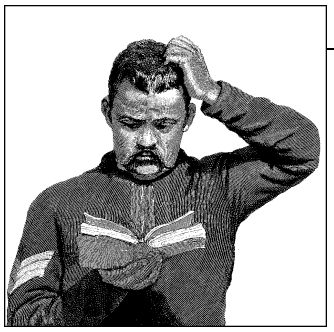

KAPITEL 2

Was ist eine Firewall?

Eine gängige Maßnahme, um sich vor den Gefahren des Internets zu schützen, besteht darin, zwischen die Rechner im eigenen Netz und das Internet eine Firewall zu installieren. Diese kann man sich wie das Burgtor einer mittelalterlichen Stadt vorstellen. Es ist der einzige Zugang zur Stadt, die ansonsten von allen Seiten durch hohe Mauern geschützt ist. Um in die Stadt gelangen zu können, muß ein Besucher an Wachen vorbei, die ihn nach seinen Papieren befragen. Erst wenn er ihnen Rede und Antwort gestanden hat, darf er die Stadt betreten.

Eine Firewall schützt in ähnlicher Weise den Zugang zum lokalen Netz. Jeglicher Verkehr muß sie passieren und wird von ihr untersucht. Damit kann ein Großteil der möglichen Angriffe schon abgefangen werden, bevor sie ihr Ziel erreichen. Allerdings ist dieser Schutz nicht vollkommen. Gerade der Fall der Stadt Troja hat eindrucksvoll bewiesen, welche Folgen es hat, wenn bei der Untersuchung des hereinkommenden Verkehrs eine falsche Entscheidung getroffen wird.

Im folgenden werden wir sehen, wie uns eine Firewall beim Schutz unserer Rechner helfen kann und was mit anderen Mitteln erreicht werden muß. Darüber hinaus werden wir uns an drei exemplarischen Fällen ansehen, wie unterschiedliche Anwendungssituationen zu unterschiedlichen Firewall-Realisierungen führen.

Was eine Firewall kann

Wie ein Stadttor alle Angriffe auf einen stark gesicherten Punkt bündelt, an dem man den Großteil seiner Kräfte konzentriert, so stellt auch die Firewall eine Möglichkeit dar, Angriffe an einer definierten Stelle abzufangen.

Besitzt man nur einen Rechner, mit dem man Dienste im Internet nutzt, so kommt man nicht umhin, ihn so zu konfigurieren, daß er keine Schwachstellen aufweist, die ein Angreifer ausnutzen kann, um unberechtigt Zugang zu ihm zu erlangen. Besitzt man aber hundert Rechner, so wird es schwierig, alle immer auf dem neuesten Stand zu halten, Patches gegen Sicherheitslücken einzuspielen und immer darauf zu achten, daß keine unsicheren Dienste auf ihnen installiert sind. Ehe man es sich versieht, hat schon ein

Benutzer eine Freigabe auf Laufwerk C erstellt, deren Paßwort nicht vorhanden oder leicht zu erraten ist. Oder er richtet sich eine .rhosts-Datei ein, die den Zugang ohne Paßwort von jedem Rechner im Internet erlaubt. Werden die Rechner gar von verschiedenen Personen administriert, so kann man darauf wetten, daß die einzelnen Rechner unterschiedlich sicher konfiguriert sind.

In so einem Fall kann man die Sicherheit des Systems verbessern, indem man an zentraler Stelle dafür sorgt, daß Angriffe abgefangen werden, bevor sie ein möglicherweise gefährdetes System erreichen. So reduziert man die Angriffspunkte von 100 auf einen und kann für dieses System eine hieb- und stichfeste Konfiguration entwickeln.

Eine Firewall untersucht den Datenverkehr und läßt nur die Netzzugriffe zu, die vorher definierten Regeln genügen. So ist es z. B. üblich, Anfragen von Rechnern im lokalen Netz an Rechner im Internet zu erlauben, nicht aber umgekehrt. D. h., wenn ein Rechner im lokalen Netz z. B. eine Webseite von einem Server im Internet anfordert, so wird die Antwort (die Webseite) von der Firewall entgegengenommen und in das lokale Netz weitergeleitet. Pakete von Rechnern im Internet werden aber nicht durchgelassen, wenn sie nicht zuvor explizit von einem Rechner im lokalen Netz angefordert wurden. Schon diese Regel verhindert, daß ein Angreifer auf möglicherweise schlecht gesicherte Dienste von Rechnern im lokalen Netz zugreift.

