# Angriffe auf Firewalls

Guido Stepken
stepken@little-idiot.de

## Inhaltsverzeichnis

# 1 Einleitung

Das Thema „Angriffe auf Firewalls“ ist unglaublich komplex. Einige Untersuchungen von Angriffen auf Datenbanken von Unternehmen im Internet und Intranet haben gezeigt, daß es prinzipiell kaum zu verhindern ist, daß wertvolle Daten entführt werden können. Da zunehmend auch Datenbanken im Internet oft einen großen Anteil am Betriebskapital der Unternehmen darstellen, ist es wichtig, herauszufinden, wie professionelle Cracker vorgehen könnten, um an die Daten zu gelangen und gleichzeitig ihr Eindringen zu verschleiern. Hierzu werden im hohem Maße DoS (Denial of Service)-Angriffe auf IDS-Systeme und Logserver gestartet. Viele dieser DoS-Angriffe auf Server funktionieren leider auch durch Firewalls hindurch, was für Betreiber von Internet Datenbanken hohe Verluste bedeuten kann. In der jüngsten Vergangenheit sind wiederholt Angriffe auch auf prominente Internet-Dienstleister bekannt geworden: SWR, Microsoft, Netscape, Articon, Yahoo, zahlreiche Computer-Fachzeitschriften (Computerwoche), CD-Special, DH-Media, ZDH, Handwerkskammern, SPD, FDP, Bundesministerium für Verkehr (BMV), Siemens, Banken... Diese waren zum großen Teil durch Firewalls gesichert. Es ist davon auszugehen, daß viele Firewalls gegen DoS-Angriffe nicht mehr ausreichend schützen können. Der Grund liegt häufig in der unzureichenden Kenntnis von Angriffsvarianten bei Betreibern und Systemberatern.

Von Firewalls wird im allgemeinen erwartet, daß diese Angriffe aus dem Internet abwehren können. In letzter Zeit wurden immer wieder Angriffe über Firewalls hinweg bekannt, die Schwächen in Anwendungsprogrammen auf Arbeitsstationen hinter der Firewall ausnutzen. Die Firewalls selber besitzen inzwischen eine hohe Qualität und Sicherheit auch gegen Fehlbedienungen. Dies sind Tatsachen, die es einem Cracker nur noch in Einzelfällen ermöglicht, einen altbekannten Fehler auszunutzen. Daher suchen sich Cracker stets die schwächste Stelle in einem Netzwerk; diese ist nicht mehr das Firewall-System selber, sondern der Arbeitsplatzrechner hinter der Firewall. Das einzig echte Problem für Cracker besteht darin, irgendeinen Anwender im Netzwerk dazu zu bringen, sein Programm zu starten.

Einige Anwendungsprogramme, wie Microsofts Winword, Excel, Outlook, und der Internet-Explorer sind entsprechend der Philosophie von Microsoft nicht nur mit der Fähigkeit ausgestattet, Makros zu starten, sondern bieten auch die Möglichkeit, untereinander verschiedenste DLLs auszutauschen. Dies ermöglicht z.B. auch den Einsatz von Visual Basic in Microsoft-Produkten. Visual Basic ist inzwischen eine ausgewachsene Programmiersprache und erlaubt es auch, über die WinSock-Bibliotheken direkten Zugang zu den Netzwerkkarten des Hosts zu

erhalten. Es lassen sich recht schnell Winword-Makros programmieren, die z.B. einen Netzwerkscanner als Basic-Code enthalten. Dasselbe trifft auf die (meist ungenutzte) Skriptsprache von Outlook zu. Je besser sich ein Cracker auf Windows spezialisiert hat, umso einfacher ist es für ihn, die Firewall zu überwinden. Da Virenscanner ausschließlich nur bekannte Viren oder Programme (NetBus, BO) erkennen können, werden speziell programmierte Angriffswerkzeuge nicht erkannt. Hierbei spielt es auch keinerlei Rolle mehr, von welchem Hersteller die Firewall oder der Filter ist.

Die Schwächen, die ein Cracker im System ausnutzt (Firewalls sind nur ein Bestandteil), sind:

- Buffer Overflows
- Trojanische Pferde
- DoS-Angriffe auf den TCP/IP Stack
- Programmierfehler in Anwendungsprogrammen (Browser)
- Makro-/Skriptsprachen in Anwendungsprogrammen (Word, Outlook Express)
- Fehler beim Aufbau des Firewall-Systems
- Unzureichende Filtermaßnahmen

# 2 Kurzer Einblick in Firewalls

Der Begriff Firewall ist leider nicht präzise definiert. Das führt mitunter dazu, daß einige Hersteller in ihrer Werbung den Begriff Firewall für Produkte verwenden, die über die Eigenschaften eines Paketfilters nicht hinausreichen. Daher seien hiermit noch einmal die wesentlichen Unterschiede zwischen Firewalls erläutert.

Firewall-Router können nach IP-Nummern und Portnummern selektieren. Dies sind im Prinzip die Grundfunktionen, die alle Firewalls gemeinsam beherrschen. Für die Übertragung von komplexeren Protokollen, wie NFS, Windows NT PDC, RPC usw. ist es beim Einsatz von diesen Filtern notwendig, daß alle Ports $> 1024$ für Protokolle wie UDP und RPC freigeschaltet werden müssen. Da auch z.B. Netmeeting und andere Videokonferenzsysteme auf UDP basieren, ergeben sich hier erhebliche Sicherheitsprobleme. Viele Firewall-Router besitzen keinen vollständigen TCP/IP-Stack. Daher erkennen diese zwar „spoofing attacks“, in den meisten Fällen sind DoS-Angriffe auf TCP/IP-Stacks der Server dahinter erfolgreich.

## 2.1 Stateful Packet Filter

SPF´s eignen sich aufgrund ihres Designs hervorragend, eine Programmiersprache hinzuzufügen, die somit nicht implementierte Proxy-Mechanismen für neue Protokolle simulieren kann. Da auch kombinierte Protokolle aus TCP und UDP (NFS, NIS+, RPC usw.) hiermit kontrolliert werden können, entsteht so schnell der Eindruck von Sicherheit, wo effektiv keine ist. Beispiel aus dem Handbuch von Checkpoint:

> Instructions for adding Sybase SQL server support to FireWall-1:
> Sybase SQL uses TCP ports above 1024. The port used is defined in the configuration of the Sybase server.
>
> To configure FireWall-1 for use with Sybase SQL:
>
> 1. From the GUI, add a TCP service called Sybase SQL Server. Define this port as using the port defined in the SQL serverconfiguration.
> 2. Accept this service in the Rulebase.
>
> Instructions for adding Microsoft NetMeeting support to FireWall-1:
> Add TCP port 1503 in GUI.

Es gibt keine Anzeichen bei der Installation eines SQL-Dienstes bei der Firewall-1, daß diese Firewall irgendwelche Kenntnisse darüber hat, was sie schützen soll, und wie sie es schützen kann. Es werden weder SQL-Befehle gefiltert, noch die Länge der übergebenen Parameter überprüft.
Die Zahl der offenen Ports reduziert sich gegenüber derjenigen bei Firewall-Routern dramatisch, da nur noch diejenigen Ports geöffnet werden, die auch wirklich gebraucht werden. Es müssen also nicht mehr pauschal alle Ports $> 1024$ freigeschaltet werden. Es verbleiben aber noch einige Risiken, da externen Hosts immer noch gestattet wird, auf interne Server oder Clients zuzugreifen. Es werden zwar laut Handbuch Proxy-Dienste hierfür angeboten, jedoch beschränkt sich tatsächlich die Funktion nur auf die Freischaltung der benötigten Ports. Es findet keinerlei inhaltliche Überprüfung statt. Kritisch wird dies, wenn Dienste wie RealAudio, RealVideo oder Netmeeting hinzugefügt werden. Hier werden für eine Zeit von ca. 30 Sekunden während des Aufbaus einer Verbindung vom SPF-Firewall eine große Zahl von Ports auf UDP zum Zielhost hin freigeschaltet. Sofern der Angreifer auf dem Host oder Konferenzserver im Internet selber sitzt, ergibt sich hier ein erhebliches Sicherheitsrisiko. Wer SPF-Firewalls studieren möchte, dem sei die SINUS-Firewall (SIFI) für Linux empfohlen.

## 2.2 Proxy-Firewalls

Proxy-Firewalls können auf Anwendungsebene filtern. Sie besitzen gegenüber SPF-Firewalls genaue Kenntnisse über Protokolle und bieten auf Kosten der Geschwindigkeit umfangreichen Schutz gegen Angriffe. Hier nur ein Ausschnitt der Fähigkeiten:

**Stärken:**

- Ausführliche Kenntnis über Protokolle und Dienste
- Umfangreiche Filtermöglichkeiten
- Schutz vor Buffer-Overflows möglich
- Authentifizierung
- Spezielle Proxies lieferbar (SQL)

- Für unbekannte Protokolle generische Proxy-Dienste verfügbar
- Keine offenen Ports
- Ausführliche LOG-Informationen
- Ausführliche Zustandsinformationen über alle Verbindungen
- Vollständiger Schutz vor TCP/IP-Angriffen
- Einfache Wartung und Installation
- Schutz vor Viren
- Schutz gegen feindliche Applets (Active-X, JAVA(script))
- Generische Proxies nachrüstbar (SOCKS)
- Aufbau als Dual Homed-Proxy möglich (Split DNS...)
- Eigener TCP/IP-Stack
- Algorithmen gegen SYS-Flooding (Random Early Drop = RED)

**Schwächen:**

- Relativ langsam
- Proxy nur für die wichtigsten Protokolle verfügbar
- Generische Proxies (allgemeine)
- Clustering schwer möglich

Zusammenfassend kann man sagen, daß viele Hersteller inzwischen dazu übergehen, Proxy´s für Dienste anzubieten, die man keinesfalls über die Firewall hinweg nutzen sollte. Wer z.B. Netmeeting mit aktiviertem Application Sharing über eine Firewall hinweg einsetzt, der sollte sich darüber klar sein, daß seine Arbeitsstation großen Gefahren ausgesetzt ist. Warum Hersteller von Firewalls diese Gefahren verschweigen, ist wohl hauptsächlich den Marketingstrategen zuzuschreiben. Wer diese Mechanismen und deren Gefahren genau studieren möchte, dem sei der Kernel von LINUX 2.2 als Studienobjekt empfohlen. Hier kann man gut die prinzipiellen Lücken von Proxy´s studieren, u.a. auch für IRC, QUAKE, VDOLIVE, RAUDIO, CUSEE-ME, (FTP !). Wer LINUX als Firewall einsetzt und diese Proxy´s aktiviert hat, der kann auch völlig auf eine Firewall verzichten, sie bietet keinen Schutz.

