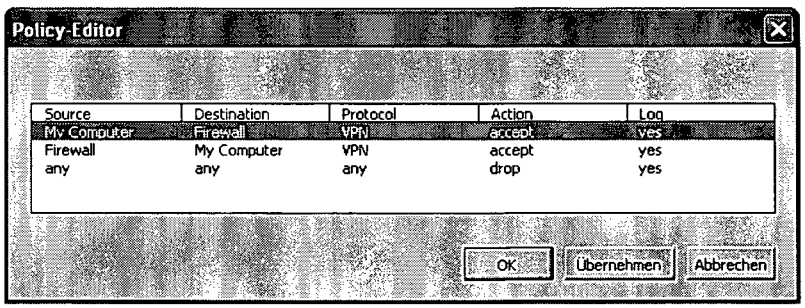


Abbildung 34: Konfiguration VPN-Traffic

Zusätzlich wird bei der entsprechenden Internetverbindung der „Client für Microsoft-Netzwerke“ und die „Datei- und Druckerfreigabe für Microsoft-Netzwerke“ aktiviert (Abbildung 35). Dies ist erforderlich, damit ein Zugriff auf Daten, Programme und Drucker möglich ist.

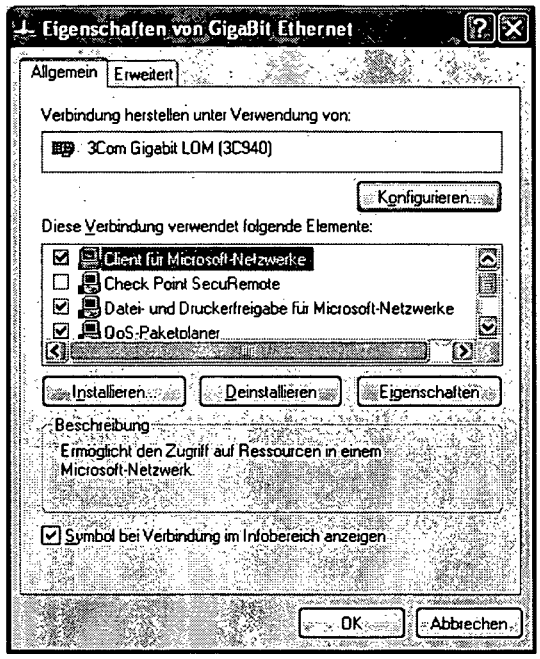


Abbildung 35: Aktivierung bei VPN-Verbindung

18.7.1 Ablauf VPN

Abbildung 36 zeigt den vorher beschriebenen Ablauf in Form eines Ablaufdiagramms.

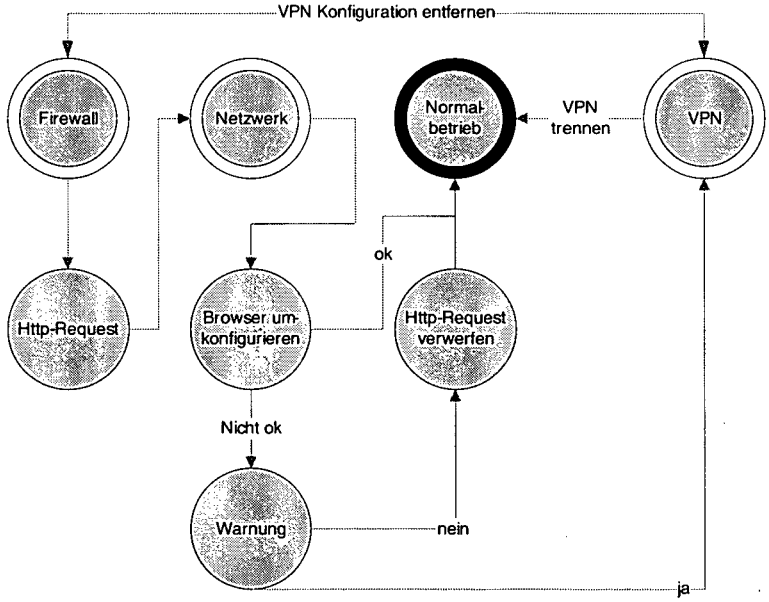


Abbildung 36: Ablauf VPN

Die VPN Komponente, die Netzwerkkomponente und die Firewallkomponente können dabei folgende fünf Zustände annehmen:

- http-Request: Der Benutzer versucht im VPN-Modus eine Webseite direkt ohne einen firmeninternen Proxy anzusteuern.
- Browser umkonfigurieren: Die Netzwerkkomponente versucht, den Browser auf einen firmeninternen Proxy-Server umzukonfigurieren.

- Warnung: Schlägt die Proxy-Einstellung fehl, wird dem Benutzer eine Warnung präsentiert. Er muss wählen, ob er den VPN-Modus verlassen möchte, oder nicht.
- http-Request verwerfen: Soll der VPN-Modus erhalten bleiben, so wird der http-Request verworfen.
- Normalbetrieb: Endzustand. Alle Komponenten befinden sich wieder im Normalbetrieb.

Erkennt die Firewall im VPN-Modus, dass versucht wird eine direkte Verbindung zum Internet herzustellen, signalisiert diese der Netzwerkkomponente, dass diese den Browser auf einen firmeninternen Proxy umleitet. Diese versucht somit den Browser umzukonfigurieren. Ist dies erfolgreich, so wird die Web-Seite angezeigt, und in den Normalbetrieb gewechselt. Kann der Browser aber nicht umkonfiguriert werden, so muss der Benutzer wählen, ob er im VPN-Modus bleiben möchte. Entschließt sich der Anwender in diesem Modus zu bleiben, wird der Request auf die Web-Seite verworfen, und in den Normalbetrieb gewechselt. Ansonsten wird von der VPN-Komponente die VPN-Verbindung getrennt, und die Firewall stellt die normale Internetkonfiguration wieder her. Auch in diesem Fall wird in den Normalbetrieb gewechselt.

18.8 OS-Hardening Software

Diese Komponente überwacht und analysiert das Betriebssystem auf Sicherheitslücken. Die Software steht in enger Verbindung mit dem Security Update-Server, und prüft dort in regelmäßigen Intervallen, ob Updates vorhanden sind. Ist ein Update vorhanden, wird dieses sofort installiert, da am Security Update-Server nur diejenigen Updates verfügbar sind, die bereits getestet wurden, und somit zur Verteilung auf die Clients freigegeben sind. Dies ist eine der Basiskomponenten, da eine Vielzahl von Angriffen auf das Ausnutzen von bereits lange bekannten Sicherheitslücken basieren, für die es oft schon ein Sicherheitsupdate gibt, bevor diese Angriffe gestartet werden. Dies betrifft aber nicht nur Angriffe, sondern auch Bedrohungen durch Viren, Würmer, usw. Zusätzlich zum Betriebssystem überprüft diese Software auch sämtliche installierten Anwendungsprogramme auf Sicherheitsprobleme. So wird zum Beispiel in den Office-Programmen der Makrovirus-Schutz aktiviert, sofern dieser deaktiviert wurde. Für die gängigsten Anwendungsprogramme werden ebenfalls Aktualisierungen durchgeführt. Ist eine Software installiert, die für Sicherheitsprobleme bekannt ist, und ist kein Update vom Server verfügbar, so wird die Software automatisch deinstalliert. Dies ist aber nur eine Option, welche von der Geschäftsleitung definiert werden muss.
Zusätzlich werden sicherheitskritische Optionen des Betriebssystems deaktiviert. Dies betrifft einerseits die Remoteunterstützung und die Remotedesktop-Verbindung. Beide werden aus Sicherheitsgründen deaktiviert (Abbildung 37).

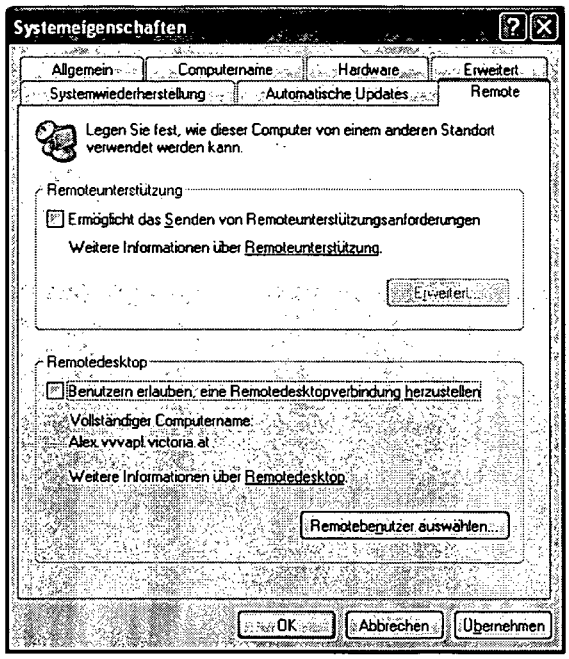


Abbildung 37: Remote

Zusätzlich werden auch die automatischen Updates deaktiviert, da dies von „Mobile Security NG“ und nicht vom Betriebssystem gehandlet wird (Abbildung 38).

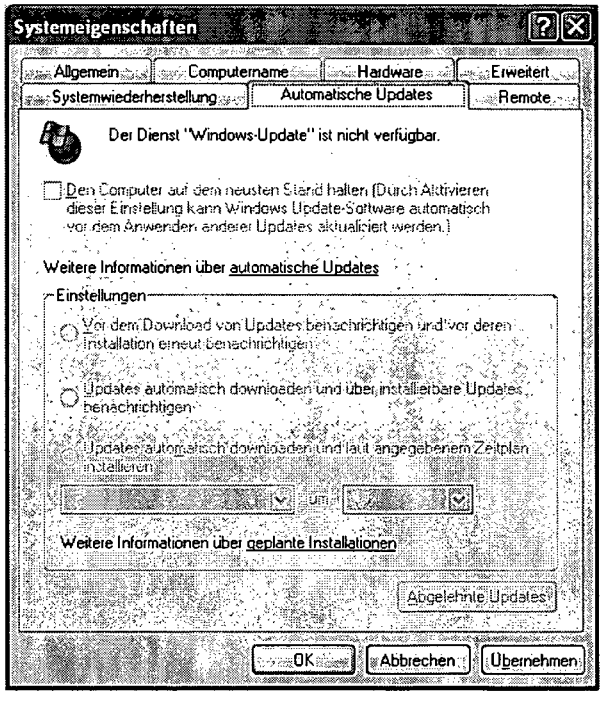


Abbildung 38: Automatische Updates

Ebenfalls deaktiviert wird die Systemwiederherstellung (Abbildung 39), was zwar kein Sicherheitsproblem im eigentlichen Sinn ist, aber ein unnötiges Feature von Windows darstellt.

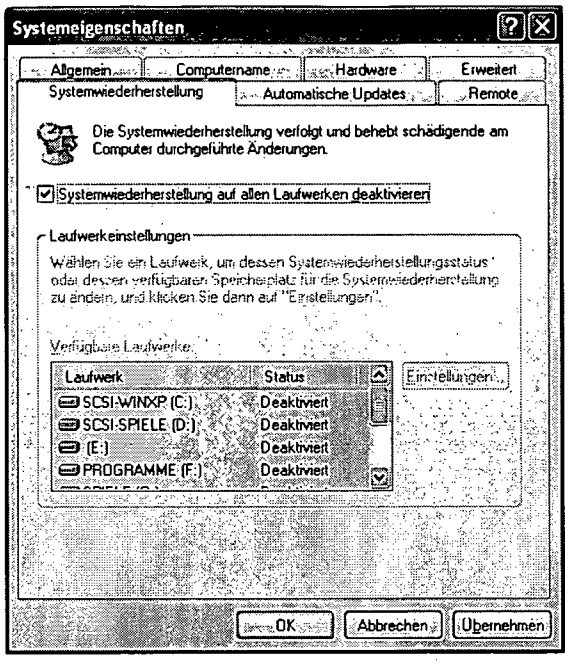


Abbildung 39: Systemwiederherstellung

Als letzter Schritt werden sämtliche Dienste deaktiviert, die nicht benötigt werden (Abbildung 40). Dies erhöht einerseits die allgemeine Performance der Workstation und andererseits treten bestimmte Sicherheitslücken nur bei bestimmten Diensten auf. Dem ist somit Einhalt geboten.

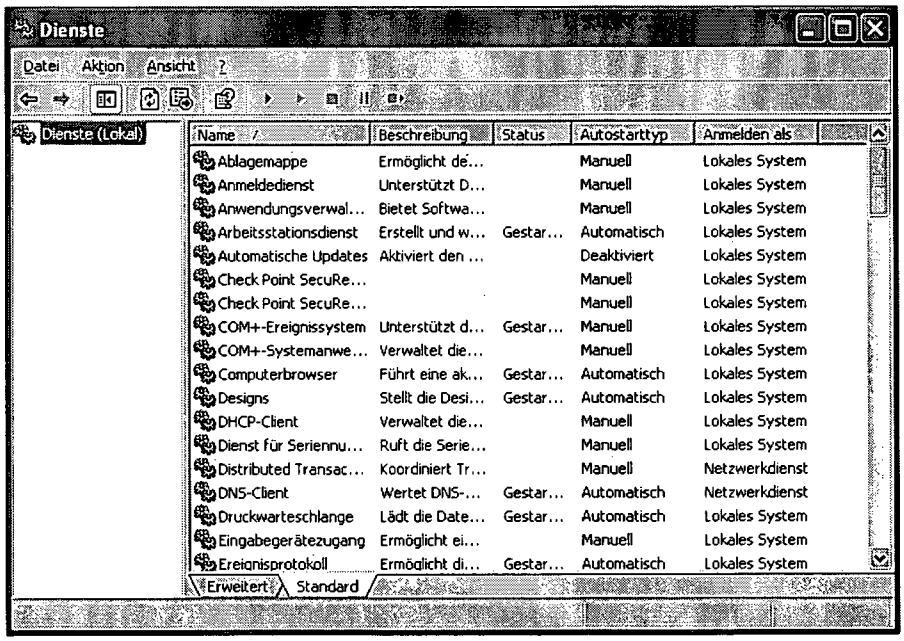


Abbildung 40: Dienste

18.8.1 Ablauf OS-Hardening

Abbildung 41 zeigt den vorher beschriebenen Ablauf in Form eines Ablaufdiagramms.

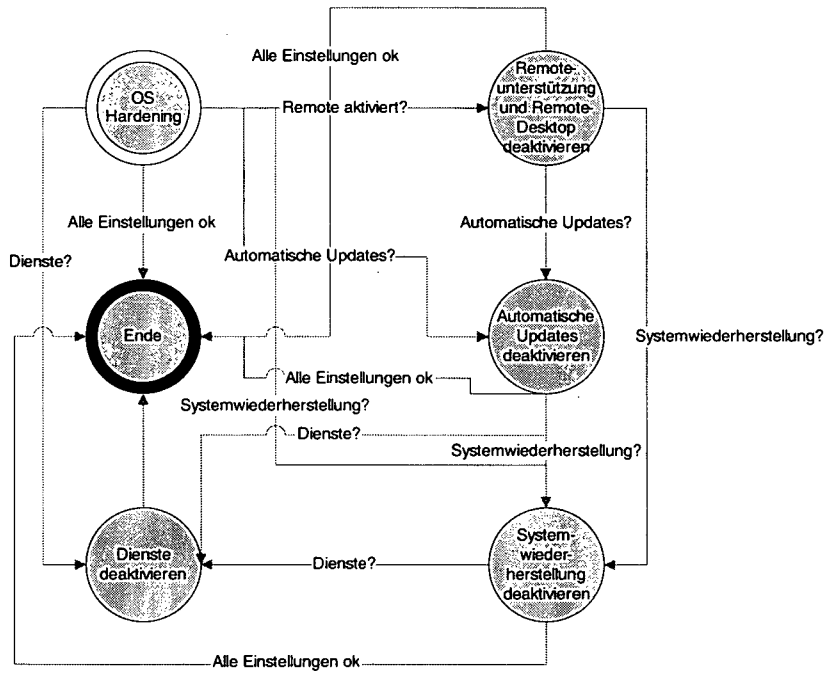


Abbildung 41: Ablauf OS-Hardening

Die OS-Hardening Komponente kann dabei folgende fünf Zustände annehmen:

- Remoteunterstützung und Remote-Desktop deaktivieren: Remoteunterstützung und Remote-Desktop werden deaktiviert.
- Automatische Updates deaktivieren: Automatische Updates werden deaktiviert.
- Systemwiederherstellung deaktivieren: Die Systemwiederherstellung wird deaktiviert.
- Dienste deaktivieren: Nicht benötigte, oder sicherheitskritische Dienste werden deaktiviert.
- Ende: Endzustand. Alle Konfigurationen wurden erfolgreich durchgeführt.