Auch kann man definieren, daß ein Benutzer auf bestimmte Dienste zugreifen darf, auf andere aber nicht. So kann man z. B. verhindern, daß er aus Unkenntnis Protokolle benutzt, bei denen das Paßwort im Klartext übertragen wird.

Wird auf Webserver zugegriffen, bieten einige Firewalls auch die Möglichkeit, unerwünschte Inhalte zu filtern. So kann man z. B. das Laden von Werbebannern unterdrücken, aktive Inhalte aus Webseiten beim Herunterladen entfernen und das Senden von Cookies verhindern.

Kommt es zu verdächtigen Zugriffen auf die eigenen Rechner, so bietet eine Firewall die Möglichkeit, diese zu protokollieren und für eine spätere Auswertung zu speichern. Ohne eine Firewall könnte dies nur auf den Zielsystemen geschehen und würde bedeuten, entweder auf jedem Rechner eigene Auswertungen durchzuführen oder eine zusätzliche Software zu installieren, die die Systemprotokolle aller Rechner an einer zentralen Stelle zusammenführt. Hinzu kommt, daß nicht alle Betriebssysteme die gleichen Protokollierungsmöglichkeiten besitzen. Auch sind die einzelnen Protokollierungsmechanismen untereinander nicht immer kompatibel.

Auch zur Verringerung der Netzlast kann eine Firewall eingesetzt werden. Laufen alle Zugriffe über einen zentralen Rechner, so bietet es sich an, an dieser Stelle einen Mechanismus zu installieren, der es erlaubt, häufig heruntergeladene Inhalte zwischenzuspeichern (*Cachender Proxy*). Fordern dann mehrere Benutzer z. B. dieselbe Webseite an, so braucht diese nur für den ersten von ihnen tatsächlich aus dem Internet heruntergeladen zu werden. Alle weiteren Nachfragen werden aus dem Zwischenspeicher bedient. Dies macht den Zugriff zwar nicht zwangsläufig sicherer, kann aber die Netzlast um 40 bis 60 Prozent verringern.

Schließlich kann man auch noch kompliziertere Strukturen aufsetzen. Wie mittelalterliche Burgen mehrere Burghöfe besaßen, die ein Angreifer überwinden mußte, bevor er vor dem eigentlichen Wohnhaus des Hausherrn anlangte, so kann auch eine Firewall-Architektur aus mehreren Netzen mit unterschiedlichem Schutzbedarf bestehen. So sind Server, die aus dem Internet zugreifbar sein sollen, einem deutlich höheren Risiko durch Angriffe ausgesetzt und könnten bei einer Kompromittierung als Ausgangsbasis für weitere Angriffe gegen das lokale Netz genutzt werden. Bringt man diese aber in einem eigenen Netz unter, einer so genannten *Demilitarized Zone* oder kurz *DMZ*, so verhindert man, daß ein erfolgreicher Angriff auf einen öffentlichen Server dem Angreifer den Zugriff auf die Arbeitsplatzrechner erleichtert (siehe Abbildung 2-1).

Was eine Firewall nicht kann

Obwohl eine Firewall ein wichtiges Werkzeug ist, um die Sicherheit Ihrer Rechner zu erhöhen, so ist sie doch nicht das eine Werkzeug, das ganz allein alle Ihre Probleme beseitigt. Eine Firewall ist nur ein Baustein in einer ganzen Reihe von technischen und organisatorischen Maßnahmen, die nötig sind, wenn Sie einen brauchbaren Schutz Ihrer Systeme erreichen wollen.[1]

Eine Firewall wird Sie z. B. nicht vor Angriffen schützen, die aus dem eigenen Netz heraus ausgeführt werden. Eine gängige Faustregel besagt, daß 80 Prozent aller computergestützten Delikte von Insidern begangen werden. Wenn sich Ihre eigenen Anwender dazu entschließen, Angriffe auf Ihre Server durchzuführen, Daten zu löschen oder fremde Dateien auszuspionieren, so ist selbst die beste Firewall absolut wirkungslos.

