NAT-Router: Hasenpfote oder Pferdefuss?

Der NAT-Router, das ist jenes Kästchen, das man zwischen das böse Internet und die PCs daheim, in der Firma oder im Studentenheim steckt, damit ... – ja, warum eigentlich?

Wenn man gewissen Zeitschriften, Computergurus oder dem verheißungsvollen Verpackungsaufdruck „Firewall" glauben dürfte, wäre der NAT-Router die Sicherheitslösung schlechthin – wie ein über der Eingangstür aufgehängter Talisman sorgt er angeblich dafür, dass die bösen Geister draußen bleiben müssen. Andere Fachleute wiederum setzen eine höhnische Grimasse auf und behaupten, mit NAT werde alles nur schlimmer. Und dann ist da noch etwas: Diese Geräte sind wie kleine Verteilerstecker – wo man eigentlich nur einen Computer anstecken darf, reicht das Internet plötzlich für alle.

Die Wahrheit liegt, wie so oft, nicht in der Mitte, sondern in der nüchternen Betrachtung. Werfen Sie nicht gleich Ihren NAT-Router aus dem Fenster, wenn in der Folge zahlreiche Risiken erörtert werden – es geht vielmehr darum, die Gefahren zu kennen, um sie einschätzen zu können. Beginnen wir die Faktensuche gleich mit der Entzauberung der Abkürzung „NAT": *Network Address Translator*[1]. Da übersetzt also jemand Netzwerkadressen, was immer das sein mag.

Übersetzen? Das kommt mir spanisch vor...

Stellen Sie sich vor, Sie schicken ihrer kürzlich übersiedelten Tante Mali zu ihrem 83. Geburtstag ein Paket mit einem Botendienst. Der Bote fährt zur angegebenen Adresse und findet eine Gasse vor, in der alle Häuser gleich aussehen und dieselbe Hausnummer haben. Es wird ihm nichts anderes übrig bleiben, als kopfschüttelnd umzukehren und das Paket zum Absender zurückzubringen. Offenbar braucht zumindest jedes Haus eine eigene Adresse, sonst geht gar nichts mehr. Das ist im Internet nicht anders.

Wenn Ihnen Ihr Provider nur eine einzige Internet-Adresse zuteilt (und das ist meistens der Fall), aber mehrere Computer angeschlossen werden sollen, müssen diese wohl oder übel mit einer Adresse auskommen. In der realen Welt wäre es undenkbar, dass sich mehrere Häuser eine Adresse teilen. Im Internet ist das zwar auch keine gute Idee, aber mit Abstrichen immerhin möglich. Hier kommt die geschickte Übersetzung von Adressen ins Spiel: Jeder Besucher wird an der angegebenen Adresse von einem Portier empfangen, erhält einen Plan, auf dem jedes Haus noch eine andere Adresse hat, und erfährt, zu welchem Haus er gehen muss. Das Verfahren hört sich befremdlich an und ist es auch.

Zwei Computer im Internet reden miteinander, indem sie einander Datenpakete zusenden. Die Postämter und Briefträger dieser Pakete heißen „Router"; die Adressen heißen „IP-Adressen" und sehen etwa so aus: 131.130.1.78[2]. Klarerweise funktioniert das System nur, wenn jede Adresse eindeutig zu einem Haus bzw. einem Computer gehört.

Das Wunder der Adressvermehrung geschieht im NAT-Router, der zwei IP-Adressen erhält: die offizielle, vom Provider zugeteilte Adresse für die Kommunikation nach außen und eine, die offiziell nicht existiert (z.B. 192.168.0.1[3]), für das interne Netz. Die Computer im privaten Netz erhalten – händisch oder automatisch vom NAT-Router – ebenfalls private Adressen. Baut einer dieser privaten Rechner dann eine Verbindung nach außen auf (z.B. indem er eine Webseite aufruft), so „fälscht" der NAT-Router dessen Absenderadresse: Er setzt stattdessen seine eigene, offizielle Adresse ein. Kommen Antwortpakete, sind diese natürlich an ihn adressiert. Der Router „erinnert" sich an seine vorangegangene Manipulation, ersetzt die Empfängeradresse dementsprechend und sendet die Daten an den privaten Rechner weiter. Dieser merkt gar nichts von der Täuschung, und alles funktioniert wie gewünscht.[4]