Die OS-Hardening Komponente fragt zuerst ab, ob nicht schon eine, oder alle Einstellungen durchgeführt wurden. Je nach Status werden nur jene Zustände durchlaufen, welche notwendig sind. Dafür wird in jedem Zustand auf die verbleibenden Konfigurationen abgefragt. Sind alle Konfigurationen ordnungsgemäß durchgeführt worden, oder ergab die Abfrage eine bereits erfolgte manuelle Durchführung, so wird der Endzustand erreicht.

18.9 Anti-Virus-Software

Hierbei handelt es sich um eine Standard-Software, die erweitert wurde um anhand von Heuristiken zu versuchen, auch nicht bekannte Viren, Würmer, Trojaner, usw. zu erkennen und zu beseitigen. Die Updates der Virendefinitionen laufen wieder zentral über den Security Update-Server.

18.10 Intrusion Detection Software

Bei der Intrusion Detection Software handelt sich um eine Applikation, die über eine Datenbank verfügt, welche alle bekannten Angriffssignaturen enthält. Diese Datenbank wird ebenfalls über den Update-Server regelmäßig aktualisiert. Findet nun eine Kommunikation statt, welche zu einem der gespeicherten Angriffsmuster passt, so wird dies als Attacke interpretiert. In diesem Fall erhält der Benutzer eine Warnmeldung, dass eine Attacke entdeckt wurde. In diesem Fall versucht die Intrusion Detection Komponente die Firewall-Regeln so anzupassen, dass die Attacke abgewehrt wird. Gleichzeitig wird auf Sicherheitsupdates überprüft, und diese bei Bedarf downgeloadet und installiert.

18.11 Content Filtering Software

Da es sich bei den Clients meist um Firmengeräte handelt, ist es ebenfalls essentiell, dass Mitarbeiter Web-Seiten mit kriminellem oder pornographischem Inhalt nicht aufrufen können. Dies kann nämlich rechtliche Konsequenzen für die Geschäfts- bzw. IT-Leitung haben. Wird versucht eine derartige Seite anzuwählen, so wird beim Benutzer eine Web-Seite angezeigt, mit dem Inhalt, dass diese Web-Seite aufgrund der Inhaltsbeschränkungen nicht angezeigt werden kann. Auch die Content Filtering Software erhält regelmäßig Updates vom Security Update-Server. Sicherlich können nicht alle Seiten mit kriminellem oder pornographischem Inhalt erfasst werden, vor allem deshalb, weil diese Seiten sehr oft umziehen. Trotzdem bietet diese Komponente einen gewissen Schutz, der aber vor allem aus rechtlichen Gründen sehr wichtig ist.

18.12 Architektur von „Mobile Security NG“

Dieser Abschnitt beschreibt die notwendige Umgebung für den Betrieb von „Mobile Security NG“ (Abbildung 42).

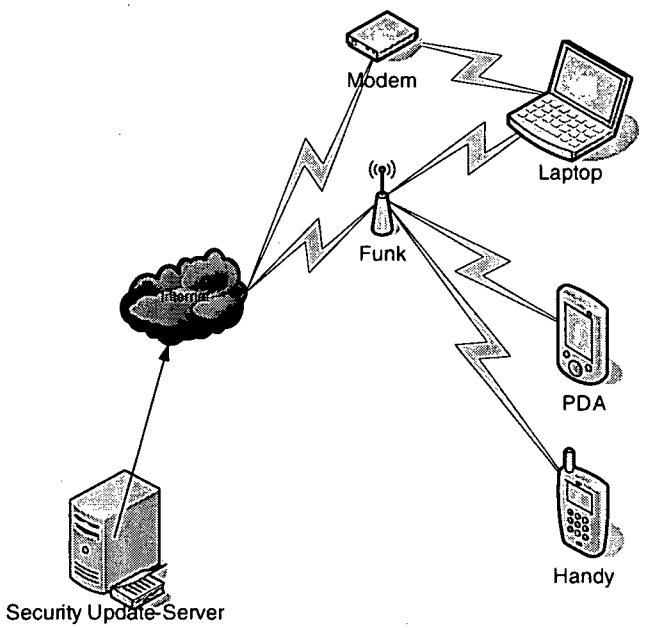


Abbildung 42: Architektur von „Mobile Security NG“

18.12.1 Der Security Update-Server

Der Security Update-Server ist ein zentraler, über das Internet zugänglicher Server, von dem die Clients mittels Pull-Methode Updates automatisch herunterladen. Dieser Server beinhaltet einerseits Updates für die Software selbst, und andererseits stellt er Betriebssystemupdates, Virendefinitionsupdates und Sicherheitsupdates für sämtliche Hardware- und Software-Komponenten der Clients zur Verfügung. Diese Server können weltweit installiert werden, um einerseits Lastverteilung zu gewährleisten und andererseits eine möglichst schnelle Kommunikation mit den Clients möglich ist. Die Server werden von den Herstellern der Software betrieben. Updates werden erst nach ausführlichen Tests von Experten auf die Security Update-Server verteilt. Damit wird sichergestellt, dass Clients nicht durch etwaige fehlerhafte Updates kompromittiert werden. Der Security Update-Server kommuniziert dabei mit den Clients über https, damit während des Downloads auf den Client keine Angriffe gestartet werden können, und die Pakete nicht verändert werden können. Die Update-Pakete sind digital signiert, und werden am Client vor der Installation auf etwaige Manipulation überprüft (Abbildung 43). Wurde das Update verändert, so erfolgt keine Installation auf den Clients, und das Paket wird erneut downgeloadet. Erst wenn das Paket fehlerfrei übertragen wurde, beginnt die Installation.

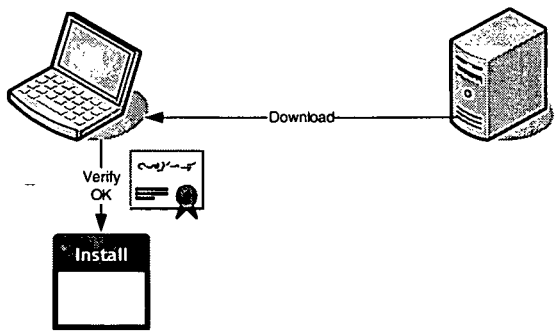


Abbildung 43: Download und Installation

18.12.1.1 Klassifizierung der Updates

Damit eine Priorisierung der Updates auf den Clients erfolgen kann, müssen die Updates zuerst klassifiziert werden. Dabei ergeben sich folgende Kategorien:

- Alle Updates: Dies beinhaltet Sicherheitsupdates für Betriebssystem, „Mobile Security NG“ und alle Client-Programme, sowie Virendefinitionsupdates, Bugfixes und Treiberupdates.
- Updates ohne Bugfixes: Dies beinhaltet Sicherheitsupdates für Betriebssystem, „Mobile Security NG“ und alle Client-Programme, sowie Virendefinitionsupdates.
- Kritische Sicherheitsupdates: Dies beinhaltet Sicherheitsupdates für Betriebssystem und „Mobile Security NG“, sowie Virendefinitionsupdates.
- Nur Virendefinitionen: Dies beinhaltet allein die Virendefinitionsupdates.

18.12.1.2 Priorisierung der Updates

Aufgrund der vom Anwender beantworteten Fragen und der verwendeten Internetverbindung des Clients muss der Server entscheiden, welche Updates eingespielt werden. Dabei ergibt sich folgende Priorisierung:

- Maximum: Alle Updates werden eingespielt. Der Client verfügt entweder über eine Breitbandverbindung und verbringt 5 Stunden/Woche oder mehr im Internet, oder verbringt bei einer schmalbandigen Verbindung mehr als 10 Stunden/Woche im Internet.
- Medium: Außer reinen Bugfixes werden alle Updates eingespielt. Der Client verfügt entweder über eine Breitbandverbindung und verbringt weniger als 5 Stunden/Woche im Internet, oder verbringt bei einer schmalbandigen Verbindung bis zu 10 Stunden/Woche im Internet.
- Low: Nur kritische Sicherheitsupdates werden eingespielt. Der Client verfügt entweder über eine Breitbandverbindung und verbringt bis zu 1 Stunde/Woche im Internet, oder verbringt bei einer schmalbandigen Verbindung bis zu 5 Stunden/Woche im Internet.
- Lowest: Nur die neuesten Virendefinitionen werden eingespielt. Der Client verfügt über keine Breitbandverbindung und verbringt bei einer schmalbandigen Verbindung bis zu 1 Stunde/Woche im Internet.

18.12.2 Clients

Bei den Clients kann es sich um Laptops, PDAs oder Handys handeln. Die Verbindung zum Internet wird durch Wählleitung, ADSL, Kabel oder drahtlos hergestellt. Zwar sind die meisten Handys heutzutage noch nicht mit entsprechend mächtigen Betriebssystemen ausgestattet, doch ist in naher Zukunft auch in diesem Bereich mit großen Weiterentwicklungen zu rechnen, weshalb die Handys auch in eine Sicherheitsarchitektur miteinbezogen werden müssen. Laptops und PDAs sind bereits mit den entsprechenden Betriebssystemen ausgerüstet, und können daher sofort integriert werden. Damit die Software universell einsetzbar ist, muss sie vom Client-Betriebssystem möglichst unabhängig sein, bzw. muss für die gängigsten Betriebssysteme eine Client-Software entwickelt werden.

18.12.3 Software auf den Clients

Dabei handelt es sich um eine sehr vielseitige Software, welche dem Benutzer ermöglicht, die Sicherheitseinstellungen anzupassen. Dabei unterstützt die Software zwei Modi. Einerseits ist dies der Easy-Modus, in welchem dem Benutzer anhand der Beantwortung einiger einfacher Fragen sämtliche Sicherheitseinstellungen automatisch vorgenommen werden. Die Fragen, welche hier zum Tragen kommen werden im folgenden Abschnitt dargestellt. Andererseits gibt es auch den Experten-Modus, bei dem jede Sicherheitseinstellung manuell aktiviert oder deaktiviert werden kann. Somit besitzt die Software die höchstmögliche Flexibilität, damit sowohl End-Anwender als auch Power-User bedient werden können. Der Experten-Modus ist standardmäßig deaktiviert, kann aber auf Wunsch der Geschäftsleitung aktiviert werden. Dabei ist wieder höchste Flexibilität gewährleistet, da dies keine generelle Konfiguration darstellt, sondern für jeden User individuell bestimmt werden kann. Der Experten-Modus ist aber nicht prinzipiell als unproblematisch anzusehen. Vor allem durch eine falsche Selbsteinschätzung der Anwender können diese Clients zu einem Sicherheitsproblem werden. Deshalb sollte die Software auch im Experten-Modus die manuell vorgenommenen Sicherheitseinstellungen überprüfen, und gegebenenfalls automatisch anpassen, ohne dass der Anwender davon etwas mitbekommt. So kann gewährleistet werden, dass auch der Experten-Modus nicht zum Sicherheitsproblem werden kann.

18.12.4 Installation und Konfiguration auf den Clients im Easy-Modus

Die Installation der Software läuft weitgehend automatisch ab. Nach Aufrufen des Setup-Programms überprüft die Software, welche Hardwarekomponenten auf dem System installiert sind. Abhängig von den installierten Hardware-Komponenten werden nur bestimmte Teile der Software installiert.

18.12.5 Installation und Konfiguration auf den Clients im Experten-Modus

Im Experten-Modus kann der Benutzer die zu installierenden Komponenten selbst auswählen (Abbildung 44).

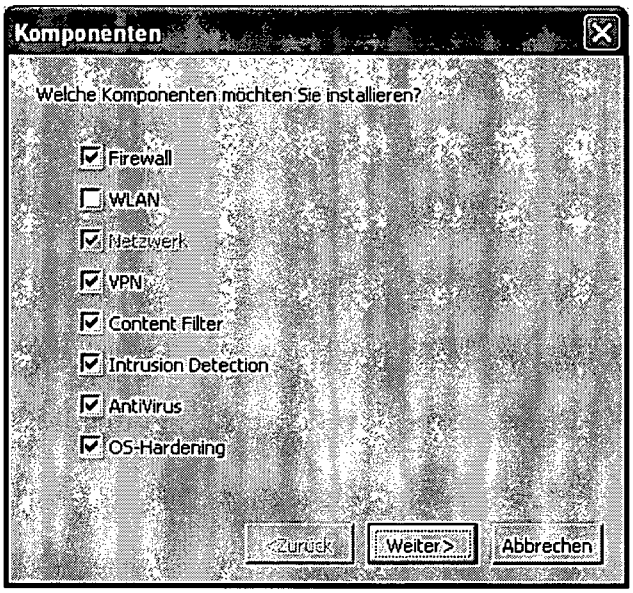


Abbildung 44: Komponenten

18.12.6 Konfiguration nach der Installation im Easy-Modus

Sobald die Installation abgeschlossen ist, werden dem Benutzer anhand der installierten Komponenten einige einfache Fragen gestellt. Anhand der Beantwortung dieser Fragen konfiguriert die Software sämtliche Komponenten voll automatisch. Die folgenden Abschnitte erläutern die für die einzelnen Komponenten relevanten Fragen, und deren Einfluss auf die Konfiguration der Software-Komponenten.

18.12.6.1 Allgemeine Fragen

Da die meisten Geräte heutzutage über mehrere Komponenten verfügen, über die eine Internet-Verbindung aufgebaut werden kann, muss zuerst identifiziert werden, welches Gerät für die Internet-Verbindung verwendet wird.

Folgende Auswahlmöglichkeiten werden dabei dem Benutzer präsentiert (Abbildung 45).

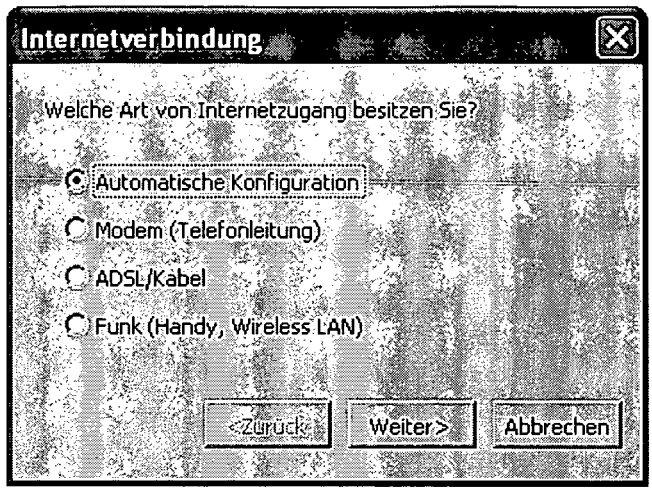


Abbildung 45: Internetverbindung

Standardmäßig wird die automatische Konfiguration vorgeschlagen. Dabei überprüft die Software sämtliche Adapter auf einen Zugang, bzw. fordert den Benutzer auf, die Installations-CD seines Providers einzulegen. Bei den anderen Optionen erfolgt die Installation gleichartig, es werden aber nicht alle Hardware-Adapter durchgescannt. Steht nur ein einziges Gerät für den Internet-Zugang zur Verfügung oder ist bereits eine Internet-Verbindung konfiguriert, erscheint kein Auswahlfenster, und die Konfiguration läuft vollautomatisch ab.

Ist die Internet-Konfiguration abgeschlossen, wird als nächstes die Häufigkeit der Nutzung abgefragt (Abbildung 46).