Dazu ist noch nicht einmal böser Wille nötig. Es reicht schon, daß einer Ihrer Anwender Software herunterlädt oder von zu Hause mitbringt und auf einem der Rechner installiert. War diese mit Viren verseucht oder handelte es sich um einen Trojaner, so kann er unwissentlich großen Schaden anrichten. Auch ein privater Laptop ohne installierten Virenschutz, der von zu Hause mitgebracht wird, kann zu einer Verseuchung des ganzen Netzes führen.

Auch kann eine Firewall keinen Netzverkehr kontrollieren, der nicht über sie geleitet wird. In größeren Netzen kann es durchaus schon einmal vorkommen, daß Angestellte, die mit dem angebotenen Internet-Zugang unzufrieden sind, ein eigenes Modem an ihren Computer anschließen. Damit umgehen sie natürlich alle Schutzmaßnahmen, die in der Firewall realisiert werden.

Um solchen Risiken zu begegnen, sind technische Maßnahmen weitgehend wirkungslos. Hier hilft einzig, organisatorische Regeln, *Policies* genannt, aufzustellen, die den Umgang des Benutzers mit den von Ihnen betreuten Systemen regeln. Darüber hinaus ist es auch nötig, Aufklärungskampagnen durchzuführen, die diese Regeln allgemein bekannt machen, und ihnen im schlimmsten Fall auch durch disziplinarische Maßnahmen Geltung zu verschaffen.