Eine Folge dieses Schwindels: Von außen kann niemand eine Verbindung zu den privaten Rechnern aufbauen. Die privaten Adressen kennt außen ja niemand – und selbst wenn, würden die Datenpakete den Weg dorthin nicht finden, weil die Adressen nicht existieren, zumindest postamtlich gesehen. Von außen kommende Verbindungen zur offiziellen Adresse gehen ins Leere, weil der NAT-Router mangels vorangegangener „Fälschung" nicht weiß, wohin er die Pakete weitersenden soll. Diese Eigenschaft kann und will man gezielt umgehen, wenn man einen Server betreibt: Die-

---

1) Das ist der ältere Begriff und bezeichnet das Gerät. Heutzutage spricht man eher von *Network Address Translation* und denkt an den Vorgang, da nicht nur spezielle Geräte, sondern alle PCs als NAT-Router geeignet sind.

2) Dies bezieht sich auf das bislang gebräuchliche IPv4. Ganz anders sehen Adressen bei IPv6 aus, auf das am Ende dieses Artikels eingegangen wird.

3) siehe Y. Rekhter, B. Moskowitz, D. Karrenberg et al.: *Address Allocation for Private Internets* (`http://ftp.univie.ac.at/netinfo/rfc/rfc1918.txt`)

4) Der Verständlichkeit zuliebe wurden hier zumindest zwei Vereinfachungen vorgenommen: Einerseits spielen bei der Umsetzung auch so genannte Port-Nummern eine Rolle – erst damit kann der NAT-Router verschiedene Verbindungen, die das gleiche Ziel haben, auseinanderhalten. Außerdem gibt es auch Spielarten von NAT, die anders funktionieren, hier aber nicht weiter behandelt werden.

5) siehe IANA, *Port Numbers* (`www.iana.org/assignments/port-numbers`)

6) Nähere Informationen dazu finden Sie im Artikel *Firewalls: Schutz vor Gefahren aus dem Internet* in *Comment 02/2*, Seite 14 bzw. unter `www.univie.ac.at/comment/02-2/022_14.html`.

ser muss ja von außen erreichbar sein. Kontaktversuche an bestimmte Ports (das sind sozusagen die Türnummern im Internet, nur dass hier gleichartige Dienste auf jedem Rechner dieselbe Nummer haben,[5)] z.B. ist der Webserver meist auf Port 80 zu finden) werden deshalb immer an einen dafür bestimmten privaten Rechner geleitet. Dieses Feature wird häufig *Port Forwarding* genannt. Es gibt davon auch eine Blankoscheckvariante, meist irreführend als DMZ (Demilitarisierte Zone) bezeichnet, bei der alle hereinkommenden Verbindungen – egal zu welchem Port – gleich an den dazu auserkorenen Rechner weiterverbunden werden.

Das ist doch wie bei einer Firewall, ...

Eine Firewall im heute gebräuchlichen Sinne funktioniert ganz ähnlich: Sie schützt die „Guten" auf ihrer Innenseite vor den Angriffen der „Bösen" im Internet, indem sie nur bestimmte – im Wesentlichen hinausgehende – Verbindungen zulässt.[6)] Da Verbindungen von außen nach innen bei NAT gar nicht möglich sind, ist eine gewisse Verwandtschaft nicht zu übersehen. Sogar die Arbeitsweise ist ähnlich, und mit wenig Aufwand kann man einen NAT-Router tatsächlich so bauen, dass er auch die Eigenschaften einer „richtigen" Firewall aufweist. Das hat allerdings mit NAT nichts zu tun: Es gibt Firewalls ohne NAT, und es gibt NAT auch ohne Firewall-Funktion.

