



KAPITEL 7

Planung einer normalen Installation

Ein Disketten-Linux dient einem ziemlich klar umrissenen Zweck und stellt keine besonderen Anforderungen an die verwendete Hardware. Auch ist es nicht nötig, sich Gedanken um die Partitionierung einer Festplatte zu machen. Verwenden wir eine Standarddistribution, sieht die Situation etwas anders aus. Hier müssen wir uns überlegen, welche Hardwareanforderungen die von uns vorgesehene Software stellt. Wir brauchen ein Konzept, wie wir bei der Installation vorgehen, um zu vermeiden, daß eine halbfertige Firewall bereits Kontakt zum Internet hat. Und wir müssen wissen, wie wir die Platte partitionieren, um DoS-Angriffen zu begegnen.

Wenn wir außerdem eine größere Anzahl Benutzer mit einem Zugang zum Internet versorgen wollen, kommen wir nicht umhin, als erstes schriftlich festzuhalten, was wir mit der Firewall erreichen wollen und an welche Regeln sich die Beteiligten halten müssen.

Im folgenden wollen wir daher erst einmal in Ruhe unsere zukünftige Firewall und ihr Umfeld planen, bevor wir dann im nächsten Kapitel mit der Installation beginnen.

Policies

Grundsätzlich ist eine Firewall kein Selbstzweck. Ihr Einsatz ist nur sinnvoll, um ein vorhandenes Sicherheitsziel technisch umzusetzen. Erst wenn klar ist, was erreicht werden soll, kann versucht werden, die aufgestellten Ziele durch den Einsatz einer Firewall zu realisieren.

Wird unsere Firewall von einer größeren Anzahl Anwender benutzt oder arbeiten wir im Rahmen einer Organisation, wie z. B. einer Universität oder Firma, so ist es notwendig, dieses Sicherheitsziel und die Regeln zu seiner Umsetzung schriftlich niederzulegen. Dies geschieht in Form einer Policy sowie mehrerer Richtlinien und technischer Spezifikationen.

Die eigentliche Policy sollte dabei einige wenige Seiten nicht überschreiten und so formuliert sein, daß sie lange Zeit ohne große Änderungen bestehen kann. Ihre Rolle ist es, Verantwortlichkeiten und generelle Vorgehensweisen festzuhalten, nicht aber, spezielle Bedrohungen, Technologien oder Rechner zu beschreiben.

Dies geschieht dann in einem zweiten Schritt in Form von Richtlinien und technischen Spezifikationen. Der Grad an Detaillierung dieser Dokumente wird dabei von der Größe des zu schützenden Netzes, der Anzahl der Benutzer und der Anzahl der beteiligten Parteien abhängen.

Eine Policy für ein Studentenwohnheim

Im Fall unseres Studentenwohnheims sollte zuerst definiert werden, ob der Zugang zur allgemeinen Nutzung des Internets oder nur zum rein wissenschaftlichen Arbeiten vorgesehen ist. Auch sollten alle Beteiligten darauf verpflichtet werden, bei der Benutzung des Netzes die Privatsphäre und die Persönlichkeitsrechte anderer Nutzer zu wahren und die Nutzung des Netzes durch ihre Mitbenutzer nicht unangemessen zu beeinträchtigen oder gar zu verhindern.

Dann wird in der Regel ein Hinweis auf den rechtlichen Status erfolgen. Dies kann zum Beispiel in der Form geschehen, daß nur der Zugang zum Internet bereitgestellt wird, die Nutzung desselben aber auf eigene Gefahr und in eigener Verantwortung durch die Benutzer geschieht. Die Universität und die Netzwerk AG werden an dieser Stelle üblicherweise jegliche Haftung sowohl für die Unterbrechung des Zugangs zum Internet, Schäden, die durch die Teilnahme des Benutzers am Netzbetrieb entstehen, und Schäden, die Dritten durch Handlungen der Benutzer entstehen, ausschließen.

Im folgenden werden dann die beteiligten Parteien aufgeführt und ihre Aufgaben und Verantwortlichkeiten definiert. In unserem Beispiel könnte dabei z. B. die folgende Aufstellung herauskommen:

Die Bewohner des Wohnheims haben ein Anrecht darauf, das Wohnheimnetz und den Internet-Anschluß zu nutzen, sofern sie sich verpflichten, die geltenden Regelwerke zu beachten. Der Anspruch erlischt zeitweilig oder permanent, wenn sie der eingegangenen Verpflichtung nicht nachkommen.