1 Eine hundertprozentige Sicherheit werden Sie nie erreichen.

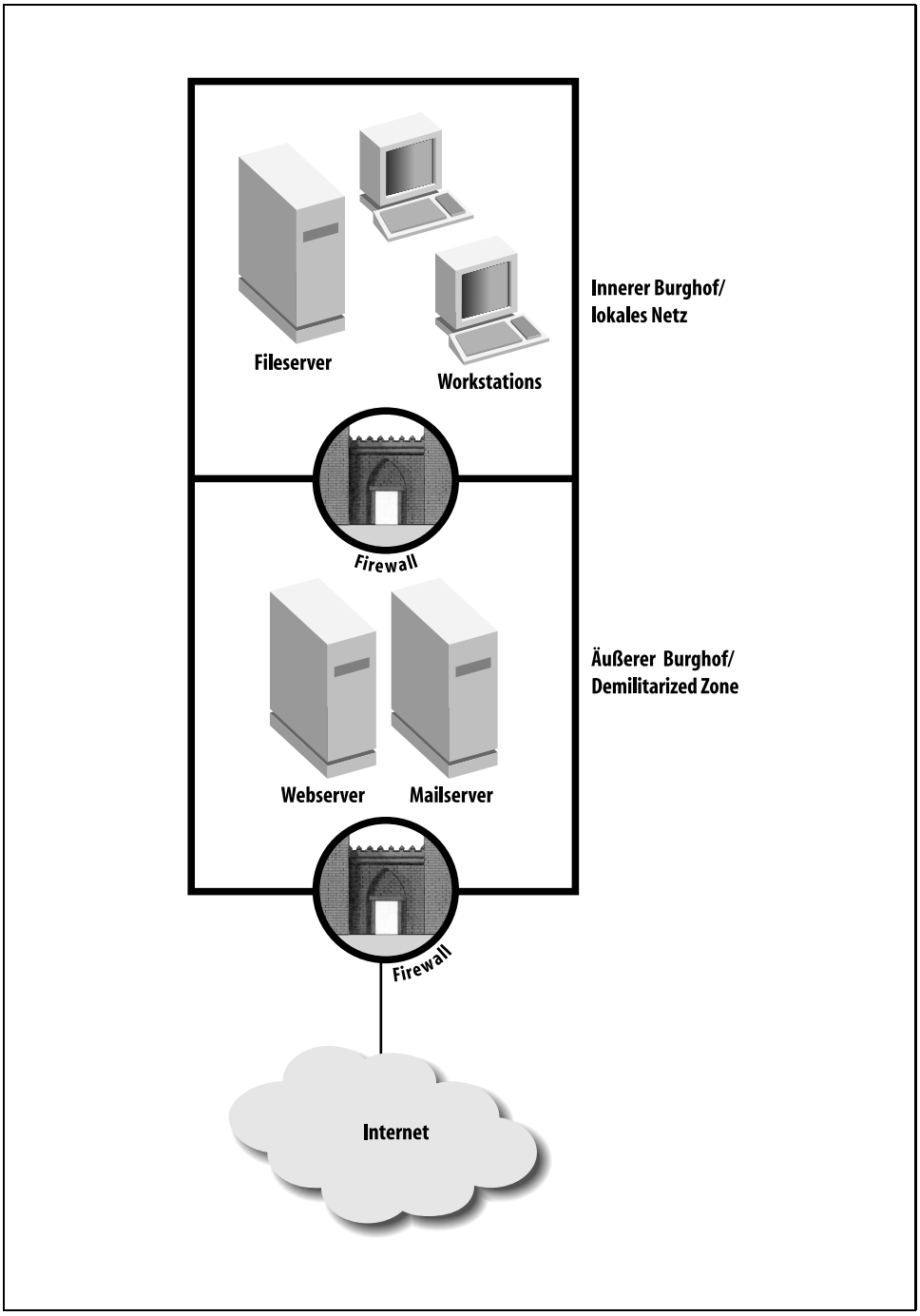

Abbildung 2-1: Demilitarized Zone (DMZ)

Bieten Sie Dienste wie Web- und Mailserver an, auf die aus dem Internet zugegriffen werden kann, so besteht darüber hinaus das Risiko, daß die Programme, die diese Dienste realisieren, fehlerhaft programmiert sind. Der Hauptteil der Schutzwirkung einer Firewall basiert ja darauf, den Zugriff auf Dienste zu verhindern. Hier aber ist genau dies erwünscht. Wenn also ein Zugriff auf einen Webserver dazu führt, daß der gesamte Rechner, auf dem der Dienst läuft, danach unter der Kontrolle eines Angreifers steht, so ist dieser Vorgang für eine Firewall in der Regel nicht von einem normalen Lesen von Webseiten zu unterscheiden.

Die Firewall kann hier nur dagegen schützen, daß auf Dienste zugegriffen wird, die nicht öffentlich zugänglich sein sollen. Haben wir z. B. einen Webserver, der zusätzlich noch ein Fileserver ist, so kann eine Firewall verhindern, daß aus dem Internet auf die freigegebenen Dateien zugegriffen wird, sie kann aber nicht vor allen Angriffen auf den Webserver schützen. Dies ist der Grund, warum die öffentlichen Server oft in einem eigenen Netz (Demilitarized Zone) zwar durch eine Firewall geschützt werden, das lokale Netz aber noch einmal durch eine weitere Firewall abgetrennt ist. Man geht davon aus, daß eine Kompromittierung der Server grundsätzlich eine realistische Möglichkeit darstellt, weswegen man die Rechner im lokalen Netz nicht nur vor dem Internet, sondern auch vor den eigenen öffentlichen Servern schützen muß.

Schließlich ist eine Firewall auch kein Schutz gegen Angriffe, die darauf abzielen, Ihren Zugang zum Internet zu unterbinden. Wenn ein Angreifer beginnt, Ihnen eine Flut sinnloser Datenpakete zu schicken, so wird irgendwann der Punkt erreicht sein, wo Ihre Datenleitung so mit den Paketen des Angreifers überfüllt ist, daß Ihre eigenen Anfragen an Server im Internet darin einfach verlorengehen. Das einzige, was Ihre Firewall hier für Sie leisten kann, ist zu verhindern, daß die Pakete in Ihr lokales Netz gelangen und auch dort die Kommunikation stören.

Trotz alledem ist eine Firewall eine sinnvolle Maßnahme, die die Gefahr von Angriffen aus dem Internet deutlich verringern kann. Man muß sich aber immer im klaren sein, daß sie nur ein Baustein in einem ganzen Gebäude von Maßnahmen ist, um die Sicherheit Ihres Systems zu gewährleisten.