# 3 Angriffe auf den TCP/IP-Stack

Angriffe auf den TCP/IP-Stack sind gegenwärtig die Ursache von immensen Ausfällen bei ISPs und innerhalb des Netzwerkes von Unternehmen. Verantwortlich sind hierbei häufig mangelhafte TCP/IP-Stacks in Servern und Routern, die empfindlich auf defekte Netzwerkkarten und speziell konstruierte TCP/IP-Pakete reagieren. Diese Pakete werden von Programmen erzeugt, die im Internet im Quellcode und als Windows-Programm veröffentlicht werden. Diese werden „Exploits“ genannt und sind im BUGTRAQ Archiv zu finden (`http://www.geek-girl.com`).

Daß diese Angriffe unter dem Thema „Angriffe auf Firewalls“ aufgeführt sind, hat einen wichtigen Grund. Cracker benutzen diese Art von Angriffen, um Log-Server und IDS-Systeme stillzulegen. Sie sind fast ohne Netzwerkkenntnisse von jedermann ausführbar und greifen Internet-Server und arglose Surfer an. Insbesondere die Fa. Microsoft hat sich hierbei nicht mit Ruhm bekleckert; die Folgen waren allerorts zu spüren: Computerwoche, SWF 3, Microsoft, Netscape... - -Internet-Server und viele andere waren wochenlang offline, hunderttausende von Surfern werden mit DoS-Angriffen belegt, die ein Einfrieren vor allem von Windows 95/98/NT-Workstations bewirken.
Für Mission Critical-Dienstleistungsbetreiber bedeutete dies erhebliche Folgekosten, die sich aus Ausfallzeiten, Schadensersatzansprüchen, Beratung, Kauf und Einrichtung einer Firewall usw. zusammensetzte. Als dann auch einige Firewallhersteller keine wirksame Lösung liefern konnten, war das Chaos perfekt. Microsoft z.B. sperrte alle direkten Zugriffe auf ihren Internet-Server und ließ über mehrere Wochen nur Pakete zu, die über bekannte Proxys bei ISPs geroutet wurden.
Proxys oder Caching-Proxys nutzen zwangsläufig ihren eigenen TCP/IP-Stack für ein- und ausgehende Pakete. Pakete von Angreifern über Proxys mußten somit scheitern. Eine vollständige Liste der unter den Namen „TEARDROP“, „LAND“, ... bekanntgewordenen Angriffe findet sich im Anschluß an diesen Abschnitt.

## 3.1 DoS-Angriff auf Firewalls mit fragmentierten Paketen

Ein einfacher aber wirkungsvoller Angriff, der IP-Fragmentierung ausnutzt, ist der sogenannte „Overlapping Fragment Attack“ [RFC 1858]. Die derzeitige Internet Protokoll Spezifikation [RFC 791] beschreibt einen Reassemblierungs-Algorithmus, der neue Fragmente produziert und dabei jeden überlappenden Teil der zuvor erhaltenen Fragmente überschreibt. Wird ein solcher Algorithmus angewendet, so kann ein Angreifer eine Folge von Paketen konstruieren, in denen das erste Fragment (mit einem Offset der Länge Null) harmlose Daten beinhaltet (und dadurch von einem Paketfilter weitergeleitet werden kann). Ein beliebiges nachfolgendes Paket mit einem Offset, der größer als Null ist, könnte TCP-Header-Informationen (z.B. Destination Port) überlappen. Diese würden durch den Algorithmus modifiziert (überschrieben). Dieses zweite Paket wird von vielen Paketfiltern nicht gefiltert. Gegenmaßnahme hierzu ist, Paketfilter zu verwenden, die ein Minimum an Fragment-Offset für Fragmente verlangen. Nur wenige neuere TCP/IP-Stacks erkennen dieses Problem und korrigieren es. Man muß aber noch hinzufügen, daß der Angreifer, um diesen Angriff auszuführen, routingtechnischßehr nahe an an die Firewall herankommen muß, um seinen Angriff genau timenßu können. Eine ständige Überwachung der näheren Umgebung ist für mission criticalSSysteme unerläßlich.

Ältere Router lassen sich mit diesem Trick einfach durchtunneln, sie bieten keinen Schutz. Besonders aber Firewalls, die auf der Basis der Stateful Paket-Filterung (SPF) arbeiten, wie z.B. RAPTOR EAGLE und FIREWALL-1 lassen sich so durchtunneln, je nach Konfiguration.

Wer diese Firewalls als NON-IP Firewall und/oder aus Gründen der Geschwindigkeit ohne vollständige Reassemblierung der IP-Fragmente installiert hat, der ist auch trotz Einsatzes dieser Markenprodukte für DoS Angriffe anfällig.

Content-Anbieter im Internet und ISPs, die mit diesen Firewalls NT-Server schützen wollten, wurden so Ziel der unzähligen Angreifer, die neue Exploits mal kurz testen wollten.

Abhilfe schafft nur eine vollständige Reassemblierung der TCP/IP-Pakete oder der Einsatz eines Proxy. Nachteil dieser Lösung ist ein enormer Einbruch in der Performance, der den Vorteil der SPF-Firewalls völlig zunichte macht. Dies zeigt aber, daß Firewalls keineswegs perfekt sind. Will man solchen Angriffen zuvorkommen, so ist man als Betreiber eines Mission Critical-Systems auf die ständige Betreuung eines Experten angewiesen. Da von diesem Angriff nur spoofende Versionen existieren, können die Täter oft nicht aufgespürt werden.

## 3.2 DoS-Angriffe auf Netzwerkscanner, Sniffer und IDS-Systeme

- Trace einer TCP/IP-Verbindung
- Gespoofte SYN-Pakete und Taubheit des Sniffers
- Einschleusung von falschen Prüfsummen zur Irreführung
- RST und Überprüfung von Sequenznummern
- Gespoofte RST-Pakete
- Änderung der Paketlängen
- Werkzeuge zur Erzeugung der Pakete

Entgegen aller Vermutungen können Netzwerkscanner, Sniffer und IDS (Intrusion Detection Systems) auch einem DoS-Angriff zum Opfer fallen. Grund dafür ist, daß Sniffer stets auf dem Kernel des Betriebssystems aufsetzen und von diesem abhängig sind.

Sniffer müssen einen eigenen TCP/IP-Stack besitzen, da ihnen ansonsten kein Trace einer Netzwerkverbindung zwischen zwei Rechnern im Netz gelingen würde.

Die meisten freien und kommerziellen Scanner haben dabei ein kleines Problem. Sind sie auf Spurenverfolgung einer Verbindung, so sind sie nicht mehr in der Lage, andere Verbindungen gleichzeitig zu observieren.

Um diese Aufgabe bewältigen zu können, müßten sie gleichzeitig die Arbeit aller TCP/IP-Stacks im Netzwerk verrichten, dies wäre wohl auf einer CPU etwas zuviel verlangt. Daher entgeht ihnen stets ein großer Prozentsatz des gesamten Traffics.

Ein Angreifer muß sich also, wenn er dynamische Angriffe ausführt, auf ein Rechnerpaar beschränken; ebenso verhält es sich mit aktiven IDS-Systemen (Intrusion Detection). Sniffer und Netzwerkscanner, die z.B. auf einem Server einen bestimmten Port überwachen, kann man mit einem einfachen Trick stillegen: Bevor er sich z.B. via Telnet auf Port 23 einloggt, sendet er ein gespooftes SYN-Paket. Falls ein Sniffer aktiv ist, wird er logischerweise nach Paketen dieses gespooften Rechners mit dem Port 23 als Zielport lauschen. So kann man sich einloggen, ohne daß der Sniffer das Passwort mitscannen kann. Später, wenn der TCP/IP-Stack die Verbindung wegen Timeout beendet, ist der Sniffer wieder aktiv.

Ein weiteres Problem liegt darin, daß ein Sniffer nicht wirklich in die Verbindungen hineinschaut, also nicht an dem Datenaustausch teilnimmt wie die beobachteten Rechner. Er trifft bezüglich IP-Paketlänge und TCP-Paketlänge daher bestimmte Annahmen und interpretiert die Pakete nach diesem Standardschema. Bei einer Änderung z.B. der Länge des TCP-Headers und der sporadischen Einschleusung von falschen Prüfsummen ist er nicht mehr in der Lage, die Inhalte dieser Pakete korrekt zu interpretieren. Der Sniffer überprüft die TCP-Prüfsummen nicht, die Kernel der überwachten Rechner hingegen werden diese „falschen“ Pakete verwerfen und somit die Übertragung korrekt ausführen. Sniffer brechen z.B. auch nach einem FIN- oder RST- Paket die Überwachung ab. Befindet sich dieses aber in einem TCP-Paket weit entfernter Sequenznummer, so werden die überwachten Rechner dieses verwerfen und mit der Verbindung fortfahren, der Sniffer hingegen hält die Verbindung jedoch für beendet und stellt seine Arbeit ein. Einige Betriebssysteme (NT und DIGITAL UNIX) überprüfen bei einem RST die TCP-Sequenznummern nicht. Ist also auf diesen Betriebssystemen ein Sniffer aktiv, so ist es einem Angreifer leicht möglich, dieses mit einem gespooften Paket mit gesetztem RST-Flag taub für alle weiteren Pakete zu machen.

Sehr erfolgreich gegen Sniffer sind „Spielchen“ mit fragmentierten IP-Paketen, diese werden im allgemeinen nie von Sniffern erkannt. Es gibt eine ganze Reihe von solchen Paketen, einige sind genauer im Phrack-Magazin beschrieben worden (`http://www.phrack.org`). Kommerzielle Pakete wie Ballista oder freie wie die Software ipsend von Darren Reed oder die Perl-Erweiterung Net::RAWIP unter FreeBSD eignen sich hervorragend, den TCP/IP-Stacks in den Betriebssystemen einmal auf den Zahn zu fühlen. Es wird sich dann unweigerlich zeigen, warum einige TCP/IP-Stacks öfter mal ausfallen. Grund hierfür können aber auch defekte Netzwerkkarten sein, die verstümmelte Pakete erzeugen. Einige Betriebssysteme verkraften diese Pakete nicht und hängen sich auf.

