



Einleitung

In Ihrer Hand halten Sie die zweite Auflage meines Buches über Firewalls unter Linux. Wenn Sie ein lokales Netz mit mehreren Rechnern betreiben, die Zugriff auf das Internet haben, dann möchte ich Ihnen zeigen, wie Sie diese vor Angriffen von außen schützen können.

Das Internet ist ein faszinierender Ort. Was immer man sucht, man wird es finden. Seien es aktuelle Nachrichten, die neuesten wissenschaftlichen Veröffentlichungen oder Fotos von hübschen jungen Mädchen, die bedauerlicherweise zu arm sind, sich richtige Kleidung kaufen zu können und deshalb in Unterwäsche herumlaufen müssen.

Diese Vielfalt hat aber leider auch ihre Schattenseiten. Neben dem normalen Surfer, der nur Informationen sucht, Kontakte knüpft und seine Geschäfte tätigt, gibt es Individuen, die versuchen, das Netz zu weniger freundlichen Zwecken zu nutzen. Sei es, daß sie nach Rechnern suchen, die sie unter ihre Kontrolle bringen können, oder daß sie Würmer schreiben, die sich automatisiert von Rechner zu Rechner verbreiten.

Wenn Sie einen ungeschützten Rechner in das Internet stellen, dann ist er in kürzester Zeit in den Besitz einer Person übergegangen, die ihn dazu benutzen wird, Werbe-E-Mails zu verteilen, andere Rechner durch das Senden von unzähligen Netzwerkpaketen lahmzulegen oder auf ihm einen Webserver mit gefälschten Seiten von Banken oder Internet-Providern zu betreiben, um ahnungslosen Opfern ihre Kreditkartendaten zu entlocken.

Es bleibt uns also nichts übrig, als Gegenmaßnahmen zu ergreifen. Geht es nur um einen einzelnen PC, so besteht eine sinnvolle Lösung darin, Antiviren-Software, Dialerschutz-Programme und eine Personal Firewall zu installieren. Darüber hinaus sollte man sicherstellen, daß für diese Software sowie für alle anderen auf diesem Rechner installierten Programme regelmäßig Updates eingespielt werden.

Sind Sie aber für mehr als einen Rechner verantwortlich, so ist es sinnvoll, zusätzlich weitere Maßnahmen zu treffen. Indem Sie einen Rechner zwischen Ihr Netz und das Internet schalten, haben Sie eine zentrale Stelle, an der Sie den kompletten Netzwerkverkehr zwischen Ihren Rechnern und dem Internet kontrollieren können. Eine gut konfigurierte Firewall erlaubt es Ihnen, die Rechner in Ihrem Netz komplett vor dem Internet zu

verbergen, Zugriffe von außen zu unterbinden und zusätzlich den Netzwerkverkehr zu verringern, indem Sie Webseiten zwischenspeichern, die immer wieder von verschiedenen Rechnern aus heruntergeladen werden.

In diesem Buch werden Sie erfahren, wie so ein Rechner unter Linux aufgesetzt werden kann. Darüber hinaus werden Sie aber auch ein paar Grundlagen kennenlernen, die Ihnen helfen zu verstehen, worin die Bedrohungen bestehen, gegen die Sie sich mit einer Firewall schützen, und gegen welche Bedrohungen auch eine Firewall machtlos ist.

Für wen ist dieses Buch nützlich?

Dieses Buch richtet sich an Personen, die über generelle Erfahrungen mit Computern und Grundkenntnisse in Linux verfügen. Als Leser dieses Buches sollten Sie daher schon einmal ein Linux administriert haben, sich auf der Kommandozeile auskennen und auch in der Lage sein, Shellskripte zu verstehen und anzuwenden. Auch gehe ich davon aus, daß Sie sich in der Verzeichnishierarchie eines normalen Linux zurechtfinden und wissen, wie Benutzer und Paßwörter unter Linux verwaltet werden.