Typische Einsatzszenarien für Firewalls

Firewalls existieren in unterschiedlichen Größen und Ausbaustufen. Je nach Anzahl der Benutzer, Schutzbedürfnis und Art der Anwendung wird man zu unterschiedlichen Ansätzen kommen, die sich in der eingesetzten Hard- und Software gravierend unterscheiden. Um Ihnen zu helfen herauszufinden, wieviel Firewall Sie wirklich brauchen, beschreibe ich im folgenden drei Szenarios und führe aus, wie die jeweils vorhandene Ausgangslage die Realisierung der Firewall bestimmt hat.

Der Privathaushalt

Beginnen wir mit Heinz. Er wohnt in einem Haus im Speckgürtel von Hamburg zusammen mit seinen Eltern und seinem jüngeren Bruder. In seiner Familie ist er derjenige

mit der meisten Computererfahrung. Zwar besitzt auch sein Bruder zwei Computer, und auch sein Vater benutzt einen alten Rechner von Heinz zur Textverarbeitung, aber die beiden haben es nie für nötig befunden, mehr zu lernen, als die von ihnen benutzten Programme zu bedienen. Wann immer es ein Problem gab, war schließlich Heinz da, um es zu beheben.

Nun hat Heinz sich vor einiger Zeit ein Modem besorgt und begonnen, im Internet zu surfen. Nach einer Weile bekommen die anderen Familienmitglieder Lust, dies auch einmal zu versuchen. Um nicht zwei weitere Telefonanschlüsse und Modems kaufen zu müssen und auch seine Familie nicht völlig ungeschützt dem Internet auszusetzen, beschließt Heinz, einen alten Rechner, den er schon eine Weile nicht mehr benutzt, auszumotten und so umzurüsten, daß er für die Arbeitsplatzrechner den Zugang zum Internet bereitstellt.

Die erste Frage, die Heinz sich stellt, ist, ob er eine normale Linux-Distribution (SuSE, Debian, ...) oder lieber ein spezielles Mini-Linux verwenden sollte, das von einer Diskette gestartet wird. Ein Disketten-Linux kommt prinzipiell ganz ohne Festplatte aus. Installiert man es trotzdem auf der Festplatte, so wird man nur wenige MB Speicherplatz benötigen. Eine Standarddistribution braucht im Gegensatz dazu in der Regel schon in der Minimalinstallation 500 bis 1500 MB.

Auch die Anforderungen an Prozessor und Hauptspeicher sind moderat. Selbst ein alter 486er mit 16 MB RAM wird mit einem Disketten-Linux noch klaglos seinen Dienst tun, während bei der Installation eines normalen Linux u. U. schon das Installationsprogramm aus Mangel an Hauptspeicher abstürzt.

Schließlich beschränkt sich die Konfiguration eines Disketten-Linux oft auf das Editieren einer Konfigurationsdatei, während das Aufsetzen einer Firewall auf Basis einer Standarddistribution ein bis drei Tage dauern kann.

Natürlich hat eine Standarddistribution auch Vorteile. Sie bietet eine Vielzahl zusätzlicher Programme, die es erlauben, z. B. Werbebanner, aktive Inhalte und Cookies zu filtern. Nach kurzem Nachdenken kommt Heinz aber zu dem Schluß, daß er diese zusätzlichen Eigenschaften nicht benötigt.

Er sucht eine Lösung, die nur dazu dient, drei Rechner über eine Leitung mit dem Internet zu verbinden. Dafür ist ein vollständiges Arbeitssystem übertrieben. Es reicht, wenn seine Firewall ihre eigentliche Aufgabe erfüllt, nämlich die Rechner im lokalen Netz vor dem Internet abzuschirmen und vor Zugriffen von außen zu schützen. Cookies und aktive Inhalte kann er bei Bedarf auch durch eine geeignete Konfiguration der Browser unterdrücken.

