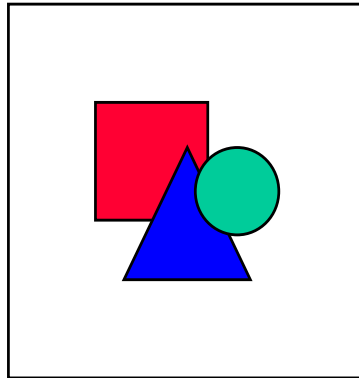


# **Fachhochschule Münster**

**Abteilung Steinfurt**

**Fachbereich Elektrotechnik**

Labor für Technische Informatik



## **Diplomarbeit**

Ein firewall-geschützter Internet-Server unter  
Windows NT

Diplomand: cand. ing. Rüdiger Schleifnig

Referent: Prof. Dr. Norbert Witt

Koreferent: Prof. Dr. Manfred Langenberg

## 0. Vorwort

Immer mehr Menschen nutzen das Internet für private oder geschäftliche Zwecke. Immer mehr Firmen und Behörden wissen die Vorteile des Intranets zu schätzen. An vielen Stellen werden heutzutage die Vorteile von beiden Netzen verknüpft, um möglichst effektives Arbeiten zu ermöglichen; Stichworte sind E-Mail, Online-Shopping, Online-Banking, Internet-Surfing, Datenkonsistenz, verteilte Systeme und Client-Server-Architekturen.

Immer weniger Menschen sind jedoch in der Lage, die komplexen Strukturen, die diese neuen Techniken mit sich bringen oder durch die sie erst möglich werden, zu durchschauen. Auf der Gegenseite der vielen Vorteile, die diese nahezu grenzenlosen Kommunikationsmöglichkeiten bieten, stehen viele nicht zu unterschätzende Sicherheitsrisiken. Anders als bei den positiven Seiten dieser Entwicklung wissen aber viele Benutzer nichts von den Risiken oder unterschätzen und ignorieren diese.

In dieser Diplomarbeit können aufgrund der knapp bemessenen Zeit, vorgesehen für die Diplomarbeit an der Fachhochschule sind etwa drei Monate, keine eigenständigen Untersuchungen über Viren oder andere Bedrohungen von Computersystemen durchgeführt werden. Diese Untersuchungen werden durch eine systematische Recherche, vor allem im Internet, ersetzt.

Die Diplomarbeit soll zeigen, dass es sowohl im homogenen wie auch in einem heterogenen Umfeld - der Windows NT Server steht in einem UNIX-dominierten Netzwerk - möglich ist, mit geringem finanziellen und personellen Aufwand einen „relativ“ sicheren Netzwerkserver mit Internetanbindung aufzubauen, welcher sowohl Angriffen von innen als auch von außen in einem gewissen Rahmen widerstehen kann.

Vollkommene Sicherheit gibt es nicht und maximale Sicherheit wird man in diesem Zeit- und Kostenrahmen nicht erreichen können. Zu erreichen ist aber ein wesentlich höherer Sicherheits-Level als ihn Windows NT standardmäßig mit sich bringt.

## 1. Danksagung

Mein ganz besonderer Dank gilt meiner Familie, die es mir ermöglicht hat, dieses Studium trotz einiger zwischenzeitlicher Probleme und Tiefpunkte zu beenden.

Weiterhin möchte ich mich bei Herrn Professor Dr.rer.nat. Norbert Witt dafür bedanken, dass er diese Diplomarbeit betreut hat, und dass er es in der ihm eigenen Art und Weise tat. Er war immer da, hat dort wo er konnte Unterstützung angeboten, aber nicht „regulierend“ in die Diplomarbeit eingegriffen, sondern lediglich Ratschläge gegeben.

Herrn Prof. Dr.rer.nat. Manfred Langenberg möchte ich dafür danken, dass er trotz terminlichem Engpass bereit war, meine Diplomarbeit als Koreferent zu betreuen.

Obwohl eine Diplomarbeit den Nachweis erbringen soll, dass der Student in der Lage ist, ein wissenschaftliches Thema in einem angemessenen Zeitrahmen eigenständig zu bearbeiten, kommt wohl keine Diplomarbeit ohne Tips, Ratschläge oder kritische Fragen anderer Personen aus.

Unter diesem Eindruck möchte ich mich auch bei Herr Dipl.Ing. Ulrich Geupel, der sich als Laboringenieur um die Beschaffung der Hardware gekümmert hat, oft den einen oder anderen Rat hatte oder die „dringend“ benötigten Teile aus dem Ärmel zauberte, bedanken.