... was kann da noch schiefgehen?

Ein Vampir kann das Haus seines Opfers erst betreten, nachdem er eingeladen wurde – dennoch fehlt es den Horrorfilmen dieses Genres nicht an Spannung: Irgendwie gelangt er ja doch immer ins Haus. Auch wenn die digitale Version dieser Stories nicht hollywoodfähig ist, sind die Plots ähnlich: Der Bösewicht nutzt die Unwissenheit oder Unachtsamkeit des Opfers aus, um eingeladen zu werden, oder er findet irgendein Schlupfloch. Wie kann das, so fern des Zelluloids, in der trockenen Netzwerkerei passieren?

- Verwenden Sie USB-Sticks? Disketten? Einen Laptop, der auch hin und wieder außerhalb des geschützten Heimathafens angeschlossen wird? Das Böse muss nicht unbedingt über das Netz kommen.

- Wer die unbestreitbaren Vorteile der drahtlosen Verbindung nutzt und sich einen WLAN-Router anschafft, läuft damit auch Gefahr, via Funk von innen angegriffen zu werden. Ein mit WPA geschütztes WLAN gilt zwar derzeit noch als hinreichend sicher, muss aber auch entsprechend eingestellt werden.

- Noch schwerer sind die Sicherheitsrisiken von Bluetooth-Geräten zu beherrschen. Prinzipiell kommt sogar das Handy als Überträger in Betracht.

- Jede Fehlkonfiguration – und Fehler passieren nun mal – kann allen Schutz zunichte machen. Dagegen kann man sich am ehesten durch kompetente Beratung und Aufpassen schützen; hilfreich ist auch eine sichere Voreinstellung des Geräts beim Neukauf.

- *Universal Plug and Play* (UPnP) ist eine relativ neue Technologie, um die Technik einfacher zu machen. Mit UPnP kann, wenn der NAT-Router das erlaubt, jedes Programm auf der Innenseite den Router nach Belieben umkonfigurieren. Das mag in einigen Fällen zum gewünschten Ergebnis führen. Besonders nützlich ist es jedoch für allerlei Schadsoftware: Hat diese einmal den Weg in den PC im Kinderzimmer gefunden, kann sie gleich den gesamten Schutz aushebeln.

- Fehler in der Software von NAT-Routern können dazu führen, dass bestimmte Verbindungen fälschlich zugelassen werden.

- Wenn man sich entschließt, gewisse Dienste mittels Port Forwarding freizugeben, gibt man damit den Firewall-Schutz für diese Services auf dem betreffenden Rechner auf. Wird das zugänglich gemachte Service nicht hochprofessionell betrieben, sondern gibt sich eine Blöße, so ist der gesamte Firewall-Schutz dahin: Bereits ein privater Webserver, der unsichere Skripts aus dem Internet beherbergt (phpBB, PHP-Nuke und tausende mehr haben sich in dieser Hinsicht einen gewissen Ruf erworben), lässt sich dazu überreden, im Auftrag des Angreifers die Attacken von innen heraus vorzunehmen. Um die Analogie zu strapazieren: Ehe man sich's versieht, wird ein Hausbewohner selbst zum Vampir. Besondere Vorsicht ist bei Online-Spielen, Filesharing-Programmen etc. geboten, die bestimmte Firewall-Einstellungen benötigen: Es wäre verrückt anzunehmen, dass ausgerechnet diese Software den Ansprüchen eines sicheren Serverbetriebs genügt.

- In den meisten Fällen gelangt schädliche Software durch Verbindungen auf den PC, die von innen heraus angefordert – und somit stets erlaubt – sind: via eMail, über Webseiten, durch das Downloaden von Programmen oder vermeintlicher Musik- und Videodateien. Davor können Firewalls keinen Schutz bieten, da ja über eine erlaubte und ausdrücklich gewünschte Verbindung etwas transportiert wird, das der User rückblickend lieber doch nicht gewollt haben würde.