Die Netzwerk AG besteht aus den Studenten des Wohnheims, die bereit sind, bei der Gestaltung des Wohnheimnetzes mitzuwirken. Als Gremium der Studentischen Selbstverwaltung ist die Netzwerk AG von den Universitätsgremien beauftragt, den Betrieb des Wohnheimnetzwerkes zu organisieren und die dafür nötigen Regelwerke zu beschließen. Die Netzwerk AG tagt regelmäßig in öffentlichen Sitzungen.

Die Netzwerkadministration ist für die technische Umsetzung der Beschlüsse der Netzwerk AG zuständig. Sie besteht aus Mitgliedern der Netzwerk AG, die sich bereit erklärt haben, in ihrer Freizeit den technischen Betrieb des Netzes durchzuführen. Im Rahmen dieser Funktion haben sie auch das Recht, Benutzer bei Verstößen gegen die geltenden Regeln zeitweise von der Teilnahme am Netzverkehr auszuschließen.

Die Universitätsgremien haben als Auftraggeber der Netzwerk AG in erster Linie eine Kontrollpflicht. Sie genehmigen neue Regelwerke und dienen auch als Berufungsinstanz, wenn Beschwerden gegen die Entscheidungen der Netzwerk AG oder der Netzwerkadministration vorgebracht werden.

Eine Policy für eine Firma

Eine Policy für eine Firma sollte zuerst festlegen, daß die Daten der Organisation oder Firma sowie die Werkzeuge zu ihrer Verarbeitung als wichtige Ressource betrachtet werden und daher von allen Beteiligten im Rahmen ihrer Kenntnisse und Fähigkeiten zu schützen sind. Auch ein Hinweis auf die Geheimhaltung von Geschäftsgeheimnissen und eine Verpflichtung zum Schutz personenbezogener Daten ist angebracht. Nicht fehlen sollte auch die Aussage, daß die Einrichtungen nur für Tätigkeiten im Rahmen der Aufgaben der Firma oder Organisation, nicht aber für private Zwecke zu nutzen sind.

Im zweiten Teil gilt es, die beteiligten Parteien zu identifizieren und ihre Rechte und Pflichten festzulegen. Hier wird man es in der Regel zumindest mit drei Parteien zu tun haben:

Der Chef verantwortet die zu treffenden Entscheidungen. Sicherheit ist letztlich eine Abwägung zwischen den entstehenden Kosten für Sicherheitsmaßnahmen und den möglichen Kosten eines Vorfalles. Aus diesem Grunde ist es die Aufgabe des Chefs zu entscheiden, welche Maßnahmen ergriffen werden sollen, und diese Entscheidungen dann auch konsequent durchzusetzen. Diese Entscheidungen sind als Richtlinien schriftlich zu dokumentieren und den Betroffenen zugänglich zu machen.

Der Techniker bereitet die Entscheidungen vor und setzt sie gegebenenfalls technisch um. Da der Chef in der Regel nicht über Detailkenntnisse der verwendeten Technik verfügt, ist es die Aufgabe des Technikers, ihm die nötigen Informationen zu liefern, anhand deren der Chef eine Entscheidung treffen kann. Des weiteren ist es die Aufgabe des Technikers sicherzustellen, daß die getroffenen Maßnahmen die Entscheidungen des Chefs auf die technisch bestmögliche Weise umsetzen. Schließlich muß er dem Anwender noch die nötigen Informationen zur Verfügung stellen, damit dieser nicht durch Unwissenheit Gefahren heraufbeschwört. Wird vom Anwender zum Beispiel erwartet, Daten zu sichern oder Dateien auf Viren zu prüfen, so muß ihm vorher erklärt werden, wie das zu geschehen hat.

Der Anwender nutzt die vom Techniker bereitgestellten Dienste. Er kann erwarten, daß diese, soweit dies im Rahmen der Sicherheitsentscheidungen möglich ist, alle Funktionen realisieren, die er für seine Arbeit braucht. Im Gegenzug wird von ihm erwartet, die Technik verantwortungsvoll im Rahmen seiner Fähigkeiten und Kenntnisse zu nutzen.

Wenn dies geschehen ist, liegt uns ein Papier vor, das klar festhält, daß Sicherheit gewünscht wird und daß es die Verantwortung aller ist, diese zu gewährleisten. Wurde dieses von der Unternehmensführung oder der Leitung der Organisation unterschrieben und an alle Beteiligten verteilt, so haben wir als technisch Verantwortliche eine Ausgangsbasis, um praktisch etwas zu erreichen.

