FILESERVICES: WILLKOMMEN IN DER DATEN-BANK

An der Uni Wien neigen sich die Zeiten des „manuellen Datentransports“ ihrem Ende zu: Wollte man bestimmte Dateien (engl. *files*) auf verschiedenen PCs bearbeiten, so trug man noch vor wenigen Jahren Disketten mit sich herum; später waren es dann ZIP-Drives, Memory-Sticks, CDs und DVDs. Mit zunehmender Verbreitung des Internet wurden Dateien auch immer öfter per eMail verschickt. Wenn sie dafür zu umfangreich waren, kamen die eigentlich für den Dateitransfer vorgesehenen Übertragungsprotokolle (FTP, SSH) zum Einsatz – oder eben wieder externe Datenträger.

Heute reichen oft schon wenige Mausklicks, um über das Netzwerk auf eine Datei zuzugreifen und diese zu bearbeiten – vorausgesetzt, sie wurde zuvor am richtigen Ort gespeichert. Vergleichbar ist dies (in groben Zügen) mit Bankomaten bzw. Telebanking: Das Ersparte ist an einer sicheren Stelle deponiert, kann aber mittels Datennetz jederzeit abgerufen werden. Als „Hüter des Datenschatzes“ fungieren in der PC-Welt die so genannten Fileserver – Rechner, die rund um die Uhr via Internet erreichbar sind, die den BenutzerInnen eine bestimmte Menge an Speicherplatz für beliebige Daten zur Verfügung stellen und auf denen in der Regel auch eine professionelle Datensicherung betrieben wird.

Der Zugriff auf den persönlichen Speicherplatz am Fileserver erfolgt über ein spezielles Netzwerkprotokoll (SMB/CIFS; Näheres siehe Kasten auf Seite 25), mit dessen Hilfe die dort abgelegten Daten genau so verarbeitet werden können wie Daten, die am lokalen PC gespeichert sind. Eine Datei kann direkt am Fileserver gelesen, verändert, gespeichert, gelöscht, umbenannt oder neu angelegt werden; das Übertragen der Datei vom Server zum PC und retour geschieht unbemerkt hinter den Kulissen. Bei entsprechend schneller Netzwerkanbindung[1)] ist das *Look & Feel* exakt dasselbe wie beim Arbeiten mit lokal gespeicherten Daten: Nach dem Verbindungsaufbau erscheint der Fileserver als zusätzliches Laufwerk am Desktop und kann einfach mittels Doppelklick geöffnet werden.

Somit ist es beispielsweise möglich, eine am Institutsrechner oder in den PC-Räumen erstellte Datei problemlos zu Hause weiter zu bearbeiten. Auch wenn man bestimmte Dateien anderen Personen zukommen lassen möchte, bietet ein Fileserver einen technisch sinnvollen Ausweg: Anstatt eine Datei mehrfach über eMail zu versenden, speichert man sie im Unterverzeichnis `html` seines persönlichen Webspace (siehe Abschnitt *Die Fileservices des ZID*) und verschickt nur den entsprechenden URL – z.B. `www.unet.univie.ac.at/a0412345/wichtig.doc`. Die EmpfängerInnen können dann selbst entscheiden, ob bzw. wann sie die Datei herunterladen möchten.

Fileservices an der Uni Wien

Das Prinzip der Fileservices ist nicht neu. Auch an der Universität Wien gibt es seit langem viele dezentrale Fileserver, die jedoch meist nur für einen eng beschränkten Benutzerkreis verfügbar sind (z.B. die MitarbeiterInnen eines Instituts) und allzu oft von technisch interessierten AssistentInnen „nebenbei“ betreut werden müssen. Seit einiger Zeit existieren jedoch die technischen Rahmenbedingungen, um Fileservices auch für die gesamte Universität anzubieten:

- **Netzwerkbandbreite:** Wie oben erwähnt, benötigt man für die sinnvolle Verwendung der Fileservices eine entsprechende Netzwerkkapazität, die seit der Realisierung des Glasfaser-Backbones für das Universitätsdatennetz im Mai 2004 (siehe *Comment 04/3*, Seite 2) an praktisch allen Standorten der Uni Wien gegeben ist. Zudem verfügen inzwischen viele BenutzerInnen zu Hause über eine Breitband-Internetanbindung (z.B. uniADSL) und können die Fileservices somit auch von daheim verwenden.

- **Server-Architektur:** Ursprünglich wurden Unet- und Mailbox-Service jeweils auf einem einzelnen Rechner betrieben, der für alle angebotenen Dienste (eMail, Webspace, interaktives Arbeiten, ...) zuständig war. Erst seit der Aufteilung dieser „monolithischen“ Server auf mehrere Rechner, die jeweils nur ein bestimmtes Service abwickeln, kann die nötige Speicherkapazität und Betriebssicherheit gewährleistet werden, um auch für einen großen Benutzerkreis „Datenschließfächer“ anzubieten. Die Umstellung des Unet-Service erfolgte im August 2003 (siehe *Comment 03/2*, Seiten 8–14), die des Mailbox-Service im Mai 2004 (siehe *Comment 04/2*, Seite 18).[2)] In beiden Fällen kommt nun ein verteiltes Filesystem zum Einsatz. Bei Bedarf können daher problemlos zusätzliche Fileserver „zugeschaltet“ werden, ohne dass sich für die BenutzerInnen irgendwelche Änderungen in der Bedienung ergeben: Der Zugriff auf den Fileserver bleibt immer gleich, egal wie viele Rechner dahinter angeschlossen sind und auf welchem dieser Rechner sich die Daten tatsächlich befinden.