- Ist ein Rechner im privaten Netz erst einmal infiziert, kann ein NAT-Router die anderen nicht mehr vor ihm schützen. Daher müssen zur sicheren Konfiguration jedes Rechners dieselben Maßnahmen ergriffen werden, als wäre der Rechner ungeschützt im Internet. Wenn überhaupt, soll der NAT-Router ja eine *zweite* Verteidigungslinie sein. Die viel zu häufige Empfehlung, die Personal Firewall oder die XP-Firewall abzuschalten, ist also Nonsens. Auf keinen Fall darf man sich dazu verleiten lassen, den Virenscanner durch einen NAT-Router zu ersetzen: Ebensogut könnte man sich ein zweites Schloss an die Wohnungstür montieren, um sich vor der Grippe zu schützen.

All das gilt, da die Firewall-Funktionalität des NAT-Routers mit NAT nichts zu tun hat, übrigens ebenso für Firewalls. Eine Auflistung der Umstände, unter denen eine Firewall versagt, ist lang und nicht einmal vollständig. Sind Firewalls also überflüssig? Keineswegs! Firewalls und NAT-Router sollten allerdings von erfahrenen Experten als Werkzeug zur Realisierung eines umfassenden Sicherheitskonzepts eingesetzt werden und schützen dann vor etlichen Bedrohungen, aber eben nicht vor allen.[7] Sie verhindern vor allem, dass Dienste, die man eigentlich gar nicht anbieten wollte oder die noch nicht abgesichert wurden, von außen missbraucht werden. An zwei Beispielen lässt sich das gut zeigen:

- Im Jänner 2003 infizierte der Wurm *SQL Slammer* innerhalb von 10 Minuten weltweit rund 75 000 Rechner und sorgte für schwere Beeinträchtigungen im Internetverkehr. Der angegriffene Dienst, Microsofts SQL-Server, wird aber normalerweise nicht außerhalb des lokalen Netzes benötigt und hätte daher in den meisten Fällen gar nicht zur Verfügung stehen sollen. Tatsächlich wussten viele User überhaupt nicht, dass auf ihrem PC ein solches Service existiert, da es sozusagen als „Nebenwirkung" von anderen Produkten mitinstalliert wird. NAT-Router und Firewalls verhindern bei vernünftiger Konfiguration effektiv den Zugriff auf solche unbeabsichtigt angebotenen Dienste. Eine konsequente Ausstattung mit Firewalls (oder NAT-Routern oder Personal Firewalls) hätte die Angriffsfläche des Wurms auf die wenigen Rechner reduziert, die dieses Service tatsächlich anbieten müssen. Die Beeinträchtigung des Internet wäre marginal geblieben und der Wurm hätte keine Berühmtheit erlangt.

- Bei Windows-Rechnern mit Internet-Verbindung wird die Zeitspanne, die zwischen der Neuinstallation per CD und dem Einnisten des ersten Virus liegt, auf wenige Minuten geschätzt. Bevor also noch das erste Servicepack heruntergeladen werden kann, ist es schon zu spät. Eine Firewall oder ein NAT-Router schützt vor Angriffen auf ein noch nicht gesichertes System – vorausgesetzt, die anderen Rechner im lokalen Netzwerk sind „sauber".

Richard Mansfield als Dr. Jekyll und Mr. Hyde, ca. 1895 (Foto von Henry Van der Weyde, London)

Das Problem der multiplen Persönlichkeiten

Durch das Zusammenschalten mehrerer Computer mit einem NAT-Router, also durch die Verwendung derselben IP-Adresse, treten sie nach außen als ein Rechner auf – nur eben mit dissoziativer Identitätsstörung. Die Komplikationen, die sich daraus ergeben, sind immens (man denke nur an *Den seltsamen Fall des Dr. Jekyll und Mr. Hyde*[8]), und es dauert lange, bis die dadurch entstehenden Rätsel gelöst werden können. Genau das will man aber aus der Sicherheitsperspektive lieber vermeiden.

