Wann macht ein Paketfilter doch Sinn?

Wer Serverdienste nur in seinem lokalen Netzwerk zulassen möchte, braucht in den allermeisten Fällen auch keinen Paketfilter, da er wohl meistens einen Router (Hardware oder PC) sein eigen nennt, der für ihn Network Address Translation (NAT) durchführt. Der Server trägt dann eine lokale Adresse wie 192.168.0.5, die aus dem Internet überhaupt nicht zu erreichen ist, außer der Router führt Forwarding aus, dann dürfte das aber wohl beabsichtigt sein.

Wichtig wird eine Firewall erst, wenn man entweder eigene Serverdienste aus einer DMZ heraus im Netz anbietet, oder wenn ein internes Netz gar öffentliche IP-Adressen besitzt. Davon sollten allerdings Neulinge besser erstmal die Finger lassen und sich informieren. Ein grafisches Tool könnte in dem Fall einem Profi vielleicht helfen, die Konfiguration schneller hinzukriegen, als manuell "iptables zu hacken", sollte aber nicht die Kenntnisse über Netzwerksicherheit ersetzen.

Richtig sinnvoll auf einem Einzelplatzrechner ist ein Paketfilter nur, wenn man nicht die Ports, sondern die Herkunft der Pakete einschränken will. Bspw. möchte man einem Kumpel ermöglichen, den eigenen FTP-Server zu benutzen, oder man will vom Arbeitsplatz aus ssh nach Hause benutzen. So etwas lässt sich oft mit iptables einfacher konfigurieren, als über hosts.allow/.deny oder dienstspezifische Konfigurationsdateien. Besonders, wenn es sich um eine ganze Reihe Dienste handelt, die alle für denselben Zugang vorgesehen sind. Das ist allerdings auch nur dann praktikabel, wenn keine dynamischen IP-Adressen involviert sind. Da die Möglichkeit des Adress-Spoofing besteht, sollte das jedoch niemals starke Authentifizierungsmechanismen des betreffenden Dienstes ersetzen. Gute Passwörter (oder noch besser Public-Keys) sind auch dann unverzichtbar, wenn "nur" der eigene Arbeitsplatzrechner freigegeben ist. Besser könnte es dann wohl sein, gleich auf VPN zu setzen. Es ist außerdem daran zu denken, dass man bei gelegentlichem Zugriff auf einen zu Hause befindlichen Testwebserver o.ä. auch ssh-Tunnel benutzen kann.

In seltenen Fällen mag es vorkommen, dass ein Dienst nicht die Möglichkeit bietet, ihn auf bestimmte Netzwerkschnittstellen zu begrenzen. Insbesondere könnte das bei Software der Fall sein, die nicht von Ubuntu unterstützt wird. In diesem Fall kann einem nichts anderes übrig bleiben, als diesen Qualitätsmangel mit der Implementation von Filterregeln zu kompensieren.

Filesharing-Tools

Diese öffnen in den meisten Fällen auch Ports nach außen, wie ja schon die Bedeutung des Wortes "Sharing" suggeriert. Dass die meisten inzwischen auch hinter einer Firewall funktionieren, liegt an einem Trick. Systeme, die hinter einer Firewall liegen, fragen einfach in gewissen Abständen ihren Server nach, ob jemand etwas von ihnen haben will, und "pushen" diese Datei dann, indem sie selber eine Verbindung zum Tauschpartner ausführen. Wenn dieser allerdings auch hinter einer Firewall sitzt, funktioniert das nicht, so dass man als Filesharer hinter einer Firewall heutzutage doch ziemlich eingeschränkt ist. BitTorrent bestraft dich dafür sogar mit geringerer Downloadrate. Deswegen öffnen viele Filesharer die Ports extra, oder stellen Port-Forwarding auf ihrem Router ein. Sollte man also auf einem Einzelplatzsystem so eine Software einsetzen, aber der Qualität der Software nicht soweit trauen, dass es nur die freigegebenen Daten rausrückt, könnte man einen Paketfilter einsetzen wollen, der diese Ports für den Zugriff von außen sperrt. Oben beschriebene Nachteile sind dann allerdings unvermeidlich.