- **Client-Software:** Mit älteren Betriebssystemen erforderte der Zugriff auf Fileserver einige EDV-technische Klimmzüge und Kunstgriffe, die AnwenderInnen mit geringen

1) Von Modem- bzw. ISDN-Verbindungen ist in diesem Zusammenhang eher abzuraten: Vor allem beim Öffnen und Speichern von Dateien macht sich die geringe Bandbreite unangenehm bemerkbar.

2) Schon vor diesen Server-Umstellungen waren in eingeschränktem Ausmaß Fileservices verfügbar, die jedoch – ganz abgesehen von der noch eher umständlichen Bedienung – aus Kostengründen nur wenig Speicherplatz boten.

SMB/CIFS und Samba

CIFS (*Common Internet File System*) ist ein von Microsoft entwickeltes Netzwerkprotokoll, das hauptsächlich dazu verwendet wird, mehreren Rechnern in einem LAN den Zugriff auf Dateien zu ermöglichen. Auch andere Ressourcen wie Drucker können über CIFS angesprochen werden. CIFS stammt aus den frühen achtziger Jahren und wurde seither kontinuierlich weiterentwickelt. Die Nomenklatur der CIFS-Varianten ist sehr verwirrend – manche haben eigene Namen wie z.B. *PC NETWORK PROGRAM 1.0* oder *NT LAN Manager 1.0*. Auch der Name CIFS ist noch relativ neu; ältere Versionen wurden als SMB (*Server Message Block*) bezeichnet.

CIFS als Applikations-Protokoll definiert nur, wie auf Dateien zugegriffen wird, nicht die Details der Netzwerkverbindung: CIFS kann auf beliebige Netzwerk-Protokolle aufgesetzt werden. Heute werden dazu fast ausschließlich die Internet-Protokolle (TCP/IP) verwendet. Daher ist eine SMB/CIFS-Verbindung zu einem bestimmten Server zwar theoretisch aus dem gesamten Internet möglich, de facto sorgen jedoch die Firewalls der Internetprovider dafür, dass die Verbindung in der Regel auf das eigene LAN (*Local Area Network*) beschränkt bleibt.

Samba nennt sich ein Open Source-Projekt, das unter dem Motto *Opening Windows to a Wider World!* eine frei erhältliche SMB/CIFS-Implementierung für Unix, Linux und andere Plattformen entwickelt. Mit Hilfe dieser Software können Fileservices für Windows-PCs auch auf Servern mit Nicht-Windows-Betriebssystem angeboten werden. Mittlerweile enthält Samba auch Client-Funktionalitäten und ermöglicht damit z.B. Linux-Rechnern den Zugriff auf Windows-Fileserver. Nähere Informationen zu Samba finden Sie unter `www.samba.org`.

Vorkenntnissen kaum zumutbar waren. Seit Windows XP und MacOS X sind die benötigten Funktionen jedoch in das Betriebssystem integriert, und ihre Handhabung ist so einfach geworden, dass sie auch von ungeübten BenutzerInnen problemlos verwendet werden können.

- **VPN (*Virtual Private Network*)**: Die Fileserver des ZID sind aus dem gesamten Universitätsdatennetz (inklusive der Wählleitungszugänge und DSL-Anschlüsse) erreichbar. KundInnen eines anderen Providers – z.B. chello – wird der Zugriff jedoch aus netzwerktechnischen Gründen unter Umständen verwehrt; auch vom Urlaubsort oder von einer anderen Universität aus kann es Probleme geben. In diesen Fällen muss ein so genannter VPN-Tunnel aufgebaut werden: Mithilfe eines speziellen Programms („VPN-Klient“) erhält der PC für die Dauer der Verbindung eine IP-Adresse aus dem Adressbereich des Uni-Datennetzes sowie eine direkte, verschlüsselte Verbindung zum gewünschten Server. Seit einigen Monaten betreibt der ZID für die BenutzerInnen an der Uni Wien einen VPN-Server und bietet VPN-Klienten für Windows, MacOS, Linux und BSD/Solaris zum Download an (siehe `www.univie.ac.at/ZID/vpn/`), sodass auch diese Hürde nun ohne großen Aufwand bewältigt werden kann.

Die Vorteile der zentralen Fileserver des ZID liegen vor allem in der Verwendung qualitativ hochwertiger, redundant ausgelegter (alle Daten werden „gespiegelt“, d.h. auf zwei verschiedenen Festplatten so abgespeichert, dass bei Ausfall einer Platte kein Datenverlust entsteht) und somit weitgehend ausfallsicherer Hardware, in der professionellen Software-Wartung und in der automatisierten Datensicherung für das gesamte System: Die Daten aller Server werden jede Nacht auf Bänder gesichert. Sollte – aus welchen Gründen auch immer – tatsächlich einmal eine Datei verloren gehen, kann die zuletzt gespeicherte Version wiederhergestellt werden. Wenden Sie sich dazu bitte an den Helpdesk (siehe `www.univie.ac.at/ZID/helpdesk/`).