Genausowenig macht es Sinn, einen cachenden Proxy zu installieren, der besuchte Webseiten zwischenspeichert, um bei weiteren Anfragen nach derselben Seite Netzzugriffe zu sparen. Ein solches Programm benötigt unverhältnismäßig hohe Ressourcen in Form von Festplattenplatz und Hauptspeicher. Darüber hinaus ist ein Proxy bei einer so kleinen Anzahl von Benutzern praktisch nutzlos, da die Chancen recht hoch sind, daß die drei so unterschiedliche Interessen haben, daß sie kaum einmal zur selben Zeit dieselben Seiten betrachten.

Der Betrieb eines Webservers scheidet für Heinz ebenfalls aus. Dies würde ja zumindest erfordern, eine kontinuierliche Verbindung zum Internet zu unterhalten. Damit hat er keinen Bedarf für eine DMZ.

Schließlich wird Heinz auch keine schriftlichen Policies aufstellen, die regeln, was seine »Kunden« im Internet tun dürfen und was nicht. Er wird sich damit begnügen, seine Verwandten auf die Gefahren und notwendigen Vorsichtsmaßregeln hinzuweisen, bevor er sie das erste Mal ins Internet läßt. Zusätzlich hat er sich schon einmal einen Virenscanner besorgt und auf den Arbeitsplatzrechnern installiert.

Das Studentenwohnheim

Sören studiert Informatik an der Universität Gabelburg[2]. Dort hat er mit seinen Mitbewohnern im Studentenwohnheim eine Netzwerk-AG gegründet, die sich dem Ziel widmet, die Wohnungen aller 200 Kommilitonen zu vernetzen und an das Internet anzuschließen.

Dieses Vorhaben hat eine ganze Weile gebraucht, aber mittlerweile konnte die Universität überzeugt werden, den Studenten den Zugang zum Universitätsnetz und damit zum Internet zu gewähren. Technisch entschloss man sich, die Entfernung von einem Kilometer zwischen dem Wohnheim und dem Campus mittels einer Funkstrecke zu überbrücken. Die dafür nötigen Hardware-Kosten konnten durch Spenden gedeckt werden.

Die Studenten besitzen damit einen direkten Anschluß an das Universitätsnetz. Lediglich die Datenrate ist mit 2 MBit/s etwas geringer als aus lokalen Netzen gewohnt.

Technisch könnte die Basisstation der Funkstrecke wie ein weiterer Rechner an das lokale Netz angeschlossen werden, das die Studenten in ihrer Freizeit im Wohnheim aufgebaut haben. Alle Rechner wären dann automatisch mit dem Internet verbunden. Einige Gründe sprechen aber dagegen. Zum einen war die Universität nicht bereit, den Studenten 200 Netzwerkadressen zuzuteilen. Dies hätte bedeutet, diese Adressen bei einer offiziellen Stelle zu registrieren, was deutliche Kosten verursacht hätte.

Zum anderen vertritt die Universität die Politik, alle ihre Rechner zentral durch das Rechenzentrum administrieren zu lassen. Da die sichere Konfiguration der Rechner dadurch gegeben ist, sieht man keinen Grund, das Universitätsnetz durch eine Firewall gegen das Internet abzuschotten. Für die Rechner der Studenten trifft diese Argumentation so nicht zu. Da jeder Student seine Rechner selbst administriert, ist es kaum wahrscheinlich, daß alle Rechner gleich sicher konfiguriert sind.

Hieraus ergibt sich wie schon bei Heinz, daß ein Rechner benötigt wird, der die Verbindung nach außen herstellt, die tatsächlichen Rechner verbirgt, von denen Zugriffe auf das Internet erfolgen, und unberechtigte Zugriffe aus dem Internet verhindert.

Dies könnte wie schon im Fall von Heinz mit einem Disketten-Linux geschehen. Sören und seine Mitadministratoren entscheiden sich aber dagegen. Ihnen steht ein Pentium II-400 mit 128 MB Hauptspeicher und einer 16-GB-Festplatte als Router zur Verfü-

2 Dieser Name ist frei erfunden. Meines Wissens existiert in Deutschland keine Universität Gabelburg.

gung, womit mehr als genug Ressourcen vorhanden sind, um eine Standarddistribution zu installieren.

