Firewall Das Regelwerk

Nur wenn die Firewall mit einem praxisgerechten Regelsatz versehen ist, wird diese ein Netzwerk auch wirklich sichern können. Die wichtigste Aufgabe beim Einbau einer neuen Firewall ist die Definition der Regeln, nach denen die Firewall arbeiten soll.

Aufsetzen des Regelsatzes
Erfolgreiche Regelsätze sind einfache Regelsätze. Je einfacher Ihre Regeln sind, umso sicherer wird Ihre Firewall sein. Wenn Ihre Firewall 30 bis 50 Regeln hat, dann liegen Sie im orangenen Bereich, mit jeder Regel wächst die Gefahr einer Fehlkonfiguaration deutlich an. Je kürzer der Regelsatz ist, umso schneller kann die Firewall ihn abarbeiten, das heisst, die Performance wird besser. Zwar arbeiten die meistem Firewalls sehr effizient, aber es kann auf keinen Fall schaden, Reserven zu haben.

Der Regelsatz

Die LAN-Nutzer erhalten nur Zugriff auf die Dienste, die sie auch wirklich brauchen. In diesem Fall sind dies DNS, HTTP, SMTP und POP. Die Regeln folgen nun in der Reihenfolge, wie sie im Regelsatz erscheinen sollen, d.h. die erste Regel steht ganz oben und die elfte wird ganz zuletzt abgearbeitet.

- Firewall-Admin-Zugang: Die folgende Lockdown-Regel verbietet sämtlichen Traffic zur Firewall, diese Regel erlaubt es den Admins, auf die Firewall zuzugreifen.

- No Logging: Die vorletzte Regel Ihres Regelsatzes sollte die "No-Logging"-Regel sein. Diese Regel bezieht sich auf internen Traffic. Geschwätzige Protokolle wie NetBIOS produzieren jede Menge nutzlose Log-Einträge. Mit dieser -Regel werden solche Protokolle ausgefiltert, und die Log-Dateien bleiben lesbar. Auch diese Regel gehört zu den Standard-Regeln, über die jede Firewall verfügen sollte.

- Lockdown: Diese Regel blockiert den Zugriff auf die Firewall. Es handelt sich hier um eine Standard-Regel, die in jedem Regelsatz vorhanden sein sollte. Niemand ausser dem Firewall-Administatoren benötigt Zugriff auf die Firewall

- DNS-Zugriff: Internet-Nutzer sollen Zugriff auf den DNS-Server in der DMZ haben.
- Mail-Zugriff : Internet- und LAN-Nutzer sollen Zugriff auf den Mail-Server via SMTP haben.
- Web-Zugriff: Internet- und LAN-Nutzer sollen Zugriff auf den Web-Server via HTTP haben.
- Admin-Zugriff: Diese Regel erlaubt den Admins den verschlüsselten Fernwartungs-Zugriff auf das LAN. Zur Erhöhung der Sicherheit sind sie dabei auf bestimmte IP-Adressen beschränkt.
- Interner POP-Zugriff: Diese Regel erlaubt den Zugriff vom LAN via POP auf den Mail-Server.
- DMZ abschotten: Diese Regel trennt die DMZ vom LAN. Kein Nutzer aus dem LAN darf auf die DMZ zugreifen.
- DMZ-Kontrolle: Normalerweise sollte die DMZ niemals versuchen, Daten an das interne LAN zu senden. Wenn dies doch passiert ist das ein Indiz für einen Hacker-Einbruch. Diese Regel blockiert sämtliche Daten, loggt alles mit und alarmiert den entsprechenden Admin.
- Drop-all: Standardmässig werden alle Pakete, auf die sich keine Regel anwenden lässt, von der Firewall verworfen. Dieser Vorgang erscheint aber nicht in der Log-Datei. Sie sollten deshalb die Regel "Verwerfen UND mitloggen" aufsetzen und ganz am Ende des Regelsatzes platzieren. Der Grund: Die meisten Angriffe erfolgen über illegitime Pakete, die keiner Firewall-Regel genügen.

Folgende Regeln sind nicht unbedingt nötig, helfen aber die Performance und Sicherheit zu verbessern.
- Blockieren Sie alle Verbindungen zu Doubleclick oder den andern grossen Anzeigen-Vermarktern im Internet. Damit werden Sie die ganzen Banner los; dies spart Ihren Nutzer Zeit und Bandbreite und verbessert die Performance.
- Um ICQ-Verbindungen zu blockieren, sollten Sie statt der betreffenden Ports direkt die Ziel-Server bei AOL blockieren.

Testen und Pflegen des Regelsatzes
Scannen Sie das Ergebnis Ihrer Arbeit mit einem Tool wie Nessus oder Nmap. Nur so können Sie feststellen, dass Sie nicht Regeln vergessen haben und ob sich die Firewall in der Praxis bewährt. Wenn die Tests keine Fehler ergeben wäre die Firewall einsatzbereit. Sobald der Regelsatz funktioniert, sollten Sie diesen unbedingt dokumentieren. Gerade in grösseren Organisationen ist es eminent wichtig, die Firewall-Regeln sauber zu dokumentieren, sonst sind der Fehlkonfiguration Tür und Tor geöffnet - einfach aus Unkenntnis heraus. Jede Regel sollte wie folgt dokumentiert werden:
- Wer hat die Regel geändert?
- Wann wurde die Regel geändert?

- Warum wurde die Regel geändert?

Damit sorgen Sie dafür, dass Ihre Firewall auch in Zukunft ein sicheres Tor zum Internet sein kann.