## 3.3 Übersicht von Angriffsvarianten auf den TCP/IP-Stack

Angriffe auf den TCP/IP-Stack gehören inzwischen zu den besonders häufigen DoS(Denial of Service)-Attacken. Unter Namen wie OOB, NUKE, LAND, TEARDROP und NEW FRAGMENTATION ATTACK bekannt geworden, führten diese zu ständigen Störungen in Intra- und Internet. Einige dieser Pakete werden von Routern und sogar von Firewalls nicht herausgefiltert, so daß Firewalls ohne eigenen TCP/IP-Stack für ein- und ausgehende Pakete (Proxy-Firewalls) hierbei das Betriebssystem nicht sichern können. Durch die Veröffentlichung von Programmen wie „latierra“, die einige kritische Kombinationen über alle IP-Nummern eines Netzwerkes und alle Portnummern durchprobieren, sind solche Angriffe leider alltäglich geworden.

- IP-Header-Länge $<$ IP-Fragment-Offset (bonk.c)
- IP-Header-Länge $>$ IP-Fragment-Offset (teardrop.c)
- IP-Version $< 4$
- IP-Version $> 4$
- IP-Header-Länge $<$ Paketgröße bei langen Paketen

- IP-Header-Länge > Paketgröße bei kurzen Paketen
- Fragmente der Länge 0 mit Offset 0x2000, 0x3000, 0xA000, 0x0100
- Paket > 63 KB-Paket + 1 KB-Fragment mit einem Offset 0x1ffe, als ICMP markiert, unter Berücksichtigung der MTU
- IP-Offset auf 0x8000 mit MSB gesetzt
- Große TTL-Werte (ist bei älteren TCP/IP-Stacks gekoppelt an eine lange Verweildauer im Stack) TTL = 0, 128, 255.
- Mehrfach fragmentierte Pakete (MF-Bit gesetzt) mit Offsets, die für eine Überlappung sorgen
- Fragmentierte Pakete mit „Reserved Bit“ gesetzt
- Ungültige IP-Optionen, die den Paketen eine völlig andere Charakteristik geben.
- Länge der Optionen ist größer als die Paketlänge
- Länge der Optionen ist 0
- Ungültige ICMP-Typen in Header
- ICMP-Typen 0-31, Code 255
- ICMP-Typ 3, Code 0-31
- ICMP-Typ 3, Code 9, 10, 13, 14, 17, 18 mit zu kurzen Paketen
- ICMP-Typ 4, Code 0, 127, 128, 129, 255
- ICMP-Typ 5, Code 0, 127, 128, 255
- ICMP-Typ 8-10, 13-18, Code 0, 127, 128, 129, 255
- ICMP-Typ 12, Code 127, 128, 129, 255
- IP-Pakete mit UDP-Headern, die ungültige Werte besitzen
- UDP Länge > Paketgröße
- UDP Länge < Paketgröße
- Source-Port 0, 1, 32767, 32768, 65535, Destination-Port 0, 1, 32767, 32768, 65535
- Etwas technisch: sizeof(struct ip) <= MTU <= sizeof(struct udphdr) + sizeof(struct ip), führt dazu, daß Pakete einer bestimmten MTU-Größe zu ungültigen Typen führen.
- IP-Pakete mit TCP-Headern, die ungültige Werte besitzen
- Alle Kombinationen von TCP-Flags: (URG, ACK, PUSH, RST, SYN, FIN)
- Sequenznummer = 0, 0x7fffffff, 0x8000000, 0xa0000000, 0xffffffff
- ACK = 0, 0x7fffffff, 0x8000000, 0xa0000000, 0xffffffff
- SYN-Paket, Fenstergröße 0, 32768, 65535
- Urgent-Pointer auf 1, 0x7fff, 0x8000, 0xffff Data Offset gesetzt
- Source-Port 0, 1, 32767, 32768, 65535, Destination-Port 0,1, 32767, 32768, 6553
- IP-Pakete, bei denen Source-IP und Destination-IP derselbe Rechner sind. Diese sinnlosen Pakete kommen normalerweise nicht vor. Bei einigen Betriebssystemen führt dieses zu einer Endlosschleife und einer Überlastung im Stack (Beispiel ping) oder zu einer Überlastung durch startende Prozesse (land.c).
- „Source Routed Frames“ enthalten im Header den Weg, den das Paket auf dem Weg durch das Internet nehmen soll. Vielfach ist es so möglich, Sperren zu umgehen ohne Log-Events auszulösen.

- Der bekannte OOB-Bug ist auf eine zweideutige Interpretation des URG-Flags des ursprünglichen RFC 793 und des „neuen“ RFC 1122 zurückzuführen (Microsoft mal wieder...).
- Spoofing, also das Vortäuschen einer internen Adresse auf einem externen Interface ist eine noch häufig unterschätzte Möglichkeit, geringfügige Fehler in einer Firewall auszunutzen.
- MBONE Paket-Kapselung erfordert eine besonders sorgfältige Auswahl und Konfiguration der Firewall, da viele Filteroptionen in einigen Firewall-Routern nicht angeboten werden. Das betrifft sowohl gekapselte AppleTalk-, IP- als auch IPX-Pakete.
- Angriff über eine große Zahl von Fragmenten, um die Zahl der Netzwerkbuffer zu erschöpfen, bevor die Reassemblierung ausgeführt wird. Hierbei kann durch Vortäuschung einer langsamen Verbindung die Verweildauer in vielen Stacks erhöht werden, wobei die Performance stark leidet.
- Angriff mit einem Zufallszahlengenerator. Es werden hierbei ausschließlich die Prüfsumme, Länge und das IP-Offset-Feld korrekt gesetzt. Dieser Angriff führt zu einer großen Zahl von Warnmeldungen in der Firewall, da hierbei keinerlei Wiederholungen vorkommen. Lücken, die die Firewall nicht abdeckt, weil sie Stateful Packet Filter-Architektur besitzt, führen dann leicht zu einem erfolgreichen DoS auf dem Server dahinter. Gerade die als besonders schnell getesteten Firewalls versagen hierbei oft. Fehlerhafte Netzwerkkarten oder Routersoftware, manchmal auch Kernel selber, erzeugen im Netz ähnliche Pakete. Dies führt zu unerklärlichen, nichtreproduzierbare Phänomenen und viel Zeitaufwand ist nötig, um den Störenfried ausfindig zu machen. Besser ist es jedoch, man verzichtet gleich auf empfindliche Server, Drucker und Desktop-Betriebssysteme.

Die oben genannten Angriffe und ihre Untervarianten lassen sich darüber hinaus auch noch (zufällig) miteinander kombinieren. Die Zahl der möglichen Varianten ist sehr hoch, die Zahl der sinnvollen Varianten beschränkt sich auf ca. 130 Stück. Firewalls mit dynamischen Regeln werden hierbei hart beansprucht und bis an die Leistungsgrenze strapaziert. Hierbei treten DoS-Phänomene auf, die von vielen Firewall-Testern/Zertifizierern nicht getestet werden können. Noch größer sind die Probleme in Hispeed Netzwerken, die mit Geschwindigkeiten höher als 100 MBit arbeiten. Erstens kann der TCP/IP Stack viel schneller überlastet werden, andererseits können durch zu kurze Zahlenwerte für die SSN (meist 32 Bit) weitere Angriffsvarianten möglich werden. Man sollte stets darauf achten, einen TCP/IP Stack für lange SSN´s (64 Bit) zu benutzen (LINUX 2.2, FreeBSD/NetBSD/OpenBSD oder Solaris)

# 4 Buffer Overflow-Angriffe auf Server hinter Firewalls

Buffer Overflows gehören mit zu den gefährlichsten Angriffen überhaupt. Betroffen sind vornehmlich Internet-Server (WWW), Dial-In-Router, Proxy-Caches, Newsserver, Mailserver, FTP-Server, FAX-Server, SQL-Server, SSL-Server und viele Sicherheitsprogramme, wie z.B.

PPTP, SSH... oder andere Authentifizierung/Verschlüsselungsprogramme. Zunehmend benutzen Angreifer Buffer Overflows auf Angriffe von Servern in Unternehmen.

Grund sind mangelhafte Längenabfragen bei den an ein Programm übergebenen Daten. Hat ein Programm eine bestimmte Anzahl von Bytes für z.B. die Annahme eines Passwortes oder einer URL (`http://www.domain.de/index.asp?Name=text` usw.) reserviert, so führt die Übergabe eines überlangen Strings zu einer Schutzverletzung in der Speicherverwaltung des Servers/Clients, der es ermöglicht, daß Programme ausgeführt werden können. Wie häufig Schutzverletzungen auftreten, hängt stark von der Memory Architektur und der Sorgfalt der Programmierer ab.

Im Internet finden sich Hunderte von vorgefertigten Programmen, auch „Exploits“ genannt, die diese Fehler in Betriebssystemen ausnutzen. Security-Scanner fragen auf dem Betriebssystem Versionsnummern ab und warnen, falls ein Problem bekanntgeworden ist.

Das bedeutet, daß Security-Scanner nicht die Sicherheit eines Betriebssystems testen, sondern nur darauf, ob ein bereits bekannter Exploit an diesem Server/Dienst Schaden anrichten könnte. Security-Scanner testen allerdings noch viele zusätzliche Dinge, vornehmlich bekannte Konfigurationsfehler, die natürlich immer sehr betriebssystemspezifisch sind. Unbekannte „Exploits“ können Security-Scanner nicht testen, weswegen die Zahl der noch unentdeckten „Exploits“ stets sehr viel größer ist, als die Zahl der veröffentlichten.

Genauere Recherchen haben aber gezeigt, daß oft schon bis 6 Monate vor dem Erscheinen eines Exploits Gerüchte über einen möglichen Buffer Overflow auf einem Betriebssystemen, Router, u.s.w in Newsgroups aufgetaucht sind (`www.dejanews.com`).

Fleißiges Mitlesen der Listen und schnelles Einspielen von Sicherheits-Patches hilft nur und ausschließlich gegen den Mob, der sich im Internet breitmacht und „Exploits“ testet. Gegen professionelle Angreifer müssen die eingesetzten Dämonen oder Dienstprogramme und Client-Anwendungsprogramme durch Filter, die die Längen der Übergabeparameter begrenzen, geschützt werden. Bei mission criticalËinsätzen, insbesondere Datenbanken und Online-Shopping Systemen müssen positivFilter eingesetzt werden. Diese lassen nur diejenigen Befehle und Parameter passieren, die ausdrücklich erlaubt sind. Die Programmiersprache, die für diesen Zweck konzipiert wurde, ist PERL. (`http://www.perl.org/CPAN/`)

Im Juli 1998 wurden der Server des BMV, ZDH und FDP Opfer solcher Angriffe. Der Grund lag in einem Fehler des POP-Servers in S.u.S.E.-Linux (qpop). Server unter RedHat-Linux und Caldera OpenLinux waren zu diesem Zeitpunkt nicht betroffen.