Mit 200 Benutzern ist es auch sinnvoll, einen cachenden Proxy zu installieren, der heruntergeladene Webseiten zwischenspeichert, um bei weiteren Anfragen nach derselben Seite Netzzugriffe zu sparen. Auch hat man sich entschlossen, den Kommilitonen optional einen Dienst anzubieten, der Webseiten ohne die darin enthaltenen Werbebanner herunterlädt. Solche Dienste können mit einem Disketten-Linux aber nicht realisiert werden.

Einen eigenen Webserver wird man nicht betreiben. Die Universität bietet ihren Studenten die Möglichkeit, Homepages auf den Servern des Rechenzentrums abzulegen. Die Einrichtung einer DMZ für aus dem Internet zugängliche Server ist damit nicht notwendig.

Schließlich hat die Universität als Provider darauf bestanden, daß eine Benutzerordnung geschaffen wird, die den Umgang der Studenten mit ihrem Netzwerkzugang regelt. Zwar hat man sich darauf geeinigt, daß das Gebäudenetz und die Anbindung an das Uni-Netz von der Netzwerk-AG eigenverantwortlich betrieben wird, es wird aber als unabdingbar angesehen, eine Verpflichtung der Nutzer auf grundlegende Policies durchzuführen. Diese sollen verhindern, daß einige Benutzer durch unverantwortliches Handeln ihre Kommilitonen oder den Ruf der Universität schädigen. Auch ist zu regeln, welche Rechte und Pflichten die Netz-Administratoren besitzen und wie bei Verstößen gegen die Richtlinien vorgegangen wird.

Die genaue Ausarbeitung der Benutzerordnung wird den Studenten überlassen. Bevor aber der endgültige Anschluß an das Universitätsnetz erfolgen kann, muß eine Genehmigung der Benutzerordnung durch die Universität erfolgt sein.

Die Firma

Herr Friedrich ist Netzwerkadministrator der Firma »Euro-Gimmicks«, wo er 40 Bildschirmarbeitsplätze und mehrere Datei- und Druckserver betreut. Gerade hat ihn der Geschäftsführer zu sich bestellt und verkündet, man müsse mit der Zeit gehen und den Mitarbeitern Zugang zum Internet gewähren. Darüber hinaus müsse man sich den Kunden auch über das neue Medium präsentieren. Der Kollege P. vom Verkauf werde deshalb einen Webserver aufsetzen, auf dem die Produkte der Firma präsentiert würden.

Die Beschaffung eines Netzzugangs stellt sich als relativ einfach heraus. Ein lokaler Anbieter macht Herrn Friedrich das Angebot, bei ihm ein DSL-Modem und einen Router aufzustellen. Zusätzlich stellt der Provider Herrn Friedrich noch mehrere registrierte Internet-Adressen zur Verfügung.

Herr Friedrich entscheidet sich nun, einen neuen PC als Firewall anzuschaffen. Ein handelsüblicher Rechner mit einem Pentium 4 mit 1,3 GHz, 256 MB Hauptspeicher und einer 40-GB-Festplatte ist mehr als ausreichend, um darauf nicht nur eine Standarddistribution zu installieren, sondern auch einen cachenden Proxy, der mehrfache Zugriffe auf die gleiche Webseite abfängt und aus einem internen Zwischenspeicher bedient.

Zusätzlich ist vorgesehen, auch eine Software zu installieren, die das Herunterladen von Active X-Controls verhindern soll. Cookies und JavaScript will man dagegen nicht verbieten, da dies dazu führen würde, daß viele Webseiten nicht mehr benutzbar wären.

Was den Webserver angeht, so hat man entschieden, eine zusätzliche Netzwerkkarte in den Rechner einzubauen, an der ein Netzwerkstrang betrieben wird, an den ausschließlich Server angeschlossen werden, auf die aus dem Internet zugegriffen werden soll. Für diese DMZ werden Filterregeln definiert, die den direkten Zugriff auf die Server aus dem Internet erlauben. Ein Zugriff von den Servern der DMZ auf die Rechner im normalen Netz wird dagegen nicht zugelassen. Sie finden das in Abbildung 2-2 dargestellt.