Die Fileservices des ZID

Der Zentrale Informatikdienst der Universität Wien betreibt derzeit Fileservices für folgende Systeme:

- **Unet:** Am Fileserver FS1.UNET.UNIVIE.AC.AT stehen für jede/n Studierende/n mit Unet-UserID 200 MB Speicherplatz („Webspace“) für beliebige persönliche Daten zur Verfügung. Die dort abgelegten Dateien finden Sie beim Login in den PC-Räumen auf Ihrer `H:`-Platte, beim SSH-Login auf dem Server LOGIN.UNET.UNIVIE.AC.AT in Ihrem Homedirectory. Eine Sonderstellung nimmt das Unterverzeichnis `html` ein, das für Ihre persönliche Homepage gedacht ist: HTML-Dokumente, Grafiken usw., die Sie in diesem Unterverzeichnis abspeichern, sind sofort im WWW unter der Adresse `www.unet.univie.ac.at/~a`*`Matrikelnummer`*`/` abrufbar.[3] Für den Verbindungsaufbau zum Fileserver ist als so genannter *Share-Name* (der Name des gewünschten Dienstes bzw. Verzeichnisses) die Unet-UserID `a`*`Matrikelnummer`* anzugeben.

- **Mailbox:** Für den Mailbox-Fileserver FS1.UNIVIE.AC.AT (der allen Uni-MitarbeiterInnen zur Verfügung steht) gilt im Allgemeinen dasselbe wie für Unet, jedoch mit vier wesentlichen Abweichungen: Als Mailbox-BenutzerIn erhalten Sie 500 MB Webspace[4], beim SSH-Login mit Ihrer Mailbox-UserID auf dem Login-Server LOGIN.UNIVIE.AC.AT liegen die Daten im Unterverzeichnis `fileserver`,

3) siehe `www.univie.ac.at/ZID/persoenliche-webseiten/`

der URL Ihrer persönlichen Webseite lautet `http://homepage.univie.ac.at/vorname.nachname/`, und als *Share-Name* benötigen Sie Ihre Mailbox-UserID (z.B. `musterm3`).

- **WWW-Server:** Die Fileservices am Webserver WWW.UNIVIE.AC.AT erleichtern das Publizieren von Instituts-Webseiten – das Übertragen der Daten vom bzw. zum Server entfällt, die HTML-Dateien können mit dem lokal installierten HTML-Editor bearbeitet werden, und alle Änderungen sind sofort im WWW sichtbar. Beim Verbindungsaufbau muss als *Share-Name* und als *Username* der für den jeweiligen Subserver vergebene Username verwendet werden.[5)]

- **SWD-Server:** Der Softwaredistributions-Server SWD.UNIVIE.AC.AT enthält lizenzpflichtige Standardsoftware sowie Gratis-Softwarepakete für Mailbox-BenutzerInnen (McAfee VirusScan, Microsoft Service Packs, StarOffice, i3v- und SAP-Klient u.a.). Die Fileservices am SWD-Server bieten Lesezugriff auf die verfügbaren Softwarepakete und damit in vielen Fällen eine komfortable Möglichkeit, die Software direkt über das Netzwerk zu installieren. Für den Zugang ist eine vorherige Authentifizierung mittels Mailbox-UserID unter `www.univie.ac.at/ZID/swd/` erforderlich. Beim anschließenden Verbindungsaufbau geben Sie als Fileserver-Name `swd.univie.ac.at` und als *Share-Name* den Kurznamen des gewünschten Produkts an (siehe `www.univie.ac.at/ZID/software-liste/`; für den Zugriff auf die Gratissoftware lautet der *Share-Name* `info`). Der *Username* ist bereits aus der Authentifizierung bekannt und muss nicht mehr eingetragen werden.

- **FTP-Server:** Analog zum SWD-Server werden auch am Server FTP.UNIVIE.AC.AT Fileservices angeboten, um einen komfortablen Zugriff auf die hier verfügbaren Freeware-, Shareware- und Open Source-Produkte zu ermöglichen. Der *Share-Name* lautet `ftp`; die Angabe des *Username* ist nicht erforderlich, da die Software-Archive auf dem FTP-Server ohne Zugangsbeschränkung für jeden frei erhältlich sind.[6)]

Darüber hinaus können am Fileserver **SHARE.UNIVIE.AC.AT** auf Wunsch auch gemeinsam nutzbare Verzeichnisse (*Shares*) für Institute oder Arbeitsgruppen eingerichtet werden. Entsprechende Hilfsprogramme zum „eigenhändigen" Anlegen und Verwalten solcher Gruppen-Lösungen sind in Vorbereitung, vorläufig erfolgt dies aber noch manuell durch die Systemadministratoren. Wenden Sie sich daher bei Interesse bitte an die eMail-Adresse `fileservices.zid@univie.ac.at`.

Des Rätsels Lösung: So geht's

Wie bereits erwähnt, benötigt man für den Verbindungsaufbau den Hostnamen des Fileservers und den so genannten *Share-Name*, der oft auch als *Freigabe* bezeichnet wird (für die Server des Zentralen Informatikdienstes finden Sie diese Angaben unter *Die Fileservices des ZID*). Zusätzlich müssen meist noch Username und Passwort für den Fileserver angegeben werden. Wenn sich Ihr Rechner innerhalb des Universitätsdatennetzes befindet, können Sie mit der nachfolgend beschriebenen Vorgangsweise auf die Fileserver zugreifen; von außerhalb – z.B. bei einer StudentConnect-Anbindung – müssen Sie in den meisten Fällen zuvor eine VPN-Verbindung herstellen (siehe *Fileservices an der Uni Wien* bzw. `www.univie.ac.at/ZID/vpn/`).