Im Mittelpunkt dieses Buches stehen kleinere und mittlere Firewallinstallationen. Das Buch beschreibt, wie man mehrere Rechner absichert, indem man an ihrem Zugang zum Internet einen zusätzlichen PC postiert, der alle Zugriffe kontrolliert und gegebenenfalls verhindert.

Dabei gehen die hier vorgestellten Szenarien davon aus, daß mehrere Arbeitsplatzrechner und vielleicht ein oder mehrere Webserver an das Internet angeschlossen werden sollen. Ferner wird vorausgesetzt, daß keiner der an das Internet angeschlossenen Server eine Verbindung zu den Arbeitsplatzrechnern aufmachen muß.

Es wird nicht beschrieben, wie man einen einzelnen Arbeitsplatzrechner zum sicheren Surfen konfiguriert oder darauf eine Personal Firewall einrichtet. Auch der Betrieb komplexer E-Commerce-Applikationen liegt außerhalb des Bereiches, den dieses Buch abdeckt. Wenn Sie also z. B. ein System aufbauen wollen, bei dem ein Webserver Bestellungen entgegennimmt, die dann an Versand, Produktions- und Lagersysteme im lokalen Netz weitergegeben werden, so werden Sie in diesem Buch keine Lösung finden.

Zwar unterscheidet sich die Lösung, die Sie brauchen, nur in einigen Firewallregeln von den hier vorgestellten, aber es gibt viele Aspekte, die ich hier nicht abdecken kann. Wenn Sie den Zugriff auf Server im lokalen Netz erlauben, so müssen Sie vorher sicherstellen, daß dieser Zugriff nicht dazu genutzt werden kann, den Server zu kompromittieren. Andernfalls verschaffen Sie dem Angreifer einen direkten Zugang zu den wichtigsten Systemen in Ihrem Netz. Einem solchen Projekt sollte eine grundlegende sicherheitstechnische Untersuchung der benutzten Protokolle, der übertragenen Daten und der verwendeten Software vorausgehen. Dies alles zu beschreiben würde den Rahmen des Buches aber sprengen.

Für welches Linux wurde dieses Buch geschrieben?

Wenn man ein Buch über Linux schreibt, muß man sich auch darüber klarwerden, welche Distribution man beschreibt. Man kann es sich einfach machen und sagen: »Linux ist Linux«. Dabei übersieht man allerdings, daß die einzelnen Distributionen sich deutlich unterscheiden. Jede Distribution verwendet eigene Werkzeuge zur Systemkonfiguration, wichtige Systemdateien liegen in verschiedenen Verzeichnissen, und auch der Umfang der mitgelieferten Software variiert zwischen einer CD und zwei DVDs.

Wenn man also ehrlich ist, bleiben einem nur zwei Möglichkeiten. Man kann explizit sagen, auf welche Version man sich bezieht, oder einen Minimalstandard annehmen und jegliche darüber hinausgehende Software manuell installieren oder selbst schreiben.

In diesem Buch habe ich einen Mittelweg gewählt. Obwohl ich hauptsächlich SuSE einsetze, habe ich meine Anleitungen auch unter Debian nachvollzogen und die Ergebnisse ebenfalls beschrieben. Darüber hinaus habe ich nach Möglichkeit darauf verzichtet, spezielle Werkzeuge einer Distribution einzusetzen, wenn das gleiche Ziel mit vertretbarem Aufwand auch mit allgemein gültigen Methoden erreichbar war.

Gegenwärtig beschreibt das Buch SuSE 9.3 und Debian 3.1.

Die zweite Auflage

Falls Sie sich die erste Auflage dieses Buches gekauft haben, dann fragen Sie sich jetzt sicherlich, weswegen Sie nun nach zwei Jahren schon wieder Geld für die zweite Auflage ausgeben sollen. Lassen Sie mich daher kurz erzählen, was sich in der Zwischenzeit getan hat.

Natürlich hat sich die Technik weiterentwickelt, und die beschriebene Software ist in neuen Versionen erschienen. Statt SuSE 8.0 ist 9.3 aktuell, Debian hat es immerhin geschafft, Version 3.0 (»Woody«) durch 3.1 (»Sarge«) abzulösen. Auch der Linux-Kernel selbst ist mit 2.6 in einer neuen Version herausgekommen.