# 5 Konkrete Angriffe auf Firewalls

Die folgenden Beispiele sind charakteristisch für Fehler beim Aufbau von Firewalls. Für einen Angreifer stellen die Firewalls selber kein ernstzunehmendes Hindernis dar, da diese ja den Datenstrom zum Server 1 / 2 passieren lassen. Das Ziel ist Server 1, auf welchem ein „Buffer Overflow“ die Ausführung beliebiger Programme erlaubt.

## 5.1 S.u.S.E. Linux-Firewall

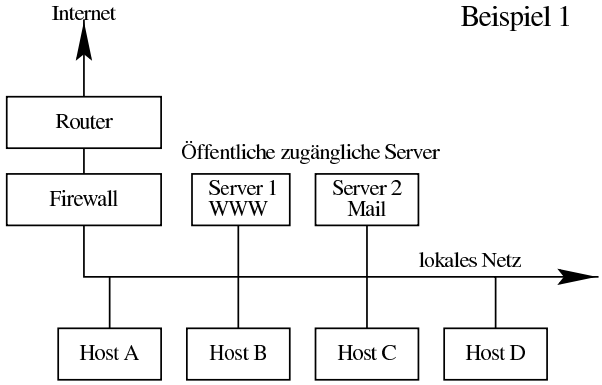


Abbildung 1: S.u.S.E.-Linux 6.0: Aufbau einer Firewall

ıbbildung 1 zum Aufbau einer Firewall findet sich in der Installationsanlei-
.-Linux 6.0. Im Grunde ist der Hersteller der Firewall völlig austauschbar. Es soll zeigen, wie ein Angreifer vorgeht, um die Firewall zu überwinden. Das Beispiel ist völlig authentisch und läßt sich auch recht einfach selber mit Hilfe einiger „Exploits“ von BUGTRAQ durchführen.

Das Netz besitzt feste, vom Provider zugewiesene IP-Nummern. Die Firewall arbeitet selber nicht als ISDN-Router, ist aber über ein Transfernetz (192.168.x.x) mit dem Router verbunden. Die Hosts A–D sind Arbeitsplatzrechner, die über den WWW-Proxy von Server 1 Zugang zum Internet besitzen. Die Firewall schirmt einige Ports des Server 1 ab, erlaubt aber Zugriffe auf den WWW-Server über Port 80 (HTTP) und Port 21 (FTP) aus dem Internet. Server 2 ist ein „store and forward“-Proxy, der als interner DNS-Server, Mail-Server und News-Server arbeitet. Die Firewall erlaubt keinen Zugriff auf Server 2 aus dem Internet. Server 2 holt seine E-Mails und News im Poll Modus aus dem Internet ab. Die Firewall erlaubt den Zugriff von Server 2 auf einen NEWS Feed Server im Internet. Ein Security-Check mit SATAN oder SAINT aus dem Internet zeigt keine Probleme, alle Filterregeln seien korrekt eingestellt.

Um es vorweg zu nehmen – ein Angreifer wäre in wenigen Minuten in das Netzwerk vorgedrungen. Wo liegen die Probleme?

### Problem 1

Der Angreifer sieht von außen nur folgende Ports: 25, 21, 53 und 3128 von Server 1, Server 2 sei abgeschirmt.

Der Angreifer ist dadurch, daß er direkten Zugriff auf die Ports der internen Server hat, in der Lage, das Betriebssystem des Servers und die verwendete Software genau zu bestimmen.

Über E-Mails aus dem Netz (kleine Anfrage) würde er genau wissen, ob eventuell das Netz mit Masquerading oder NAT aufgebaut ist. Er kennt dann genau das E-Mail-Gateway (Ser-

ver 2) und kann anhand der Headerinformationen das dort verwendete Betriebssystem genau identifizieren.

Nun sucht er in den einschlägigen Archiven nach „Exploits“, die von innen oder von außen her einen „Buffer Overflow“ initiieren, beispielsweise das neue Problem mit „wuftpd“ oder „proftpd“.

Angenommen, Server 1 hätte ein solches Problem. Es werden immer neue bekannt, im Prinzip muß der Angreifer nur warten. Dann wäre Server 1 im Netzwerk verloren. Der Angreifer könnte alle Dienste mit Supervisorrechten starten. Da die Firewall offene Ports hat, kann der Angreifer weitere Programme von Server 1 aus dem Internet downloaden. Dies könnten z.B. Netzwerksniffer sein, der ihm dann die Passworte zu allen Servern im Netzwerk und jeden Zugriff auf alle Server im Netz ermöglichen würde. Die Firewall selber interessiert den Angreifer nicht, da er nach eigenem Belieben Tunnel über die offenen Ports aufbauen kann.

**Problem 2**

Angenommen, er würde auf die Schnelle keinen Exploit finden. In diesem Falle kann er irgendeinem User ein trojanisches Pferd via E-Mail senden, und darauf warten, daß dieser es installiert. Da er den Namen des E-Mail-Gateways kennt, kann er mit diesem ein Gateway in das Internet aufbauen, sofern die Firewall die Funktion „Transparent Proxy“ aktiviert hat. Verschiedene Proxy-Module der Firewall erleichtern dem Angreifer den Aufbau eines Tunnels von einem Arbeitsplatz aus zu einem Server im Internet. Harmlose Varianten eines solchen Werkzeuges sind „netbus“ und „bo“, welche künstlich „entschärft“ wurden, indem diese nicht das TCP Protokoll, sondern das UDP Protokoll benutzen, welches fast überall abgeblockt wird.

**Problem 3**

Es ist ein Split-DNS-Server aufgebaut, der eventuell ein Problem mit „Additional Informations“ haben könnte. Ein eingeschleustes trojanisches Pferd könnte den MX-Eintrag des internen DNS-Servers auf eine IP-Nummer im Internet umändern. Die Folge wäre, daß der Angreifer sämtliche internen und externen E-Mail aus dem Netzwerk erhalten würde, die er kopieren und in das Netzwerk zurücksenden könnte.

**Problem 4**

Er nutzt die typischen Fehler der Browser auf den Arbeitsstationen (Host A–D) aus. Ein vorbereitetes, auf die internen IP-Nummern angepaßtes Active-X-Applet könnte somit beliebige Angriffe auf Server intern starten. Er muß hierzu nur die Aufmerksamkeit eines Users im Intranet auf einen beliebigen Internet-Server lenken, damit dieser das Applet auf seine Arbeitsstation lädt und es startet.

**Problem 5**

Eine UNIX-Firewall könnte er versuchen, direkt von innen her mit einem „Buffer Overflow“ anzugreifen, in der Hoffnung, daß diese einige wohlbekannten Ports nach innen hin geöffnet hat.

**Problem 6**

Hat er auch nur ein einziges mal die Firewall überwunden, so kann er trojanische Pferde installieren, die später von alleine aktiv werden. Wird der Angriff entdeckt und das Sicherheitsproblem beseitigt, so wird wohl kaum der Systemadministrator alle Server im Intranet neu installieren. Finden würde er ein trojanisches Pferd wohl nicht.

## 5.2 Angriff über beliebige Proxy-Firewalls

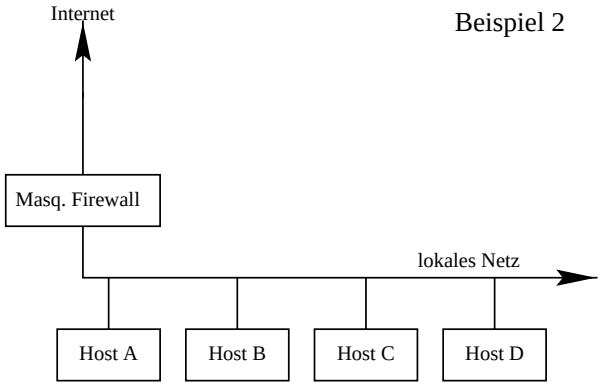


Abbildung 2: Masquerading Firewall

;t ein typisches Beispiel für ein kleines Unternehmen, welches seinen Mitarbeitern Anschluß an das Internet ermöglichen möchte. Die Firewall-Software mit Masquerading ist häufig auf einem Windows NT Server installiert, die eingesetzte Software ist ein Windows Proxy. Da keinerlei Ports nach außen hin offen sind, ist es einem Angreifer nicht möglich, ein „Buffer Overflow“-Problem auszunutzen. Hier muß der Angreifer ein trojanisches Pferd einschleusen.

## 5.3 Angriff über eine beliebige Firewall hinweg

Dieses Beispiel ist ein Aufbau, der häufig verwendet wird. Der Typ der Firewall ist ohne jede Bedeutung. Der WWW-Proxy kann entweder der bekannte SQUID oder dessen kommerzielle Variante Netscape Proxy-Server sein. Hierbei sind alle Ports von außen durch zwei Firewalls gesichert. Der Austausch von E-Mails läuft über Server 2 intern, der die von außen kommenden E-Mails aus einem Sammelpostfach (POP3/IMAP4) aus dem Internet stündlich abholt.

Dies könnte beispielsweise ein Exchange-Server mit VPOP oder UNIX mit Fetchmail sein. Beide Programme haben ein „Buffer Overflow“-Problem. Dieses setzt voraus, daß der Angreifer bereits den Server im Internet, auf welchem das Sammelpostfach lagert, unter Kontrolle hat, was gewöhnlicherweise kein großes Problem darstellt. Auch die WWW-Proxy-Server besitzen ein Problem mit Buffer Overflows, jedoch lassen sich auch diese nur mit dynamischen Angriffen ausnutzen. Hierzu muß der Angreifer wiederum in Besitz eines WWW-Servers im Internet sein, und die Aufmerksamkeit eines Users im lokalen Netz auf seinen Server lenken.