Bitte beachten Sie auch, dass die Verwendung von Fileservices ein gewisses „Ansteckungsrisiko" im Hinblick auf virenverseuchte Daten in sich birgt. Der Fileserver selbst ist zwar immun gegen die meisten Software-Schädlinge, die sich in Dateien verstecken können; ein mangelhaft geschützter PC kann jedoch durch ein unbedacht übertragenes, infiziertes Dokument schnell in Mitleidenschaft gezogen werden. Jede Kette ist nur so stark wie ihr schwächstes Glied – verwenden Sie daher unbedingt aktuell gehaltene Antivirenprogramme[7)] auf Ihren Rechnern!

MacOS X

Unter MacOS X versteckt sich der SMB/CIFS-Klient hinter der Funktion *Mit Server verbinden*: Klicken Sie im ***Finder*** auf das Menü ***Gehe zu*** und dann auf ***Mit Server verbinden***. Im nun erscheinenden Dialogfenster geben Sie unter *Server-Adresse* den Pfad **`smb://Fileserver-Name/Share-Name`** an (z.B. `smb://fs1.unet.univie.ac.at/a0412345`). Durch Klick auf das **+** neben dem Eingabefeld wird dieser Pfad in die Liste *Bevorzugte Server* übernommen und muss künftig nicht mehr eingetippt werden. Klicken Sie anschließend auf ***Verbinden*** und geben Sie im folgenden Fenster *Benutzername* und *Kennwort* für den Fileserver an (das Feld *Arbeitsgruppe/Domain* wird nicht benötigt). Nach Klick auf ***OK*** werden Sie mit dem Fileserver verbunden, und das entsprechende Symbol erscheint auf Ihrem Desktop.

---

4) Zusätzlich stehen für Mailbox-BenutzerInnen 100 MB Speicherplatz am Login-Server LOGIN.UNIVIE.AC.AT zur Verfügung, auf die jedoch nur mittels SSH bzw.Telnet zugegriffen werden kann (nähere Informationen dazu finden Sie unter `www.univie.ac.at/ZID/mailbox/umstellung.html#login`).

5) siehe `www.univie.ac.at/ZID/www/`

6) Bei Verwendung des Cisco-VPN-Klienten kann es unter manchen Betriebssystem-Versionen vorkommen, dass der Verbindungsaufbau zum FTP-Server nicht funktioniert. Die Ursachen dieses Problems konnten nicht vollständig geklärt werden; vermutlich handelt es sich um einen Programmfehler im Cisco-Klienten, der dadurch ausgelöst wird, dass der Server sowohl über IPv4 als auch über IPv6 erreichbar ist (siehe auch Seite 31). Es gibt jedoch eine Notlösung: Sollten Sie mit dem Hostnamen FTP.UNIVIE.AC.AT nicht ans Ziel gelangen, verwenden Sie bitte die IP-Adresse `131.130.1.72` anstelle des Hostnamens.

7) siehe Artikel *McAfee VirusScan – Ihr Goalkeeper im Einsatz gegen virale Offensiven* (*Comment 04/1*, Seite 21 bzw. `www.univie.ac.at/comment/04-1/041_21.html`)

MS-Windows

- Unter **Windows XP** und **Windows 2000** wird der Zugriff auf Fileserver mit Hilfe der Funktion *Netzlaufwerk verbinden* realisiert: Wählen Sie im Ordner ***Arbeitsplatz*** aus dem Menü ***Extras*** den Punkt ***Netzlaufwerk verbinden***. Es erscheint nun das entsprechende Dialogfenster, wo Sie unter *Laufwerk* ein beliebiges freies Lauf werk und unter *Ordner* den Pfad **`\\Fileserver-Name\Share-Name`** eintragen müssen (z.B. `\\fs1.unet.univie.ac.at\a0412345`). Wenn die Verbindung dauerhaft eingerichtet werden soll, aktivieren Sie zusätzlich die Option ***Verbindung bei der Anmeldung wiederherstellen***. Wählen Sie dann ***Verbindung unter anderem Benutzernamen herstellen*** und geben Sie anschließend Username und Passwort für den gewünschten Fileserver ein. Klicken Sie auf ***Fertig stellen***. Sobald die Verbindung hergestellt ist, erscheint das Symbol für das Netzlaufwerk auf dem Desktop und kann mittels Doppelklick geöffnet werden.

- Bei **Windows 98/ME** ist die Vorgangsweise komplizierter, da das nötige Klientenprogramm nicht in das Betriebssystem integriert ist. Der PC muss daher zuerst für die Verwendung von Fileservices konfiguriert werden. Eine Beschreibung finden Sie unter `www.univie.ac.at/ZID/anleitungen/fileservices-win98me/`.