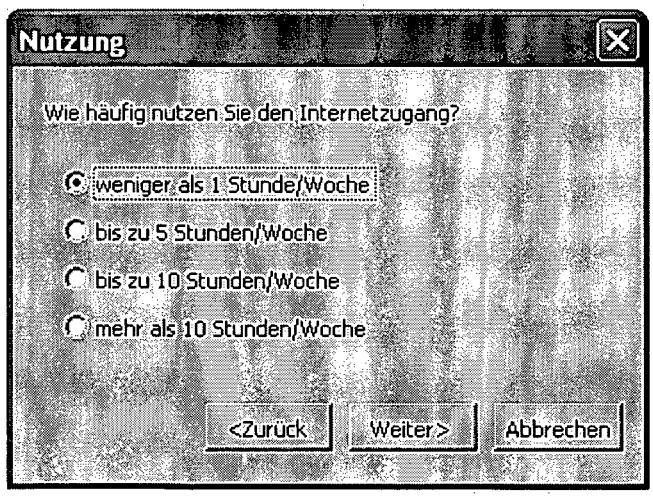


Abbildung 46: Internet-Nutzung

Diese Information ist für die Software deshalb sehr wichtig, denn anhand der Bandbreite der Internetverbindung und der Nutzungsdauer der Verbindung kann berechnet werden, welche Arten von Updates bzw. wie häufig die Updates installiert werden können. Die Intelligenz steckt aber hierbei im Update-Server, der vom Client diese Informationen mitgeteilt bekommt und anhand dessen die Updates priorisiert und für den Client bereitstellt. Die Priorisierung erfolgt dabei, wie schwerwiegend eine bestimmte Sicherheitslücke angesehen wird. Außerdem wird auch auf Ausgewogenheit der Updates geachtet. So kann es z.B. nicht vorkommen, dass permanent nur Betriebssystemupdates installiert werden, und die

Virendefinitionen über längere Zeiträume nicht aktualisiert werden. Wäre dies der Fall, so könnte die Sicherheit nicht mehr gewährleistet werden. Dies würde die Anwendung der Software ad absurdum führen.

18.12.6.2 Fragen zur Firewall-Software und VPN

Danach wird der Benutzer aufgefordert, bekannt zu geben, ob er mittels VPN auf Firmendaten oder Anwendungen zugreift (Abbildung 47).

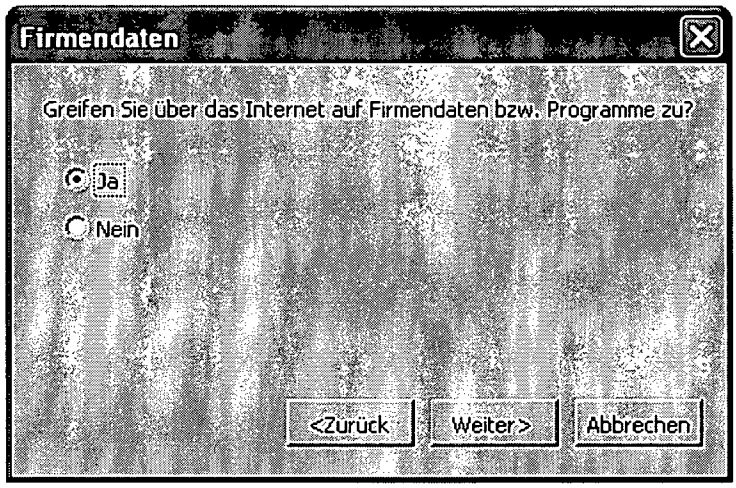


Abbildung 47: Firmendaten

Bejaht der Anwender diese Frage, wird die VPN-Software aktiviert, und der Benutzer muss sich an der Firmenfirewall authentifizieren. Danach wird die Firewall so umkonfiguriert, dass sobald der Anwender eine VPN-Verbindung zum Firmennetzwerk herstellt, der Zugriff auf das Internet selbst gesperrt wird, und nur mehr die Kommunikation zwischen Firma und Client durchgelassen wird. Dies bietet den Sicherheitsvorteil, dass der Computer vom Internet aus nicht mehr erreichbar ist, und deshalb kein Eindringen vom Internet in das Firmennetzwerk möglich ist.

Der folgende Dialog für die Firewall-Konfiguration kann aktiviert werden, vorausgesetzt die Anwender verfügen über den entsprechenden Wissensstand (Abbildung 48).

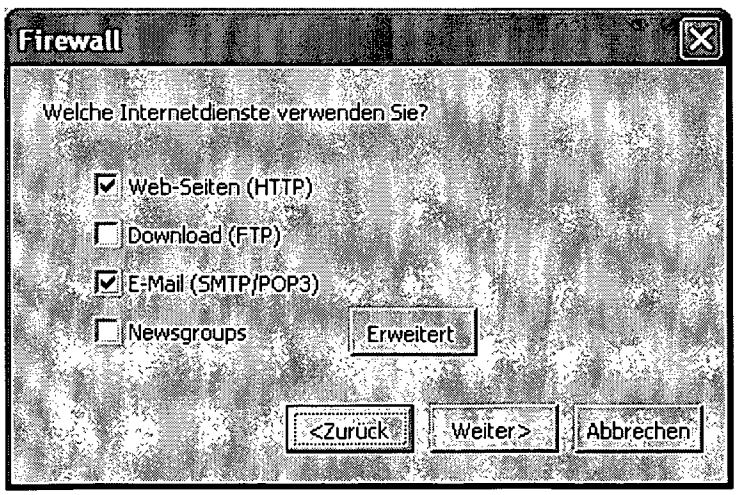


Abbildung 48: Firewall

Dies bietet den Vorteil, dass auch die Konfiguration für den Power-User ansprechend bleibt. Geht für ihn nämlich zu viel automatisch vonstatten, fühlt er sich in seiner Kompetenz eingeschränkt, und die Akzeptanz der Software sinkt dramatisch.
Standardmäßig sind die gebräuchlichsten Dienste angewählt. Über den Button „Erweitert" ist es möglich in einem Policy-Editor die Firewall-Regeln völlig frei zu definieren (Abbildung 49).

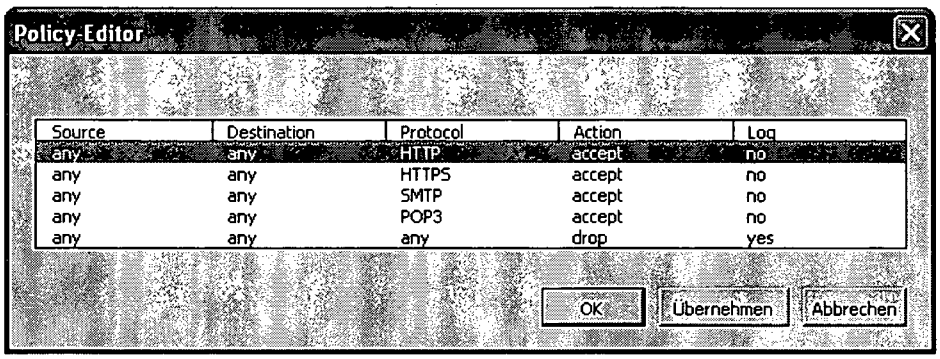


Abbildung 49: Policy-Editor

Damit dies aber nicht zum Sicherheitsproblem wird, werden die Regeln nachfolgend von der Software auf Sinnhaftigkeit überprüft, und bei entsprechenden Sicherheitsproblemen automatisch angepasst, ohne dass der Benutzer davon etwas mitbekommt.
Mit der Beantwortung dieser Fragen ist die Konfiguration der Software abgeschlossen. Alle anderen Komponenten werden vollautomatisch konfiguriert. Fragen sind dabei nicht notwendig.
Dabei ergeben sich folgende Default-Einstellungen:

- Content Filter: alle Kategorien (Crime, Sex & Pornography, Games, Chat und MP3-Downloads) werden aktiviert
- Intrusion Detection: Diese wird so konfiguriert, dass alle Angriffe erkannt und blockiert werden.
- AntiVirus: Alle Dateien werden durch eine Echtzeitprüfung bei Zugriff gescannt, wöchentlich wird eine Prüfung des gesamten Systems gestartet und alle ein- und ausgehenden E-Mails werden überprüft. Wird ein Virus gefunden, wird zuerst versucht, diesen zu entfernen. Ist dies nicht möglich, wird die Datei gelöscht.
- OS-Hardening: Die Konfiguration wird wie bereits in Kapitel 18.8 beschrieben, durchgeführt.

18.12.7 Konfiguration nach der Installation im Experten-Modus

Im Experten-Modus läuft die Konfiguration anders ab, als im Easy-Modus. Dieser Abschnitt soll die Unterschiede aufzeigen.
Während im Easy-Modus anhand einfacher Fragen sämtliche Konfigurationen vorgenommen werden, muss der Anwender im Experten-Modus zuerst die Internetverbindung aus einer Liste der erkannten Verbindungen auswählen (Abbildung 50).

Abbildung 50: Internetverbindung

Danach muss der Anwender angeben, welche Updates er vom Security Update-Server empfangen möchte (Abbildung 51).

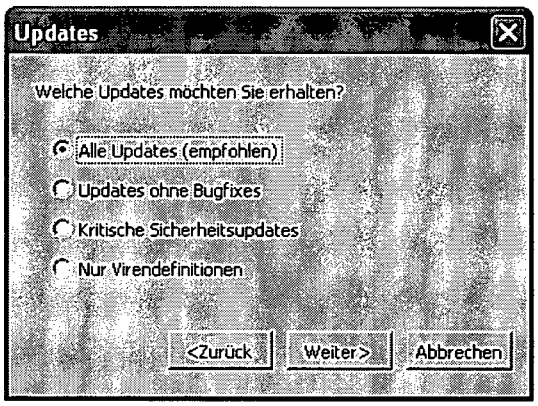


Abbildung 51: Updates

Als nächsten Schritt muss der Anwender die Firewall-Regeln definieren, wobei als Default die nur die Browser- und E-Mail-Protokolle aktiviert sind (Abbildung 49).

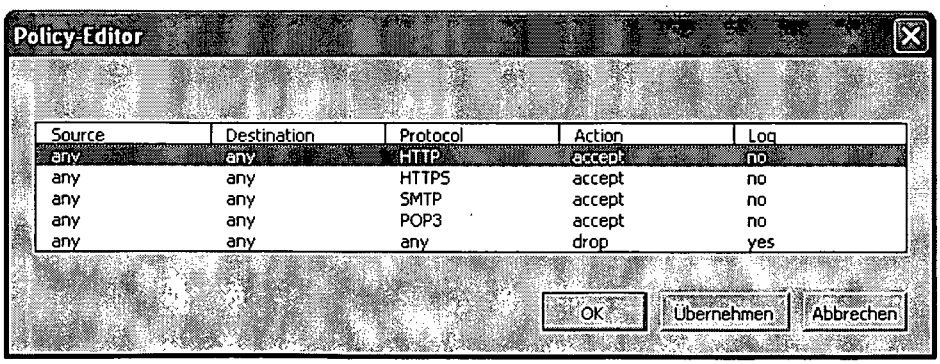


Abbildung 52: Firewall-Konfiguration

Danach erscheint der Dialog zur Auswahl der VPN-Verbindung (Abbildung 53).

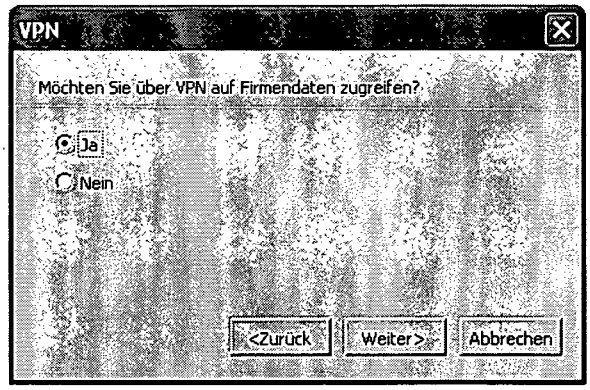


Abbildung 53: VPN

Im nächsten Schritt muss der Anwender die Kategorien auswählen, die vom Content Filter blockiert werden sollen (Abbildung 54). Wenn der Anwender keine Kategorie auswählt wird der Content Filter deaktiviert.

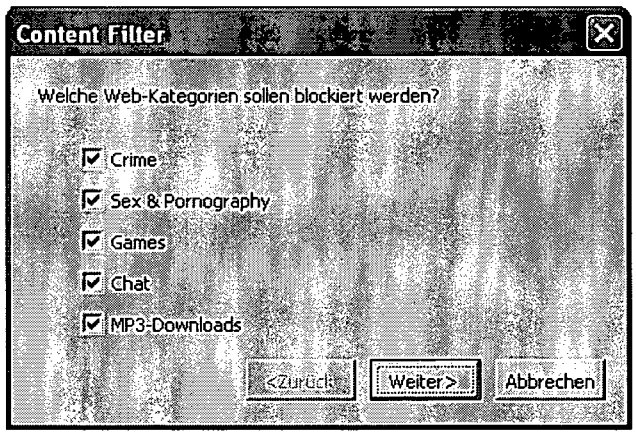


Abbildung 54: Content Filter

Danach muss der User auswählen, in welchem Modus die Intrusion Detection arbeiten soll (Abbildung 55). Im automatischen Modus werden alle Angriffe erkannt und blockiert. Entscheidet sich der Anwender für die benutzerdefinierte Konfiguration, so muss er aus einer Liste der bekannten Angriffssignaturen jene auswählen, welche erkannt und blockiert werden sollen. Die Deaktivierung der Funktion wird aus Sicherheitsgründen nicht empfohlen.

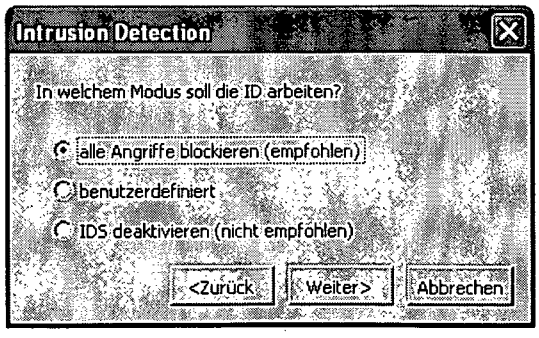


Abbildung 55: Intrusion Detection

In einem weiteren Schritt muss die Konfiguration der AntiVirus-Software durchgeführt werden (Abbildung 56). Bei der automatischen Konfiguration werden die Default-Einstellungen (Kapitel 18.12.6.2) vorgenommen. Bei der benutzerdefinierten Konfiguration können diese Einstellungen beliebig verändert, aktiviert oder deaktiviert werden. Die Deaktivierung der Funktion wird aus Sicherheitsgründen nicht empfohlen.

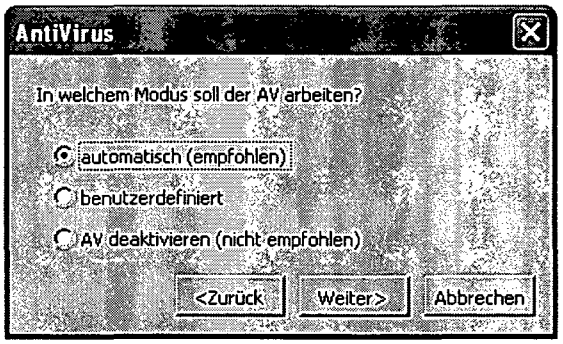


Abbildung 56: AntiVirus

Im letzten Schritt wird die Konfiguration des OS-Hardening abgefragt (Abbildung 57). Bei der automatischen Konfiguration werden die Default-Einstellungen (Kapitel 18.12.6.2) vorgenommen. Bei der benutzerdefinierten Konfiguration können diese Einstellungen beliebig verändert, aktiviert oder deaktiviert werden. Die Deaktivierung der Funktion wird aus Sicherheitsgründen nicht empfohlen.

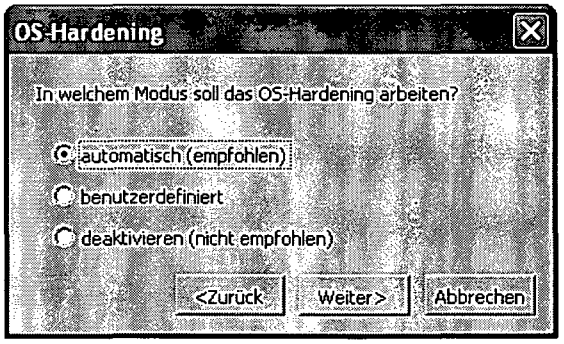


Abbildung 57: OS-Hardening

Damit ist die Konfiguration im Experten-Modus abgeschlossen. Selbstverständlich können alle Einstellungen nachträglich über eine integrierte Konfigurationskonsole modifiziert werden.

