Firewall-Techniken, die selbst harte Angriffe vereiteln

Scheitern garantiert

An diesen Mauern streckt jeder Angreifer die Waffen: Moderne Linux-Firewalls arbeiten auf beliebigen Protokollschichten und erkennen damit einen unerwünschten Datenansturm. Der Schwerpunkt dieses Linux-Magazins erklärt neue Techniken und beschreibt praktische Admin-Helfer. Achim Leitner

Inhalt

Keine Firewall ist wie die andere. Sie ist kein fertiges Rundum-sorglos-Paket, das sich – einmal installiert – um alle Probleme kümmert. Für die Auswahl der Technik, Konfiguration und den täglichen Betrieb ist Grundlagenwissen nötig. Der Admin muss entscheiden, auf welcher Protokollschicht sein Paketfilter ansetzt und aus welchen Schichten seine Filterkriterien stammen.

Die klassische Firewall arbeitet als Router, im OSI-Modell also auf Schicht 3 (siehe Abbildung 1). Ein Router beachtet eigentlich nur das IP-Protokoll und entscheidet, wohin er ein Paket leitet. Als Firewall sieht er zusätzlich in die Header der Schicht 4 (TCP oder UDP), um Dienste zu unterscheiden und Flags auszuwerten.

Das schichtübergreifende Arbeiten lässt sich nach unten ausdehnen: Bridgewalls arbeiten auf Schicht 2. Während eine herkömmliche Bridge nur MAC-Adressen auswertet, blickt sie bis hinauf zur Schicht 4 und arbeitet damit als vollwertiger Paketfilter (Seite 30).

Auch nach oben ist mehr möglich: Ein Application Level Gateway trennt die TCP-Verbindung und setzt sich als Proxy zwischen Client und Server. Damit erhält die Firewall tiefe Einblicke in das Applikationsprotokoll und erkennt Verstöße gegen die Protokollvorschriften aus dem RFC (Seite 52).

Der Blick in die höheren Schichten ist allerdings nicht immer möglich: Das IP Security Protocol soll genau das verhindern. Auf dem Übertragungsweg gelingt es auch. Im Endsystem erhält eine lokale Firewall aber sehr wohl Zugriff auf die IPsec-verpackten Pakete. Warum beim Filtern auch an dieser Stelle unerwartete Probleme auftreten, erklärt der Beitrag ab Seite 34.

GUI-gestützt

Bei der Konfiguration der Filterregeln helfen GUI-Tools wie Guarddog (Seite 40). Das KDE-Programm befreit den Admin davon, sich die »iptables«-Optionen merken zu müssen. Auch beim Auswerten der Logfiles darf er auf Hilfe hoffen: Was moderne Analysetools leisten, steht im Artikel ab Seite 44.

Eine Firewall soll nicht nur unerwünschte Verbindungen verhindern, sie muss die gewünschten gezielt zulassen. Der Weg von außen nach innen gilt dabei als besonders gefährlich. Per Port-Knocking verschleiern Admins sogar, dass ein Eingang existiert: Wer den geheimen Port (auf Schicht 4) und das Passwort nicht kennt, kann auch nicht feststellen, ob es eine Tür gibt. Wie das funktioniert, beschreibt der Artikel ab Seite 48. Er stellt eine neu entwickelte Variante dieser Technik vor. ■

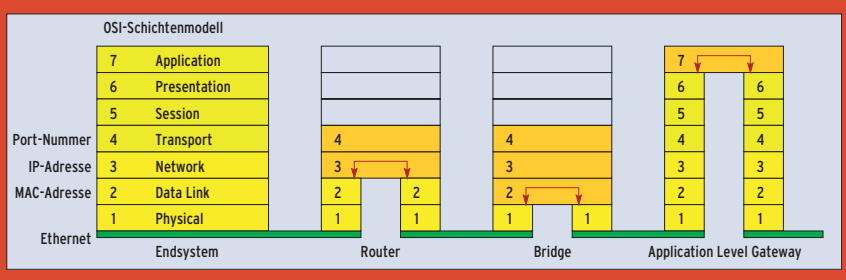

Abbildung 1: Moderne Firewalls können als Router, Bridge oder Application Level Gateway arbeiten.