- **Windows 95 und NT** sind in diesem Zusammenhang beinahe hoffnungslose Fälle – um Ihr Nervenkostüm zu schonen, sollten Sie hier auf die Verwendung von Fileservices verzichten und die Dateien mittels SSH/FTP vom bzw. zum Server übertragen. Dazu können Sie entweder ein spezielles SSH-/FTP-Programm benutzen – oder aber den Internet Explorer, indem Sie in dessen Adresszeile den URL **`ftp://username@servername`** eingeben. Direkte SSH-/FTP-Verbindungen zum Fileserver sind allerdings nicht möglich; Unet-BenutzerInnen müssen daher eine Verbindung zum Server LOGIN.UNET.UNIVIE.AC.AT, Mailbox-BenutzerInnen zum Server LOGIN.UNIVIE.AC.AT aufbauen, um auf die Daten am Fileserver zuzugreifen. Die hier beschriebene Methode mittels Internet Explorer funktioniert mit diesen beiden Servern sowie mit dem Server WWW.UNIVIE.AC.AT, nicht jedoch mit dem SWD-Server. Am FTP-Server wird kein Username benötigt, daher lautet der URL in diesem Fall `ftp://ftp.univie.ac.at/`.

Linux

Unter Linux muss ein Samba-Klient installiert sein, was bei den meisten Linux-Distributionen der Fall ist (ansonsten kann der Quellcode unter `www.samba.org` bezogen werden). Der Zugriff auf den Fileserver erfolgt mit dem Befehl
`mount -t smbfs -o username=Ihr-Username,password=Ihr-Passwort //Fileserver-Name/Share-Name /lokaler/Pfad`
(z.B. `mount -t smbfs -o username=a0412345,password=xyzabc //fs1.unet.univie.ac.at/a0412345 /mnt`).

Fazit

Auch wenn der Dateitransfer zwischen verschiedenen Rechnern mittlerweile auf vielerlei Arten vor sich gehen kann: Ein modernes Betriebssystem und eine schnelle Netzwerkanbindung vorausgesetzt, bieten Fileservices beim heutigen Stand der Technik sicherlich die bequemste Möglichkeit zur „Mobilisierung“ und gleichzeitigen Sicherung größerer Datenmengen.

Elisabeth Zoppoth ■

ENUM: Eine Nummer Und Mehr

Telefonie und Internet verbünden sich

ENUM (*Electronic NUmber Mapping*) ist eine relativ neue Technik, um in einer global erreichbaren Datenbank zu Telefonnummern die zugehörigen Internet-Kontaktadressen – z.B. Internet-Telefonanschluss, eMail-Adresse – abzuspeichern. Der Besitzer einer Rufnummer kann somit unter dieser Nummer auf verschiedenen Wegen erreicht werden. Die Möglichkeiten, die ENUM bietet, reichen von der vereinfachten (weil Rufnummer-basierten) Anwahl von IP-Telefonen über die Fax-Umleitung an Mailadressen bis zum gebührenfreien Telefonieren via Internet. Ob und wie schnell sich diese Technologie weltweit etablieren kann, wird die nähere Zukunft zeigen: Die erste ENUM-Registrierungsstelle wurde im Dezember 2004 in Betrieb genommen – in Österreich, was auch der Anlass für den vorliegenden Artikel ist.

Internationale Entwicklung

Als John Perkins im Oktober 1999 anregte, mittels einer globalen Datenbank die Rufnummern von Faxgeräten mit den entsprechenden eMail-Adressen zu verknüpfen, um ein Fax unter derselben Telefonnummer auch an eine Mailbox versenden zu können, wurde er an die soeben gegründete *ENUM Working Group* der IETF [1)] verwiesen. Er schrieb als erster an die neu eingerichtete Mailingliste dieser Arbeitsgruppe und machte diesen guten Vorschlag, kam aber leider mit seiner Idee zu spät: In einschlägigen Kreisen wurde sie längst diskutiert. Bereits im August 1998 hatte Patrik Fältström im Rahmen eines BOF-Treffens [2)] empfohlen, das *Domain Name System* (DNS) – eine weltweit verteilte, hier-

archische und vor allem tadellos funktionierende Datenbank für die automatische Umwandlung von Hostnamen in IP-Adressen – auch für solche Zwecke zu verwenden. Auf diesem Vorschlag gründete schließlich auch die Zielsetzung der ENUM-Arbeitsgruppe, nämlich die Definition eines DNS-basierten Systems zur Verknüpfung einer Telefonnummer mit einer Reihe von Attributen (z.B. URIs[3]), die es ermöglichen, unter dieser Rufnummer auch Internet-Services zu erreichen.

Ausgehend vom allseits bekannten E.164-Nummernschema der ITU-T[4] für global erreichbare Telefonnummern entwickelte die ENUM-Arbeitsgruppe ein Regelwerk, wie mithilfe spezieller DNS-Einträge – der so genannten *NAPTR*- und *SRV-Resource Records* – aus einer E.164-Telefonnummer die korrespondierenden Server-Adressen für Internet-Dienste eruiert werden können.[5] John Perkins' Idee wurde also verwirklicht und ist jetzt im Detail so gelöst: Ein ENUM-taugliches Endgerät führt im DNS eine NAPTR-Abfrage nach der in einen Domainnamen umgewandelten Telefonnummer durch, filtert aus allen Antworten jene heraus, die das gewünschte Service betreffen, und extrahiert aus diesen wiederum die entsprechenden URIs. Nun kann es mit den dahinter liegenden Servern Verbindung aufnehmen, um z.B. ein Fax an eine eMail-Adresse weiterzuleiten.