18.12.8 Zielgruppen

18.12.8.1 Zielgruppen für den Easy-Modus

Der Einsatz von „Mobile Security NG“ im Easy-Modus richtet sich an folgende Zielgruppen:

- Firmen ohne Administrator(en)
- Anwender haben nur geringe EDV-Kenntnisse
- Kleinbetriebe mit und ohne Firewall

18.12.8.2 Zielgruppen für den Experten-Modus

Der Einsatz von „Mobile Security NG“ im Experten-Modus richtet sich an folgende Zielgruppen:

- Firmen ohne Administrator(en)
- Anwender haben mittlere bis hohe EDV-Kenntnisse
- Kleinbetriebe mit und ohne Firewall

18.12.8.3 Zusammenfassung Zielgruppen

Der Hauptunterschied zwischen dem Easy-Modus und Experten-Modus liegt in der Fragestellung und Konfigurationsmöglichkeit. Firmen sollten deshalb genau überlegen, welchen Modus Sie einsetzen wollen, da bei geringen EDV-Kenntnissen seitens der Anwender der Easy-Modus wesentlich komfortabler ist, und dadurch auch die Akzeptanz wesentlich höher einzuschätzen ist.

18.12.9 Zusammenfassung „Mobile Security NG“

Diese Software bietet für Kleinbetriebe, welche nicht die Personalkapazität besitzen, sämtliche mobilen Geräte zu konfigurieren und zu warten, ein Optimum an Sicherheit. Die einzelnen Komponenten der Software stellen sicher, dass der Client optimal gegen Angriffe und Bedrohungen geschützt ist. Zusätzlich bietet es dem Anwender den Vorteil, sich im Easy-Modus selbst nicht mit dem Thema Sicherheit intensiv beschäftigen zu müssen, da die meisten Vorgänge automatisch durchgeführt werden, und keine Benutzer-Interaktion notwendig ist. Ein weiterer Vorteil ist, dass auch ein Experten-Modus existiert, sodass erfahrene Anwender die Konfiguration selbst vornehmen können. Sollte diese Software realisiert werden, und zum Einsatz kommen, würde das ein großer Schritt in die Richtung von umfassender Sicherheit für private Netzwerke darstellen.

18.13 Architektur von „Mobile Security NG Corporate“

Dieser Abschnitt beschreibt die notwendige Umgebung für den Betrieb von „Mobile Security NG Corporate“.
Die Architektur unterscheidet sich bei dieser Variante durch die zentrale Administrierbarkeit (Abbildung 58). Aufgrund der Definition einer Sicherheitspolitik der Entscheidungsträger, muss diese von den Administratoren implementiert werden. Die Anwender haben bei dieser Architektur keinen Einfluss auf die Konfiguration der Software.

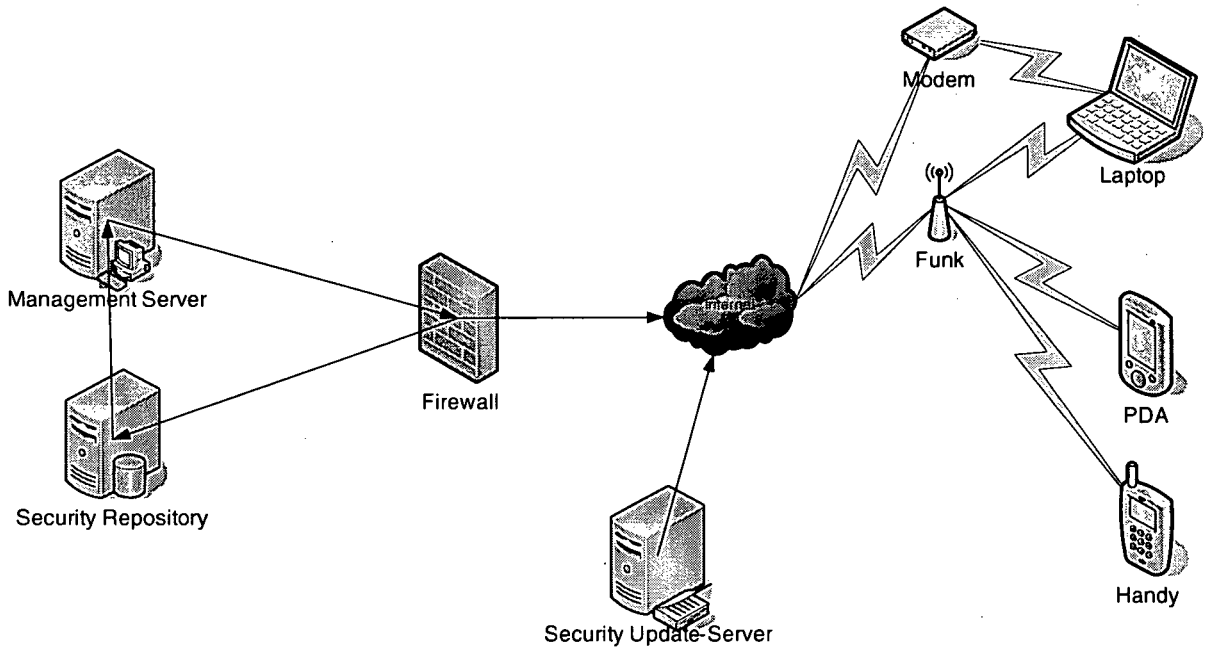


Abbildung 58: Architektur von „Mobile Security NG Corporate“

18.13.1 Der Security Update-Server

Der Security Update-Server ist ein zentraler, über das Internet zugänglicher Server, von dem das Security Repository mittels Pull-Methode Updates automatisch herunterlädt. Dieser Server beinhaltet einerseits Updates für die Software selbst, und andererseits stellt er Betriebssystemupdates, Virendefinitionsupdates und Sicherheitsupdates für sämtliche Hardware- und Software-Komponenten der Clients zur Verfügung. Diese Server können weltweit installiert werden, um einerseits Lastverteilung zu gewährleisten und andererseits eine möglichst schnelle Kommunikation mit den Clients möglich ist. Die Server werden von den Herstellern der Software betrieben. Updates werden erst nach ausführlichen Tests von Experten auf die Security Update-Server verteilt. Damit wird sichergestellt, dass Clients nicht durch etwaige fehlerhafte Updates kompromittiert werden. Der Security Update-Server kommuniziert dabei mit dem Security Repository über https, damit während des Downloads keine Angriffe gestartet werden können, und die Pakete nicht verändert werden können. Die Update-Pakete sind digital signiert, und werden am Security Repository auf etwaige Manipulation überprüft. Wurde das Update verändert, so erfolgt keine Installation auf den Clients, und das Paket wird erneut downgeloadet. Erst wenn das Paket fehlerfrei übertragen wurde, gibt das Security Repository die Updates zur Installation frei.

18.13.2 Der Management Server

Dieser Server dient zum zentralen Management aller externen Clients. Hier werden die Sicherheitspolicy und das Intervall für Updates definiert. Die Sicherheitspolicy wird dann mittels Push-Methode auf die Clients ausgerollt. Dabei wird dem Administrator eine Konsole zur Verfügung gestellt, mit der er graphisch alle Einstellungen vornehmen kann. Die Konsole verfügt dabei über einen integrierten Firewall-Editor. Dieser Editor ermöglicht die Konfiguration der Firewall-Regeln auf den Clients. Wurden die Regeln geändert, wird beim nächstmaligen Anmelden des Clients die neue Regelbasis installiert.
Für die Updates der Virendefinitionen kann der Administrator Intervalle festlegen und angeben, ob der Anwender auch manuelle Updates durchführen darf.
Weiters kann konfiguriert werden, dass der Anwender weder die Möglichkeit hat, die Anti-Viren-Software zu deaktivieren, noch diese zu deinstallieren.
Für das Content Filtering können die Kategorien festgelegt werden, welche blockiert werden sollen. Diese umfassen Crime, Sex & Pornography, Games, Chat und MP3-Downloads.
Zusätzlich verfügt die Konsole über den Priorisierungs- und Intervall-Konfigurator. Dort wird festgelegt, welche Updates, wann übertragen werden. Dabei ist sehr fein justierbar, nach welchen Mustern die Updates installiert werden.
Als besonderes Feature kann der Administrator auch festlegen, welche Software auf den Clients installiert sein darf. Sämtliche andere Software wird dann automatisch deinstalliert. Dies ist nicht nur ein Vorteil für die Sicherheit, sondern bringt auch eine bessere Verwaltung der Lizenzen, da die Installation von nicht freigegebener Software erst gar nicht möglich ist, bzw. wenn so eine Software bereits installiert wurde, wird sie sofort und automatisch deinstalliert. Der Management-Server verfügt auch über ein zentrales Log, welches die Logs der Clients sammelt, und diese für die Auswertung zentral speichert. Der Administrator kann in der Konsole auch Alerts für bestimmte Sicherheitsprobleme definieren, die dann per Mail oder SMS (Short Message Service) an den Administrator versandt werden.

18.13.3 Das Security Repository

Dieser Server hostet eine Datenbank, in der einerseits alle Clients definiert sind, und andererseits verwaltet dieser Server das Ausrollen der Updates mittels Push-Methode auf alle Clients. Die Datenbank enthält daher Informationen sowohl über die Hardwareausstattung der Clients als auch Informationen über bereits eingespielte Updates und noch ausständige Updates. Das Security Repository arbeitet dabei eng mit dem Management Server zusammen, denn dieser definiert die Regeln, nach welchen die Updates ausgerollt werden.

18.13.4 Die Firewall

Die Firewall dient einerseits als zentrales Instrument für die Absicherung des Firmennetzwerkes und ermöglicht es den Clients auf Daten und Anwendungen im lokalen Netzwerk zuzugreifen. Die Anbindung der Clients basiert auf einem virtuellen privaten Netzwerk. Analog zu „Mobile Security NG“ ist es dem Client nicht möglich direkt mit dem Internet zu kommunizieren, sobald eine VPN-Verbindung zum Firmennetzwerk hergestellt wurde.

18.13.5 Software auf den Clients

Im Gegensatz zur Software für Kleinbetriebe, befindet sich hier auf den Clients neben der Basissoftware auch ein Agent der anhand der ausgerollten Security-Policy sämtliche Einstellungen am Client vornimmt. Zusätzlich ist dieser Agent auch für das Management der Updates zuständig und kommuniziert ständig mit dem Security Repository, damit der Datenbankbestand immer aktuell gehalten wird (Abbildung 59).

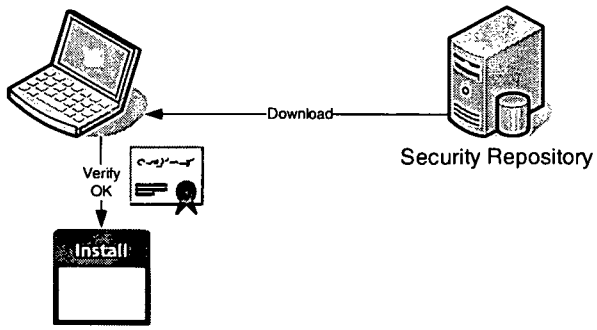


Abbildung 59: Download und Installation

Der Benutzer hat im Gegensatz zu „Mobile Security NG" keine Möglichkeit in die Sicherheitseinstellungen aktiv einzugreifen. Hier werden alle Sicherheitseinstellungen zentral verwaltet, und können nur von einem Administrator verändert werden.

18.14 Analyse „Mobile Security NG" und „Mobile Security NG Corporate"

18.14.1 Kriterien

Um die beiden Software-Produkte vergleichen zu können, müssen Kriterien definiert werden, anhand derer ein Vergleich möglich wird.
Diese Kriterien umfassen:

- Sicherheit
- Performance
- Skalierbarkeit
- Kosten

Die Kriterien umfassen hierbei eine Skala von 1 (sehr gut) bis 5 (nicht genügend).

18.14.1.1 Kriterium Sicherheit

Dieses Kriterium soll bewerten, wie sicher die Software einzustufen ist. Dabei spielt vor allem eine Rolle, inwiefern der Faktor Mensch auf die Sicherheitseinstellungen Einfluss nimmt.

18.14.1.2 Kriterium Performance

Dieses Kriterium beschreibt die Auslastung der Clients durch die zusätzlich installierte Software.

18.14.1.3 Kriterium Skalierbarkeit

Dieses Kriterium bewertet die Einfachheit der Integration von zusätzlichen Clients und den damit verbundenen Aufwand.

18.14.1.4 Kriterium Kosten

Dieses Kriterium beschreibt die Effizienz der Kosten und gibt Hinweise auf den sinnvollen Einsatz der jeweiligen Software.

18.14.2 Bewertung „Mobile Security NG“

18.14.2.1 Sicherheit

Für „Mobile Security NG“ kann die Sicherheitsstufe nicht global definiert werden. Es muss hierbei zwischen dem Easy-Modus und dem Experten-Modus differenziert werden. Dies begründet sich durch den unterschiedlichen Einfluss des Faktors Mensch.

18.14.2.1.1 Easy-Modus

Nachdem im Easy-Modus nur ein Minimum an Interaktion mit dem Benutzer gefordert ist, kann menschliches Versagen durch fehlerhafte Konfigurationen ausgeschlossen werden. Nachdem die Software selbst aber von Menschen erstellt wurde, kann natürlich nicht von absoluter Sicherheit gesprochen werden. Unter der Annahme, dass die Software keine kritischen Sicherheitslücken aufweist, und auch nicht durch Dritte manipuliert werden kann, ergibt sich eine Bewertung von 2 (gut). Diese Bewertung begründet sich auf dem Faktum, dass die Software immer nur bekannte Sicherheitslücken und Probleme abfangen kann. Eine künstliche Intelligenz der Software, welche auf jede Art von neuen Bedrohungen reagieren kann, ist zum derzeitigen Zeitpunkt nicht realistisch, und kann deshalb ausgeschlossen werden.

18.14.2.1.2 Experten-Modus

Im Experten-Modus gestaltet sich die Bewertung schon wesentlich diffiziler.
Nimmt man an, dass die Anwender über das entsprechende Wissen verfügen, sämtliche Konfigurationen ordnungsgemäß durchzuführen, kann aufgrund der Argumentation in Abschnitt 18.14.2.1.1 ebenfalls eine Bewertung von 2 (gut) gegeben werden.
Nimmt man aber an, dass die Anwender nicht über das entsprechende Wissen verfügen, sämtliche Konfigurationen ordnungsgemäß durchzuführen, kann keine eindeutige Bewertung definiert werden. Dies ergibt sich durch die mögliche Varianz an Wissen im Sicherheitsbereich. In diesem Fall läge das Ergebnis im Intervall 3 (befriedigend) bis 5 (nicht genügend).
Da somit keine eindeutige Bewertung erfolgen kann, darf das Kriterium Sicherheit im Experten-Modus keine Bewertung erhalten. Einzig durch empirische Studien kann festgestellt werden, in welchem Bereich eine sinnvolle Bewertung liegt.

18.14.2.2 Performance

Wie auch bei der Sicherheit muss hier eine Differenzierung zwischen dem Easy-Modus und dem Experten-Modus durchgeführt werden. In diesem Fall begründet sich dies durch die Wahlmöglichkeit im Experten-Modus bestimmte Komponenten nicht zu installieren. Dadurch kann die Performance gesteigert, aber dadurch bedingt die Sicherheit sinken.

18.14.2.2.1 Easy-Modus

Im Easy-Modus wird der Performance-Verlust am deutlichsten zu spüren sein. Hier sind alle Software-Komponenten aktiviert. Zieht man derzeitige Implementationen von Sicherheitssoftware in Betracht, so ist anzunehmen, dass die Performance sicher um 20-30% sinken wird. Aufgrund dieser Tatsache ergibt sich eine Bewertung von 3 (befriedigend).

18.14.2.2.2 Experten-Modus

Im Experten-Modus ergibt sich eine ähnliche Konstellation, wie beim Kriterium Sicherheit. Werden alle Software-Komponenten für maximale Sicherheit konfiguriert, ergibt sich wie im Easy-Modus eine Bewertung von 3 (befriedigend).
Zieht man aber die Möglichkeit der Deaktivierung von Software-Komponenten in Betracht, so ergibt sich auch bei der Performance eine Bewertung im Intervall 3 (befriedigend) bis 1 (sehr gut). Vor allem bei Deaktivierung von allen bzw. fast allen Komponenten kann die Performance bis zur Bestnote gesteigert werden.