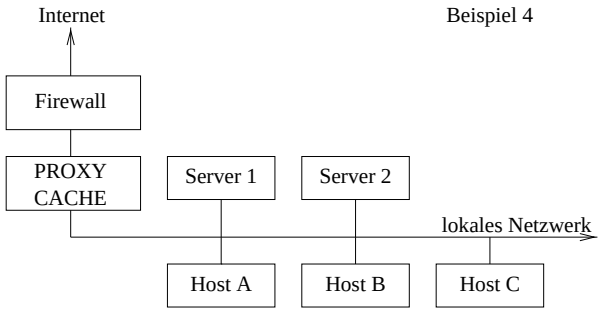


Abbildung 3: Firewall und Proxy-Server

m in Abbildung 3 sind im Prinzip ähnlich wie in Beispiel 1. Auch hier muß der Angreifer in der Lage sein, ein Buffer Overflow-Problem im Proxy-Cache auszunutzen. Der Angriff selber muß aber aus dem lokalen Netzwerk heraus gestartet werden. Um in Kenntnis des Betriebssystems und der Proxy-Versionsnummer zu kommen, muß irgendein User aus dem lokalen Netzwerk den WWW-Server des Angreifers besuchen. Dies könnte so ablaufen:

Der Angreifer,der sich telefonisch im Sekretariat davon überzeugt hat, daß Herr Mitarbeiter am 24.12.2000 auch wirklich Zeit hat, schickt diesem eine E-Mail:

> Sehr geehrter Herr Mitarbeiter!
>
> Zur Eröffnung unserer neuen Filiale möchten wir Sie gerne persönlich einladen. Neben Vorstellungen neuer Internet-Technologien durch unsere Referenten XY, Microsoft und WV, Sun möchten wir Sie gerne auch mit leiblichen Überraschungen verwöhnen. Wir bitte Sie daher, uns mitzuteilen, ob wir Sie am 24.12.2000, 10 Uhr, in unserer neuen Filiale begrüßen dürfen. Elektronische Anmeldung bitte auf `http://www.little-idiot.de/cgi-bin/test.cgi`
>
> [Diese URL liefert u.a. Informationen]
>
> Mit freundlichen Grüßen,
> gez. Boss

Herr Mitarbeiter, sichtlich erfreut angesichts der leiblichen und geistigen Überraschungen, sagt via Browser zu. Kurze Zeit später ist der Angreifer im Besitz folgender Informationen:

```
REMOTE_ADDR = 212.53.238.2
```

```
REMOTE_HOST = 212.53.238.2
QUERY_STRING = Name=Mueller
HTTP_USER_AGENT = Mozilla/4.0 (compatible; MSIE 4.01; Windows 98)
HTTP_ACCEPT = {*}/{*}
HTTP_ACCEPT_ENCODING = gzip, deflate
HTTP_X_FORWARDED_FOR = 212.53.238.130
HTTP_VIA = 1.0 cache:8080 (Squid/2.0.PATCH2)
```

Was sagt dem Angreifer das? Er weiß, bei welchem Provider die Firma einen Internet-Zugang besitzt, wer gerade zugesagt hat, daß er mit Windows 98 in der Standardversion und dem Internet-Explorer (kein Fehler!) arbeitet, daß er mit einem Linux-Router als Proxy (SQUID) an das Internet angeschlossen ist, WINZIP so installiert hat, daß ZIP-Files automatisch ausgepackt werden, seine IP-Adresse hinter dem Router 212.53.238.130 ist und keinerlei HTTP-Filter o.ä. eingesetzt werden.Er weiß weiterhin, daß jedes Programm über die IP-Nummer 212.53.238.2 und Port 8080 als Gateway Daten aus dem Intranet an einen beliebigen Server im Internet senden kann, sowohl mit HTTP- und FTP-Protokoll. Ein Netzwerk-Scanner wird zeigen, daß alle Ports außer Port 25 (sendmail) auf dem Router geschlossen worden sind. Weiterhin ist mit einger Wahrscheinlichkeit eine Linux-Version mit Kernel $< 2.0.34$ und allen bekannten Sicherheitlücken aktiv, diese sollen aber den Angreifer (noch nicht) interessieren. Weiterhin ist die Firma über einen Provider mit reserviertem Subnetz an das Internet angebunden.

Was braucht ein Angreifer also, um die Festplatte dieses Users zu durchforsten? Ersteinmal VC++ oder EGCS (`http://www.cygnus.com`), Bibliotheken für den Proxy-Mechanismus , z.B. TIS FWTK von (`http://www.nai.com`), und den Quellcode von Tetris. Heraus kommt nach ein paar Tagen Arbeit ein Tetris-Spiel, welches ein paar Geheimnisse birgt.

Es fragt nach der IP-Nummer des Rechners, auf dem es gestartet wird. Ist die IP-Nummer = 212.53.238.130, dann baut es über die IP-Nummer 212.53.238.2 und Port 8080 eine FTP-Verbindung in das Internet auf, und versendet alle `.doc`-Files aus `C:\Eigene_Dateien` in das Internet, installiert einen Tastatursniffer und einen Netzwerkscanner, welches es von einem FTP-Server im Internet holt. Nach einigen Tagen wird es folgende Informationen auf die Festplatte geschrieben haben: Sämtliche Telnet-Passworte, die an 212.53.238.130 gesandt worden sind, sämtliche Passworte, die an 212.53.238.130, Port 110 gesandt worden sind, sämtliche Passworte, die an den Novell/NT-Server gesandt worden sind. Bei jedem Start des Tetris-Spiels verschwinden diese Informationen in das Internet und werden gelöscht.

Kurze Zeit später bekommt Herr Mitarbeiter via E-Mail einen Geburtstagsgruß, eine animierte Grafik von einem Kollegen, ein paar Türen weiter. Er startet dieses „Geburtstagsgruß“Programm und freut sich über Glückwünsche. In diesem Moment wird eine Telnet-Verbindung zum Router aufgebaut, alle externen Firewallregeln ausgeschaltet und eine E-Mail versandt. Der Router ist völlig offen, der Angreifer ist in Besitz einiger oder sogar aller User-Accounts und des Administrator-Passwortes. Er stoppt mit dem Signal-Handler (kill) alle Logdämonen, installiert das Protokoll IPX und NCPFS während der Laufzeit, ein Neustart ist unter Linux nicht notwendig. Da er einige/alle Passworte des Novell-Servers, die IP-Nummern, IPX-Nodenummern und die Hardware-Adressen der Netzwerkkarten der Mitarbeiterrechner kennt,

kann er im Prinzip den Novell-Server komplett in das Filesystem von Linux einklinken. Er hat dabei nur wenige Hindernisse zu überwinden:

1. Kopplung Login/Passwort an eine Mac-Adresse
2. Der Mitarbeiter darf seine Arbeitsstation nicht gestartet haben.

Also wartet der Angreifer bis zur Mittagspause, vergewissert sich, daß Mitarbeiter XY nicht vor seinem Rechner sitzt und arbeitet, startet einen kleinen DoS-Angriff auf den Rechner des Mitarbeiters. Der Rechner ist abgestürzt, die Netzwerkkarte deaktiviert. Nun fährt er in Linux ein virtuelles Interface hoch, mit derselben IP-Nummer und Mac-Adresse, die vorher der Windows 98 Rechner von Mitarbeiter XY besaß. Der Angreifer loggt sich mit Linux in den Novell-Server ein und beginnt, DOC-Files auf den Linux-Rechner zu übertragen. Nach 2 Minuten ist er fertig, loggt sich wieder aus und beginnt, mit einem Winword → ASCII-Konverter die Datenmenge zu reduzieren. Mit ZIP komprimiert er diese und versendet sie an eine E-Mail-Adresse im Internet. Er „korrigiert“ die Firewallregeln, bereinigt die Log-Files, aktiviert die Logdämonen und verschwindet ungesehen. Der Sicherheitsexperte mag entgegnen, daß heutzutage kaum mehr eine Firewall ohne Verschlüsselungsalgorithmus für die Fernwartung ausgeliefert wird. Dem muß man aber entgegen, daß z.B. `http://www.linuxhq.com` und `http://www.rootshell.com` genau so abgesichert waren. Es waren nur Port 80 für HTTP und der Port für SSH (Fernwartung) offen. Das Problem war in diesem Falle der SSH Dämon selber, der ein Sicherheitsloch hatte. Da sehr viele Firewallhersteller inzwischen aus kostengründen viel Software der GPL (GNU PUBLIC License) einsetzen, kann man niemals sicher sein, daß die eigene Firewall nicht exakt denselben Fehler hat, wie z.B. eine LINUX Firewall.

## 5.4 Korrekter Aufbau einer Firewall

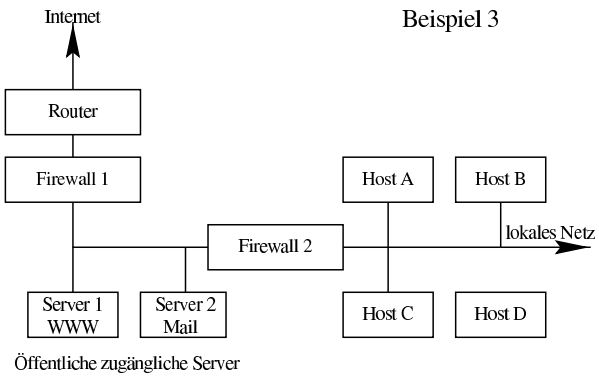


Abbildung 4: Konfiguration mit zwei Firewalls

gehören immer 3 Komponenten: ein äußerer Router, ein innerer Router und die Firewall selber. Soll ein Zugriff auf einen Server im Intranet aus dem Internet heraus möglich sein, so ist eine DMZ („DeMilitarisierte Zone“) aufzubauen, die selber von Firewalls umgeben ist. In dieser sind die Server, die von außen erreichbar sein sollen, zu installieren. Der

Grund besteht darin, daß man stets damit rechnen muß, daß ein von außen erreichbarer Server mit Buffer Overflows angreifbar ist. In diesem Falle muß unter allen Umständen noch einen Firewall als Sicherung gegen Zugriffe aus der DMZ auf das interne Netzwerk. Der korrekte Aufbau wäre also folgender:

Für den Fall, daß Server 1 erfolgreich angegriffen wird, muß Firewall 2 Angriffen standhalten können. Firewall 1 und der Router bieten dann im Prinzip keinen Schutz gegen professionelle Angreifer mehr, halten aber viele DoS-Angriffe und weniger erfahrene Angreifer fern. Sie dienen im Prinzip nur dazu, die Verfügbarkeit der Server zu erhöhen. Im Gegensatz zu früheren Empfehlungen (Einrichten von Firewalls Chapman/Zwicky) sollten die Firewalls mindestens „Stateful Packet Filter“ (SPF-Firewalls) sein und über verschlüsselte Protokolle zur Fernwartung und Analyse der Logfiles verfügen.