Auch bei Herrn Dr. Dirk Böhme, der als Leiter der DVZ mit Rat und Tat bei der Realisierung des technischen Umfeldes des Internet-Servers zur Verfügung stand und als Windows-NT-Kenner die eine oder andere Anregung zum Einsatz und zur Optimierung des Betriebssystems gegeben hat, möchte ich mich bedanken.

Steinfurt, im Juni 1999

## 2. Inhaltsverzeichnis

<b>0. Vorwort.....</b>	<b>2</b>
<b>1. Danksagung.....</b>	<b>3</b>
<b>2. Inhaltsverzeichnis .....</b>	<b>4</b>
<b>3. Die Aufgabenstellung .....</b>	<b>10</b>
<b>4. Die eingesetzte Hardware .....</b>	<b>11</b>
<b>5. Das ISO-OSI Referenzmodell und die wichtigsten Protokolle.....</b>	<b>12</b>
5.1 Die 7 Schichten des ISO-OSI-Referenzmodells .....	12
5.1.1 Schicht 1: Physical Layer.....	12
5.1.2 Schicht 2: Data-Link-Layer .....	12
5.1.3 Schicht 3: Network Layer .....	13
5.1.4 Schicht 4: Transport Layer.....	13
5.1.5 Schicht 5: Session Layer .....	14
5.1.6 Schicht 6: Presentation Layer.....	14
5.1.7 Schicht 7: Application Layer .....	14
5.2 Netzübergänge und deren Funktionsweise .....	15
5.2.1 Repeater .....	15
5.2.2 Bridges.....	15
5.2.3 Router .....	16
5.2.4 Gateways.....	16
5.3 Die wichtigsten Protokolle.....	19
5.3.1 Das Internet-Protocol (IP).....	19
5.3.2 Das Transport Control Protocol (TCP) .....	21
5.3.3 Das User Datagram Protocol (UDP).....	22
5.3.4 Das Internet Control Message Protocol (ICMP) .....	23
5.3.5 Das Routing Information Protocol (RIP) .....	23
5.3.6 Das Address Resolution Protocol (ARP) .....	23
5.3.7 Das Reverse Address Resolution Protocol (RARP).....	24
5.3.8 Das Simple Mail Transfer Protocol (SMTP) .....	24
5.3.9 Das (Trivial) File Transfer Protocol (TFTP, FTP).....	24
5.3.10 Das Serial Line Internet Protocol (SLIP) .....	24
5.3.11 Das Point To Point Protocol (PPP) .....	25
5.3.12 Das Hypertext Transfer Protocol (HTTP).....	25
5.3.13 Das Domain Name System (DNS).....	26
5.3.14 Die Terminal Emulation (Telnet).....	27
5.4 Portnummer .....	30

<b>6. Sicherheitskonzepte moderner Betriebssysteme, hier Windows NT 4.0 .....</b>	<b>31</b>
<b>7. Sicherheitsrisiken im Intranet und Internet .....</b>	<b>32</b>
7.1 Einleitung.....	32
7.2 Die Täter und deren Angriffsmotivation.....	34
7.3 Angriffe auf Computersysteme und Daten und deren Prävention .....	38
7.3.1 Viren und „Malicious Code“ .....	38
7.3.1.1 Allgemeines zu Computerviren .....	38
7.3.1.1.1 Definitionen.....	38
7.3.1.1.2 Viren-History.....	39
7.3.1.1.3 Voraussetzungen für Virenbefall .....	40
7.3.1.1.4 Was sind Viren und wozu sind sie in der Lage .....	42
7.3.1.2 Virenarten.....	45
7.3.1.2.1 Boot(sektor)-Viren und deren Funktionsweise .....	45
7.3.1.2.2 Programm- oder Datei (File) –Viren.....	50
7.3.1.2.3 Hybrid- oder Multipartite-Viren .....	50
7.3.1.2.4 Daten- oder Makroviren .....	51
7.3.1.3 Tarnmechanismen der Viren .....	53
7.3.1.3.1 Polymorphismus.....	53
7.3.1.3.2 Stealth - Mechanismus.....	53
7.3.1.3.3 Slow - Mechanismus .....	53
7.3.2 Trojanische Pferde .....	54
7.3.3 Würmer .....	55
7.3.4 Hoaxes .....	56
7.3.5 Logische Bomben .....	56
7.3.6 „Back Orifice“ und „NetBus“ .....	57
7.3.6.1 „Back Orifice“ .....	57
7.3.6.2 „NetBus“ .....	59
7.3.7 Cookies .....	60
7.3.8 Virenschutz und Virenbekämpfung .....	61
7.3.8.1 Sensibilisierung von Benutzern.....	62
7.3.8.2 Viren-Schilde .....	63
7.3.8.3 Viren-Scanner.....	63
7.3.8.4 Checksummen-Prüfer .....	64
7.3.8.5 „Mutation Engines“ .....	64
7.3.9 Entwicklung der Viren während der Diplomarbeit .....	65
7.4 Sicherheitslücken moderner Betriebssysteme, hier Windows NT 4.0 .....	66
7.4.1 Account- und Passwortangriffe.....	66
7.4.1.1 Passwortraten .....	66
7.4.1.2 Passwort-Cracking-Angriffe.....	68
7.4.1.2 Passwort Spionage.....	68
7.4.1.4 GetAdmin.Exe - Angriffe.....	68
7.4.1.5 Registry-Angriffe .....	69
7.4.1.6 NTFSDOS.exe - Angriffe.....	69