18.14.2.3 Skalierbarkeit

Bei der Skalierbarkeit ist keine Trennung zwischen Easy-Modus und Experten-Modus nötig, da die Skalierbarkeit durch die Software selbst limitiert ist. Dies begründet sich dadurch, dass jeder Client manuell installiert werden muss. Geht man von der Annahme aus, dass ein Administrator alle Clients manuell mit der Software ausstatten muss, steigt der Arbeitsaufwand des Administrators linear mit der Anzahl der Clients. Selbst wenn die Anwender die Software selbsttätig installieren, ergibt sich für jeden Anwender ein gewisser Installations- und Konfigurationsaufwand. Dadurch erscheint eine Bewertung mit 3 (befriedigend) als zielführend.

18.14.2.4 Kosten

Bei den Kosten muss wieder zwischen Easy-Modus und Experten-Modus unterschieden werden. Dies begründet sich durch eventuelle Fehlkonfigurationen der Anwender im Experten-Modus, wodurch zusätzlicher Installations- und Supportaufwand entsteht.

18.14.2.4.1 Easy-Modus

Im Easy-Modus sind die Kosten im Vorhinein gut abschätzbar, da Lizenzen für die Anzahl der zu installierenden Clients, Kosten für Software-Updates und Support ebenfalls in direktem Zusammenhang mit der Anzahl der Clients steht. Da hierbei alle Konfigurationen automatisch auf die optimalen Sicherheitsbedingungen abgestimmt sind, entfallen zusätzliche Kosten für etwaige Fehlkonfigurationen. Die Kosten sind daher mit 1 (sehr gut) zu bewerten.

18.14.2.4.2 Experten-Modus

Im Experten-Modus sind die Kosten im Vorhinein nicht abschätzbar. Dies ergibt sich durch etwaige Fehlkonfigurationen der Anwender, was entweder die Support-Anforderungen ausufern lässt, aber auch Folgekosten beinhaltet, die durch Attacken auf die Clients entstehen. Dabei können Firmendaten entwendet werden, die Software auf den PCs unbrauchbar gemacht werden, und dergleichen. Geht man aber davon aus, dass die Anwender gut geschult, und über einen hohen Wissensstand verfügen, können die Kosten aufgrund der möglichen Unschärfe aber nur mit 3 (befriedigend) bewertet werden.

18.14.2.5 Bewertung

Aufgrund der Auswertung der Einzelbewertungen ergibt sich folgendes Ergebnis:

	Easy-Modus	Experten-Modus
Sicherheit	2	4
Performance	3	2
Skalierbarkeit	3	3
Kosten	1	3
Durchschnitt	**2,25**	**3**

Für die Kriterien Sicherheit und Performance wurden aufgrund der Unschärfe, Mittelwerte genommen. Wie man aus der Tabelle sieht, ergibt der ungewichtete Mittelwert eine etwas bessere Bewertung für den Easy-Modus.

18.14.2.6 Zusammenfassung Bewertung „Mobile Security NG“

Die Bewertung anhand der definierten Kriterien hat ergeben, dass es sinnvoller ist, wenn nicht eindeutig klar ist, welchen Wissensstand die einzelnen Anwender besitzen, die Software im Easy-Modus zu verwenden. Falls aber für alle Anwender eindeutig festgelegt werden kann, dass diese einen entsprechenden Wissensstand besitzen kann durchaus der Experten-Modus bedenkenlos aktiviert werden.

18.14.3 Bewertung „Mobile Security NG Corporate“

18.14.3.1 Sicherheit

Da in der Corporate-Variante sämtliche Einstellungen von hochqualifizierten Administratoren durchgeführt werden, die auch bei Auftreten einer neuen Sicherheitslücke sehr rasch reagieren können, ergibt sich eine deutlich bessere Sicherheit für die Clients. So kann z.B. durch die Anpassung der Firewall-Regeln eine Attacke geblockt werden, die von der Intrusion Detection noch nicht erkannt wird. Dadurch ergibt sich ein wesentlicher Vorteil gegnüber der anderen Version im Easy-Modus. Deshalb ist die Sicherheit unter der Annahme, dass die Software nur von hochqualifizierten Administratoren konfiguriert wird, hierbei mit 1 (sehr gut) zu bewerten.

18.14.3.2 Performance

Bei der Performance kann durch den Eingriff der Administratoren ebenfalls mehr erreicht werden, als bei der anderen Variante. So können z.B. Firewall-Regeln getunet werden, und die Konfiguration auf den Clients entsprechend der Client-Performance eingestellt werden. Trotzdem ist sicherlich ein gewisser Performance-Verlust durch die Komplexität und Rechenintensität der Software gegeben. Deshalb ergibt sich eine Bewertung von 2 (gut).

18.14.3.3 Skalierbarkeit

Die Skalierbarkeit ist hierbei um vieles höher, da alle Clients zentral verwaltet und konfiguriert werden. Somit ist es nicht notwendig jeden Client einzeln zu konfigurieren, sondern dies wird zentral verwaltet. Damit spielt die Anzahl der Clients eine nicht so große Rolle. Somit ergibt sich für die Skalierbarkeit eine Bewertung von 1 (sehr gut).

18.14.3.4 Kosten

Durch den wesentlich höheren Administrationsaufwand und die Bereitstellung von zusätzlicher Hardware (Security Repository, Management Server, Firewall) ergeben sich deutlich höhere Kosten. Vor allem die permanente Schulung der Administratoren, um gegen zukünftige Sicherheitsprobleme gewappnet zu sein, und die Kosten für die Verwaltung der Server und der Software bringen neben den Software-Lizenzen wesentlich höhere Kosten mit sich. Dadurch ergibt sich für die Kosten eine Bewertung von 2 (gut).

18.14.3.5 Bewertung

Aufgrund der Auswertung der Einzelbewertungen ergibt sich folgendes Ergebnis:

	Bewertung
Sicherheit	1
Performance	2
Skalierbarkeit	1
Kosten	2
Durchschnitt	**1,5**

„Mobile Security NG Corporate“ erzielt somit eine sehr gute Bewertung, was die einzelnen Kriterien betrifft.

18.14.3.6 Zusammenfassung Bewertung „Mobile Security NG Corporate“

Die Bewertung ergibt, dass bei richtiger Implementation und Betreuung durch geschulte Administratoren ein sehr gutes Ergebnis zu erzielen ist.

18.14.4 Zielgruppen

Der Einsatz von „Mobile Security NG Corporate“ richtet sich an folgende Zielgruppen:

- Firmen mit hochqualifizierten Administratoren
- Großbetriebe mit Firewall

18.14.5 Zusammenfassung „Mobile Security NG Corporate“

Diese Software bietet zusätzlich zu „Mobile Security NG“ die Möglichkeit zur zentralen Verwaltung. Sie eignet sich daher für mittlere und große Unternehmen, die über Administratoren und eine Vielzahl von mobilen Geräten verfügen. Somit kann die Sicherheitspolitik zentral definiert werden, und auf alle mobilen Clients ausgerollt werden. Der Anwender hat somit keine Möglichkeit mehr in die Sicherung der Systeme einzugreifen. Der einzige Nachteil, welcher sich in diesem Szenario darstellt, ist dass durch menschliches Versagen der Administratoren Sicherheitslücken in den mobilen Geräten entstehen können. Hierbei ist es aber extrem schwierig Automatismen anzubieten, da die Akzeptanz der Administratoren meist nicht gegeben ist. Zu diesem Thema müssten noch weitere Nachforschungen angestellt werden, wie auch für Administratoren automatische Funktionen implementiert werden können, die aber die Arbeitsabläufe und Konfigurationen nicht stören. Um menschlichem Versagen wirkungsvoll vorbeugen zu können, sind Schulungsmaßnahmen absolut unerlässlich.
Für mittlere und große Unternehmen, die über eine eigene Firewall verfügen bietet diese Software aber trotzdem ein Höchstmaß an Sicherheit. Ein großer Vorteil ist dabei die zentrale Verwaltung. Somit haben Administratoren immer den Überblick über alle im Einsatz befindlichen mobilen Geräte. Zusätzlich ist die Konfiguration einheitlich, d.h. vom Betriebssystem am Client völlig unabhängig. Die Policies werden zentral definiert, und sind somit für jedes Gerät und jedes Betriebssystem einheitlich.

18.14.5.1 Features

Die folgende Tabelle fasst noch einmal übersichtlich sämtliche wichtigen Features der einzelnen Varianten zusammen.

	Mobile Security NG Easy Modus	Mobile Security NG Experten Modus	Mobile Security NG Corporate
Firewall	Ja	Konfigurierbar	Konfigurierbar
WLAN	Ja	Konfigurierbar	Konfigurierbar
Netzwerk & Modem	Ja	Konfigurierbar	Konfigurierbar
VPN	Ja	Konfigurierbar	Konfigurierbar
OS-Hardening	Ja	Konfigurierbar	Konfigurierbar
Anti-Virus	Ja	Konfigurierbar	Konfigurierbar
Intrusion Detection	Ja	Konfigurierbar	Konfigurierbar
Content Filter	Ja	Konfigurierbar	Konfigurierbar
Manuelle Konfiguration	Nein	Ja	Ja
Einfache Konfiguration	Ja	Nein	Nein
Erweiterte Konfiguration	Nein	Ja	Ja
Administrator-Konfiguration	Nein	Nein	Ja
Automatische Updates	Ja	Konfigurierbar	Konfigurierbar

Ein „Ja“ bedeutet, dass das jeweilige Feature inkludiert und für optimale Sicherheit konfiguriert ist. „Konfigurierbar“ bedeutet, dass das Feature sowohl aktiviert, als auch

deaktiviert werden kann, und zusätzlich konfiguriert werden kann. „Nein“ bedeutet, dass das Feature nicht verfügbar ist.

18.15 Problematik

Prinzipiell ergibt sich durch den Einsatz von Software immer die Problematik, dass diese zur Laufzeit verändert und blockiert werden kann. Deshalb kann auch bei Kommunikation über das sichere https nicht hundertprozentig gewährleistet werden, dass die Software nicht bereits verändert wurde und damit nicht mehr korrekt arbeitet. Abhilfe könnten hierbei Hardware-Einheiten darstellen, welche entweder in die Endgeräte fix integriert sind, oder als Add-On eingebaut werden könnten. Für diese Hardware-Komponenten ergibt sich eine Vielzahl von möglichen Aufgaben. Einerseits könnte die Hardware sicherstellen, dass selbst bei Manipulation der Software der Update-Server immer die gesicherte Information erhält, ob das Update wirklich erfolgreich installiert wurde, oder nicht. Bei der Corporate Variante würde die Hardware sicherstellen, dass jegliche Kommunikation mit dem Management-Server nicht unterdrückt oder verändert werden kann. Das bedeutet, die Hardware muss über Sensoren verfügen, welche die korrekte Funktionalität der Software gewährleistet. Diese Sensorik muss unabhängig von der Software arbeiten. Dazu gehört auch ein Schutzsystem, sodass auch die Firmware auf dieser Hardware-Komponente nicht verändert werden kann. Stellt diese Sensorik fest, dass die Software nicht mehr korrekt arbeitet, und eine Kompromittierung somit eindeutig festgestellt wird, muss die Hardware reagieren. Einerseits könnte sie das Endgerät komplett sperren, sodass dieses nur durch einen Techniker wieder reaktiviert werden kann. Dies wäre die strengste Vorgehensweise, die sich zwar für den Anwender als unbefriedigend darstellt, aber definitiv die sicherste Variante ist. Damit wird nämlich verhindert, dass das Firmennetzwerk ebenfalls einer Bedrohung ausgesetzt wird. Andererseits könnte der Vorfall auch einen Alarm beim Hersteller bzw. beim Systemadministrator bei der Corporate-Variante generieren. Der Alarm muss ohnedies auch bei der Deaktivierungs-Variante erfolgen. Welcher Möglichkeit der Vorzug gegeben wird, hängt aber auch von der Sicherheitspolitik der Organisation ab. Persönlich würde ich aber die Deaktivierung vorziehen. Es kann nämlich von keiner noch so hoch entwickelten Sensorik für jeden Sicherheitsvorfall eindeutig festgestellt werden, ob es eine Bedrohung auch für das private Netzwerk darstellt.
Weiters könnte auch in die Hardware von Netzwerkkarten oder Modems eine Firewall bzw. ein Intrusion Detection System eingebaut werden. Dies ergebe den Vorteil, dass auch diese Komponenten vor etwaiger Manipulation geschützt wären.

18.15.1 Zusammenfassung Problematik

Wie im letzten Abschnitt diskutiert, kann die Sicherheitssoftware alleine nicht alle Bedrohungen abfangen. Dies ergibt sich durch die immer mögliche Manipulation jeglicher Software. Zusätzliche Hardware-Komponenten könnten hier ein weiterer wichtiger Schritt zu mehr Sicherheit in privaten Netzwerken sein. Durch die unabhängige Sensorik und den Schutz vor Manipulierbarkeit stellen sie einen zentralen Aspekt in sicheren privaten Netzwerken dar.

18.16 Pervasive Computing

18.16.1 Einleitung

Der erst in jüngerer Zeit geprägte Begriff des „Pervasive Computing" oder „Ubiquitous Computing" beschreibt die Tendenz intelligente Elektronik in sämtliche Alltagsgegenstände zu integrieren. Dies ergibt einen Wandel von den derzeit PC-basierenden Computern zu Kleinstcomputern, welche unsichtbar in jede Art von Gegenstand eingebettet werden können. So können Informationen über den gegenwärtigen Aufenthaltsort, den Kontext, in welchem der Gegenstand benutzt wird, und Informationen über den User selbst gespeichert und mit drahtloser Kommunikation übertragen werden [73]. Ermöglicht wird dieser Trend erst durch den anhaltenden Fortschritt in der Informationstechnik, welcher immer kleinere und leistungsfähigere Geräte hervorbringt, Fortschritte in der Kommunikationstechnik, welche es besonders im drahtlosen Bereich ermöglichen, dass es bald kleinste und spontan miteinander kommunizierende Rechner im Überfluss geben wird, die kaum mehr als solche wahrgenommen werden dürften, da sie in Gebrauchsgegenstände eingebettet werden und so mit der alltäglichen Umgebung verschmelzen [74].
Um das Konzept des „Pervasive Computing" zu konkretisieren, einige mögliche Anwendungsfälle:

- Bibliothek: Bibliotheken können sämtliche Bücher mit berührungslosen Chips ausstatten. So wäre es möglich, dass der Standort jedes einzelnen Buches immer genau festgestellt werden kann. Dadurch ist einerseits der Bestand im EDV-System immer aktuell, und falsch eingeordnete Bücher können lokalisiert und an die richtige Stelle verfrachtet werden.
- Fernseher und sonstige Haushaltselektronik: Diese Geräte können mit leistungsfähigen Computern ausgestattet werden, die mithilfe von Sensoren den Status des Gerätes permanent überwachen. Tritt ein Fehler auf, oder steht eine Fehlfunktion bevor, so wird automatisch der Kundendienst per Mail oder SMS mit der genauen Fehlerbeschreibung kontaktiert. Dieser kann dann eine Verbindung zum Endgerät aufbauen, und entscheiden, ob eine Reparatur vor Ort notwendig ist, oder ob der Fehler remote behoben werden kann. Ist keine Remote-Behebung möglich, kann der Kundendienst den Besitzer zwecks eines Reparaturtermins kontaktieren.
- Supermarkt: Sämtliche Produkte können mit berührungslosen Chips ausgestattet werden. Somit braucht der Kunde bei der Kassa den Einkaufswagen nicht entladen, sondern es wird mithilfe eines Scanners überprüft, welche Produkte sich in dem Einkaufswagen befinden. Das EDV-System errechnet dann einen Gesamtpreis, und sobald der Kunde bezahlt hat, öffnet sich ein Schranken, und der Kunde kann den Supermarkt verlassen. Kassiererinnen im klassichen Sinn werden somit obsolet.