Wenn es nämlich passiert, dass sich ein hinter einem NAT-Router befindlicher Rechner ein Virus einfängt (er also mit Spam um sich wirft, andere Rechner attackiert usw.), dann sieht die ganze Welt die offizielle Adresse als den Schuldigen an. Dass sich mehrere Computer für einen ausgeben, kann von außen niemand erkennen – das war ja der Zweck der Übung –, und daher werden alle, auch die Unschuldigen, in einen Topf geworfen. Das hat im Krisenfall unangenehme Folgen:

- Die Wahrscheinlichkeit, dass „die IP-Adresse" unangenehm auffällt und sogar gesperrt wird, vervielfacht sich mit der Zahl der dahinter verborgenen Rechner.

- Wenn „die IP-Adresse" gesperrt wird, ist nicht nur der infizierte Rechner aus dem Verkehr gezogen, sondern auch alle anderen mit derselben Adresse.

- Im Falle von Problemen ist der wichtigste Schritt die schnelle Diagnose. Dank des Versteckspiels muss man hier den Patienten aber erst suchen gehen.

- Man weiß nicht einmal, ob lediglich ein Rechner betroffen ist oder ob auch die anderen bereits infiziert sind.

- Illegale Vorgänge – etwa das rechtswidrige Bereitstellen von urheberrechtlich geschützten Werken – können nicht mehr einem einzelnen PC zugeordnet werden. Ohne den Teufel an die Wand malen zu wollen: Es ist nur eine Frage der Zeit, bis die ersten Verfahren wegen Schadenersatz (vielleicht sogar einmal nach dem Strafrecht) gegen Netzbetreiber angestrengt werden, die keine Auskunft über den Täter geben.[9]

---

7) Für Institute der Universität Wien bietet der ZID die so genannte Institutsfirewall an (siehe *Comment 03/2*, Seite 17 bzw. unter `www.univie.ac.at/comment/03-2/032_17.html`).

8) Fachleute auf diesem Gebiet mögen eine gewisse psychologische Unschärfe verzeihen.

9) Ein Beitrag zu diesem Thema ist für die nächste Ausgabe des *Comment* geplant.

Auch in Friedenszeiten bringt die „Adressen-WG“ Nachteile mit sich. Mitunter werden bestimmte Dienste für einzelne handverlesene IP-Adressen freigeschaltet[10] in der Erwartung, dass der damit verbundene Rechner von einer Person benutzt wird, die entweder besonders vertrauenswürdig ist oder einer bestimmten Benutzergruppe angehört. Mit NAT gibt es zwei Szenarien: Entweder die Erlaubnis wird verweigert, um nicht Unberechtigte ebenfalls zuzulassen, oder – noch schlimmer – es werden versehentlich mehr Zugänge gewährt als beabsichtigt.

Was mit NAT nicht funktioniert

Das aus dem Security-Blickwinkel vielleicht prominenteste Opfer von NAT ist das IPsec-Protokoll.[11] Geht eine Verbindung über einen NAT-Router, so erkennt IPsec, dass die IP-Adressen und eventuell Port-Nummern verändert wurden, und weist sie daher konsequent zurück. Die Wahrnehmung dieser wirksamen NAT-Verweigerung ist aber: IPsec funktioniert nicht! IPsec lässt sich zwar in gewissen Spielarten auch mit NAT betreiben; dennoch haben diese Probleme dazu geführt, dass Microsoft in Windows XP mit dem Service Pack 2 die IPsec-Unterstützung für NAT-Umgebungen nachträglich abgestellt hat.[12]