---

7.4.1.7 Linux NT-Angriffe .....	69
7.4.1.8 Samba-Angriffe .....	69
7.4.2 Netzwerkangriffe .....	70
7.4.2.1 SMB-Angriffe .....	70
7.4.2.2 RPC-Angriffe .....	71
7.4.2.3 Red-Button-Angriff .....	71
7.4.2.4 DLL-Angriffe .....	72
7.4.3 Sabotageangriffe .....	72
7.4.3.1 Ping of Death .....	72
7.4.3.2 SYN-Flooding-Angriffe .....	73
7.4.3.3 CPU-Angriffe .....	73
7.4.3.4 SMB-Crashes .....	73
7.4.3.5 Out of Band Data .....	73
7.4.4 Applikationsangriffe .....	74
7.5 Angriffe durch Sicherheitslücken in den Kommunikationsprotokollen .....	75
7.5.1 Angriffe durch Internet Protokolle .....	75
7.5.1.1 Internet Adress-/Name-Spoofing .....	75
7.5.1.2 TCP-Sequenznummer Angriff .....	76
7.5.1.3 ICMP Angriffe .....	79
7.5.1.3.1 "Destination Unreachable" .....	79
7.5.1.3.2 „Source Quench“ .....	80
7.5.1.3.2 „Redirect“ .....	80
7.5.1.4 IP-Fragment-Angriff .....	80
7.5.1.5 Internet Routing Angriffe .....	81
7.5.1.5.1 Der Source-Routing-Angriff .....	81
7.5.1.5.2 Der RIP-Angriff .....	82
7.5.1.6 Broadcast Stürme durch ARP Missbrauch .....	82
7.5.1.7 UDP Spoofing .....	82
7.5.2 DNS-Angriffe .....	83
7.5.3 Mail-Spoofing auf Basis von SMTP .....	83
7.5.4 Telnet .....	84
7.5.5 FTP .....	85
7.5.6 EGP Spoofing .....	85
7.6 Sicherheitslücken im World Wide Web .....	86
7.6.1 Browser .....	86
7.6.1.1 Ausspähung persönlicher Daten .....	86
7.6.2 Risiken durch Search-Engines .....	86
7.7 Sicherheitslücken von Java und Active - X .....	87
7.7.1 Java-Angriffe .....	87
7.7.1.1 Sabotageangriffe .....	87
7.7.1.2 System-Manipulation und Informationsausspähung .....	87
7.7.1.3 Inter-Applet-Manipulation .....	88
7.7.1.4 Ausnutzung von Implementationsfehler .....	88

7.7.1.5 Nutzung von Java-Funktionen.....	88
7.7.2 Java Script-Angriffe.....	89
7.7.2.1 MIME-Angriffe.....	89
7.7.2.2 Webseiten-Monitoring.....	89
7.7.2.3 Webseiten-Hijacking.....	89
7.7.2.4 LiveConnect-Angriffe.....	90
7.7.3 Active-X.....	90
7.8 Das Jahr 2000 Problem (Y2K).....	91
<b>8. Kryptographie.....</b>	<b>92</b>
8.1 Grundlagen.....	92
8.2 Verschiedene kryptographische Verfahren zur Datenübertragung.....	92
8.2.1 Symmetrische Verschlüsselungsverfahren.....	92
8.2.2 Asymmetrische Verschlüsselungsverfahren.....	93
8.2.3 Hash-Funktionen.....	94
8.2.4 Beispiele.....	95
8.2.4.1 IDEA.....	95
8.2.4.2 RSA.....	95
8.2.4.3 Pretty Good Privacy (PGP).....	96
<b>9. Grundlagen von Firewall-Systemen.....</b>	<b>97</b>
9.1 Grundlagen.....	97
9.2 Firewall-Architekturen.....	99
9.2.1 Verschiedene Ebenen der Zugriffskontrolle.....	99
9.2.1.1 Paketfilter.....	99
9.2.1.2 Circuit Relays.....	99
9.2.1.3 Application Relays.....	100
9.2.2 Die verschiedenen Firewall-Topologien.....	100
9.2.2.1 Begrenzungs-Router.....	100
9.2.2.2 Begrenzungs-Router mit abgesichertem Zwischennetz.....	101
9.2.2.3 Dual (Multi-) Home Bastion Host mit Paketfilter.....	101
9.2.2.4 Dual (Multi-) Home Bastion Host mit Circuit Relay.....	101
9.2.2.5 Dual (Multi-) Home Bastion Host mit Application Relay.....	101
9.2.2.6 Dual (Multi-) Home Bastion Host mit demilitarisierter Zone (DMZ).....	101
9.2.2.7 Kaskadierte Dual (Multi-) Home Bastion Hosts.....	102
9.2.3 Grenzen von Firewall-Systemen.....	103
<b>10. Aufwertung des Betriebssystems und Einrichtung einer Firewall-Lösung.....</b>	<b>104</b>
10.1 Anpassung und Aufwertung des Betriebssystems NT 4.0.....	106
10.1.1 Generelles Sicherheitskonzept (Security Policy).....	106
10.1.2 Service Packs und Hotfixes.....	107
10.1.3 Antiviren Programm, hier Norton-Anti-Virus 5.0 für NT.....	108