18.16.2 Problematik

Die Problematik welche sich durch diese Vielzahl an Kleinstcomputern ergibt, ist einerseits im Sicherheitsbereich und andererseits im Administrationsbereich und auch im Bereich des Schutzes der Privatsphäre. Betrachtet man den Aspekt der Privatsphäre, so ergibt sich die Problematik, dass personenbezogene Informationen, sofern keine Sicherheitsrestriktionen vorhanden sind, jederzeit und überall abgerufen werden können. So kann ein Gegenstand, welchen eine Person bei sich trägt, eindeutig identifiziert, sein genauer Aufenthaltsort, Alter usw. überprüft werden. Vor allem Gesetze können hier einen guten Schutz der Privatsphäre bewirken. Im Administrationsbereich ergibt sich das Problem der Wartung und Konfiguration der Billionen von Kleinstcomputern und das Anfallen von gewaltigen Datenmengen und

deren Speicherung. So müsste zum Beispiel eine Textilfirma, die dem Kunden spezifische Angebote machen möchte, die auf ihn massgeschneidert sind, den Kunden bei Eintritt in das Geschäft scannen, um von jedem Textil, dass dieser am Körper trägt, Informationen über Herkunft, Alter usw. zu erhalten. Danach muss aber für jedes Produkt festgestellt werden, worum es sich überhaupt handelt, wodurch Suchanfragen an Datenbanken gestartet werden, deren Dimension kaum vorstellbar ist. Anhand dieser Information kann ermittelt werden, welche Produkte für den Kunden eventuell interessant sein könnten. Selbstverständlich tangiert dieses Szenario wiederum den Privatbereich, denn kein Mensch möchte vollständig „gläsern" werden, und selbst entscheiden können, welche Informationen er preisgibt, und welche nicht. Auch das Zusammenspiel mit der Sicherheit illustriert dieses Beispiel sehr anschaulich. Prinzipiell sollte es nämlich keinesfalls möglich sein, dass jede beliebige Person die Daten aus diesen Kleinstcomputern auslesen kann. Deshalb müssen Vorkehrungen getroffen werden, dass einerseits die Daten nur von Befugten abgerufen werden können, und auch wenn eine selbsttätig ausgelöste Kommunikation der Geräte stattfindet, so müssen die daten welche übertragen werden mit kryptographischen Methoden gegen das Abhören von Dritten geschützt werden.
Geht man davon aus, dass die Kleinstcomputer mit der Leistungsfähigkeit eines heutigen Desktop-PCs vergleichbar ist, ergibt sich zusätzlich die Gefahr, dass Viren oder Würmer diese Kleinstcomputer befallen und damit ihre Funktionalität gefährlich beeinträchtigen. Ein Beispiel hierfür wäre das vollautomatisierte Haus, welches bei schlechter Luftqualität im Innenbereich die Fenster öffnet. Wird dieses System von einem Virus befallen, so könnten die Fenster während des gesamten Winterurlaubs geöffnet bleiben, sodass beträchtliche Schäden vor allem im Bereich der Sanitärinstallationen entstehen können. Man könnte zwar an dieser Stelle argumentieren, dass es sich hierbei einerseits um reine Science Fiction handelt und andererseits, dass niemand einen Nutzen davon hat, das Eigentum anderer, wahrscheinlich sogar unbekannter Personen zu beschädigen. Die Entwicklung der letzten Jahrzente hat aber definitiv gezeigt, dass Dinge, die vor einigen Jahren noch als unmöglich dargestellt wurden, heute alltägliche Realität sind. Auch was die Angreifbarkeit von Systemen betrifft, brauch man sich nur die Berichte über Viren- und Wurmattacken der letzten Monate vor Augen führen. Diese beweisen eindeutig, dass jede Sicherheitslücke ausgenutzt wird, und findige Programmierer immer einen Weg finden diese für einen Angriff zu nutzen.

Anhand der vorhin angesprochenen Anwendungsfälle, soll im folgenden die Problematik dieser erläutert werden:

- Problematik Bibliothek: Die Problematik, die sich hier stellt ist weniger ein Sicherheitsproblem, da die Chips in den Büchern nicht selbstständig zu kommunizieren anfangen, und auch kein administratives Problem, da die Datenbank nur die endliche Anzahl der Bücher enthalten muss, die in der Bibliothek vorhanden sind, aber nicht sämtliche Bücher dieser Welt. Betrachtet man aber den Bereich der Privatsphäre, so könnten z.B. Buchgeschäfte die nach dem Besuch einer Bibliothek aufgesucht werden, die Buch-Daten in den Chips auslesen, und diese als Marketing-Instrument einsetzen.
- Problematik Fernseher und sonstige Haushaltselektronik: In diesem Fall stellt sich das Problem, dass durch unzureichende Schutzmaßnahmen, auch unberechtigte Personen Verbindungen zu den Engeräten aufbauen können. Dadurch können Viren oder Würmer eingeschleust werden, oder verärgerte Nachbarn können die Geräte unbrauchbar machen, oder so umkonfigurieren, dass Brände, Überflutungen oder dergleichen ausgelöst werden.
- Problematik Supermarkt: Die Problematik hierbei gestaltet sich ähnlich, wie bei der Bibliothek. Ein weiteres zusätzliches Problem ergibt sich hier aber durch den Verlust von vielen Arbeitsplätzen, da hiermit der Trend weg von unqualifizierten Tätigkeiten zu hochqualifizierten Spezialisten noch weiter verstärkt wird.

18.16.3 Lösungsmöglichkeiten

Auch bei dieser Zukunftsentwicklung kann die Software „Mobile Security NG (Corporate)" zu einem wichtigen Instrument für die Absicherung dieser Kleinstcomputer werden. Dies setzt aber natürlich eine Leistungsfähigkeit, wie sie auch heutige Desktop-PCs besitzen voraus.
Wie schon im vorigen Abschnitt erläutert, spielt die sichere Kommunikation unter den Einzelgeräten eine sehr wichtige Rolle. Hier kann die VPN-Komponente der Software eingesetzt werden, um jegliche Kommunikation zwischen den Geräten zu verschlüsseln. Auch im Bereich des Schutzes der Privatsphäre spielt diese Komponente eine wichtige Rolle. Mit ihr wird sichergestellt, dass nur autorisierte Personen eine Verbindung zum Endgerät herstellen können um mit diesem dann zu kommunizieren. Somit werden Daten für Dritte völlig unzugänglich.
Auch die Komponenten Firewall, Intrusion Detection, Virenschutz und OS-Hardening spielen bei der Abwehr von Angriffen und diversen Bedrohungen eine wichtige Rolle.
Eindeutig klar ist aber, dass für dieses Szenario die Software immer zentral konfiguriert werden muss. Dies kann einerseits durch Berater des Herstellers bei „Mobile Security NG" sichergestellt werden, bei der Corporate-Variante ist sowieso die zentrale Konfiguration der primäre Aspekt.
Anhand der vorhin angesprochenen Anwendungsfälle, soll im folgenden die Lösungsmöglichkeiten dieser erläutert werden:

- Lösungsmöglichkeiten Bibliothek: Hier könnten die Daten verschlüsselt auf den Chips abgespeichert werden. Dadurch ist nur ein Auslesen von autorisierten Personen möglich.
- Lösungsmöglichkeiten Fernseher und sonstige Haushaltselektronik: Dies ist der klassische Anwendungsfall für „Mobile Security NG (Corporate)". Die Komponenten Firewall, Intrusion Detection, Virenschutz und OS-Hardening spielen bei der Abwehr von Angriffen und diversen Bedrohungen eine wichtige Rolle. Zusätzlich kann die VPN-Komponente der Software eingesetzt werden, um jegliche Kommunikation zwischen den Geräten zu verschlüsseln. Auch im Bereich des Schutzes der Privatsphäre spielt diese Komponente eine wichtige Rolle. Mit ihr wird sichergestellt, dass nur autorisierte Personen eine Verbindung zum Endgerät herstellen können um mit diesem dann zu kommunizieren. Somit werden Daten für Dritte völlig unzugänglich.
- Lösungsmöglichkeiten Supermarkt: Auch hier könnten, wie im Fall der Bibliothek, die Daten verschlüsselt auf den Chips abgespeichert werden. Dadurch ist nur ein Auslesen von autorisierten Personen möglich.

18.16.4 Zusammenfassung

Auch für die zukünftigen Herausforderungen des Pervasive Computing bietet „Mobile Security NG (Corporate)" Ansätze für deren Lösung. Es muss aber in diesem Fall immer von der Annahme ausgegangen werden, dass die Leistungsfähigkeit solcher Kleinstcomputer mit heutigen PC-Systemen vergleichbar ist. Ist dies nämlich nicht der Fall, und diese Computer verfügen über eine geringere Leistungsfähigkeit, so wird es nicht möglich sein eine derart komplexe Software darauf zu implementieren.
Die Frage bleibt aber weiterhin offen, ob die Akzeptanz dieser Geräte überhaupt gewährleistet ist. Einerseits werden solche Geräte anfangs um vieles teurer sein, als vergleichbare herkömmliche Geräte. Vor allem wenn man an intelligente Haushaltsgeräte, wie Waschmaschinen oder Fernseher denkt, die im Fall eines Defekts automatische eine SMS mit der Fehlerbeschreibung an den Kundendienst sendet, damit dieser mit dem Kunden wegen eines Reparaturtermins Kontakt aufnehmen kann.

Wie diese „schöne neue Welt“ aussehen wird, kann nicht eindeutig abgeschätzt werden. Sicher ist aber, dass große Veränderungen in diesem Bereich zu erwarten sind, die unser Alltagsleben entscheidend verändern werden.

18.17 Telefonanlagen der Zukunft in Verbindung mit „Mobile Security NG Corporate“

18.17.1 Einleitung

Heutige Telefonanlagen basieren auf signalorientierten analogen und digitalen Technologien, wie ISDN und PSTN. Durch die Entwicklung von paketbasierenden Technologien, wurden Protokolle, wie H.323 und SIP erst ermöglicht. Dadurch wird die Audio- und Videokommunikation der Zukunft nur mehr über IP-basierende Netze ablaufen. Dadurch ergibt sich die Problematik, diese Paketströme abzusichern. Dieses Kapitel soll beleuchten, wie „Mobile Security NG Corporate“ zu diesem Zweck eingesetzt werden kann. Dabei wird hier nur die Corporate-Variante untersucht, da auf Telefonanlagen niemals von Anwendern gearbeitet wird, sondern nur von erfahrenen Administratoren.

18.17.2 Rahmenbedingungen

Damit IP-basierende Audio- und Video-Kommunikation möglich wird, müssen einige Rahmenbedingungen erfüllt sein.
So müssen Telefonieprovider über eine IP-basierende Schaltstelle bzw. eine IP-basierende Groß-Telefonanlage verfügen, wo Firmen ihre IP-Telefonanlagen anbinden können. Zusätzlich muss der Telefonieanbieter die Möglichkeit der VPN-Anbindung zu seinen Anlagen bereitstellen. Schließlich muss er auch Gateways zur Verfügung stellen, die Verbindungen zu den veralteten Technologien, wie PSTN, ISDN, GSM und dergleichen ermöglichen.
Nur wenn all diese Punkte erfüllt sind, wird es erst möglich sein diese neue Technologie einsetzen zu können.

18.17.3 Architektur

Die Verbindung zwischen Telefonanlage und Endgeräten bzw. zwischen mehreren Telefonanlagen erfolgt dabei über IP-basierende Netze. Dies wird erst dadurch möglich, dass immer mehr Bandbreite zu immer günstiger werdenden Preisen zur Verfügung steht. Dies beseitigt somit die heutige Hauptproblematik, dass die Übertragung von Audio und Video in Echtzeit sehr bandbreitenabhängig ist, und hohe Bandbreite derzeit noch sehr teuer ist.

18.17.3.1 Simple Architektur

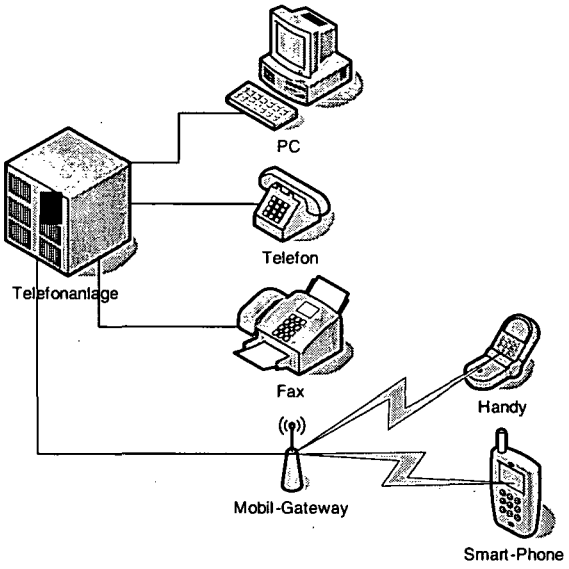


Abbildung 60: Simple Architektur

Die Telefonanlage ist bei dieser Architektur (Abbildung 60) über IP-basierende Netzwerke mit den Endgeräten verbunden. Endgeräte wie Telefon und PC sind dabei direkt mit dem Netzwerk verbunden. PCs sind ebenfalls direkt angebunden, müssen aber über Software-Clients für die Telefon- und Fax-Kommunikation ausgestattet sein. Zusätzlich benötigen PCs eine Soundkarte, sowie ein Mikrophon und Lautsprecher oder Kopfhörer für die Audio-Kommunikation. Mobile Endgeräte werden über ein Mobil-Gateway angesteuert. Dieses Gateway baut ebenfalls eine IP-basierende Verbindung zu den Endgeräten auf, allerdings ist es auch in der Lage ältere Geräte über GSM anzubinden.

18.17.3.2 Verteilte Architektur

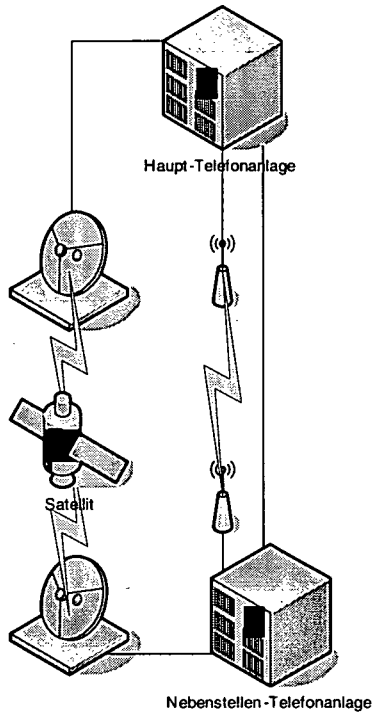


Abbildung 61: Verteilte Architektur

Bei der verteilten Architektur (Abbildung 61) werden Telefonanlagen miteinander verbunden. Dabei existiert im Normalfall eine Haupt-Telefonanlage, welche die gesamte Kommunikation innerhalb der verteilten Architektur steuert. Filialen und Zweigstellen werden somit mit einer Nebenstellen-Telefonanlage angebunden. Sowohl die Hauptstellen-Telefonanlage als auch die Nebenstellen-Telefonanlagen inkludieren somit die simple Architektur. Das bedeutet, dass Engeräte sowohl an der Haupt-Telefonanlage als auch an den Nebenstellen-Telefonanlagen angebunden werden können. Die Anbindung der Nebenstellen an die Zentrale wird bei dieser Architektur entweder durch Standleitungen, IP-basierende Satellitennetzwerke, oder drahtlose Verbindungen hergestellt.
Die Verbindung zu externen Teilnehmern wird ebenfalls über diese Architektur abgebildet. Dabei kommuniziert die Haupt-Telefonanlage über die gleichen Technologien, wie bei der Verbindung mit den Nebenstellen-Telefonanlagen, mit Telefonanlagen des Telfondienstanbieters oder direkt mit Telefonanlagen von vertrauten Firmen.

18.17.4 Problematik

In IP-basierenden Netzen ergibt sich immer die Notwendigkeit der Absicherung der Datenströme, da diese leicht abgehört werden können. Somit ist es für ein rein IP-basierendes Telefonnetz essentiell, dass sowohl die Signalisierung, als auch die Video- und Datenströme verschlüsselt übertragen werden. Den zweiten Angriffspunkt stellen die Engeräte bzw. die Telefonanlage selbst dar. Durch die Anbindung über IP ergeben sich ähnliche Angriffsmöglichkeiten wie bei PCs oder anderen Netzwerkkomponenten. Somit müssen alle Geräte gegen eventuelle Angriffe, Ausnutzung von Sicherheitslücken und Manipulation der auf den Geräten implementierten Software abgesichert werden. Der folgende Abschnitt zeigt Lösungsmöglichkeiten auf, wie dies bewerkstelligt werden kann.