Probleme gibt es außerdem mit allen Protokollen, bei denen die IP-Adresse in den Steuerinformationen vorkommt.[13] Das trifft zum Beispiel auf FTP (*File Transfer Protocol*) und SIP (das bei der IP-Telefonie verwendete *Session Initiation Protocol*) zu. Je nach Software des Routers helfen so genannte NAT-Helper: Sie klinken sich in den Datenstrom ein und übersetzen die darin enthaltenen Adressen. Bei Bedarf schalten sie auch weitere Verbindungen frei – beim Telefonieren wird beispielsweise über einen Steuerkanal das Gespräch vermittelt, die Töne werden aber über eine andere Verbindung transportiert. Die Gefahr dabei: Ist der NAT-Helper zu hilfreich, kann es vorkommen, dass er mit manipulierten SIP- oder FTP-Verbindungen dazu überredet wird, auch einmal einem Angreifer die Tore zu öffnen.

Bock oder Gärtner?

Nach diesen technischen Feinheiten zu einem ganz einfachen Gesichtspunkt: Ein NAT-Router ist eine zusätzliche Komponente im Netzwerk, die die Komplexität des Gesamtsystems erhöht. Es liegt auf der Hand, dass damit auch die Gefahr von Fehlern, zum Beispiel bei der Konfiguration des Ganzen, steigt.

Fehler kann aber auch der Hersteller gemacht haben. Mit etwas Pech ist der Router selbst angreifbar – wird er gehackt, so ist der, der für Sicherheit sorgen sollte, plötzlich der Angreifer. Das ist nicht weiter verwunderlich, immerhin sind NAT-Router auch nichts anderes als kleine Computer.

ADSL-Router bergen noch eine besondere Gefahr in sich: Sie kennen das Zugangspasswort ihres Benutzers – damit wählen sie sich ja ein. Wird der Router gehackt, liest der Angreifer wahrscheinlich auch das Passwort aus. Eine Variante davon, die schon in Richtung Fahrlässigkeit geht: Wenn der Router nicht mehr benötigt wird und im Mistkübel landet oder gar über eine Gebrauchtwarenbörse versteigert wird, wandert meistens das Passwort ebenfalls mit und kann mit nicht allzu großem Aufwand auch ausgelesen werden.

Der Mythos der Adressknappheit

Als in den 90er-Jahren der große Internet-Boom einsetzte, begann man sich Sorgen zu machen, dass es bald nicht mehr genug IP-Adressen geben könnte. Angesichts der Tatsache, dass theoretisch 4 294 967 296 verschiedene Adressen existieren, erscheint das schwer zu glauben. Tatsächlich gibt es aber beträchtlichen „Verschnitt“: Ein guter Teil des Adressraums ist für spezielle Zwecke vorgesehen; der Rest wird in Blöcken verteilt, die aus technischen und organisatorischen Gründen um einige Schuhnummern zu groß sind. Die aktuellen Prognosen deuten jedenfalls darauf hin, dass frühestens im nächsten Jahrzehnt die letzten Adressblöcke an die *Regional Registries* (z.B. an das RIPE NCC für Europa) vergeben werden. Diese haben den Schätzungen zufolge dann noch Reserven für ein weiteres Jahr.[14]

Bis auf Weiteres ist es also problemlos möglich, IP-Adressen in der benötigten Menge zu erhalten.[15] Die Notwendigkeit muss jedoch entsprechend dokumentiert werden, da die Registries eine gewisse Minimalauslastung der vergebenen Adressen sicherstellen müssen.[16] Zudem ist ein gewisses Minimalgewicht erforderlich: Die kleinste beim RIPE NCC erhältliche Verpackungseinheit umfasst 2048 Adressen. Den Detailvertrieb besorgen die Provider: Institute der Universität Wien erhalten die benötigten IP-Adressen vom ZID, während sich ACOnet-Teilnehmer (z.B. Studentenheime) dazu an ACOnet wenden können.

10) Eine „wasserdichte“ Maßnahme ist das nicht – zumindest ist es recht leicht, die IP-Adresse von einem Rechner zu übernehmen, der im selben LAN angebunden, aber abgeschaltet ist.