Ohne ein solches Papier bewegen wir uns auf sehr unsicherem Terrain. Die Anwender werden bei jeder sich bietenden Gelegenheit von unseren Vorgesetzten verlangen, bestimmte Sicherheitsmaßnahmen abzuschalten, da diese ihre Arbeit behindern würden. Unser Vorgesetzter könnte ihnen durchaus nachgeben und uns dann später verantwortlich machen, wenn daraus ernsthafte Vorfälle resultieren. Hat er dagegen ein Papier un-

terschrieben, in dem er anerkennt, daß Sicherheit auch seine Verantwortung ist, so ist er unseren Argumenten etwas zugänglicher.

Richtlinien und Spezifikationen

Im nächsten Schritt gilt es dann, Richtlinien festzulegen, die beschreiben, wie die hehren Ideale der Policy konkret für bestimmte Problemfelder umgesetzt werden sollen. Dabei geht es allerdings weniger darum, Soft- und Hardware in ihrer konkreten Version zu benennen, sondern festzulegen, was unter welchen Umständen durch wen getan werden soll. Eine Richtlinie für die Erstellung von Backups wird dabei z. B. festhalten, daß Backups des Servers zumindest an jedem 3. Werktag zu erstellen sind und daß diese außerhalb des Rechenzentrums in einem feuerfesten Schrank mindestens ein Jahr zu lagern sind. Darüber hinaus werden die Benutzer verpflichtet, keine Daten auf den lokalen Rechnern zu lagern. Daß für das Backup auf den Unix-Servern das Programm `dump` sowie DAT-Bänder verwendet werden, ist dagegen nicht Gegenstand der Richtlinie, sondern einer technischen Spezifikation, die regelmäßig an Änderungen von Hard- und Software angepaßt werden muß.

Mit etwas Glück kann die Richtlinie relativ unverändert bestehen bleiben, solange die zugrundeliegenden Technologien sich nicht gravierend ändern. Außerdem erleichtert es das Verständnis der Richtlinie durch die genehmigende Instanz und die betroffenen Benutzer enorm, wenn statt einer konkreten technischen Implementation vielmehr aufgezeigt wird, was warum geschehen soll. Damit wäre eine Formulierung

»Um die Netzlast zu vermindern, ist ein Rechner einzusetzen, der angeforderte Webseiten zwischenspeichert und Werbegraphiken ausfiltert.«

ihrem Gegenstück

»Es ist ein 486DX2 PC mit Internet Junkbuster Version x.y und der Filterliste von <http://x.y.z> als Proxy einzusetzen.«

deutlich überlegen. Die genaue technische Umsetzung ist dagegen in erster Linie ein Problem der Techniker und wird den »Chef« in der Regel nur insoweit interessieren, als er Geld für die benötigte Hard- und Software beschaffen muß.

Der Zugang zum Internet sollte in mindestens zwei Richtlinien geregelt werden. Eine ist für die Anwender bestimmt und sollte regeln, in welcher Weise diese das Internet nutzen dürfen. Einige Punkte, die dabei sicher zu bedenken wären, sind:

- der Besuch von Seiten mit anstößigen Inhalten (Pornographie, Rassismus, ...),
- der Download großer Dateien (z. B. Spiele),
- die Installation und/oder Ausführung von Programmen, die aus dem Internet heruntergeladen oder als E-Mail empfangen wurden,
- das Versenden von Nachrichten (E-Mails, Newspostings, ...) mit anstößigen Inhalten,

- das Versenden von Nachrichten mit vertraulichen Daten,
- die Installation zusätzlicher Modems, ISDN- oder anderer Zugänge, die die Firewall umgehen,
- der Anschluß eigener Rechner der Benutzer oder ihrer Gäste,
- das Mitlesen von Datenübertragungen Dritter,
- der unberechtigte Zugriff auf Rechner anderer Benutzer,
- die Benutzung von Paßwörtern, die auch im internen Netz verwendet werden, zur Anmeldung an Server im Internet,
- die Benutzung von Virenscannern,
- die Weitergabe von Paßwörtern an Dritte (Kollegen, vorgebliche Servicetechniker, Fremde im IRC, . . .) und
- welche Konsequenzen gezogen werden, wenn gegen die Richtlinien verstoßen wird.