18.17.5 Lösungsmöglichkeiten

18.17.5.1 Eignung der Komponenten von „Mobile Security NG Corporate“

Dieser Abschnitt soll den Einsatz der einzelnen Komponenten von „Mobile Security NG Corporate“ und deren Verwendbarkeit im Hinblick auf die Absicherung von IP-basierenden Telefonnetzen analysieren. Dabei wird nicht unterschieden, ob es sich um firmeninterne Kommunikation oder um externe Kommunikation handelt. Zwar ist es nicht unbedingt erforderlich, auch die interne Kommunikation genauso stark abzusichern, wie die externe Kommunikation, doch ist es wesentlich vernünftiger, wenn die Technologien existieren, diese möglichst flächendeckend einzusetzen. Damit wird verhindert, dass erfolgreiche externe Attacken auch die interne Kommunikation kompromittieren.
Zusätzlich muss genau, wie in Kapitel 18.16 angenommen werden, dass sowohl die Telefonanlagen, als auch sämtliche Endgeräte über entsprechende Leistungsfähigkeit verfügen.

18.17.5.1.1 Firewall

Diese Komponente ist essentiell für den Einsatz in IP-basierenden Telefonnetzen. Dies begründet sich durch die Notwendigkeit der Überwachung und Sperrung von Ports. Damit können unberechtigte Personen keine Verbindung zu den Telefonanlagen bzw. den Endgeräten herstellen, da die Ports nur für bestimmte IP-Adress-Bereiche freigegeben sind. Zusätzlich haben Viren oder Würmer, die sich über bestimmte Ports verbreiten keine Chance, da alle nicht mit der Telefonie in Zusammenhang stehenden Ports gesperrt sind.
Zusätzlich muss die Firewall sämtliche gängigen Internet-Telefonie-Protokolle unterstützen. Auf Signalisierungsseite sind dies derzeit SIP und H.323, auf der Payload-Seite sind dies Protokolle wie z.B. RTP. Daher ist in diesem Fall eine Erweiterung der Funktionalität notwendig, da wie schon in Kapitel 4.6 diskutiert, diese Protokolle aufgrund von dynamisch allokierten Ports funktionieren.

18.17.5.1.2 WLAN

Auch diese Komponente ist dann essentiell, wenn Endgeräte oder Telefonanlagen über drahtlose Verbindungen miteinander kommunizieren. Die Komponente stellt sicher, dass sämtliche WLAN-Verbindungen verschlüsselt und auf maximale Sicherheit konfiguriert werden.

18.17.5.1.3 Netzwerk

Diese Komponente ist das Kernstück, da die meisten Verbindungen über kabelbasierende Netze abgewickelt werden. Die Komponente stellt sicher, dass die Netzwerkverbindungen richtig konfiguriert sind, und somit keine Sicherheitslücken geöffnet bleiben.

18.17.5.1.4 VPN

Diese Komponente spielt ebenfalls eine zentrale Rolle. Um Nebenstellen-Telefonanlagen, oder Telefonanlagen von Drittanbietern anzubinden, empfiehlt sich jedenfalls eine VPN-Verbindung zwischen diesen Telefonanlagen. So wie heute Firmen, die über mehrere Standorte oder Zweigstellen verfügen, den Datenverkehr zwischen diesen über VPN-Verbindungen gegen den Zugriff von Dritten absichern, wird dies auch bei Telefonanlagen der Zukunft eine entscheidende Rolle spielen. Da bei Telefongesprächen oder sonstiger

Audio-Kommunikation oft wesentlich vertraulichere Information, als bei Datenverkehr weitergegeben wird, ist eine Verschlüsselung unbedingt notwendig. Zusätzlich zu den Nutzdaten, sollte aber auch die Signalisierung über diese VPN-Verbindung laufen, damit auch keine Auswertungen von Unbefugten über die Etablierung von Kommunikationsverbindungen erstellt werden können.

18.17.5.1.5 Content Filter

Der Content Filter im herkömmlichen Sinn ist bei der Telefonie der Zukunft nicht wirklich einsetzbar. Er müsste dahingehend modifiziert werden, dass über ihn gesteuert wird, zu welchen Teilnehmern Verbindungen etabliert werden dürfen, bzw. von welchen Teilnehmern Verbindungen akzeptiert werden. Wie in [39] gezeigt, ergibt sich mit SIP hier die elegante Möglichkeit mittels Scripts der Call Processing Language für eingehende (Abbildung 62) und ausgehende Anrufe (Abbildung 63) Filterungen durchzuführen. Somit ist es erforderlich, dass der Content Filter in der Lage ist, Call Processing Language Scripts, welche auf XML basieren zu interpretieren und zu verarbeiten.

```
<?xml version="1.0" ?>
<!DOCTYPE cpl PUBLIC "-//IETF//DTD RFCxxxx CPL 1.0//EN" "cpl.dtd">
<cpl>
      <incoming>
            <address-switch field="origin" subfield="user">
                  <address is="anonymous">
                        <reject status="reject"
                         reason="I don't accept anonymous calls" />
                  </address>
            </address-switch>
      </incoming>
</cpl>
```

Abbildung 62: Incoming Call Screening

```
<?xml version="1.0" ?>
<!DOCTYPE cpl PUBLIC "-//IETF//DTD RFCxxxx CPL 1.0//EN" "cpl.dtd">
<cpl>
      <outgoing>
            <address-switch field="original-destination"
             subfield="tel">
                  <address subdomain-of="0190">
                        <reject status="reject" reason="Not allowed to
                         make 0190 calls." />
                  </address>
            </address-switch>
      </outgoing>
</cpl>
```

Abbildung 63: Outgoing Call Screening

18.17.5.1.6 Intrusion Detection

Die Intrusion Detection ergibt zusammen mit der Firewall den optimalen Schutz gegen Angriffe, da bekannte Angriffssignaturen erkannt und automatisch blockiert werden. Dies ist auch bei telefonanlagen und den dazugehörigen Endgeräten wichtig, da diese auch Ziele von Angriffen werden können.

18.17.5.1.7 AntiVirus

Auch diese Komponente spielt eine entscheidende Rolle in der IP-Telefonie-Welt. Sie dient hier zur Blockierung von Viren und Würmern, um so die Verbreitung auch auf Telefonie-Engeräte und Telefonanlagen zu unterbinden.

18.17.5.1.8 OS-Hardening

Da die Betriebssysteme auf den Endgeräten und den Telefonanlagen vorraussichtlicherweise sehr komplex gestaltet sein werden, wird es auch notwendig sein, das Betriebssystem selbst auf etwaige Angriffsmöglichkeiten und Sicherheitslücken hin zu untersuchen.

18.17.5.2 Ergebnisse

Wie man sieht, sind die meisten Komponenten ohne große Anpassungen auch in der Telefoniewelt einsetzbar. Nur an Firewall und Intrusion Detection werden für die Telefonwelt spezifische Anforderungen zusätzlich benötigt. Der Kern der Firewall muss dabei nicht angetastet werden. Einzig die zusätzliche Unterstützung für SIP und H.323 muss die Firewall beherrschen. Der Content Filter muss von Grund auf geändert werden, da hier keine Filterung auf http-basierende Seiten möglich ist, sondern bestimmte Sender- und Empfänger-Adressen blockiert werden müssen.
Daher kann man sagen, dass auch in der zukünftigen IP-basierenden Telefoniewelt, „Mobile Security NG Corporate“ einen wichtigen Beitrag zu mehr Sicherheit im Unternehmensnetz leistet.

18.17.5.3 Analyse „Mobile Security NG Corporate“ in der Telefoniewelt

18.17.5.3.1 Kriterien

Um das Software-Produkt in der Telefoniewelt bewerten zu können, müssen Kriterien definiert werden, anhand derer eine Bewertung möglich wird.
Diese Kriterien umfassen:

- Sicherheit
- Performance
- Skalierbarkeit
- Kosten

Die Kriterien umfassen hierbei eine Skala von 1 (sehr gut) bis 5 (nicht genügend).

18.17.5.3.1.1 Kriterium Sicherheit

Dieses Kriterium soll bewerten, wie sicher die Software einzustufen ist. Dabei spielt vor allem eine Rolle, inwiefern der Faktor Mensch auf die Sicherheitseinstellungen Einfluss nimmt.

18.17.5.3.1.2 Kriterium Performance

Dieses Kriterium beschreibt die Auslastung der Telefonanlage und der Endgeräte durch die zusätzlich installierte Software.

18.17.5.3.1.3 Kriterium Skalierbarkeit

Dieses Kriterium bewertet die Einfachheit der Integration von zusätzlichen Endgeräten und Telefonanlagen und den damit verbundenen Aufwand.

18.17.5.3.1.4 Kriterium Kosten

Dieses Kriterium beschreibt die Effizienz der Kosten und gibt Hinweise auf den sinnvollen Einsatz der Software.

18.17.5.3.2 Bewertung „Mobile Security NG Corporate"

18.17.5.3.2.1 Sicherheit

Da in der Corporate-Variante sämtliche Einstellungen von hochqualifizierten Administratoren durchgeführt werden, die auch bei Auftreten einer neuen Sicherheitslücke sehr rasch reagieren können, ergibt sich eine deutlich bessere Sicherheit für die Endgeräte und Telefonanlagen. So kann z.B. durch die Anpassung der Firewall-Regeln eine Attacke geblockt werden, die von der Intrusion Detection noch nicht erkannt wird. Deshalb ist die Sicherheit unter der Annahme, dass die Software nur von hochqualifizierten Administratoren konfiguriert wird, hierbei mit 1 (sehr gut) zu bewerten.

18.17.5.3.2.2 Performance

Bei der Performance kann durch den Eingriff der Administratoren ebenfalls mehr erreicht werden, als bei der anderen Variante. So können z.B. Firewall-Regeln getunet werden, und die Konfiguration auf den Endgeräten entsprechend der Endgerät-Performance eingestellt werden. Trotzdem ist sicherlich ein großer Performance-Verlust, vor allem durch die Komplexität und Rechenintensität der Verschlüsselung des Payloads gegeben. Deshalb ergibt sich eine Bewertung von 3 (befriedigend).

18.17.5.3.2.3 Skalierbarkeit

Die Skalierbarkeit ist hierbei sehr hoch, da alle Endgeräte zentral verwaltet und konfiguriert werden. Somit ist es nicht notwendig jedes Endgerät einzeln zu konfigurieren, sondern dies wird zentral verwaltet. Damit spielt die Anzahl der Endgeräte eine nicht so große Rolle. Somit ergibt sich für die Skalierbarkeit eine Bewertung von 1 (sehr gut).

18.17.5.3.2.4 Kosten

Durch den wesentlich höheren Administrationsaufwand und die Bereitstellung von zusätzlicher Hardware (Security Repository, Management Server, Firewall) ergeben sich deutlich höhere Kosten. Vor allem die permanente Schulung der Administratoren, um gegen zukünftige Sicherheitsprobleme gewappnet zu sein, und die Kosten für die Verwaltung der Server und der Software bringen neben den Software-Lizenzen wesentlich höhere Kosten mit sich. Neben diesen Kosten entstehen auch Kosten für die Adaptierung der Firewall-Software und des Content Filters. Diese müssen hierbei natürlich mit einbezogen werden. Dadurch ergibt sich für die Kosten eine Bewertung von 3 (befriedigend).

18.17.5.3.2.5 Bewertung

Aufgrund der Auswertung der Einzelbewertungen ergibt sich folgendes Ergebnis:

	Bewertung
Sicherheit	1
Performance	3
Skalierbarkeit	1
Kosten	3
Durchschnitt	**2**

„Mobile Security NG Corporate“ erzielt somit eine gute Bewertung, was die einzelnen Kriterien betrifft.

18.17.5.3.2.6 Zusammenfassung Bewertung „Mobile Security NG Corporate“

Die Bewertung ergibt, dass bei richtiger Implementation und Betreuung durch geschulte Administratoren ein gutes Ergebnis zu erzielen ist.

18.17.5.3.3 Vergleich „Mobile Security NG Corporate“ im Netzwerk und in der Telefoniewelt

Aufgrund der Auswertung der Einzelbewertungen ergab sich folgendes Ergebnis:

	Telefonie	Netzwerk
Sicherheit	1	1
Performance	3	2
Skalierbarkeit	1	1
Kosten	3	2
Durchschnitt	**2**	**1,5**

„Mobile Security NG Corporate“ erzielte somit eine sehr gute Bewertung im Netzwerk, und eine gute Bewertung in der Telefonwelt, was die einzelnen Kriterien betrifft.

Die Bewertung im Netzwerk und in der Telefoniewelt differiert vor allem aus dem Grund, dass die zu erwartende Performance in der Telefoniewelt deutlich unter der im Netzwerk liegt. Dies begründet sich durch den drastischen Performanceverlust durch die Verschlüsselung der Echtzeitkommunikation. Da diese sehr bandbreitenintensiv im Vergleich zu Daten, die keine Echtzeitübertragung erfordern sind, ist somit bewiesen, dass der Performanceverlust deutlich sichtbar wird.
Zusätzlich unterscheidet sich die Bewertung im Faktor Kosten. Dieser Unterschied entsteht einerseits durch die Portierungskosten in die Telefonwelt und andererseits durch die veränderten Anforderungen an Firewall und Content Filter.

19 Zusammenfassung und Ausblick

Man sieht, dass Sicherheit ein sehr facettenreiches Thema ist, dass bei sehr hohen Anforderungen daran zu einer extrem schwierigen und umfangreichen Aufgabe werden kann. Wir haben gesehen, dass einer der zentralsten Punkte eines umfassenden Sicherheitskonzeptes die Implementation von Firewall-Systemen mit den dazugehörigen Komponenten, wie Proxy-Systeme und Content Filter ein wichtiger Schritt bei der Sicherung eines privaten Netzwerkes darstellt. Weiters wurde gezeigt, welche technischen und organisatorischen Aspekte mit dem Thema eng verwoben sind. Zu den technischen Aspekten zählen Virenschutz, Kryptographie, Datensicherungen, Intrusion Detection Systeme, und die Einbindung von Multimedia-Protokollen. Bei den organisatorischen Maßnahmen kommen vor allem Katastrophenpläne, IT-Regelungen und Benutzerbewusstsein zum Tragen. Man darf aber nie vergessen, dass Sicherheit kein Thema ist, dass nach Einführung und Durchsetzung einer Sicherheitspolitik abgeschlossen ist. Es ist ein kontinuierlicher Verbesserungsprozess, der niemals enden darf. Es treten täglich neue Bedrohungen und Sicherheitslücken auf, und die verantwortlichen Personen müssen laufend darauf richtig reagieren, damit es nicht zur Katastrophe kommt. Die Arbeit hat versucht, die wichtigsten Aspekte aufzuzeigen, beansprucht aber keinen Anspruch auf Vollständigkeit. Es wurde außerdem versucht, möglichst allgemeine Konzepte zu veranschaulichen, die nicht mit bestimmten Technologien in Zusammenhang stehen, um auch für die Zukunft Gültigkeit zu behalten. Wenn die Technologien und Konzepte gewissenhaft eingesetzt werden, und permanent verbessert werden, kann ein Unternehmen derart geschützt werden, dass selbst wenn es zu einem Einbruch in das System kommt, die Folgen nicht zur Katastrophe führen, und das System innerhalb kurzer Zeit wieder verfügbar ist.
Kein Unternehmen kann heutzutage mehr ohne EDV-System existieren. Das EDV-System stellt das Herz eines jeden Unternehmens dar, und wenn es zu schlagen aufhört, dann bedeutet dies bei unzureichenden Vorbeugemaßnahmen meist das Ende des Unternehmens. Die Abhängigkeit von Informationssystemen ist aber nicht mehr rückgängig zu machen. Darum sollte sich das Management bewusst sein, dass fehlende Investitionen im Sicherheitsbereich, vor allem wenn dieser Bereich lange Zeit vernachlässigt wurde, irgendwann zur Katastrophe führen wird.