Aber ich habe nicht nur die bestehenden Beschreibungen aktualisiert, es sind auch neue hinzugekommen. So ist mit dem Privoxy ein filternder Webproxy herausgekommen, der bisher unbekannte Freiheitsgrade in der Filterung von Werbung erlaubt.

SuSE hat mit dem `ftp-proxy` einen Proxy für FTP herausgebracht, der nicht nur dazu eingesetzt werden kann, den Zugriff der Klienten im LAN auf das Internet zu sichern. Vielmehr kann er auch dazu genutzt werden, FTP-Server in einer DMZ zu schützen. Dazu kam man unter anderem definieren, welche Befehle überhaupt an den FTP-Server gestellt werden dürfen.

Auch der Checksummer Tripwire hat mit AIDE Konkurrenz bekommen. Der Herausforderer kann zwar seine Datenbanken nicht verschlüsseln, dafür ist es aber durchaus möglich, das Programm selber und seine Datenbank auf eine CD zu brennen und damit vor jeglicher Veränderung zu schützen.

Um das System noch sicherer zu gestalten, werden die meisten Netzwerkdienste jetzt in einem chroot-Käfig betrieben. Wenn Sie `syslog-ng` verwenden, dann gilt dies sogar für den Systemprotokolldienst.

Apropos `syslog-ng`. Der Wechsel von SuSE vom `syslogd` auf `syslog-ng` und von LiLo auf Grub wurde ebenfalls berücksichtigt.

Schließlich ist auch noch ein neuer Abschnitt hinzugekommen, in dem die Logrotation mit `logrotate` beschrieben wird.

Eine Reihe von Programmen mußte ich allerdings auch aufgeben. Prominentestes Beispiel ist hierbei Red Hat Linux. Kurz nach Erscheinen der ersten Auflage beschloß man, keine Software unter dem Namen Red Hat mehr an Privatanwender zu verkaufen. Statt dessen wurde ein neues Projekt namens Fedora aus der Taufe gehoben, das zusammen mit den Entwicklern der Linux-Gemeinschaft weiterentwickelt werden sollte.

Ich habe mir seinerzeit Fedora Core 1 angesehen, und mir drängte sich der Eindruck auf, daß die Zielgruppe für diese Distribution in erster Linie Desktop-Anwender sind. Für diesen Zweck machte die Distribution schon damals einen guten Eindruck. Die grafische Oberfläche war sehr ansprechend gestaltet, und die Installation war recht problemlos. Als ich aber versuchte, meine typische Firewall-Konfiguration darauf einzurichten, stieß ich ziemlich schnell auf Probleme.

Das Wichtigste bestand darin, daß es praktisch nicht möglich war, ein vernünftiges Minimalsystem aufzusetzen, das nur die Programme enthielt, die ich wirklich benötigte. Bei der Installation wurden zuviele Pakete standardmäßig installiert, und es gab kein vernünftiges Werkzeug, mit dem man im Textmodus festlegen kann, welche Software benötigt wird und welche nicht.

Am Ende kam ich zu dem Schluß, daß Fedora als Server-Betriebssystem nicht wirklich geeignet ist und habe darauf verzichtet, es hier zu beschreiben. Red Hat Enterprise Linux steht mir nicht zur Verfügung, weshalb es ebenfalls kein Ersatz ist.

Auch unter den Proxies gab es Ausfälle zu beklagen. Das Firewalling Toolkit ist nach langem schwerem Kampf endgültig verstorben. Auf dem offiziellen Server ist es nicht mehr zu finden. Als ich das letzte Mal suchte, gab es zwar noch einen FTP-Server, auf dem eine Version zu finden war, aber dieser Server war von keiner offiziellen Seite verlinkt.

Noch nicht ganz verstorben ist der Internet Junkbuster. Es sind allerdings seit dem Erscheinen der ersten Auflage dieses Buches keine neuen Versionen herausgekommen. Dies wiegt um so schwerer, als zwischenzeitlich eine ernsthafte Sicherheitslücke entdeckt wurde. Nachdem SuSE und Debian ihn inzwischen nicht mehr mitliefern, kann ich ihn hier auch nicht mehr guten Gewissens empfehlen.