Eine zweite Richtlinie sollte den Betrieb der Firewall(s) regeln. Dabei ist unter anderem zu regeln,

- ob überhaupt eine Firewall verwendet werden soll oder die Sicherung der einzelnen Rechner im lokalen Netz ausreicht,
- ob Rechner, die Dienste anbieten, auf welche aus dem Internet heraus zugegriffen werden kann (Web-, FTP-Server, . . .), in einem eigenen Netz untergebracht werden sollen, auf das aus dem internen Netz nur auf gesichertem Wege zugegriffen werden kann,
- unter welchen Umständen gegebenenfalls Zugriffe aus dem Internet auf Rechner im lokalen Netz zulässig sind (Mitarbeiter auf Reisen, Fremdfirmen, E-Commerce-Anwendungen, . . .) und welche Schutzmaßnahmen dabei zu treffen sind,
- ob bestimmte Inhalte durch technische Maßnahmen gefiltert werden sollen (Werbe-graphiken, aktive Inhalte, . . .),
- ob gegebenenfalls Rechner existieren, die zu sensitiv sind, als daß sie mit demselben Netz verbunden sein dürften, in dem sich Rechner mit Zugang zum Internet befinden,
- in welchem Maße und zu welchem Zweck der Netzwerkverkehr durch die Firewall-administration beobachtet und protokolliert werden darf,
- ob und in welcher Form Daten aus der Beobachtung des Netzwerkverkehrs an Dritte weitergegeben werden dürfen,
- wer entscheidet, ob der Zugriff auf einen Dienst durch die Firewall erlaubt werden soll.

Zusätzlich zur Richtlinie sollte eine Liste derjenigen Dienste geführt werden, die auf ihre Auswirkungen für die Sicherheit des lokalen Netzes überprüft wurden und deren Benutzung genehmigt wurde.

Bevor man allerdings daran geht, diese Richtlinien aufzustellen, sollte man zuerst die Benutzer fragen, wozu sie das Internet benötigen. Versäumt man dies, so gelangt man

schnell in eine Situation, in der zwar eine technisch ausgefeilte Lösung realisiert wurde, diese aber wertlos ist, da sie am tatsächlichen Bedarf vorbei geplant wurde. Dies bedeutet natürlich nicht, daß jeder Benutzerwunsch unbesehen umgesetzt werden sollte, aber wenn ein berechtigtes Interesse nach einer bestimmten Funktionalität besteht, sollte ein hinreichend sicherer Weg gefunden werden, diese umzusetzen.

Ein Benutzer könnte z. B. verlangen, aus dem Internet auf einen Rechner im lokalen Netz per Telnet zugreifen zu dürfen. Nun ist Telnet kein sicheres Protokoll. Das Paßwort wird im Klartext übertragen, und auch die IP-Adresse des Absenders kann gefälscht werden. Es ist daher durchaus denkbar, daß ein Angreifer die übertragenen Daten (insbesondere auch das Paßwort) belauscht und diese Informationen nutzt, um sich an einem Rechner in unserem lokalen Netz anzumelden. Unser erster Impuls wird daher sein, das Ansinnen kategorisch abzuweisen. Nun könnte es aber sein, daß dieser Benutzer z. B. einen Server betreut und dafür in Notfällen auch von zu Hause aus Zugriff haben muß. In diesem Fall können wir als Techniker noch so große Bedenken haben, der Zugang ist aus Firmensicht sinnvoll und wird letztendlich gewährt werden.

Es bleibt uns nur, einen Kompromiß zu finden. Eine naheliegende Lösung stellt z. B. SSH dar, das vielen Linux-Distributionen beiliegt. Hierbei handelt es sich um ein Protokoll, das eine durchaus ähnliche Funktionalität wie Telnet bietet, zusätzlich aber starke Verschlüsselungsverfahren unterstützt. Bei der Verwendung digitaler Zertifikate zur Authentisierung kann sichergestellt werden, daß sich nur der Besitzer des passenden geheimen Schlüssels auf dem Rechner anmelden kann. Jeglicher Versuch, die Verbindung zu belauschen, ist von vorneherein zum Scheitern verurteilt, falls der Rechner des Mitarbeiters als sicher betrachtet werden kann.

Letzteres ist der große Pferdefuß dieser Lösung. Ist der Rechner unsicher konfiguriert oder wurde auf ihm ein Virus oder Trojaner installiert, so kann ein Angreifer den geheimen Schlüssel des Mitarbeiters herunterladen und sich an seiner Stelle am Zielrechner anmelden. Es sind zusätzliche Regelungen nötig, um dies zu verhindern. Diese kann z. B. darin bestehen, dem Benutzer einen speziellen, sicher konfigurierten Rechner zur Verfügung zu stellen, den er nur dazu verwenden darf, sich mit dem internen Netz zu verbinden. Jegliche private Nutzung ist strikt zu untersagen.

Prinzipiell kann so eine Lösung erreicht werden, die durchaus einen brauchbaren Schutz gewährleistet. Die konkrete Konfiguration der beteiligten Rechner muß allerdings mit größter Sorgfalt durchgeführt werden. Auf eine genaue Beschreibung soll daher hier verzichtet werden. Sie würde den Rahmen dieser Darstellung sprengen.