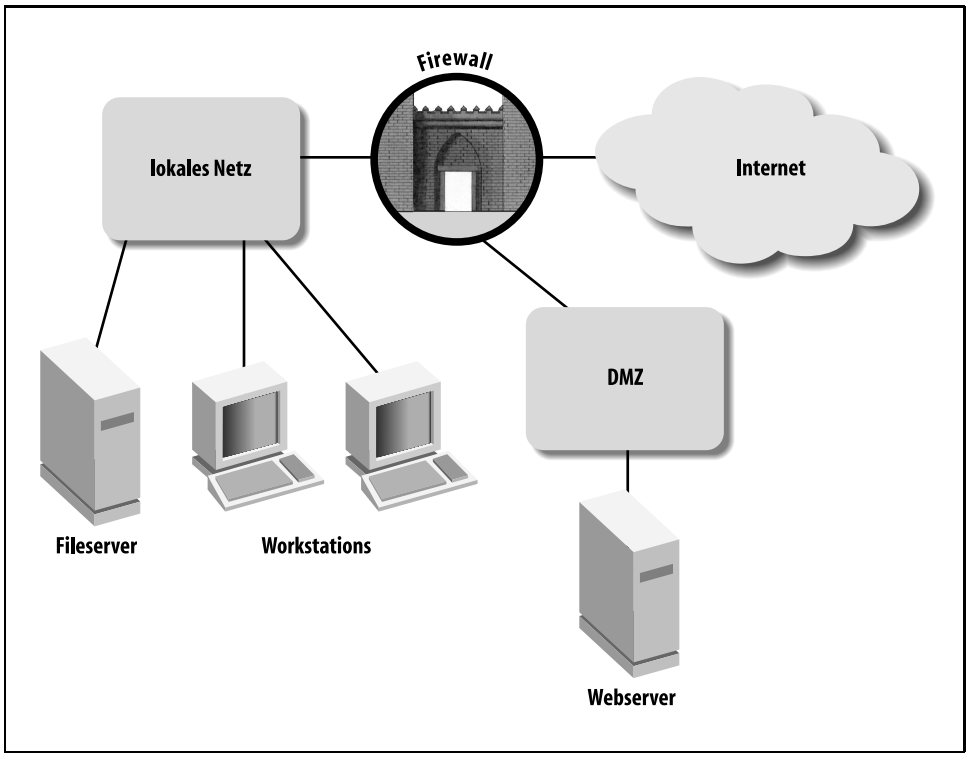

Abbildung 2-2: Die Anbindung eines Firmennetzwerks

Schließlich gilt es noch, sich abzusichern. Herr Friedrich weiß, daß ein neues Medium wie das Internet auch neue Gefahren birgt, die man durch technische Mittel allein nicht in den Griff bekommt. Nur wenn es ihm gelingt, die Benutzer arbeitsrechtlich darauf zu verpflichten, sorgfältig mit den neuen Möglichkeiten umzugehen, kann er vermeiden, daß das Netz kurz nach dem Anschluß an das Internet von Trojanern, Würmern und Raubkopien wimmelt.

Auch gehört es zu seiner Arbeit als Firewall-Administrator, den Zugang zum Internet einzuschränken, um auf diese Weise mögliche Angriffswege zu blockieren. Dies kann im

Einzelfall zu Konflikten mit den Anwendern führen, die ein berechtigtes Interesse daran haben, das Internet möglichst ungehindert zu nutzen. Um getroffene Entscheidungen auch tatsächlich durchzusetzen, müssen organisatorische Regelungen geschaffen werden, die festlegen, auf welche Weise die Entscheidungen für sicherheitskritische Änderungen getroffen werden. Dabei muß dokumentiert sein, daß die getroffenen Sicherheitsregeln eine Managemententscheidung der Geschäftsleitung sind, die von Herrn Friedrich lediglich technisch umgesetzt werden.

Dem Administrator ist klar, daß er ohne diese Rückendeckung damit rechnen muß, regelmäßig von Abteilungsleitern zu Änderungen der Firewall-Konfiguration gezwungen zu werden und dann auch noch Kritik ausgesetzt zu sein, wenn die Firma durch Angriffe aus dem Internet geschädigt wurde.