ENUM-Features

Die einzigen Schriftzeichen, die fast überall auf der Welt gelesen und verstanden werden können, sind die zehn arabischen Ziffern. Diese haben außerdem den Vorteil, dass sie auf jeder Telefon- und Computertastatur zu finden sind, unabhängig vom jeweils verwendeten Zeichensatz. ENUM ermöglicht es also, verschiedene Kommunikationsdienste mit Hilfe einer simplen Zahlenfolge – nämlich der gewünschten E.164-Rufnummer – zu adressieren. Vor allem bei Endgeräten, mit denen die Eingabe alphanumerischer URLs schwierig oder unmöglich ist, bringt dies Erleichterungen. So ist es beispielsweise sicherlich einfacher, eine WAP-Seite mittels Handy abzurufen, wenn man anstelle des URLs nur die entsprechende Telefonnummer eintippen muss.

ENUM – das Akronym

Ursprünglich (laut BOF-Protokoll vom August 1998) steht ENUM für ***E**.164 **NU**mber to IP Address **M**apping*. Da mögliche Telefonnummern aber auch abseits der E.164-Norm existieren, verstand man ENUM bald als Abkürzung für *T**E**lefon **NU**mber **M**apping*. Einerseits störte nun, dass das Akronym nicht mit dem Anfangsbuchstaben des ersten Wortes beginnt, andererseits deckt ENUM mehr als nur Telefonie ab. So wurde eine neue Deutung gesucht und auch gefunden: ***E**lectronic **NU**mber **M**apping*.

Das primäre Einsatzgebiet für ENUM ist jedoch die Internet-Telefonie mittels *Voice over IP* (VoIP). VoIP-Terminals müssen normalerweise mit URIs der Form `sip:user@sipgateway.domain.tld` angewählt werden. Dank ENUM kann dafür nun auch eine normale Telefonnummer verwendet werden, was insbesondere bei IP-Telefonen hilfreich ist, die nur mit einer Telefontastatur (10 Ziffern mit `*` und `#`) ausgestattet sind. Weiters sind VoIP-Terminals dadurch theoretisch auch aus dem normalen Telefonnetz erreichbar – vorausgesetzt, der Telefon-Provider sorgt dafür, dass Gespräche aus dem Telefonnetz in das Internet weitergeleitet werden.

Darüber hinaus bietet ENUM folgende Möglichkeiten:

- Gebührenfreies Telefonieren via Internet: Die Verbindung zwischen zwei „klassischen" Telefonanlagen mit IP-Anschluss wird über das Internet hergestellt, wenn die Anlage des Anrufers ENUM-tauglich ist und die angewählte Rufnummer eine ENUM-Registrierung aufweist. Dadurch entfallen die Telefongebühren, was vor allem für größere Firmen bzw. Organisationen eine immense Kostenersparnis bringen kann.

- Umleitung von SMS und Fax an eMail-Postfächer: Das kann einerseits aus dem Telefonnetz eine Zusatzfunktion sein, wie sie z.B. beim Pilotprojekt AT43 (siehe `www.at43.at`) für Faxe verwirklicht ist. Andererseits können Internet-Programme ENUM-Einträge auch direkt auswerten und somit z.B. ein eingescanntes Fax-Bild direkt an die gewünschte eMail-Adresse versenden.

- Mit Hilfe der NAPTR-Einträge ist es in ENUM möglich, Prioritäten für die Verbindungsaufnahme zu setzen – z.B.

---

1) IETF, die *Internet Engineering Task Force* (`www.ietf.org`), ist das Standardisierungs-Gremium im Internet.

2) BOF ist das Akronym für den Anfang des Reimes ***B**irds **O**f a **F**eather Flock Together*. Im IETF-Umfeld bezeichnet es ein Treffen von am selben Thema interessierten Personen: Bereits vor der Einrichtung einer Arbeitsgruppe schwärmen diese in Konferenzpausen aus, um einen Platz zu finden, wo in Ruhe über das Thema gesprochen werden kann.

3) Ein URI (*Uniform Resource Identifier*) ist ein einfaches und erweiterbares System, um eine Ressource im Netzwerk zu kennzeichnen. Untergruppen davon sind z.B. URLs (*Uniform Resource Locators*; eindeutige Bezeichnungen, die Typ und Standort eines Objekts beinhalten – z.B. Webadressen) und URNs (*Uniform Resource Names*; eindeutige Objektnamen ohne Inhalts- und Lokations-Information – z.B. ISBN, die *International Standard Book Number*).

4) Das E.164-Nummernschema basiert auf einem geografisch orientierten, hierarchischen Aufbau der Rufnummern mit Ländercodes für die einzelnen Staaten (z.B. +43 für Österreich) und Ortsvorwahlen. ITU-T steht für *International Telecommunication Union – Telecommunication Standardization* (`www.itu.int/ITU-T/`). Es handelt sich dabei um das in Genf beheimatete ehemalige CCITT (*Comité Consultatif International Télégraphique et Téléphonique*), das Pendant zum IETF in der Telefonie.

5) Details dazu finden Sie u.a. in den RFCs 2396, 3401 – 3404, 3761, 3762, 3764 und 3861 (`http://ftp.univie.ac.at/netinfo/rfc/`).