Hardware

Eine Firewall unter Linux stellt prinzipiell keine allzu hohen Anforderungen an die verwendete Hardware. Ich habe schon Paketfilter auf 486DX-PCs mit einem Systemtakt von 50 MHz und 16 MB Hauptspeicher eingerichtet, die über eine 10-MBit-Leitung an das Internet angebunden waren. Selbst bei dem Versuch, sie mutwillig hohen Lasten auszusetzen, stieg die Prozessorauslastung nie über 20 %. Dabei handelte es sich um ein System mit einem 2.2er Kernel mit komplizierten Filterregeln, da neben einem Netz-

werkstrang für normale Klientenrechner auch noch ein zweiter Strang für einen Web- und FTP-Server bedient wurde.

Dabei habe ich allerdings ein selbst zusammengestelltes Mini-Linux verwendet. Will man dagegen eine Standarddistribution verwenden, ist schon eine gewisse Überredungskunst nötig, um es auf einem Pentium 90 mit 32 MB Hauptspeicher zu installieren. Insbesondere der beschränkte Hauptspeicher führt z. B. bei einer Installation von SuSE 7.3 dazu, daß das Installationsprogramm nach langwieriger Auswahl der zu installierenden Pakete abstürzte. Erst die manuelle Aktivierung einer Swap-Partition in einer zweiten Konsole brachte Abhilfe.

Ich würde Ihnen daher derzeit mindestens 64 MB, besser noch 128 MB Hauptspeicher empfehlen, falls Sie eine Standarddistribution installieren wollen. Da diese Angaben aber schnell veralten, sollten Sie sich immer vergewissern, welche Hardware-Anforderungen der Hersteller der von Ihnen verwendeten Distribution stellt. Auch sollten Sie nicht am Festplattenplatz sparen. Zirka 2 GB würde ich auf jeden Fall vorsehen. Wollen Sie einen cachenden Proxy wie den squid verwenden, so sollten es lieber ein paar GB mehr sein, um die zwischengespeicherten Webseiten aufzunehmen.

Für die Installation wird man in der Regel ein CD-ROM- oder DVD-Laufwerk benötigen. Zwar existiert auch die Möglichkeit einer Netzwerkinstallation von einem FTP- oder NFS-Server, dies ist aber deutlich umständlicher und auch unter Sicherheitsaspekten nicht wirklich ratsam.

Schließlich sollte man sich auch Gedanken über die Möglichkeiten eines Backups machen. Da eine Installation leicht einen Grundumfang von mehreren 100 MB hat, scheiden Disketten aus. Sinnvoll wäre z. B. die Anschaffung eines SCSI-DAT-Streamers oder eines CD- bzw. DVD-Brenners, der ohne großen Aufwand mit Standardwerkzeugen angesprochen werden kann.

Auch eine zusätzliche Platte, auf der man im Bedarfsfall Images der Partitionen der Firewall (siehe Kapitel 17 ab Seite 539) erstellen kann, wäre sinnvoll. So eine Platte sollte man aber im normalen Betrieb nicht anschließen. Andernfalls kann man nicht sicher sein, daß ein eventueller Angreifer sie nicht gemountet und für eigene Zwecke genutzt hat.

Vorgehen bei der Implementation

Bevor man nun darangeht, die Firewall aufzusetzen, sollte man erst einmal überlegen, wie man vorgehen will. Ein Extrem bestünde darin, den Rechner physikalisch an das Internet anzuschließen, ihn von einer Diskette zu booten und nach einer kurzen Konfiguration der Netzwerkeinstellungen alle benötigten Softwarepakete direkt aus dem Internet zu laden.

Es existieren Distributionen, mit denen dieses Vorgehen möglich ist. Für die Installation einer Firewall wäre es allerdings unangebracht. Sinnvoller wäre es, das System von CD zu installieren und erst dann mit dem Internet zu verbinden, wenn es fertig konfiguriert ist und gründlich getestet wurde.

Das Problem hierbei sind allerdings die notwendigen Tests. Um sicherzustellen, daß eine Firewall wie geplant funktioniert, müßte man sowohl das lokale Netz als auch das Internet simulieren. Dazu dient ein Rechner als Klient, der an den internen Anschluß der Firewall angeschlossen wird. Ein weiterer Rechner dient dazu, den Provider sowie Server und Angreifer im Internet zu simulieren. Nun testet man, ob Rechner im Internet vom Klienten aus erreichbar sind und unerlaubte Anfragen aus dem Internet geblockt werden. Schließlich kann man noch testen, ob Verbindungen aus dem lokalen Netz möglich sind, die man nicht vorhergesehen hat.