Die Überwachung von Firewall 1 und der Server 1 und 2 in der DMZ stellt allerdings ein Problem dar, dessen Lösung nicht ganz trivial ist. Logserver sind ebenfalls anfällig gegen Buffer Overflows und können von Angreifern stillgelegt werden. (DoS-Angriff) Es darf unter keinen Umständen Firewall 2 (Beispiel 4) für die kontinuierliche Übertragung von Logfiles auf einen Logserver im lokalen Netz geöffnet werden. Es bietet sich an, den WWW-Server in der DMZ als Logserver für Router und Firewall 1 einzusetzen. Mit FTP z.B. könnte eine Arbeitsstation die puren ASCII-Logfiles von Router und Firewall 1 herunterladen und auswerten. Besser ist jedoch ein eigener Server in der DMZ, der nur eine Aufgabe hat, nämlich die Logfiles zu speichern. Da auf diesem alle weiteren Funktionen deaktiviert sind, ist dieser höchstwahrscheinlich nicht anfällig gegen Buffer Overflows, weil er viel weniger Angriffspotential bietet. Ein Auswertungsprogramm könnte aber so geringe Differenzen zwischen den Logfiles von Router, Server 1 und dem Logserver sofort bemerken. Es ist höchst unwahrscheinlich, daß ein Angreifer zur gleichen Zeit beide Logserver angreifen kann. Zum Abgleich von Logfiles untereinander kann man sich für eines der beiden Softwarepakete entscheiden: Network Flight Recorder oder LogSurfer von Wolfgang Ley.

Firewall 2 hat also nicht nur die Aufgabe, das lokale Netz gegen Angreifer zu schützen, denen ein Angriff auf Server 1 und 2 gelungen ist, sondern auch zu verhindern, daß trojanische Pferde in das Netzwerk eindringen können. Hierzu sind Filter auf Anwendungsebene notwendig. Diese Filter dürfen sich logischerweise nicht auf Server 1 oder 2 befinden. Es bleibt nur noch die Firewall selber als Filter übrig. Andernfalls muß eine zweite DMZ eingerichtet werden, in der dann ein Host mit dem Filter angesiedelt ist. Das würde dann drei Firewalls bedeuten (Abbildung 5).

Ein weiteres Problem stellt dann noch der Log-Server dar, der die Log-Einträge zumindest der inneren Firewalls miteinander vergleichen muß. Firewall 1 erfüllt hier nur Kontrollaufgaben und erhöht sehr die Zuverlässigkeit des Systems, indem sie die häufigen DoS-Angriffe von dem WWW/FTP/Mail-Server in der DMZ 1 fernhält. In der zweiten DMZ befindet sich dann der Filter auf Anwendungsebene, der E-Mails mit Attachments herausfiltert und z.B. FTP-Clients vor Buffer Overflow-Problemen und WWW-Clients vor Active X-Programmen schützt. Im internen Netzwerk sollten sich dann auch die Server für interne E-Mails und die DNS-Server befinden.

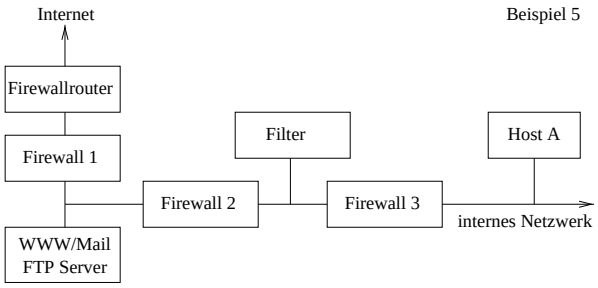


Abbildung 5: Konfiguration mit drei Firewalls

Standardlektüre sei das Buch Ëinrichten von Firewalls von Chapman/Zwicky aus dem O'Reilly Verlag empfohlen. Hier werden Architekturen genau beschrieben, leider ist diese Buch aufgrund der stark angewachsenen Gefahren auf Anwendungsebene völlig veraltet und stark korrektur- bzw. ergänzungsbedürftig.

## 5.5 Ein Unternehmen ohne Firewall

Zahlreiche Unternehmen besitzen eine E-Mail-Adresse, jedoch keinen WWW-Server oder Firewall. Sie rufen die E-Mails über einen T-Online-Account oder einen Account bei AOL über einen Arbeitsplatzrechner ab. Es gibt Firmen, die auf vielen Arbeitsplätzen ISDN-Karten installiert haben, um so Bandbreitenprobleme zu vermeiden und einen Faxserver einzusparen. Ein gezielter Angriff erscheint den Systemadministratoren völlig unwahrscheinlich. Es gibt Millionen AOL- und Telekom-Kunden, wie sollte ein Angreifer zu einem genauen Zeitpunkt die Dial-In-IP-Nummer derjenigen Arbeitsstation ausfindig machen können, die zu diesem Unternehmen gehört? Unmöglich? Wie es funktionieren kann, zeigt ein Beispiel:

Eine telefonische Anfrage bei einem Mitarbeiter dieser Firma, ein gewöhnliches Gespräch:

**Angreifer:** Ich habe da eine Anfrage. Kann ich Ihnen unsere Ausschreibung zusenden?

**Mitarbeiter:** Ja, meine Faxnummer ist 0xxxxyyyyy

**Angreifer:** Haben Sie auch E-Mail? Das ist bequemer!

**Mitarbeiter:** Ja, schicken Sie´s an `Mitarbeiter23.Firma@t-online.de`

**Angreifer:** Können Sie gezippte WinWord-Files lesen?

**Mitarbeiter:** Auch das können wir!

**Angreifer:** OK ich verpack´s dann sicherheitshalber in ein selbstextrahierendes `.exe`-File, falls wir unterschiedliche Versionen haben.

**Mitarbeiter:** Wenn Sie meinen...

Kurze Zeit später ist die E-Mail in der Firma angekommen, der Mitarbeiter extrahiert das Dokument, läßt es nach Viren durchsuchen, und macht sich an die Arbeit. Die ISDN-Verbindung bleibt noch ein paar Minuten bestehen, danach beendet die Software die Verbindung. Am nächsten Tag schaltet der Mitarbeiter seinen PC wie gewohnt an, ruft seine E-Mail ab, surft, faxt.

Was der Mitarbeiter nicht bemerkt hat, ist, daß in der `Autoexec.xxx`-Datei stets ein kleines Programm als Treiber mitgestartet wird, welches im Taskmanager nicht weiter auffällt, da es z.B. auch „findfast“ (findfast erscheint auch so öfter mal mehrmals...) genannt wurde. Das eingeschleuste Programm kontrolliert die Routen des Kernels (DOS-Shell: route -print), es stellt fest, daß eines oder mehrere Gateways aktiv sind, und sendet in dem Moment, wenn eine ISDN-Verbindung besteht, fleißig WinWord- und Excel-Dokumente als gezippte ASCII-Datei zu einem unbekannten Server im Internet. Das EXE-File ist zwar ein selbstextrahierendes ZIP-File, nur kommt es aber nicht von PKWARE. Es ist ein Eigenbau, welcher auf freien Quellen basiert. Dieses Programm könnte sich auch z.B. an `Netscape.exe` oder `explorer.exe` angehängt haben, so daß es stets mitstartet. Es wartet, wenn die ISDN-Verbindung unterbrochen wird. Es wäre auch möglich gewesen, ein kleines Programm, wie BO mit Plugins oder NetBUS zu installieren, welches sich stets zu den Zeiten meldet, wenn der User online ist, und somit unauffällig Fernadministration zuläßt. Da nur bekannte trojanische Pferde von den Virenscannern erkannt werden, bleibt die Installation unentdeckt. Durch Hinzufügen einer Löschroutine lassen sich sämtliche Spuren wieder beseitigen. Da sich nun der Arbeitsplatzrechner aus dem Unternehmen bei einem beliebigen Server im Internet mit einem „ping“ melden kann, ist somit der Angreifer in der Lage, die dynamisch vergebene IP-Nummer des Unternehmens direkt auf seinem Terminal zusehen. Er könnte nun die komplette Arbeitsstation fernwarten, und sich nach Belieben im Netzwerk umschauen.

Die Erstellung eines solchen trojanischen Pferdes ist relativ einfach, sofern man die Quellen kennt, ein wenig programmieren kann und genügend Einfallsreichtum besitzt. Dank ausgereifter Compiler und umfangreichen, freien Bibliotheken ist noch nicht einmal der Einsatz von Original-Microsoft-Software notwendig. (`http://www.cyrus.com`). Da die Fa. Microsoft mit der Einführung der winsock 2.0/2.1 die Kompatibilität zu UNIX weitestgehend hergestellt hat, reduzieren sich die Entwicklungszeiten besonders im Bereich Netzwerk erheblich. Ebenso einfach ist auch die Einbindung eines Makros in die Benutzeroberfläche von Windows 95/98/NT 4.0, dem Internet-Explorer. Diese Oberfläche ist beliebig umprogrammierbar. Da in relativ vielen Unternehmen Mitarbeiter einen eigenen Anschluß besitzen, ist die Wahrscheinlichkeit relativ hoch, daß ein Angreifer mit diesen Tricks eine Firewall umgehen oder sogar unauffällig ausschalten kann.

## 5.6 Angriffe auf DNS-Server

Angriffe auf DNS-Server in der DMZ sind aus vielerlei Gründen für Cracker interessant. DNS-Server tragen alle wichtigen Informationen über die Mail-Exchange-Server (MX-Eintrag) und Sites, von denen Systemadministratoren Software-Updates herunterladen. Besteht nun eine Kette von Abhängigkeiten von DNS-Servern untereinander, so ist es relativ einfach mög-

lich, die Einträge an geeigneter Stelle so zu verändern, daß auch die DNS-Server im Intranet mit falschen Informationen beliefert werden. Da in den Konfigurationsfiles jeder Windows-Arbeitsstation stets der interne DNS-Server angegeben ist, ist es einem Cracker möglich, die internen IP-Nummern des DNS-Servers herauszufinden (die externen kennt er sowieso), und zu versuchen, eine alte Lücke auszunutzen (Additional Information Trick), den zuletzt Eugene Kashpureff mit der Umleitung tausender Domains auf `www.alternic.net` in großem Stil 1998 benutzt hatte. Hierzu muß wiederum ein trojanisches Pferd von einem arglosen Anwender im lokalen Netzwerk gestartet werden. Im Jahr 1998, also ca. 4 Jahre nach Bekanntwerden des Sicherheitsproblems, gingen z.B. bei SNI München ca. 4 Gigabyte E-Mails in wenigen Wochen verloren. Grund: Falsche DNS-Informationen (Abbildung 6).