Wie dieses Buch aufgebaut ist

Dieses Buch beginnt mit einem theoretischen Teil, den Kapiteln 1 bis 5. Hier werden erst einmal die technischen Grundlagen erklärt, die für den Aufbau und Betrieb von Firewalls notwendig sind. Anschließend folgt ein Ausflug in die Welt der Mini-Linuxe, die gezielt für den Einsatz als einfache Firewall gedacht sind (Kapitel 6). Schließlich wird im letzten Block, den Kapiteln 7 bis 16, erklärt, wie man ausgehend von einer Standarddistribution eine Firewall von Grund auf neu aufsetzt, testet und wartet.

Im einzelnen finden Sie in diesem Buch die folgenden Kapitel:

Kapitel 1, *Wer braucht eine Firewall?*, beschäftigt sich mit der Frage, welche Gefahren Ihnen durch Angriffe aus dem Internet drohen.

Kapitel 2, *Was ist eine Firewall?*, beschreibt auf einer abstrakten Ebene, was eine Firewall leisten kann und was nicht. Anhand von drei Anwendungsszenarien wird dargestellt, wie unterschiedliche Bedürfnisse zu unterschiedlichen technischen und organisatorischen Lösungen führen.

Kapitel 3, *Netzwerkgrundlagen*, enthält eine kurze Einführung in die Grundlagen der relevanten Netzwerkprotokolle.

Kapitel 4, *Welche Angriffe gibt es?*, gibt einen Überblick über die gängigsten Angriffe, denen Rechner im Internet ausgesetzt sind.

Kapitel 5, *Firewall-Architekturen*, erklärt aus technischer Perspektive die unterschiedlichen Bausteine, aus denen sich eine Firewall zusammensetzt.

Kapitel 6, *Eine Firewall auf einer Floppy*, beschreibt dedizierte Firewall-Distributionen, bei denen die eigentliche Firewall auf eine Diskette paßt. Diese bieten sich insbesondere in Privathaushalten mit wenigen Nutzern an.

Kapitel 7, *Planung einer normalen Installation*, beschreibt die Überlegungen, die man anstellen sollte, bevor man mit der eigentlichen Installation einer Standarddistribution beginnt. Hier sind deutlich mehr Vorüberlegungen nötig als bei einer Floppy-Firewall. Dafür können Sie dann aber auch Funktionalität realisieren, die Sie für einen größeren Benutzerkreis oder für den Betrieb von eigenen Internetservern benötigen.

Kapitel 8, *Installation der Software*, beschreibt die Installation eines Minimal-Linux mit selbst kompiliertem Kernel. Dabei wird insbesondere darauf eingegangen, inwiefern sich die Installation einer Standarddistribution für ein sicherheitskritisches System von der für einen normalen Arbeitsplatzrechner unterscheidet.

In Kapitel 9, *Das System sicher konfigurieren*, sehen wir, wie wir ein System so konfigurieren, daß es auch ohne Firewalling nur minimale Angriffspunkte bietet. Dazu ist es nötig, alle nicht benötigten Netzwerkdienste abzuschalten und die Dateirechte so zu konfigurieren, daß nur die unbedingt nötigen Zugriffe möglich sind.

Kapitel 10, *Das Netzwerk einrichten*, behandelt die Einrichtung des Netzwerkes. Dabei wird auf die Verbindung zum Internet durch Modem, ISDN und DSL und die direkte Verbindung über eine Ethernet-Leitung eingegangen.

Kapitel 11, *Konfiguration der Paketfilter mit ipchains*, beschreibt die Paketfilter-Mechanismen der 2.2er Kernel.

Kapitel 12, *Konfiguration der Paketfilter mit iptables*, beschreibt die Paketfilter-Mechanismen der 2.4er und 2.6er Kernel.