Finden sowohl der Anschluß an das lokale Netz als auch die Anbindung an das Internet über eine normale Netzwerkkarte statt, so sollte es nicht besonders schwierig sein, den beschriebenen Testaufbau zu realisieren. Als Klient kann hier einer der Rechner dienen, mit denen man später auch tatsächlich surfen will, als Provider/Server/Angreifer sollte man einen Linux-Rechner vorsehen. Dieser braucht allerdings nicht besonders aufgesetzt zu werden. Lediglich zwei kleine Hilfsprogramme müssen installiert werden. Darüber hinaus sollte seine IP-Adresse auf die Adresse des Routers des Providers eingestellt werden, damit unser »Internet« auch korrekt von der Firewall angesprochen wird.

Problematisch wird es, wenn die Einwahl beim Provider über Modem oder ISDN erfolgen soll. Dann müßte unser »Testprovider« über eine Telefonanlage mit der Firewall verbunden sein. Außerdem müßte er die komplette Funktionalität eines Einwahl-Gateways realisieren. Dieser Aufwand kann durchaus sinnvoll sein, wenn man täglich Firewalls aufsetzt, ist aber in allen anderen Fällen kaum zu rechtfertigen, da es neben dem zusätzlichen Aufwand auch bedeutet, eine ganze Reihe zusätzlicher Fehlerquellen zu schaffen.

In diesem Buch wird daher ein anderer Ansatz beschrieben. Wir werden zuerst die Einwahl beim Provider testen. Hierbei wird ein minimaler Satz von Firewallregeln zum Einsatz kommen, der kaum Zugriffe ermöglicht, es aber erlaubt, die Funktionalität der Netzwerkanbindung zu testen, ohne befürchten zu müssen, unser erst halb konfigurierter Rechner könnte kompromittiert werden. Danach richten wir das Firewalling gemäß unseren Bedürfnissen ein.

Für die Tests des Firewalling bauen wir eine zusätzliche Netzwerkkarte in den Rechner ein und simulieren die Einwahl über Modem nur. Die Tests erfolgen dann wie zu Beginn beschrieben mit zwei Testrechnern an den Netzwerkkarten. Sind die Tests abgeschlossen, kann die zusätzliche Netzwerkkarte wieder ausgebaut werden, und nach ein paar minimalen Änderungen an der Konfiguration findet die Einwahl über Modem bzw. ISDN statt. Nun besitzen wir eine voll funktionierende Firewall.

Rechnerdaten

Für eine reibungslose Installation ist es wichtig, das verwendete System zu kennen. Plug-and-Play hat in der Linux-Welt noch nicht ganz denselben Stand erreicht, den man von Windows her gewohnt ist. Man sollte daher als erstes die technischen Dokumentationen aller verwendeten Komponenten (Handbuch des Mainboards, Faltblätter der Netzwerkkarten, etc.) zusammensuchen und in einem eigenen Ordner abheften, wo man sie bei Bedarf schnell wiederfindet.

Als nächstes gilt es, Daten der aktuellen Konfiguration zu sammeln. Mit etwas Glück wird man nur einen Teil der im folgenden aufgeführten Informationen tatsächlich brauchen, es ist aber immer besser, zuviel vorbereitet zu haben, als mitten in der Installation nach der einen Information gefragt zu werden, die man gerade nicht parat hat. Eine Aufstellung, welche Daten Sie eventuell benötigen, finden Sie in Tabelle 7-1.

Tabelle 7-1: Checkliste für die Konfigurationsdaten

Komponente	Benötigte Angaben
Für alle Komponenten (falls anwendbar)	Interrupts Ports DMA-Kanäle
Festplatten	Hersteller Modell Größe SCSI oder IDE SCSI-ID bzw. die wievielte Platte an welchem Controller
Hauptspeicher	Chipsatz des Controllers Größe in MB
CD-ROM-Laufwerk	siehe Festplatten
SCSI-Adapter	Hersteller Modell
Netzwerk- oder ISDN-Karte	Hersteller Modell zukünftige IP-Adresse falls möglich: Chipsatz
Maus	seriell oder PS/2 Protokoll (mman (MouseMan) oder ms (Microsoft) für serielle Mäuse, ps2 für normale PS/2-Mäuse, imps2 für PS/2-Mäuse mit Rad) ggf. serielle Schnittstelle, an die die Maus angeschlossen ist
Netzwerk	Rechnername Domainnamen von lokalem und externem Netz IP-Adressen der zuständigen DNS-Server

Neben der Papierdokumentation, die manchmal nicht so umfassend ist, wie man sich das wünschen würde, kann man die Informationen teilweise auch aus dem laufenden System entnehmen. Dies gilt insbesondere, wenn der installierte Kernel des Herstellers die Hardware unterstützt. Es kann aus diesem Grund auch sinnvoll sein, ein Floppy-Linux oder eine Live-CD zu starten. Manche Varianten haben eine recht gute Hardware-Erkennung und unterstützen eine Vielzahl von Komponenten.