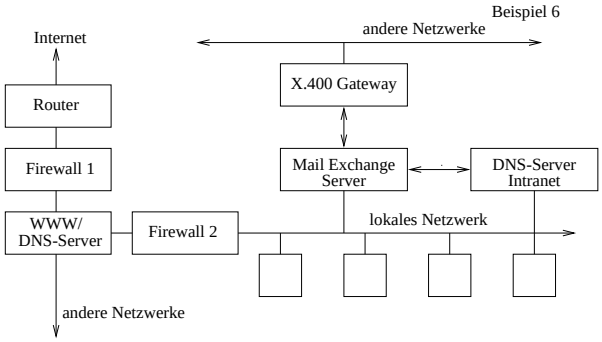


Abbildung 6: Angriff auf DNS-Server möglich

Es bieten sich gerade in größeren Unternehmen gute Chancen, einem internen DNS-Server zu manipulieren, von welchem viele andere abhängig sind (Cache-Modus). Das muß allerdings über ein eingeschleustes trojanisches Pferd geschehen. Da aber Unternehmen, wie SNI fast alles über E-Mail versenden (Bilanzen, Angebote, Pläne zu Sicherheitskonzepten für Banken. . . ) und viele Mitarbeiter surfen dürfen, ist die Wahrscheinlichkeit beinahe gleich 1, daß Cracker das Netzwerk bereits durchforstet haben. Das zeigen die unzähligen fehlgelaufenen E-Mails an die Domain `sni.mch.de` (statt `mch.sni.de`), die das Marketing-Center Handwerk bereits erhalten hat. Das Gesamtvolumen betrug ca. 5 Gigabyte an E-Mails aus dem Hause Siemens, welches auf diese Domain fehlgeleitet wurde. Dazu gehören auch unzählige E-Mails aus dem Bereich des X.400, die über das SNI-Gateway ins Internet versandt wurden. (SNI ist informiert!) Siemens hat das Problem seit April 1997 bis heute nicht im Griff. Im Grunde sind aber viele Banken und Versicherungen, die X.400 benutzen ebenfalls betroffen. Ein Grund liegt darin, daß viele Benutzer mit der Umsetzung der X.400 Mail Adresse in das Internet Format nicht klarkommen. Hier sollten Systemadminitratoren schon in der Firewall bzw. der DNS Konfiguration die typischen Verdreher abfangen. Ein andere Grund liegt in veralteten DNS Servern innerhalb des Unternehmens, welche für additional informationsnoch anfällig sein könnten. Sehr problematisch sind die Windows NT Exchange Server, die auch als DNS Server arbeiten. Microsoft ist ein Sumpf an Fehlern, Ungereimtheiten, Eigenwilligkeiten, Unerklärlichkeiten ,ein Musterbeispiel für schlechte Dokumentation, abgesehen einmal davon, daß Microsoft oftmals erst nach einem halben Jahr einen Patch für dringende Probleme anbietet. Wer seinem solchen Betriebssystem Sicherheitsrelavante Informationen anvertraut, dazugehören immer auch die Einträge des DNS Servers, der sollte sich darüber im Klaren sein, daß ihm ähnliches wie

Siemens wiederfahren kann. (Es soll hiermit nicht behauptet werden, daß Siemens ein solcher Angriff wiederfahren ist, obwohl meiner persönlichen Meinung nach einiges dafürspricht)

## 5.7 Angriff auf einen Datenbankbetreiber im Internet

Im Mai 1998 erfolgte ein Angriff der besonders bösen Art auf einen Dienstleistungsbetreiber der Handwerksorganisation, der für Handwerkskammern Datenbanken im Internet anbietet. Diese Datenbanken sind über Internet direkt erreichbar, und durch eine Firewall (Hersteller RAPTOR EAGLE, jedoch unwensendlich) gesichert. Für die Zeit von ca. 3 Wochen wurde ein DoS-Angriff auf Server hinter der Firewall von unbekannter Herkunft gestartet. Das Problem war der Datenbankserver dahinter, der auf diese Pakete allergisch reagierte und neu bootete. Im konkreten Fall war dies Windows NT. Für das Unternehmen bedeutete dies quasi einen Totalausfall des Dienstleistungsangebotes. Häufiger Grund für diese Art von Angriffen sind fragmentierte, verschachtelte Pakete, die die Firewall in Abhängigkeit der Konfiguration durchtunneln können, und den TCP/IP-Stack des Servers dahinter zum Absturz bringen. Von diesen Angriffen waren auch zahlreiche Dienstleistungsanbieter im Internet betroffen, die Archive für Zeitungen betreiben.

## 5.8 Angriff auf Video-/Audioserver im Internet

Betroffen war u.a. der Radiosender SWF3, nun SWR. Dieser war für längere Zeit sporadisch offline. Vermuteter Grund war ebenfalls ein Angriff mit fragmentierten, verschachtelten Paketen aufgrund eines „Buffer Overflow“-Problems mit dem REALAUDIO-Server. Unzählige ISPs, die einen solchen Server im Angebot hatten, wurden Opfer von solchen Angriffen, die bis zur Zerstörung des Systems reichten.

## 5.9 Angriff auf SQL-Server

Problematisch sind Angriffe auf SQL-Server. SQL-Datenbanken gehören bekanntermaßen zu den langsamsten überhaupt. Angriffe mit „Buffer Overflows“ sind inzwischen schwieriger, da die WWW-Server bei der Übergabe der Parameter an die Datenbank nur eine maximale Länge zulassen. Daher erfolgen die Angriffe (auch durch Firewalls hindurch) anders. Es wird ein Suchstring übergeben, der garantiert nicht in der Datenbank vorhanden ist, oder der besonders häufig zu finden ist. Da in beiden Fällen die Datenbank hoch belastet ist, genügen nur wenige Anfragen pro Sekunde, um das System völlig zu überlasten. Die Sicherung gegen solche Angriffe ist eine schmale Gratwanderung zwischen Einstellungen in der Firewall und den Einstellungen bzw. der Leistungsfähigkeit des Systems. Hier müssen detailliert genaue Informationen über RAM-Verbrauch, Antwortzeiten usw. vorliegen, bzw. einstellbar sein. Mit echtzeitfähigen Betriebssystemen oder Systemen, die eine Antwortzeit garantieren können, ist die richtige Abstimmung kein Problem, bei bestimmten Herstellern von Systemen sind diese Informationen nicht verfügbar.

## 5.10 Normale Surfer am Netz und Erpressungen?

Es gibt in Deutschland bald 4 Millionen User mit Internet-Anschluß. Kaum jemand fühlt sich durch Hackerangriffe bedroht, da ja Kontakte über Internet weitestgehend anonym bleiben können. Es gibt aber mit rasant wachsender Anzahl Hacker, die mit z.B. SMB-Scannern riesige Listen von IP-Nummern von Dial-In-Anschlüssen von Providern tagelang durchforsten. Wer es nicht glaubt, der möge sich einen Scanner installieren und die Pakete, die am PC ankommen genauer betrachten. Es sind pro Stunde einige Dutzend Einschläge zu verzeichnen. Wer´s nicht glaubt, installiere sich einen Scanner, und warte. (`http://www.signal9.com`) Diese Hacker sind auf der Suche nach PC´s, auf denen das Laufwerk C: zum Schreiben freigegeben ist. Haben sie einen gefunden, so installieren sie schnell BO und durchforsten die Festplatte nach Briefen usw. Sehr viele pädophile oder homosexuelle Surfer benutzen IRC-Clients, um untereinander zu kommunizieren, oder, was weit häufiger der Fall ist, gesetzlich verbotene Bilder auszutauschen. Diese IP-Nummern von IRC-Mitgliedern werden routinemäßig von Hackern auf Verletzbarkeiten überprüft, um evtl. BO zu installieren. Man kann davon ausgehen, daß Tausende von Lehrern, Professoren, Angestellte usw. auf diesem Wege Opfer von Erpressungen werden. Andererseits gibt es im Internet einige zwielichtige Personen, die als selbsterklärte Polizisten auf diesem Wege die Kinderpornografie bekämpfen. Diese geben nach solchen Angriffen Tips an die Polizei.

## 5.11 Tricks von Crackern auf Anwendungsebene

Trojanische Pferde sind ein unerläßliches Hilfsmittel für gezielte Angriffe auf Unternehmen. Sie werden von unzähligen Hackern eingesetzt, weil sie unauffällig sind, und mit höchster Wahrscheinlichkeit zum Erfolg führen. Professionelle Angreifer arbeiten mit trojanischen Pferden, die sie im Internet plazieren, und dann dafür sorgen, daß diese von den Systemadministratoren auch geladen und installiert werden. Trojanische Pferde aktivieren sich nach Abfrage bestimmter Kriterien, beispielsweise genau dann, wenn sich ein bestimmter Name in einem File findet (Absender in der Konfigurationsdatei des E-Mailprogrammes), oder die Arbeitsstation eine bestimmte IP-Nummer besitzt, die der Angreifer vorher ausgespäht hat. So ist es z.B. ohne Probleme möglich, einer Weihnachtsmann-Animation noch einen Portscanner oder Sniffer hinzuzufügen, der sich im Hintergrund betätigt. Angreifer erfragen zuvor Namen – Hauptziel sind Systemadministratoren - – und übermitteln der Zielperson dann freundliche Grüße mit o.a. URL als Anhang (Den mußte mal testen!). Um dann weitere Daten ausspähen zu können, muß der Angreifer zuerst einen Tunnel durch die Firewall konstruieren. Hierzu wird er mit Sicherheit Port 80 oder den Default Proxy-Port 8080 wählen und den Benutzer dazu irgendwie veranlassen, ein Programm zu starten, welches eine Verbindung zum Internet herstellt. Ist ersteinmal dieses Programm entweder im Hintergrund (vom Taskmanager verborgen, wie BO oder NETBUS) gestartet, so hat der Benutzer keinen Überblick darüber, ob ein trojanisches Pferd aktiviert ist und was es macht. Ein Eintrag in das Autostartverzeichnis ermöglicht es dem Angreifer, stets zu gewöhnlichen Bürozeiten sein Unwesen im Netz des Unternehmens im Internet zu treiben. Die Werkzeuge und Bibliotheken für z.B. Proxy-Routinen, SOCKS o.ä.

sind aufgrund der Open-Source-Bewegung allen frei zugänglich. Das erspart einem Cracker enorm viel Zeit.

## 5.12 Welche Programme können trojanische Pferde enthalten?

### Bildschirmschoner

Bildschirmschoner (`http://www.bildschirmschoner.de`) sind beliebte trojanische Pferde. Da sie aber Geschmackssache sind, kann ein Angreifer nicht damit rechnen, daß die Zielperson einen bestimmten auf seinem Arbeitsplatzrechner installiert.