Kapitel 13, *Eine DMZ – Demilitarized Zone*, beschreibt die Einrichtung eines eigenen Netzwerkstrangs zum Betrieb eines Servers, auf den man aus dem Internet zugreifen können soll. Dabei kann es sich z. B. um einen Webserver handeln.

Kapitel 14, *Proxies*, beschreibt die Einrichtung von Netzwerkdiensten, die auf der Firewall Verbindungen der Rechner im LAN entgegennehmen und dann anstelle des Klienten Anfragen an Server im Internet durchführen. Damit ist es möglich, die Anfragen zu protokollieren, das Laden von Werbefrafiken zu unterbinden und bis zu einem gewissen Grad die Weitergabe personenbezogener Daten durch den Browser einzuschränken.

Kapitel 15, *Abnahmetests*, behandelt die Überprüfung, ob die Firewall tatsächlich wie gewünscht funktioniert.

Kapitel 16, *Wie Sorge ich dafür, daß meine Firewall sicher bleibt?*, beschreibt die täglichen Arbeiten, die nötig sind, um zu gewährleisten, daß eventuelle Angriffe erkannt und bekannt gewordene Sicherheitslöcher gestopft werden. Angesprochen wird auch, was Sie tun können, damit die Anwender im lokalen Netz nicht aus Unkenntnis die Sicherheitsmechanismen aushebeln, und wie Sie sicherstellen, daß bei Wartungsarbeiten bekannt ist, wie das System konfiguriert ist.

Kapitel 17, *Vorfallsbehandlung*, geht von der Situation aus, daß ein Linux-Rechner von einem Angreifer kompromittiert wurde. Um die Schilderung etwas farbenfroher zu gestalten, wird dabei allerdings nicht von einer Firewall, sondern von einem FTP-Server ausgegangen. Sie werden sehen, wie man nach einem Einbruch vorgeht, um die Spuren zu sichern, herauszufinden, was eigentlich geschehen ist, und das System schließlich wieder in einen sicheren Zustand zu versetzen.

Anhang A, *Internet-by-Call ohne Anmeldung*, enthält die Angaben zu einigen Internet-Providern, die Ihnen ohne vorherige Anmeldung Zugang zum Internet verschaffen.

Anhang B, *Der vi*, enthält eine Kurzanleitung zum Umgang mit dem Editor vi. Insbesondere wenn man unter einem Rettungssystem arbeitet, führt oft kein Weg an diesem Editor vorbei.

Anhang C, *Copyright-Informationen*, beschreibt die Bedingungen, unter denen die Online-Version dieses Dokumentes vervielfältigt, gedruckt, verteilt und verändert werden darf.

Typographische Konventionen

In diesem Buch werden die folgenden typographischen Konventionen benutzt:

Kursiv

benutzen wir für Datei- und Verzeichnisnamen, E-Mail- und Netzwerk-Adressen sowie zur Hervorhebung von neuen Begriffen, Variablen und für solche Stellen, die der Benutzer durch seine eigenen Texte ersetzen muß

Nichtproportionalschrift

kennzeichnet Befehle, wörtliche Wiedergabe von Bildschirminhalten, UserIDs, GruppenIDs.

KAPITÄLCHEN

weisen auf Menü-Einträge und Schaltflächen hin.

[<Option>]

kennzeichnet optionale Teile eines Befehls.

>,

Bei der interaktiven Eingabe von Befehlen wird ein unterschiedlicher Prompt angezeigt, je nachdem, ob der Benutzer root oder nur ein normaler Anwender ist. Ein »#« gibt an, daß ein Befehl mit root-Rechten ausgeführt werden muß, während »>« darauf hinweist, daß der Befehl besser ohne administrative Rechte aufgerufen werden sollte.

Danksagungen (Acknowledgements)

Ich möchte an dieser Stelle die Gelegenheit nutzen, all jenen zu danken, ohne die es das Buch in dieser Form nicht geben würde. Da wären zuerst meine Eltern, Erika und Eberhardt Lessig. Nicht nur hätte das Buch ohne sie keinen Autor, ich habe auch ihr Haus an den Wochenenden als Testlabor für meine Firewall-Aufbauten genutzt, so daß sie damit leben mußten, wenn ich an den Wochenenden zu Besuch kam und gleich nach oben zu den Computern verschwand, wo ich dann für den Rest des Wochenendes nicht ansprechbar war.

