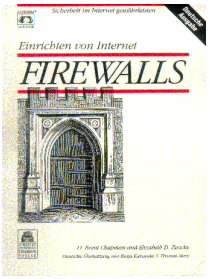
Internet Firewalls

Einrichten von Internet Firewalls von D. Brent Chapman und Elizabeth D. Zwicky; Verlag O´Reilly, International Thomson-Verlag, 1996, ISBN 3-930673-31-2, 576 Seiten, öS 538,-

Hans Blocher



In jeder Gesellschaft gibt es einen gewissen Prozentsatz von Personen, die anderen mutwillig schaden. Das Internet umfaßt derzeit schätzungsweise 40 Millionen Benutzer. Auch wenn der Anteil böswilliger Benutzer weniger als ein Prozent der Gesellschaft ausmacht, ist er doch groß genug, um sich damit auseinandersetzen zu müssen. Manche Sicherheitslücken (z.B. Schwachstellen in Betriebssystemen) sind hinlänglich bekannt, es gibt inzwischen aber auch höchst raffinierte Angriffsmethoden. Wie kann man sein eigenes System vor solchen Bedrohungen schützen, ohne daß der eigene Zugang ins Internet unnötig erschwert wird? Derzeit stellen Internet-Firewalls die effektivste Verteidigung dar.

Was ist ein Firewall? In einem Gebäude dient eine Brandmauer (firewall) dazu, das Übergreifen eines Feuers von einem Gebäudeteil auf einen anderen zu verhindern. Im Prinzip verfolgt ein Internet-Firewall einen ähnlichen Zweck: Er gewährt nur an einem streng kontrollierten Punkt Zutritt; er hält Angreifer davon ab, anderen Schutzvorrichtungen zu nahe zu kommen; er sorgt dafür, daß das System nur an einem einzigen Punkt verlassen werden kann.

Ein Firewall soll daher trennen, einschränken und analysieren. Die physikalische Implementation sieht bei jedem Standort anders aus. Meistens besteht er jedoch aus verschiedenen Hardware-Komponenten (Router, Computer, ...) mit geeigneter Software.

Das Buch „Einrichten von Internet-Firewalls“ gibt eine praktische Anleitung zur Konzeption, Einrichtung und Verwaltung von Firewalls. Es enthält unter anderem:

- Ausführliche Beschreibungen zum Aufbau von Firewalls mit Paketfilterung oder Proxy-Diensten sowie Anleitungen zur Konfiguration von Internet-Diensten (E-Mail, FTP, DNS, Telnet, WWW) für die Zusammenarbeit mit Firewalls.
- Allgemeine Kapitel über die Gefahren im Internet, Firewall-Architekturen, Sicherheitsstrategieen, Methoden zur Benutzerauthentifizierung, Betreuung von Firewalls und Reaktionen auf Einbrüche.
- Eine Übersicht über Informationsquellen und frei verfügbare Tools (hauptsächlich für Unix-Systeme), die man für den Aufbau eines effektiven Firewalls nutzen kann.

Für wen ist dieses Buch gedacht? Obwohl es sich in erster Linie an Personen richtet, die Firewalls einrichten müssen, ist es in weiten Teilen auch für Leute geeignet, die sich allgemein mit der Sicherheit im Internet befassen.

Frei gehaltene Auszüge aus dem Buch:

Was können Firewalls?

Ein Firewall ist das Zentrum für Sicherheitsmaßnahmen

Die Bündelung von Sicherheitsmaßnahmen ist wesentlich effizienter, als die sicherheitsrelevanten Entscheidungen und Technologien über die ganze Organisation zu verteilen und alle Schwachstellen stückweise abzudecken. Die Kosten für den Aufbau eines Firewalls können in die Zehntausende (DM) gehen.

Ein Firewall kann die Sicherheitspolitik durchsetzen

Viele der Dienste, die die Anwender vom Internet verlangen, sind von Haus aus unsicher. Ein Firewall läßt nur anerkannte Dienste passieren, und auch diese nur innerhalb der dafür festgelegten Regeln. Er kann aber auch die Aufgabe haben, kompliziertere Richtlinien durchzusetzen. Zum Beispiel dürfen nur bestimmte Systeme innerhalb des Firewalls Dateien vom und zum Internet übertragen. Zu diesem Zweck werden oft Paketfilter-Systeme verwendet. Sie routen Pakete zwischen internen und externen Rechnern, gehen dabei aber selektiv vor. Sie lassen bestimmte Pakettypen passieren oder blockieren sie auf eine Art, die die Sicherheitspolitik eines Standortes widerspiegelt. Der in einem Paketfilter-Firewall verwendete Routertyp wird Überwachungsrouter genannt.

