HELPDESK

Firewalling: Typen und Techniken

Jede Woche beantworten Sicherheitsexperten Leserfragen und geben Ratschläge, wie sich die Sicherheit in einem Unternehmen erhöhen lässt.

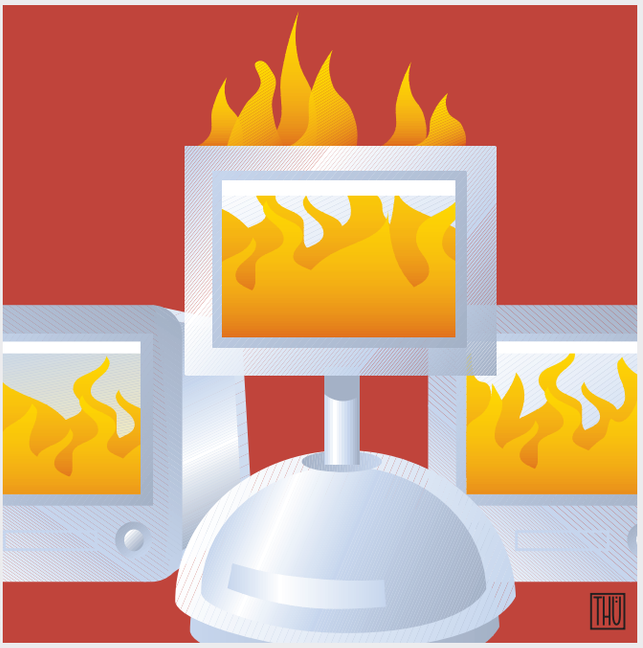

ILLUSTRATION: CW/THÜ

Frage: Welche unterschiedlichen Firewall-Typen gibt es und welche Vor- beziehungsweise Nachteile gehen mit ihnen einher?

Antwort: Die klassische Firewall-Diskussion kennt lediglich zwei unterschiedliche Firewall-Typen. Die ursprüngliche Variante ist in einem Paketfilter (PF) gegeben. Dieser analysiert die Kommunikationen auf der Netzzugangs-, der Netzwerk- und der Transportebene. Lediglich anhand von IP-Adressen und Port-Nummern des Absenders sowie Empfängers werden Entscheidungen über die Zulassung der Verbindung getroffen. In modernen Implementierungen werden ebenfalls die Header-Optionen der Pakete sowie Verbindungs-Stati des Daten-Austauschs analysiert. Dies soll komplexe Angriffe und Attacken mittels korrupten Paketen (z.B. Firewalking) verhindern.

Vorteil derartiger Lösungen ist ihre Einfachheit. Verhältnismässig simpel lassen sie sich entwickeln und ihre Regeln anwenden. Eine solche technische Primitivität ist sicherheitstechnisch stets ein Vorteil, denn es ergibt sich aus ihr eine geringere Chance auf Fehler bei der Umsetzung. Ihre einfache Analysetechnik ist aber ebenfalls ihr grösster Nachteil. So können Paketfilter nicht erkennen, ob die über einen freigegebenen Port umgesetzte Kommunikation auch wirklich jene ist, für die sie sich ausgibt. Durch das Aufsetzen eines modifizierten Mailservers liessen sich nämlich auch Mail-Verbindungen über den TCP-Port 80, der eigentlich für Web-Verbindungen (HTTP) vorgesehen ist, abwickeln.

«Firewalling steckt bei vielen Herstellern noch immer in den Kinder schuhen.»

Um derlei Tunnelling-Angriffe zu verhindern, wurden sogenannte Application Gateways (AG) entwickelt. Diese greifen auf einzelne Proxies zurück, die für dedizierte Dienste angeboten werden. Ein solcher Proxy nimmt eine Anfrage auf einem Port entgegen, überprüft die Daten der Netzwerkanwendung und leitet sie gegebenenfalls weiter. Die Entkoppelung und die erweiterte Einsicht auf der Applikationsebene erlauben das genaue Erkennen von fehlerhaften Kommunikationen. Eine Webverbindung (HTTP) ist über einen Mail-Proxy (SMTP) aufgrund der Protokoll-Unterschiede gar nicht (oder nur mit erheblichem Zusatzaufwand) möglich – Irrelevant, ob diese nun über den Port 80 oder 12345 stattfindet.

Diese erweiterten Analyse-Fähigkeiten sind aber ebenfalls zeitgleich der Nachteil der Lösung. So erfordern sie eine erhöhte Komplexität des Produkts, was dazu führt, dass derartige Implementierungen statistisch fehleranfälliger sind. Hinzu kommt, dass viele Proxy-Produkte relativ einfach gestrickt sind und die Möglichkeiten der Technik bei weitem noch nicht ausschöpfen. So wären seit jeher pattern-basierte Überprüfungen möglich, die frühzeitig Angriffsmuster auf Applikationen erkennen können: So deutet etwa eine sehr lange Zeichenkette auf einen Pufferüberlauf-Versuch hin. Die Entwickler von Application Gateways sind aber zunehmends darum bemüht, neue und verbesserte Proxies anzubieten und damit die Qualität der Kontrolle zu steigern.

Die Werber der Firewall-Hersteller kommen dann gerne von dieser simplen Begriffs-Definition ab und werfen skurrile Eigenkreationen in den Raum. Phrasen wie «Intelligent Defense» oder «Next Generation» werden sodann als vermeintlich etablierte Firewall-Techniken verkauft. In den meisten Fällen handelt es sich dabei jedoch lediglich um die Adaption oder Weiterentwicklung altbekannter Verfahren oder die Kombination verschiedener Sicherheits-Technologien wie zusätzliche Einbruchserkennung oder Antiviren-Mechanismen. Derlei Zusatz-Features bringen erhöhte Komplexität, was ein Mehr an Fehleranfälligkeit verspricht. Dies ist ein klarer Verstoss gegen den Grundsatz von Firewall- oder Sicherheits-Systemen: «Keep it simple, keep it save.» ■

Der Autor
Marc Ruef ist Security Consultant beim Sicherheitsunternehmen Scip, Zürich.
www.scip.ch

Unsere Experten beantworten Ihre Fragen. Schreiben Sie uns: it-security@computerworld.ch

Ein Archiv der Helpdeskartikel finden Sie im Internet: www.computerworld.ch