# Sicherheit in Netzwerken

Ein erster Ansatz ist es, die Welt in Innen und Außen aufzuteilen. Das "Innen" ist dann vor dem "Außen" zu schützen. Innen sind die Guten, außen die Bösen.

Telearbeit, Mobile Computing und auch Fusionen (bzw. das Gegenteil) verkomplizieren diese einfache Einteilung in Innen und Außen. Eine Lösung wird dann in VPNs gesehen (die Guten, haben dann z.B. ein gemeinsames Geheimnis). Mit der Einrichtung einer Firewall selbst ist es daher noch nicht getan.

Allen Sicherheitskonzepten liegt zugrunde, dass die als verbindlich angesehenen Regeln (Policies) überwacht werden müssen. Das muss lückenlos im gesamten Netz geschehen, also auch auf der Ebene der Netzhardware.

Wir brauchen daher eine Netzüberwachung: Welche Stationen (MAC− und IP−Adressen) sind am Netz, sind diese bekannt oder nicht (Intrusion Detection) und auf dem jeweiligen Segment zugelassen. Wer redet mit wem (eigene und fremde Adressen) über welchen Port, über welches VLAN. Gerade beim Einsatz von Tunneling Protokollen (PPTP, IPSec ..) keine leichte Aufgabe.

Da heute alle Netze geswitcht bzw. geroutet sind, ist es gar nicht mehr so einfach an diese Informationen heran zu kommen. Wenn z.B. ein Mitarbeiter über einen seriellen Port an seinem PC über ein Handy eine eigene Verbindung zur Außenwelt aufbaut, so kann dies kaum entdeckt werden. Wenn er dabei jedoch anderen darüber "Routingdienste" über vom Firmen−Intranet getrennte IP−Netze anbietet, so kann man dies "beobachten" (ARPs verbreiten sich auch über Switchgrenzen hinweg als Broadcasts).

Beobachten kann man auch am WAN−Anschluss (z.B. bei DSL am PPPOE Interface) sämtlichen Verkehr nach außen. Hierzu eignet sich z.B. NetControl for Windows. Mit dem AddressWizard von RzK kann man einen Adress−Scan zyklisch auf den eigenen IP−Netzen durchführen (Erreichbarkeitstests) und zusätzlich das Netz beobachten, um auch andere, beliebige fremde IP−Adressen festzustellen (Detection old / new Addresses).

### RzK Security

- NetControl
- AddressWizard Pro