Anhang A: Literaturverzeichnis

Bücher:

[1] David Chapman, Andy Fox: Cisco Secure PIX Firewalls, Februar 2002
[2] Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman: Einrichten von Internet-Firewalls, 2001
[3] Norbert Pohlmann: Firewall-Systeme, 2001
[4] Michael Näf, Patrick Streule, Werner Hartmann: Risiko Internet?, 2000
[5] Claudia Eckert: IT-Sicherheit, 2003
[6] N. Haller: The S/Key one-time password system, February 1994
[7] A. Fiat, A. Shamir: How To Prove Yourself: Practical Solutions to Identification and Signature Problems, 1986
[8] Simone Fischer-Hübner: IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms, 2001
[9] D.E. Bell, L. LaPadula: Secure Computer Systems: A Mathematical Model, 1973
[10] D.E. Bell, L. LaPadula: Secure Computer Systems: Unified expositions and Multics Interpretation, 1976
[11] K.J. Biba: Integrity Considerations for Secure Computer Systems, 1977
[12] D.Denning: A Lattice Model of Secure Information Flow, 1976
[13] D.Denning: Cryptography and Data Security, 1982
[14] D. Brewer, M. Nash: The Chinese Wall Security Policy, 1989
[15] D. Everett: Identity Verification and Biometrics, 1992
[16] Othmar Kyas, Markus a Campo: IT-Crackdown – Sicherheit im Internet, 2000
[17] Bundesamt für Sicherheit in der Informationstechnik: Mit IT-Sicherheit gegen Internet-Kriminalität?!, 2002
[18] Joel Scamvray, Stuart McClure: Das Anti-Hacker-Buch für Windows, 2002
[19] B. Christianson, B. Crispo, J. A. Malcolm, M. Roe: Security Protocols, 1999
[20] M. Sloman, J. Lobo, E. C. Lupu: Policies for Distributed Systems and Networks
[21] Kai Martius: Sicherheitsmanagement in TCP/IP-Netzen, 2000
[22] Gerald Reischl: Gefährliche Netze, 2001
[23] Simson Garfinkel, Gene Spafford: Practical Unix and Internet Security, 1996
[24] S. Northcutt, J. Novak: IDS: Intrusion Detection-Systeme – Spurensuche im Internet, 2001
[25] Egbert Wald: Backup & Disaster Recovery, 2002
[26] Christian Reiser: Internet – Die Sicherheitsfragen, 2000
[27] Dr. Gerald Kelnhofer: Security, 2001
[28] Matt Curtin: Introduction to Network Security, 1997
[29] Darren Bolding: Network Security, Filters and Firewalls, 2001
[30] Horst Gaigg: Security Tutorial, 2002
[31] Krzysztof Janowicz: Sicherheit im Internet, 2002
[32] Lisa Yeo: Personal Firewalls for Administrators and Remote Users, 2003
[33] Jens Mander: Schutzlos im Internet?, 2001
[34] Martin Raepple: Sicherheitskonzepte für das Internet, 2001
[35] Wolfgang Barth: Das Firewall-Buch, 2001
[36] Keith Strassberg, Richard Gondek, Gary Rollie: Firewalls – The Complete Reference, 2002
[37] Aviel D. Rubin: Hackerabwehr und Datensicherheit, 2002
[38] Mick Tobor: Persönliche Firewalls, 2002
[39] Alexander Dusch: Untersuchung bestehender SIP Serverkomponenten in Zusammenhang mit der Call Processing Language

Artikel:

[40] Axel Sikora: Security im Überblick (Teil 1), 7.1.2003
[41] Axel Sikora: Security im Überblick (Teil 2), 22.1.2003
[42] Jörg Luther: Security im Überblick (Teil 3), 19.3.2003
[43] Axel Sikora: Security im Überblick (Teil 4), 5.5.2003
[44] Axel Sikora: Security im Überblick (Teil 5), 25.6.2003
[45] Axel Sikora: Security im Überblick (Teil 6), 19.3.2003
[46] CERT Coordination Center: Overview of Attack Trends, 2002
[47] Vormetric White Paper: Core Security, 2003
[48] CarnegieMellon Technical Report: State of the Practice of Intrusion Detection Technologies, 2000
[49] CERT Coordination Center: Securing an Internet Name Server, 2002
[50] CERT Coordination Center: Trends in Denial of Service Attack Technology, 2001
[51] Astaro Network Security Whitepaper: Virus Protection Strategies to Combat Electronic Attacks, 2003
[52] Microsoft: Virtual Private Networking in Windows 2000 Whitepaper, 1999
[53] Christopher W. Klaus: Wireless LAN Security FAQ, 2002
[54] CERT Coordination Center: Securing Networks Systematically – The SKiP Method, 2002
[55] CarnegieMellon Technical Report: Foundations for Survivable System Development: Service Traces, Intrusion Traces, and Evaluation Models, 2001
[56] CRA Reports: Security Risk Management: Strategies for Managing Vulnerabilities and Threats to Critical Digital Assets, 2003
[57] Norman ASA: The Norman Book on Computer Viruses
[58] Tom Dunigan: Virtual Private Networks, 2002
[59] GFI Software: Why anti-virus software is not enough: The urgent need for server-based email content checking
[60] GFI Software: Protecting your network against email threats: How to block email viruses and attacks
[61] GFI Software: One Virus Engine Is Not Enough: The Case for Maximizing Network Protection with Multiple Anti-Virus Scanners
[62] Matt Blaze, John Ioannidis, Angelos D. Keromytis: Trust Management and Network Layer Security Protocols
[63] CERT Coordination Center: Managing the Threat of Denial-of-Service Attacks
[64] Singapore IT Security Techno Portal: How to develop a Network Security Policy, 2002
[65] William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan: Your 802.11 Wireless Network has No Clothes, 2001
[66] J. Walker: Unsafe at any key size: an analysis of the WEP encapsulation Tech. Rep. 03628E, IEEE 802.11 committee, März 2000
[67] N. Borisov, I. Goldberg, D. Wagner: Intercepting Mobile Communications: The Insecurity of 802.11, 2001
[68] Joshua Wright: Detecting Wireless LAN MAC Address Spoofing, 2003
[69] ISS Technical White Paper: Wireless LAN Security – 802.11b and Corporate Networks
[70] Chris Kozup: Secure Your WLAN now, 2001
[71] Tanja Moehler: Sicherheitsrisiko Phishing, 2004
[72] Christian Wagner: Spyware/Adware/Malware FAQ and Removal Guide
[73] Pervasive Computing - a Whatis.com definition
[74] Friedemann Mattern: Pervasive Computing / Ubiquitous Computing

RFCs und IEEE-Standards:

[75] RFC 2196: Site Security Handbook
[76] RFC 2401: IPSec
[77] RFC 791: IP Protocol
[78] RFC 1889: RTP Protocol
[79] RFC 3605: RTCP Protocol
[80] RFC 793: TCP Protocol
[81] RFC 768: UDP Protocol
[82] RFC 792: ICMP Protocol
[83] RFC 959: FTP Protocol
[84] RFC 821: SMTP Protocol
[85] RFC 854: Telnet Protocol Specification
[86] RFC 1945: HTTP Protocol
[87] RFC 1918: Adress Allocation for Private Internets
[88] IEEE Standard 802.11: Wireless LAN medium access control (MAC) and physical layer(PHY) specification, 1997

Anhang B: Abbildungsverzeichnis

Abbildung 1: Entwicklung [47] 8
Abbildung 2: Tools und Angreiferwissen 9
Abbildung 3: 4-Schichten Modell 23
Abbildung 4: Simpler Firewall-Aufbau 36
Abbildung 5: Firewall-Aufbau mit DMZ 37
Abbildung 6: Überwachungsrouter 38
Abbildung 7: Dual-Homed-Host 39
Abbildung 8: Architektur mit überwachtem Host 41
Abbildung 9: Architektur mit überwachtem Teilnetz 42
Abbildung 10: Ablauf NAT 44
Abbildung 11: VPN-Verbindung 52
Abbildung 12: Das Security Wheel 54
Abbildung 13: Firewall-Aufbau 72
Abbildung 14: Ad-hoc Modus 78
Abbildung 15: Infrastrukutr-Modus 79
Abbildung 16: Sicherheitsvorfälle in Prozent 2002 [51] 81
Abbildung 17: Virusinfektionen nach Quelle [51] 82
Abbildung 18: Modell Zutrittssystem mit Chip 89
Abbildung 19: Modell Zutrittssystem mit Biometrie 90
Abbildung 20: Architektur mit Chip 91
Abbildung 21: Architektur mit Biometrie 91
Abbildung 22: Sicherer SMTP-Server 93
Abbildung 23: Software-Architektur 99
Abbildung 24: Schnittstellen 100
Abbildung 25: Internetverbindungsfirewall 102
Abbildung 26: Netzwerkkarten-Konfiguration 103
Abbildung 27: Modem-Konfiguration 104
Abbildung 28: Kennwort-Konfiguration 104
Abbildung 29: Ablauf Vorabkonfiguration 105
Abbildung 30: Einbruchsversuch 106
Abbildung 31: Deaktivierung der Internetverbindung 106
Abbildung 32: Ablauf Echtzeitkonfiguration 107
Abbildung 33: VPN-Software 108
Abbildung 34: Konfiguration VPN-Traffic 108
Abbildung 35: Aktivierung bei VPN-Verbindung 109
Abbildung 36: Ablauf VPN 109
Abbildung 37: Remote 111
Abbildung 38: Automatische Updates 111
Abbildung 39: Systemwiederherstellung 112
Abbildung 40: Dienste 112
Abbildung 41: Ablauf OS-Hardening 113
Abbildung 42: Architektur von „Mobile Security NG“ 115
Abbildung 43: Download und Installation 116
Abbildung 44: Komponenten 118
Abbildung 45: Internetverbindung 119
Abbildung 46: Internet-Nutzung 119
Abbildung 47: Firmendaten 120
Abbildung 48: Firewall 120
Abbildung 49: Policy-Editor 121
Abbildung 50: Internetverbindung 122
Abbildung 51: Updates 122
Abbildung 52: Firewall-Konfiguration 122
Abbildung 53: VPN 123
Abbildung 54: Content Filter 123
Abbildung 55: Intrusion Detection 123
Abbildung 56: AntiVirus 124
Abbildung 57: OS-Hardening 124
Abbildung 58: Architektur von „Mobile Security NG Corporate“ 126
Abbildung 59: Download und Installation 128

Abbildung 60: Simple Architektur 140
Abbildung 61: Verteilte Architektur 141
Abbildung 62: Incoming Call Screening 143
Abbildung 63: Outgoing Call Screening 143

Anhang C: Liste der wichtigsten Ports

Port	Type	Keyword	Description
7	TCP	echo	Echo
7	UDP	echo	Echo
9	TCP	discard	Discard
9	UDP	discard	Discard
11	TCP	systat	Active Users
11	UDP	systat	Active Users
13	TCP	daytime	Daytime (RFC 867)
13	UDP	daytime	Daytime (RFC 867)
17	TCP	qotd	Quote of the Day
17	UDP	qotd	Quote of the Day
18	TCP	msp	Message Send Protocol
18	UDP	msp	Message Send Protocol
19	TCP	chargen	Character Generator
19	UDP	chargen	Character Generator
20	TCP	ftp-data	File Transfer [Default Data]
20	UDP	ftp-data	File Transfer [Default Data]
21	TCP	ftp	File Transfer [Control]
21	UDP	ftp	File Transfer [Control]
22	TCP	ssh	SSH Remote Login Protocol
22	UDP	ssh	SSH Remote Login Protocol
23	TCP	telnet	Telnet
23	UDP	telnet	Telnet
25	TCP	smtp	Simple Mail Transfer
25	UDP	smtp	Simple Mail Transfer
43	TCP	nicname	Who Is
43	UDP	nicname	Who Is
49	TCP	tacacs	Login Host Protocol (TACACS)
49	UDP	tacacs	Login Host Protocol (TACACS)
53	TCP	domain	Domain Name Server
53	UDP	domain	Domain Name Server
65	TCP	tacacs-ds	TACACS-Database Service
65	UDP	tacacs-ds	TACACS-Database Service
66	TCP	sql*net	Oracle SQL*NET
66	UDP	sql*net	Oracle SQL*NET
67	TCP	bootps	Bootstrap Protocol Server
67	UDP	bootps	Bootstrap Protocol Server
68	TCP	bootpc	Bootstrap Protocol Client
68	UDP	bootpc	Bootstrap Protocol Client
69	TCP	tftp	Trivial File Transfer
69	UDP	tftp	Trivial File Transfer
70	TCP	gopher	Gopher
70	UDP	gopher	Gopher
79	TCP	finger	Finger
79	UDP	finger	Finger
80	TCP	www-http	World Wide Web HTTP
80	UDP	www-http	World Wide Web HTTP
88	TCP	kerberos	Kerberos
88	UDP	kerberos	Kerberos
110	TCP	pop3	Post Office Protocol - Version 3

110	UDP	pop3	Post Office Protocol - Version 3
111	TCP	sunrpc	SUN Remote Procedure Call
111	UDP	sunrpc	SUN Remote Procedure Call
119	TCP	nntp	Network News Transfer Protocol
119	UDP	nntp	Network News Transfer Protocol
123	TCP	ntp	Network Time Protocol
123	UDP	ntp	Network Time Protocol
135	TCP	epmap	DCE endpoint resolution
135	UDP	epmap	DCE endpoint resolution
137	TCP	netbios-ns	NETBIOS Name Service
137	UDP	netbios-ns	NETBIOS Name Service
138	TCP	netbios-dgm	NETBIOS Datagram Service
138	UDP	netbios-dgm	NETBIOS Datagram Service
139	TCP	netbios-ssn	NETBIOS Session Service
139	UDP	netbios-ssn	NETBIOS Session Service
143	TCP	imap	Internet Message Access Protocol
143	UDP	imap	Internet Message Access Protocol
161	TCP	snmp	SNMP
161	UDP	snmp	SNMP
162	TCP	snmptrap	SNMPTRAP
162	UDP	snmptrap	SNMPTRAP
177	TCP	xdmcp	X Display Manager Control Protocol
177	UDP	xdmcp	X Display Manager Control Protocol
194	TCP	irc	Internet Relay Chat Protocol
194	UDP	irc	Internet Relay Chat Protocol
389	TCP	ldap	Lightweight Directory Access Protocol
389	UDP	ldap	Lightweight Directory Access Protocol
443	TCP	https	http protocol over TLS/SSL
443	UDP	https	http protocol over TLS/SSL
445	TCP	microsoft-ds	Microsoft-DS
445	UDP	microsoft-ds	Microsoft-DS
500	TCP	isakmp	isakmp
500	UDP	isakmp	isakmp
514	UDP	syslog	
546	TCP	dhcpv6-client	DHCPv6 Client
546	UDP	dhcpv6-client	DHCPv6 Client
547	TCP	dhcpv6-server	DHCPv6 Server
547	UDP	dhcpv6-server	DHCPv6 Server
565	TCP	whoami	whoami
565	UDP	whoami	whoami
601	TCP	syslog-conn	Reliable Syslog Service
601	UDP	syslog-conn	Reliable Syslog Service
614	TCP	sshell	SSLshell
614	UDP	sshell	SSLshell
636	TCP	ldaps	ldap protocol over TLS/SSL (was sldap)
636	UDP	ldaps	ldap protocol over TLS/SSL (was sldap)
691	TCP	msexch-routing	MS Exchange Routing
691	UDP	msexch-routing	MS Exchange Routing
749	TCP	kerberos-adm	kerberos administration
749	UDP	kerberos-adm	kerberos administration
989	TCP	ftps-data	ftp protocol, data, over TLS/SSL
989	UDP	ftps-data	ftp protocol, data, over TLS/SSL
990	TCP	ftps	ftp protocol, control, over TLS/SSL

990	UDP	ftps	ftp protocol, control, over TLS/SSL
992	TCP	telnets	telnet protocol over TLS/SSL
992	UDP	telnets	telnet protocol over TLS/SSL
993	TCP	imaps	imap4 protocol over TLS/SSL
993	UDP	imaps	imap4 protocol over TLS/SSL
994	TCP	ircs	irc protocol over TLS/SSL
994	UDP	ircs	irc protocol over TLS/SSL
995	TCP	pop3s	pop3 protocol over TLS/SSL (was spop3)
995	UDP	pop3s	pop3 protocol over TLS/SSL (was spop3)

Anhang D: Lebenslauf

Persönliche Daten:

Name	Alexander Dusch
akademischer Grad	Dipl.-Ing.
Adresse	Leibnizgasse 55-57/16 1100 Wien
Geburtsdatum	29. Dezember 1975
Geburtsort	Wien
Staatsangehörigkeit	Österreich

Ausbildung:

1982-1986	Volksschule „Lutherschule“ in 1180 Wien
1986-1994	AHS Geblergasse in 1170 Wien
Juni 1994	Matura
1994-2001	Studium „Informatik“ an der TU-Wien mit Schwerpunkt „Informations- und Kommunikationssysteme“
August 2000-Jänner 2001	Diplomarbeit mit dem Thema „Untersuchung bestehender SIP-Serverkomponenten in Zusammenhang mit der Call-Processing-Language“
2002-2004	Doktoratsstudium der technischen Wissenschaften an der Fakultät für Technische Naturwissenschaften und Informatik