10.1.4	Sicherung durch Veränderung der Standardeinstellungen des Betriebssystems .....	109
10.1.4.1	Änderungen des Registry.....	110
10.1.4.2	Benutzerrechte.....	117
10.1.4.3	Zugriffsrechte auf Dateien und Ressourcen.....	122
10.1.5	Zusätzliche Programme zur Gefahrenabwehr .....	125
10.1.5.1	NetBuster.....	125
10.1.5.2	UltraScan.....	125
10.1.6	Überwachung aller wichtigen Vorgänge und Zugriffe.....	126
10.2	Anpassung und Aufwertung des MIIS 2.0.....	127
10.2.1	Sicherung durch Veränderung der Standardeinstellungen des MIIS.....	127
10.2.1.1	Änderungen des Registry.....	127
10.2.1.1	Zugriffsrechte auf Dateien und Ressourcen.....	140
10.2.2	Protokollierung aller wichtigen Vorgänge und Zugriffe.....	140
10.3	Anpassung und Aufwertung des MIE 4.1 .....	141
10.4	Firewall-System .....	144
10.4.1	Installation des Betriebssystems Windows NT 4.0.....	144
10.4.2	Einrichtung des „NetGuard-Firewall-Systems“ .....	145
10.5	Intrusion Detection Systems (IDS) .....	147
10.5.1	Erkennung von Anomalien im Datenverkehr.....	147
10.5.2	Erkennung von Einbruchssignaturen .....	148
10.6	Vorgehensweise bei eingetretenem Sicherheitsfall.....	148
10.6.1	Die Schadensbegrenzung .....	149
10.6.2	Die Täterermittlung.....	149
<b>11.</b>	<b>Sicherheits-Check des konfigurierten Computers.....</b>	<b>150</b>
11.1	Viren .....	150
<b>12.</b>	<b>Schutz der Daten und Erhöhung der Verfügbarkeit .....</b>	<b>151</b>
12.1	Erhöhung der Datenverfügbarkeit.....	151
12.1.1	Spiegelplatten.....	151
12.1.2	Simulation eines Festplattenausfalls .....	151
12.1.3	Inkonsistenter Spiegelplattensatz .....	152
12.2	Erhöhung der Rechnerverfügbarkeit.....	152
12.2.1	Die Umsetzung im Rahmen der Diplomarbeit .....	153
<b>13.</b>	<b>Die Homepage für das Labor Technische Informatik .....</b>	<b>154</b>
13.1	Grundlagen.....	154
13.2	Umsetzung .....	157
13.2.1	Das Layout .....	157
13.2.2	Passwortabfragen .....	159
13.2.3	Download von Praktikumsaufgaben .....	160
13.3	Struktogramm der Homepage .....	161

---



<b>14. Zusammenfassung .....</b>	<b>162</b>
<b>Anhang A: Einige wichtige „Well-Known-Ports“ .....</b>	<b>165</b>
<b>Anhang B: Abbildungsverzeichnis.....</b>	<b>166</b>
<b>Anhang C: Quellennachweis .....</b>	<b>167</b>
<b>Anhang D: Glossar .....</b>	<b>170</b>
<b>Anhang E: Quellcodes der Homepage .....</b>	<b>172</b>
E1: Quellcode der Seite index.htm .....	172
E2: Quellcode der Seite java.htm.....	177
E3: Quellcode der Seite Java-Downloadseite .....	180
<b>Anhang F: Bugfixes der Service Packs 1 – 4 für NT 4.0 .....</b>	<b>182</b>
<b>Anhang G: Die CD-ROM.....</b>	<b>217</b>