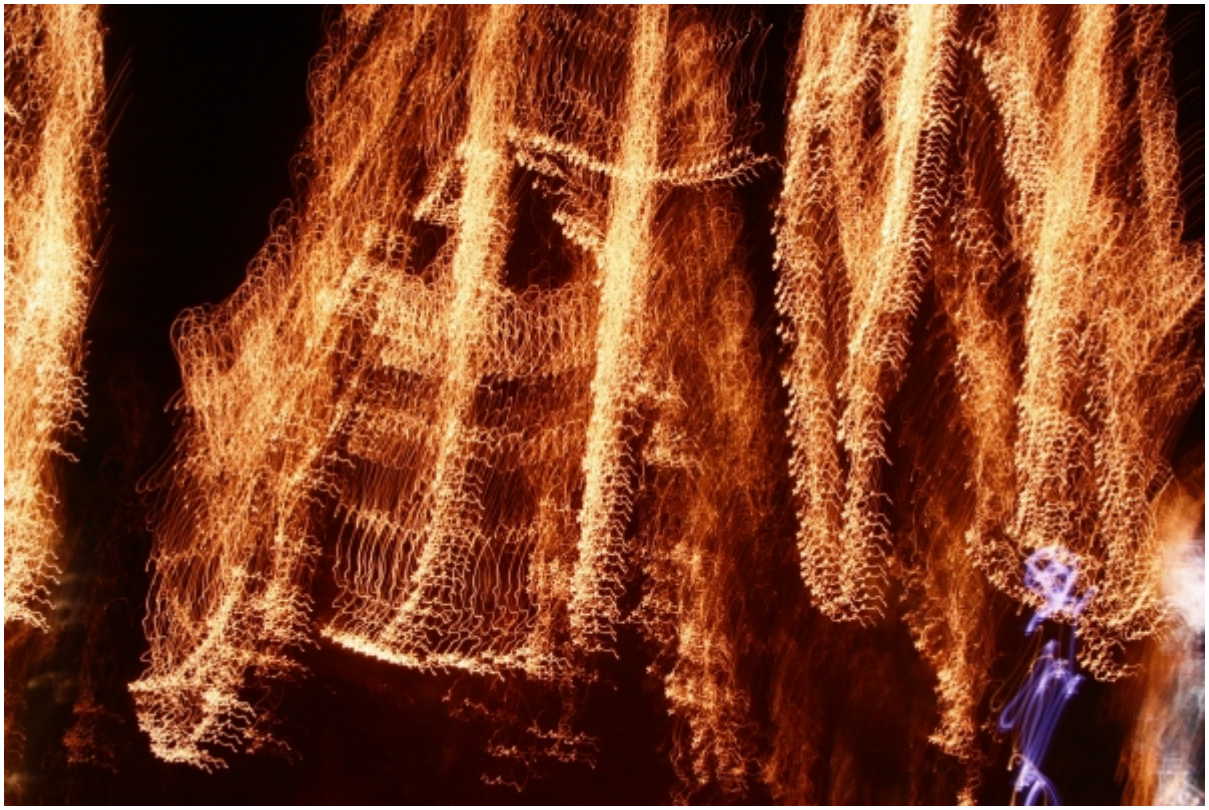
von Thomas Barlen

In diesem Teil widme ich mich OS/400 Funktionen, die zur Verbesserung von Netzwerksicherheit eingesetzt werden können. Dabei ist erwähnenswert, daß diese Funktionen nicht nur für Umgebungen geeignet sind, die eine Verbindung zum Internet oder Extranet haben. Wie aus einigen Studien bekannt, werden 60- 70% aller Schäden aus dem Intranet heraus verursacht.

Über den Autor

Thomas Barlen, IBM Technical Sales Support iSeries, ist zu erreichen unter barlen@de.ibm.com



IP Paket Filter

Eine Funktion, die schon seit V4R3 im OS/400 integriert ist, ist IP Paket Filtering. Allerdings mußte die Person, welche die Filterregeln administrierte bisher recht fundierte IP Protokollkenntnisse haben. Auf Grund einer komplett neuen graphischen Oberfläche und mehreren Configuration Wizards ist es mit V5R2 wesentlich einfacher geworden, IP Filter einzurichten.

IP Filter können eingesetzt werden, um auf einem Netzwerkadapter (LAN, WAN oder VLAN) IP Pakete nach folgenden Kriterien zu filtern:

- IP Quellenadresse
- IP Zieladresse
- IP Quellenport
- IP Zielport
- IP Protokoll

Mit dieser Möglichkeit kann kontrolliert werden, welcher Service (über Port Nummern) von welchen IP Adressen, Adressbereichen oder Subnetzen genutzt werden kann. Zum Beispiel, interne Benutzer können über eine ungeschützte 5250 Emulation arbeiten, während Benutzer aus dem Internet nur über SSL-geschützte Verbindungen arbeiten können. Ich möchte an dieser Stelle darauf hinweisen, daß IP Paket Filtering im OS/400 als zusätzliche Barriere zu betrachten ist und keine vollwertige Firewall ersetzen kann.

Bevor mit der Konfiguration begonnen wird, ist es wichtig, eine sorgfältige Planung durchzuführen. Dazu sollten Sie genaue Aufzeichnungen über die Art der genutzten Services (z.B. Telnet, FTP, SMTP, etc.) sowie die Adressen der entsprechenden Benutzer PCs haben, denn jeder IP Datenverkehr, der nicht explizit erlaubt ist, wird automatisch blockiert. Der OS/400 CL Befehl NETSTAT *CNN oder die entsprechende Funktion im iSeries Navigator kann ein Großteil der

benötigten Informationen liefern.

Im nächsten Schritt werden die entsprechenden Filterregeln eingerichtet. Dies geschieht über den iSeries Navigator unter Netzwerk und IP Richtlinien. Abbildung 1 zeigt die graphische Oberfläche des Packet Rules Editors mit gestartetem Wizard.

Der Vorteil eines Wizards ist besonders gut bei Client Access (iSeries Access) zu erkennen. Anstatt ca. 24 Regeln für eingehenden und ausgehenden Datenverkehr von Client Access manuell hinzufügen, nimmt Ihnen der Wizard diese Fleißaufgabe ab. Nachdem alle Regeln erstellt sind, können Sie die Filter aktivieren. Dazu noch einen guten Rat, testen Sie die Filter ausserhalb der normalen Arbeitszeit. Eventuell vergessene Filter haben dann keine unangenehmen Auswirkungen.