11) IPsec ist eine Erweiterung des IP-Protokolls um Methoden, welche die Authentizität und Integrität der IP-Pakete gewährleisten.

12) siehe *The default behavior of IPsec NAT traversal (NAT-T) is changed in Windows XP Service Pack 2* (`http://support.microsoft.com/kb/885407`)

13) siehe T. Hain: *Architectural Implications of NAT* (`http://ftp.univie.ac.at/netinfo/rfc/rfc2993.txt`)

14) siehe IANA, *Internet Protocol v4 Address Space* (`www.iana.org/assignments/ipv4-address-space`)

15) siehe RIPE NCC, *IPv4 Address Allocation and Assignment Policies for the RIPE NCC Service Region* (`www.ripe.net/ripe/docs/ipv4-policies.html`)

16) siehe Geoff Huston: *IPv4 – How long have we got?* (`www.ripe.net/info/info-services/ipv4/summary.html`) und *IPv4 Address Report* (`www.potaroo.net/tools/ipv4/index.html`)

Ottilie und Otto Normalverbraucher haben weniger Glück. Zwar ist es technisch möglich, auch über den heimischen Modem-, Kabel- oder ADSL-Anschluss jedem Familien- oder WG-Mitglied eine eigene Adresse zu spendieren. Dem steht aber ein beträchtlicher Verwaltungsaufwand gegenüber – das ist wohl auch der Grund, warum bei kommerziellen Providern diese Möglichkeit im Billigsegment keinen Einzug gefunden hat.

Stell dir vor, es ist IPv6 und keiner geht hin

Eine grundlegende Änderung bringt die nächste Version des Internet-Protokolls, IPv6, die das seit 1981 verwendete IPv4 nach einer langjährigen Phase der Koexistenz ablösen soll. Diese „Neuauflage" des Internet räumt mit zahlreichen unzeitgemäßen Eigenschaften auf, vor allem macht sie aber NAT überflüssig: Die in IPv6 verwendeten Adressen sind so großzügig ausgelegt, dass selbst normale Teilnehmeranschlüsse mehr Adressen zur Verfügung haben als heute das gesamte Internet.[17)]

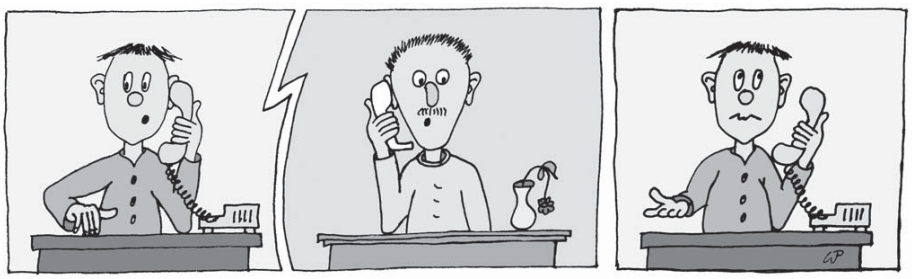
IPv6 ist keineswegs ein neues Protokoll.[18)] An der Uni Wien bzw. im ACOnet wurde mit dessen Einführung bereits im vorigen Jahrtausend begonnen, und seit einigen Jahren sind praktisch alle Betriebssysteme sowie die für die Netzwerkinfrastruktur benötigten Geräte in der Lage, mit IPv6 umzugehen. Seit Anfang 2005[19)] ist IPv6 im ACOnet-Backbone und an der Universität Wien im Produktionsbetrieb verfügbar; zahlreiche Services des ZID (Mailing, Nameservice, FTP-Server, ...) sind seit geraumer Zeit auch über IPv6 erreichbar.