Rufe mich zuerst am Internettelefon an; wenn ich dort nicht erreichbar bin, versuche es am Festnetz; sollte das scheitern, so versuche es am Handy. Andererseits kann man auch alle Anschlüsse gleichzeitig ansprechen lassen, d.h. sowohl Internettelefon als auch Festnetzanschluss und Handy läuten, wenn die entsprechende Nummer angerufen wird. Ein Problem ist allerdings, dass diese Logik auch in den Endgeräten implementiert sein muss; es gibt also keine Garantie für diese Funktionalität. Eine Fehlersuche kann sich demnach entsprechend kompliziert gestalten.

ENUM in Österreich

In Österreich fanden im September 2001 erste Gespräche zu diesem Thema bei der Rundfunk und Telekom Regulierungs-GmbH (RTR) statt. Zur selben Zeit etablierte die Telekom Austria zusammen mit der Österreichischen Fernmeldetechnischen Entwicklungs- und Förderungsgesellschaft (ÖFEG) eine interne *ENUM Task Force*. Besonders hervorzuheben ist dabei eine Person, die sowohl national die treibende Kraft als auch international wesentlich an der Entwicklung von ENUM beteiligt war: Richard Stastny von der ÖFEG. Er war es, der schon sehr früh die vielen Vorteile dieses Konzepts erkannte – z.B. dass ENUM rasch und mit geringem Risiko realisiert werden kann, da es auf relativ simplen technischen Standards basiert und die erforderliche Infrastruktur im Wesentlichen bereits vorhanden ist.

Im Februar 2002 gab es zu diesem Thema einen ersten Workshop; die daran teilnehmenden Firmen (Alcatel, Infonova, Kapsch, nic.at mit Mitarbeitern des ZID[6)], ÖFEG, RTR, Telekom Austria und Siemens) definierten und starteten einen *ENUM Trial* mit ca. 500 TeilnehmerInnen. In diesem Rahmen wurden die Möglichkeiten bzw. Problembereiche von ENUM und den DNS-Abfragen im Telefoniebereich getestet, wobei man besonderes Augenmerk auf die Registrierung und Validierung der Telefonnummern legte. Als notwendige Voraussetzung dafür wurde im Mai/Juni 2002 die österreichische ENUM-Subdomain `3.4.e164.arpa` eingerichtet (Näheres zu ENUM-Domains siehe weiter unten). Im September 2002 war es dann soweit: Die ersten Telefonnummern wurden registriert und waren nun mit ENUM-tauglichen Geräten bzw. Programmen (z.B. dem frei erhältlichen SIP-Klienten X-Lite für IP-Telefonie mittels Computer; siehe `www.xten.com`) auch via Internet erreichbar. Im Dezember 2003 wurde schließlich ein umfassender österreichischer Testbetrieb gestartet, an dem sowohl KundInnen mit Festnetz- als auch mit Mobilnetz-Rufnummern teilnehmen konnten. Die einzige Voraussetzung war ein Eintrag im öffentlichen Telefonbuch, weil die Anmeldedaten zu Validierungszwecken mit jenen im Telefonbuch verglichen werden mussten.

Die äußerst positiv verlaufenden ENUM-Tests, die auch international große Beachtung fanden, veranlassten die RTR, einen Regelbetrieb ins Leben zu rufen. Mit der Abwicklung der österreichischen ENUM-Registry wurde die neu gegründete Firma enum.at (`www.enum.at`), eine Schwestergesellschaft der nic.at, beauftragt. Die bewährte Zusammenarbeit zwischen dem ZID der Uni Wien und nic.at fand auch hier ihren Niederschlag, und so wurden Teile der technischen Voraussetzungen für ENUM – nämlich die Registry-Software und das Einrichten und Betreiben der DNS-Infrastruktur – durch Mitarbeiter des Zentralen Informatikdienstes verwirklicht. Am 9. Dezember 2004 nahm in Österreich die weltweit erste ENUM-Registrierungsstelle den kommerziellen Betrieb auf.

ENUM-Registrierung

Für die im Zusammenhang mit ENUM registrierten Telefonnummern ist im globalen DNS ein eigener Namensbereich definiert: `e164.arpa`.[7)] Damit die Übereinstimmung zwischen Telefonnummern und ENUM-Registrierungen langfristig sichergestellt werden kann, wurde die Verantwortung für die Domainvergabe in der Zone `e164.arpa` in drei hierarchische Stufen (so genannte *Tiers*) geteilt:

- **Tier 0** – die höchste Autorität – ist derzeit für alle Staaten das RIPE NCC[8)] in Amsterdam. Das RIPE NCC delegiert in Zusammenarbeit mit dem ITU-T TSB (*Telecommunication Standardization Bureau*) Subdomains für die einzelnen Landesvorwahlen (z.B. `3.4.e164.arpa` für Österreich) an den Tier 1.

- **Tier 1** ist eine von der jeweiligen Regierung ermächtigte, nationale Organisation (in Österreich: RTR), welche die Regeln für die Vergabe von ENUM-Domains in der jeweiligen Landeszone definiert und dann die Registrierung der einzelnen Telefonnummern an den Tier 2 delegiert.