Die folgenden Stellen lohnen einen näheren Blick:

Bootmeldungen In den Bootmeldungen kann man sehen, welche Hardware von den Treibern gefunden wurde. Wenn Sie Ihnen zu schnell vorbeihuschen, sollten Sie den folgenden Befehl verwenden:

```
# dmesg | less
```

Geladene Module Auch die Namen der Module, die mit `lsmod` angezeigt werden, können im Einzelfall bei der Ermittlung der Identität einer Hardware-Komponente helfen.

lspci Dieser Befehl listet die installierten PCI-Karten mit den von ihnen reservierten Ressourcen auf.

/proc-Dateisystem Unter `/proc` finden sich viele Dateien, deren Inhalt angibt, welche Hardware welche Ressourcen belegt. Die Dateien variieren je nach Kernelversion, aber die folgenden sind häufig anzutreffen:

- `/proc/cpuinfo`
- `/proc/dma`
- `/proc/interrupts`
- `/proc/iomem`
- `/proc/ioports`
- `/proc/pci`
- `/proc/cpuinfo`
- `/proc/ide/<Controllertreiber>`
- `/proc/scsi/scsi`

Partitionen und ihre Mountpoints festlegen

Es gibt eine Reihe von Gründen, die Festplatte in mehrere Partitionen aufzuteilen. Bis vor kurzem brauchte LiLo einen Bereich für seine Dateien, der sich auf den ersten 1024 Zylindern der ersten Festplatte befinden mußte. Das liegt daran, daß der Boot Loader LiLo¹ das BIOS für den Zugriff auf diese Dateien benutzt. BIOSe vor 1998 konnten aber nur auf die ersten 1024 Zylinder zugreifen. Dann wurde *Logical Block Addressing* eingeführt, das diese Hürde überwand. Seit Version 21-3 vom 24.2.2000 wird dies auch von LiLo unterstützt, wenn er dahingehend konfiguriert wurde.

Wenn Ihr Rechner ein altes BIOS oder Ihr Linux einen alten LiLo verwendet, ist es sinnvoll, als erstes eine Partition von z. B. 6 MB einzurichten, die dann auf `/boot` gemountet wird.²

1 Der Boot Loader ist das Programm, das beim Starten des Rechners das eigentliche Betriebssystem lädt. Er ist normalerweise im ersten Sektor einer Diskette oder Festplatte untergebracht. Er selbst wird vom BIOS, einem fest im Rechner eingebauten Programm gestartet. Der Boot Loader erlaubt es z. B. beim Starten des Rechners auszuwählen, ob man gerade Windows oder Linux starten will.

2 Nötig sind etwa 1 bis 2 MB, aber es ist immer besser, etwas Platz für zusätzliche Kernel zu lassen, um auf eine ältere Version zurückgreifen zu können, falls man neue Einstellungen probiert hat und nun feststellen muß, daß das System in der neuen Konfiguration nicht mehr bootet. Falls man tatsächlich mit jedem MB rechnen muß, ist die Platte vermutlich sowieso zu klein, als daß man eine eigene Partition für `/boot` bräuchte.

Ferner empfiehlt es sich, eine Partition als Swap-Partition einzurichten, die nicht gemountet wird. Sie entspricht der Auslagerungsdatei unter Windows und sollte etwa so groß wie der zur Verfügung stehende Hauptspeicher sein. Hat man weniger als 128 MB oder verwendet man einen 2.4er Kernel vor Version 2.4.10, sollte man das Doppelte rechnen³.

Weiterhin wird eine Partition für das eigentliche System und die darauf installierten Anwendungen benötigt, die auf »/« gemountet werden. Hierbei kann es sich um den verbleibenden Rest der Festplatte handeln, es sollten aber mindestens 1,5 GB zur Verfügung stehen.⁴

Man könnte an diesem Punkt abbrechen. Tatsächlich hätte man damit in etwa die Partitionierung erreicht, die das SuSE-Linux wählt, wenn man ihm bei der Partitionierung freie Hand läßt.