ACOnet und die Uni Wien haben somit, wie es einem Forschungsnetz geziemt, die Pionierleistung bereits erbracht. Speziell im asiatischen Raum und aus dem Bereich der mobilen Endgeräte gibt es verstärktes Interesse an IPv6. Offenbar scheuen jedoch die großen kommerziellen Internet Service Provider und Content Provider den Sprung in eine neue Technologie, solange die alte so hervorragend funktioniert: Von rund 100 000 eMail-Nachrichten, die Tag für Tag die Uni Wien erreichen, werden sage und schreibe 500 über IPv6 transportiert. Die Mehrheit der Kristallkugeln ist sich jedoch einig, dass IPv6 sehr schnell kommen wird, sobald die IP-Adressen knapp werden.

Fazit

NAT-Router haben – gewissermaßen als Nebenwirkung – firewallähnliche Eigenschaften, mit denen sie vor Einbrüchen in verwundbare Dienste eines Rechners schützen können. In der Praxis ist aber das häufigere Problem, dass Viren und Trojaner über Webseiten oder eMail den Weg auf den PC finden. Davor schützt ein NAT-Router nicht; in diesem Fall erschwert er sogar die Problembehebung und ist damit aus der Sicherheitsperspektive in Summe kontraproduktiv.

Uni-Institute und ACOnet-Teilnehmer wie Universitäten, Studentenheime oder Schulen sollten sich auf keinen Fall auf das Himmelfahrtskommando NAT einlassen: Erstens erhalten sie leicht die benötigten Adressen und zweitens sind die mit NAT einhergehenden Gefahren umso größer, je höher die Teilnehmerzahl ist. Mit IPv6 steht die Lösung für den Tag, an dem die Adressen wirklich knapp werden, schon bereit. Es gibt also keinen Grund, mit IP-Adressen am falschen Platz zu sparen.



„Guten Tag, ACOnet-CERT hier. Von der IP-Adresse 192.0.2.34 werden Viren verschickt."

„Das ist unser NAT-Router, da hängen 300 PCs dran. Keine Ahnung, welcher das Virus hat!"

„Womit hab' ich das verdient?"

Cartoon von Peter Wienerroither

Für den Anschluss zu Hause bleibt, solange IPv6 nicht kommt, der NAT-Router wohl oder übel der einzige Weg zu einer flächendeckenden Anbindung an die Datenautobahn. Hier gilt es aber, die vorhandenen Sicherheitsfeatures zu nutzen, kein Port Forwarding für Spiele oder Filesharing einzurichten, UPnP abzuschalten – und vor allem keinem trügerischen Sicherheitsgefühl zu erliegen, sondern jeden Rechner abzusichern, als wäre er in der freien Wildbahn. Mit zwei oder drei gut gewarteten PCs hinter einem NAT-Router bleibt dann das Risiko in vertretbarem Rahmen.

Auch wenn „Security" auf der Verpackung steht und der Glaube an die schützende Wirkung dieser Wunderwerke noch so fest ist – eine Sicherheitslösung ist ein NAT-Router nicht. Der erste Hauptsatz der Security lautet nicht zu unrecht: *Sicherheit ist kein Produkt, sondern ein Prozess.*

Alexander Talos

---

17) Es sind mindestens 18 446 744 073 709 551 616 (= 2^{64}) Adressen pro Teilnehmer (siehe *RFC 3177*, `http://ftp.univie.ac.at/netinfo/rfc/rfc3177.txt`). Diesen Adressraum wird niemand auch nur annähernd ausschöpfen; er ermöglicht aber den Betrieb von einem oder mehreren Rechnern an jedem Anschluss bei völlig automatischer Konfiguration, ohne Konflikte wegen irrtümlich doppelt verwendeter Adressen befürchten zu müssen.

18) siehe Artikel *IPv6 – Das Internetprotokoll der nächsten Generation* in *Comment 03/1*, Seite 35 bzw. unter `www.univie.ac.at/comment/03-1/031_35.html`

19) siehe Artikel *IPv6 im Uni-Datennetz* in *Comment 05/1*, Seite 31 bzw. unter `www.univie.ac.at/comment/05-1/051_31.html`