Ein normaler Router sieht sich einfach die Zieladresse eines jeden Pakets an und wählt den besten ihm bekannten Weg aus, um das Paket in Richtung seines Bestimmungsortes zu senden. Wie das Paket zu behandeln ist, wird nur vom Zielort bestimmt. Ein Überwachungsrouter dagegen sieht sich die Pakete genauer an. Er entscheidet nicht nur, ob er ein Paket in Richtung des Zielortes routen kann, sondern auch, ob er es überhaupt soll.

Ein Beispiel für die Art, wie ein Überwachungsrouter programmiert sein könnte, um Pakete selektiv von und zum Standort zu routen:

> *Blockiere alle Verbindungen von Systemen außerhalb des internen Netzes. Lasse lediglich eintreffende SMTP-Verbindungen passieren, damit E-Mail empfangen werden kann.*

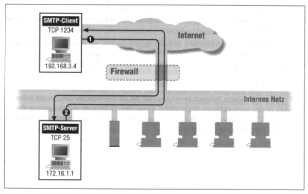
Im folgenden Faksimile-Auszug wird beschrieben, wie so ein Regelsatz entsteht. Die Filter werden dazu schrittweise entwickelt und nicht gleich in ihrer endgültigen Fassung angeführt.

Regel	Richtung	Quell-Adresse	Ziel-Adresse	Proto-koll	Ziel-Port	Aktion
A	ein	extern	intern	TCP	25	zulassen
B	aus	intern	extern	TCP	>1023	zulassen
C	aus	intern	extern	TCP	25	zulassen
D	ein	extern	intern	TCP	>1023	zulassen
E	beliebig	beliebig	beliebig	beliebig	beliebig	verbieten

- Die Regeln A und B erlauben eingehende SMTP-Verbindungen (eintreffende E-Mail).
- Die Regeln C und D lassen hinausgehende SMTP-Verbindungen zu (hinausgehende E-Mail).
- Regel E ist die Standardregel, die angewandt wird, wenn keine der anderen Regeln greift.

Betrachten wir nun anhand einiger Beispiele, wie Pakete behandelt werden. Angenommen, Ihr Rechner besitzt die IP-Adresse 172.16.1.1, und jemand möchte Ihnen Post von einem fernen Rechner mit der IP-Adresse 192.168.3.4 senden. Ferner benutzt der SMTP-

Abb. 6-10: Paketfilterung: nach innen gerichtetes SMTP (Beispielpakete 1 und 2).



Client des Absenders Port 1234, um mit dem SMTP-Server an Port 25 zu kommunizieren. Wie in der Beschreibung von SMTP in Kapitel 8 erwähnt, benutzen SMTP-Server die Standardportnummer 25.

Paket	Richtung	Quell-Adresse	Ziel-Adresse	Proto-koll	Ziel-Port	Aktion (Regel)
1	ein	192.168.3.4	172.16.1.1	TCP	25	zulassen (A)
2	aus	172.16.1.1	192.168.3.4	TCP	1234	zulassen (B)

Abbildung 6-10 zeigt diesen Fall.

Die Paketfilterregeln erlauben bei Ihnen eingehende E-Mail:

- Regel A läßt zu, daß Pakete vom SMTP-Client des Absenders bei Ihrem SMTP-Server eintreffen (siehe Paket Nummer 1).
- Regel B erlaubt, daß Ihr Server dem Client des Absenders antwortet (siehe Paket Nummer 2).

Aus dem Inhaltsverzeichnis des Buches:

Zusammenfassung:

Wer sich von diesem Buch konkrete, leicht umsetzbare Beispiele erwartet, wird enttäuscht sein. Das Gebiet der Schutzeinrichtungen für das Internet ist zu komplex, als daß es an Hand von einigen Musterinstallationen erklärt werden könnte. Aufgrund dieser Tatsache können die Redundanzen, die bei dem Versuch auftraten, eine möglichst erschöpfende Abhandlung aller Aspekte der einzelnen Internet-Dienste bezüglich Paketfilterung, Proxy-Diensten, Konfiguration etc. anzubieten, doch teilweise als störend empfunden werden.

Ein Hinweis dieses Buches erscheint mir jedoch besonders wichtig: auch ein gutes Firewall-System kann keinen 100%igen Schutz gewährleisten. Man wird Kompromisse schließen müssen zwischen dem gewünschten Maß an Sicherheit, den dadurch entstehenden Kosten für Installation und Betreuung, und den Einschränkungen, den gewisse Sicherheitsstufen für den alltäglichen Betrieb mit sich bringen. □