Professor Dr. Klaus Brunnstein weckte mit seinen Vorlesungen zu IT-Sicherheit und Datenschutz nicht nur mein Interesse an dem Thema, er gab uns Studenten auch die Möglichkeit, unsere theoretischen Kenntnisse im Labor des Arbeitsbereiches in die Praxis umzusetzen.

Amon Ott und Karim Senoucci halfen mir dabei, mich in die Firewalladministration unter Linux einzuarbeiten. Zuvor kannte ich Unix-Systeme nur aus der Perspektive eines normalen Benutzers von Solaris-Systemen.

Sven Meinhardt sehe ich immer noch mit einem Hunderterpack Disketten an einer der wenigen Sparc-Stations mit Diskettenlaufwerk sitzen und eine der ersten Linux-Distributionen herunterladen. Dieses Hobby hat er beibehalten, auch wenn es heute dank einer DSL-Anbindung und eines CD-Brenners nicht mehr so aufwendig ist wie früher. Dank ihm war es mir möglich, immer auf dem neuesten Stand zu bleiben, was die hier vorgestellten Distributionen angeht. Kaum lag die jeweilige Distribution auf dem FTP-Server des Herstellers, konnte ich sicher sein, daß Sven bei unserem nächsten Treffen einen Stapel CDs dabeihaben würde.

Ariane Hesse gebührt besonderer Dank. Sie machte mir damals den Vorschlag, doch ein Buch für den O'Reilly-Verlag zu schreiben, und stand mir dann die ganzen drei Jahre, die dieses Projekt schon dauert, als Lektorin mit Rat und Tat zur Seite.

Eine ganze Reihe von Leuten haben dieses Buch probegerlesen und mir wertvolle Ratschläge gegeben. Da wären (in keiner bestimmten Reihenfolge): Martin Freiss, Bruno Hopp, René Kermis, Dr. Kerstin Hoef-Emden und Sven Riedel. Kerstin erlaubte mir darüber hinaus mehrmals, ihren DSL-Anschluß und einen ihrer Rechner für den Test meiner Beschreibung einer DSL-Anbindung zu benutzen, obwohl das bedeutete, daß sie an dem jeweiligen Tag von ihrer Anbindung an die Universität und damit von ihrer Forschungsarbeit abgeschnitten war.

Auch nachdem die erste Auflage erschienen war, nahmen Leser die Gelegenheit wahr, mich über E-Mail auf Fehler hinzuweisen und wertvolle Anregungen für Verbesserungen zu geben. Mein Dank geht an: Reinhard Holler, Ingo Kemper, JK¹, Axel Wagner, Armin Wasicek und Karin Capey. Karin gebührt mein besonderer Dank, da sie die Beschreibungen im Beruf umsetzt und dabei Gelegenheit hatte, meine Skripte im praktischen Einsatz zu testen. Sie hat dabei leider noch den einen oder anderen Fehler gefunden, der so bei mir nicht auftrat.

¹ Leider war die E-Mail nur mit Initialen unterzeichnet.

Versionshistorie (History)

Dies ist der Abschnitt History, der in der GNU Free Documentation Licence gefordert wird. Wenn Sie eine veränderte Version dieses Dokuments herausbringen, müssen Sie diesen Abschnitt beibehalten und der Liste einen neuen Eintrag mit dem Titel des neuen Dokuments, seinem Erscheinungsjahr, Ihrem Namen sowie den Namen eventueller Koautoren und dem Verleger Ihrer Version angeben.

- Andreas Lessig, *Linux-Firewalls – Ein praktischer Einstieg (2. Auflage)*, 2006, O’Reilly Verlag GmbH & Co. KG
- Andreas Lessig, *Linux-Firewalls – Ein praktischer Einstieg*, 2003, O’Reilly Verlag GmbH & Co. KG