Für eine Firewall ist es aber sinnvoll, die Einrichtung weiterer Partitionen in Betracht zu ziehen. Liegen alle interessanten Verzeichnisse auf derselben Partition, so bedeutet dies, daß das ganze Dateisystem gefüllt werden kann, indem man nur genug temporäre Daten speichert. Es gibt hinreichend Tricks, dies zu erreichen. Steht nun aber kein Speicherplatz mehr zur Verfügung, so ist es auch nicht mehr möglich, Logdateien zu schreiben. Eventuell folgende Angriffe bleiben unprotokolliert. Aus diesem Grund erscheint es sinnvoll, für */var/log* eine eigene Partition einzurichten, die ausreichend groß bemessen ist. Auch */var* selbst sollte eine eigene Partition erhalten, wenn auf dem System Dienste installiert sind, die regelmäßig größere temporäre Dateien schreiben. So muß z. B. der WWW-Proxy Squid Webseiten zwischenspeichern, was er standardmäßig in */var/squid/cache* tut.

Auf einem Server, auf dem sich normale Benutzer anmelden dürfen, wäre es darüber hinaus auch sinnvoll, */home* und */tmp* auf eigene Partitionen zu legen, damit normale Benutzer nicht versehentlich den Platz für Log- oder Spooldateien beschränken.

³ Hierbei handelt es sich nur um eine Faustregel. Die Größe der Auslagerungsdatei bestimmt den zur Verfügung stehenden virtuellen Speicher. Bei einem 2.2er Kernel oder einem 2.4er Kernel, dessen Versionsnummer größer als 2.4.9 ist, gilt

$$\text{virtueller Speicher} = \text{RAM} + \text{Swap},$$

bei einem 2.4er Kernel bis zur Version 2.4.9 dagegen

$$\text{virtueller Speicher} = \max(\text{RAM}, \text{Swap})$$

Der virtuelle Speicher sollte insgesamt so groß sein, daß er alle zu erwartenden Anfragen nach Hauptspeicher erfüllen kann. Wenn man also sicher ist, daß niemals mehr als 256 MB Hauptspeicher benötigt werden und diese schon in Form von RAM vorliegen, so kann man durchaus überlegen, ob man wirklich eine 512-MB-Partition opfern will. Ganz auf virtuellen Speicher zu verzichten, empfiehlt sich allerdings nicht, da noch so genau errechnete Werte prinzipiell immer überschritten werden können. Es wäre allerdings ebenfalls ein Fehler, ins andere Extrem zu verfallen und auf den Kauf von RAM zu verzichten und statt dessen mehr virtuellen Speicher einzurichten. Dies wird zu nicht akzeptablen Performance-Einbrüchen führen. Im Normalbetrieb sollte der virtuelle Speicher so gut wie nicht genutzt werden. Er dient lediglich als Reserve für Hochlast-Zeiten.

⁴ Debian käme mit deutlich weniger aus, aber SuSE 9.3 braucht selbst in einer Minimalinstallation mehr als 1 GB.

Für eine Firewall mit einer 6-GB-IDE-Festplatte und 64 MB Hauptspeicher könnte sich unter Beachtung der obigen Regeln eine Aufteilung ergeben, wie sie in Tabelle 7-2 dargestellt ist. Dort ist rechts die Partition mit ihrer Device-Bezeichnung angegeben, dann das Verzeichnis, auf das sie gemountet werden soll, und das Dateisystem der Partition. Die letzten beiden Spalten bedürfen vielleicht einer Erklärung. Unter Vorgabe habe ich angegeben, was ich dem Installationsprogramm vorgegeben habe. +6M bedeutet hier z. B. soviel wie »Lege eine Partition von 6 MB an«. Unter Blocks ist angegeben, wie viele Blocks dabei wirklich auf der Platte belegt wurden. Ein Block hat unter Linux eine Größe von 1024 Bytes (andere Unixes benutzen z. T. 512 Bytes). Wir sehen also, daß die Aufforderung, eine Partition von 6 MB zu erstellen, tatsächlich eine Partition von 8 MB geschaffen hat. Dies liegt daran, daß immer nur ganze Zylinder auf der Platte reserviert werden können.

Tabelle 7-2: Beispiel für eine Festplattenpartitionierung

Device	Mountpoint	Dateisystem	Blocks	Vorgabe
/dev/hda1	/boot	ext2fs	8001	+6M
/dev/hda2		swap	128520	+125M
/dev/hda3	/	ext2fs	2104483	+2028M
/dev/hda4	erweiterte Partition, die die restliche Platte umfaßt			
/dev/hda5	/var/log	ext2fs	2104483	+2048M
/dev/hda6	/var	ext2fs	1951897	der Rest

Ein weiterer Punkt, der bei der späteren Einrichtung des Systems zu beachten ist, ist, daß */var* vor */var/log* gemountet wird. D. h., der Eintrag für */var* muß vor dem für */var/log* in der Datei */etc/fstab* stehen.