### Aufsätze auf den Internet-Explorer

NeoPlanet z.B. ist ein Aufsatz auf den Internet-Explorer, welcher ein schöneres Design verspricht. Nachteil: Dieser Browser verrät Informationen von der Festplatte und sendet diese an seinen Homeserver. Welche dies sind, ist leider unbekannt, da die Informationen verschlüsselt übertragen werden. Eine weitere unangenehme Eigenschaft ist, daß dieser Browser eigenständig die ISDN-Leitung in das Internet öffnet, also sowohl Telefonkosten verursacht als auch eigenständig Informationen von der Festplatte in das Internet versendet. Das könnten z.B. die schlecht verschlüsselten Passwortdateien des WS-FTP sein, als auch die PWL-Dateien, in welchen die Zugangspassworte zum Server stehen. Ein ideales Werkzeug, da ein Angreifer davon ausgehen kann, daß das Programm längere Zeit auf der Arbeitsstation läuft. Mit Hilfe des von Microsoft angebotenen Kits, mit welchem man nach eigenem Geschmack Aufsätze auf den Internet-Explorer basteln kann, gelingt es einem Angreifer schnell, ein trojanisches Pferd zusammenzubasteln.

### Makroviren via E-Mail

Makroviren, die via E-Mail in ein Unternehmen eingeschleust werden, können im Quellcode so ziemlich alle möglichen Programme versteckt haben. Grund ist die Hinterlegung von Office 97 mit dem Visual Basic 5.0 und einem Update auf Winsock 2.0/2.1. Hiermit ist es nun möglich, Netzwerksniffer direkt in die Makros von Excel, WinWord oder PowerPoint hineinzuprogrammieren. Auch BO könnte man via Winword-Makro auf dem Arbeitsplatzrechner installieren. Schwachpunkt ist immer der Internet-Anschluß. Erst kürzlich wurde entdeckt, daß auch unter Windows NT 4.0 mit Excel-Makros voller Zugriff auf das System möglich ist. (Vasselin Bontchev, BUGTRAQ) Virenscanner können einen solchen Angriff leider noch nicht erkennen.

### E-Mail-Attachments

Wer hat sie noch nicht erhalten. Unter Bekannten tauscht man gerne mal einen EXE-Gruß aus. Wer kennt sie nicht: Elchtest aus PCWELT, X-MAS.EXE, Getränkehalter: Die CDROM fährt aus). Aus vermeintlich vertrauenswürdiger Quelle vermutet niemand ein trojanisches Pferd. Angreifer kennen meist aber Mail-Adressen von Kollegen und externen Mitarbeitern, da einem Angriff immer eine genaue Untersuchung der Logfiles des E-Mail Exchangers/Relays vorausgeht. Über abgefangene E-Mails, die zumeist noch CC:-Adressen enthalten ist der Angreifer durchaus im Bilde, wer in den Augen des Systemadministrators vertrauenswürdig ist, und wer nicht. E-Mail-Exchange-Server von Providern sind oft sehr schlecht gesichert. Die Logfiles enthalten aber wichtige Schlüsselinformationen über Kontaktpersonen, Kunden, Bekannte...

### Tastatur-Makros

Tastatur-Makros können via E-Mail in ein Unternehmen eingeschleust werden. Der Angreifer findet sicherlich einen User, der nicht mit der Umprogrammierung seiner Tastatur und den daraus resultierenden Konsequenzen rechnet. Lotus-Notes z.B. kann so umprogrammiert werden, daß jeder Tastendruck eine neue E-Mail in das Internet versendet: Inhalt: die Taste selber. Ein Angreifer bekommt so via E-Mail-Passworte, Briefe... in die Hände – ein mächtiges Werkzeug, welches schon häufig gebraucht wurde.

### Eingeschleuste Pseudo-Updates

Fast alle größeren Firmen besitzen einen Wartungsvertrag über Softwareupdates. Man stelle sich vor, der Systemadministrator bekommt eine Microsoft-CDROM: Update SP4 von seinem Lieferanten zugesandt (CompuNet, Digital...). Auf der CDROM ist aber nicht SP4, sondern SP1 mit all seinen bekannten Sicherheitslücken, und das Installationsprogramm ist eine gut gemachte Imitation, welche zudem noch ein trojanische Pferd auf dem Server installiert. Warnungen, es könnte eine neuere Version überschrieben werden, erscheinen nicht, alles läuft wie gewohnt. Kurze Zeit später wird der gut betreute Server aus dem Internet ferngesteuert. Auch CDROMs kann man in kleinen Stückzahlen zu Preisen von ca. 5 DM incl. Aufdruck herstellen lassen. Installationssoftware, die Microsofts Installationsprogramm nachahmt, gibt es im Internet gratis, viele Hersteller von Freeware benutzen es (`http://www.w3.org/amaya/`). Der Aufwand für einen Angreifer, sich alte SP1 Updates, DLLs, Systemfiles aus einem installierten System zu kopieren, diese in ein File zusammenzuschreiben und mit einem Installationsprogramm zu versehen, würde ein paar Stunden in Anspruch nehmen. Die Herstellung der CDROM mit Glasrohling, Aufdruck ... ca. 200 DM. Danach wären alle NT-Server, Workstations... im Netz mit NETBUS verseucht und beliebig fernsteuerbar. Viel einfacher ist natürlich, einem Bekannten die neuesten Service-Packs brandaktuell aus dem Internet auf CDROM zu kopieren, damit er Downloadzeit spart...

### Angriffe über IRC, Quake, ICQ, Netmeeting

Häufig sind Firewall-Einstellungen zu freizügig gehandhabt, sodaß es möglich ist, Dienste, die normalerweise über verbotene Ports laufen (ICQ, IRC) über den freigegebenen Port 80 (HTTP) der Firewall laufen zu lassen. Hacker kennen diese Möglichkeit und verleiten Mitarbeiter, die in Ihrer Freizeit von zuhause aus an ICQ oder IRC teilnehmen, innerhalb der Firma einen ICQ/IRC Client zu installieren und sich über Port 80 an einem „speziellen“ IRC/ICQ Server anzumelden. In diesem Falle ist es bei vielen Firewalls nicht möglich, zwischen HTTP-Traffic und IRC-Traffic auf Port 80 zu unterscheiden. Bespielsweise werden bei dem Einsatz der S.u.S.E.-Linux 5.3 und 6.0-Distribution als Firewall genau diese IRC- und Quake-Proxys per default aktiviert. Über IRC, ICQ und Quake lassen sich die Verzeichnisse von Arbeitsplatzrechnern und den angeschlossenen Servern beliebig auslesen und ins Internet übertragen. Diese Funktionen sind fester Bestandteil der IRC/ICQ-Philosophie und somit immer aktiv. Die meisten Angriffe erfolgen inzwischen über IRC. Netmeeting erlaubt zudem noch den Start von Shared Applications, um z.B. gemeinsam in einem EXCEL-Sheet arbeiten zu können. Netmeeting ist an sich eine Punkt zu Punkt-Verbindung, über NetShow werden Konferenzschaltungen möglich, ein wichtiger Angriffpunkt. Quake ist ein beliebtes Netzwerkspiel, welches gerne in der Mittagspause gespielt wird. Es besitzt große Sicherheitsprobleme.

### Microsoft Windows als trojanisches Pferd

Auch wenn es einigen Entscheidern nicht passen mag: Man kann es nicht deutlich genug sagen. Wer Microsoft Windows 98 oder NT 4.0 im Netzwerk installiert hat, hat gleich mehrere trojanische Pferde installiert, welches den Möglichkeiten von BO, NETBUS, IRC, ICQ oder Netmeeting entspricht. Eine Firewall kann nicht verhindern, daß ein Angreifer in dem Moment, wenn jemand vom Arbeitsplatz aus surft, Zugriff auf das Netzwerk hat. Zahlreiche und immer neue Fehler in der Benutzeroberfläche von Windows 98/NT 4.0, die dem Internet-Explorer entspricht, ermöglichen es einem Angreifer, über Javascript, Active-X und in wenigen Fällen über Java, direkt auf die Festplatte zuzugreifen. Falls ein Angreifer nur einen einzigen WWW-Server im Internet kennt, der von Mitarbeitern häufig besucht wird (oft ist es der eigene WWW-Server), so wird ein professioneller Angreifer wenig Mühe haben, einigen WWW-Seiten des Servers einige sicherheitsrelavante Skripte unterzuschieben. Oft wird behauptet, daß die Sicherheit des WWW-Servers unwichtig sei, da er ja ohnehin keine geheimen Informationen beinhalte, und somit für Angreifer uninteressant sei. Das Gegenteil ist der Fall. Zudem fungiert dieser Server oft noch als E-Mail-Relaystation und enthält wertvolle vertrauenswürdige E-Mail-Adressen, welche der Angreifer spooft, um trojanische Pferde in das Netzwerk einzuschleusen.

Hier also kurz diejenigen Programme, die von Crackern inzwischen sehr häufig benutzt werden, um einen Angriff über eine Firewall hinweg zu starten:

- WinWord Makros
- Excel Makros

- Outlook Scriptsprache
- Internet Explorer Active-X
- Internet Explorer Plugins
- Trojanische Pferde (WINUNZIP, PKSFX, NEOPLANET Browser Addon)

Mit relativ geringem Arbeitsaufwand, der nötig ist, um einen solchen Angriff vorzubereiten, muß damit gerechnet werden, daß die Angriffe nicht mehr von außerhalb, sondern von innerhalb des Netzwerkes initiiert werden. Um dies in der Praxis zu testen, wurden willkürlich an beliebige E-Mail-Adressen von Verlagen, Forschungszentren, Pharmakonzernen, Logistikunternehmen und die größten Telekommunikationsunternehmen in Deutschland harmlose E-Mails mit kleinen Animationen als .EXE Files verschickt. Die Erfolgsquote lag bei 100%, alle „.EXE“ Dateien erreichten ihren Adressaten im Intranet und wurden gestartet. Dies ist ein Anzeichen dafür, daß offensichtlich die Gefahren völlig unterschätzt werden. Wer glaubt, man könne einen geschickten Angreifer dingfest machen, der möge sich vor Augen führen, daß im Internet in IRC-Channeln Passorte zu UNIX Workstation in Japan, Singapur, USA, Mexiko....gehandelt werden. Darüber hinaus ist es mit address spoofing immer möglich, sogenannte blinde Angriffe auszuführen, die ohne Rückmeldung von der Workstation auskommen. Erfahrene Angreifer können nach dem Auskundschaften der Software ihre Angriffe blind oder automatisiert ausführen. Wer mehr über diese Angriffsmöglichkeiten erfahren möchte, dem sei der Anhang des LINUX Firewallbuches auf der Site `http://www.little-idiot.de` empfohlen.