- Als **Tier 2** und somit als Ansprechpartner für die EndkundInnen fungieren ENUM-Registrare. Diese sind dafür verantwortlich, dass die betreffende Telefonnummer korrekt im DNS registriert wird. Um eine E.164-Telefonnummer (das ist die vollständige Rufnummer mit führendem Pluszeichen und Landesvorwahl – für die Universität Wien z.B. `+43 1 4277`) in einen gültigen ENUM-Domainnamen umzuwandeln, geht man wie folgt vor:
  1. Alle Nichtziffernzeichen werden entfernt:
     `4314277`
  2. Die Reihenfolge der Ziffern wird umgekehrt:
     `7724134`

---

6) Die *nic.at Internet Verwaltungs- und Betriebsgesellschaft m.b.H.* (`www.nic.at`) führt die Vergabe und Verwaltung von Domains innerhalb der `.at`-Topleveldomain durch. Der Zentrale Informatikdienst der Uni Wien ist dabei für die technische Entwicklung und den Betrieb des Registry-Service verantwortlich.

7) Die Topleveldomain `.arpa` (*Address and Routing Parameter Area*) wird ausschließlich für die Internet-Infrastruktur verwendet (Reverse DNS für IPv4 und IPv6, ENUM).

8) Das RIPE (*Réseaux IP Européens*) NCC (*Network Coordination Centre*) ist eine von weltweit vier *Regional Internet Registries* (RIRs) und u.a. für die Verwaltung von IP-Adressen im Großraum Europa und Nordafrika verantwortlich (siehe `www.ripe.net`).

3. Nach jeder Ziffer wird ein Punkt eingefügt:
   `7.7.2.4.1.3.4.`
4. Das Ergebnis wird mit `e164.arpa` ergänzt:
   `7.7.2.4.1.3.4.e164.arpa`

Wenn man also seine Telefonnummer registrieren lassen möchte, muss man sich an einen nationalen ENUM-Registrar wenden. Dieser trägt den nach obigem Schema gebildeten Domainnamen in das DNS ein und fügt die entsprechenden *NAPTR-* bzw. *SRV-Resource Records* für alle Services an, die unter dieser Telefonnummer erreichbar sein sollen. Um beispielsweise an die Rufnummer der Universität Wien gerichtete eMail-Nachrichten zur Mailadresse `helpdesk.zid@univie.ac.at` umzuleiten, wird folgender NAPTR-Eintrag benötigt:

```
7.7.2.4.1.3.4.e164.arpa. IN NAPTR 10 10
"u" "E2U+email" "!^.*$!mailto:helpdesk.zid@
univie.ac.at!" .
```

Festnetz- und Mobilnetz-Rufnummern sind bereits an bestimmte (juristische oder natürliche) Personen vergeben. Deswegen dürfen diese Nummern nur im Auftrag der entsprechenden Person registriert werden. Diese muss den Besitz dieser Rufnummer nachweisen, wobei derzeit als Validierungskriterium die Telefonrechnung (bei Festnetz-Rufnummern) bzw. eine Antwort-SMS (bei Mobilnetz-Nummern) verwendet wird. Nachdem sich die Zuweisungen solcher Telefonnummern ändern können, muss der Besitznachweis für die registrierte Rufnummer in regelmäßigen Abständen neuerlich erbracht werden; nach der Revalidierung kann die Nummer weiter für ENUM-Services genutzt werden.

Ein Spezialfall sind Rufnummern, die in einem für Internet-Telefonanschlüsse reservierten Nummernbereich liegen. Internet-Telefone haben weder einen festen Bezug zu einer geografischen Adresse, noch sind sie Mobilnetz-Nummern im herkömmlichen Sinn. Aus diesem Grund wurden für solche Anschlüsse eigene Nummernbereiche freigegeben – einerseits von der ITU-T die internationale Vorwahl +87810, andererseits von der RTR die nationale Vorwahl +43780. Nummern in diesen Zonen werden gemeinsam mit der entsprechenden ENUM-Registrierung vergeben; das bei Festnetz- und Mobilnetz-Rufnummern bestehende Revalidierungsproblem taucht daher in diesen Fällen nicht auf.

Eine Liste österreichischer ENUM-Registrare finden Sie unter `www.enum.at/`. Zur Zeit haben alle Registrare ein einheitliches Preisschema für eine ENUM-Registrierung, nämlich € 1,– pro Monat zuzüglich der Validierungskosten (€ 25,– für die erstmalige Validierung und je € 5,– für die halbjährlichen Revalidierungen). Daraus ergibt sich für Festnetz- und Mobilnetz-Rufnummern ein Gesamtpreis von € 42,– inkl. USt für das erste Jahr und € 22,– inkl. USt für jedes folgende Jahr.

ENUM-Links

Deutschland	`www.denic.de/de/enum/`
IETF	`www.ietf.org/html.charters/enum-charter.html`
ITU-T	`www.itu.int/osg/spu/enum/`
NetNumber	`www.netnumber.com`
NeuStar	`www.enum.org`
Österreich	`www.rtr.at/enum/`, `www.enum.at`
RIPE NCC	`www.ripe.net/enum/`
Schweiz	`www.bakom.ch/de/telekommunikation/numad/internet/`
US ENUM Forum	`www.enumf.org`

Ausblick

ENUM ermöglicht mit geringen Investitionen einen beträchtlichen Mehrwert durch die globale Verfügbarkeit. Die Technologie stößt weltweit auf entsprechendes Interesse: In einer ganzen Reihe von Staaten laufen zur Zeit ENUM-Tests, um einen kommerziellen ENUM-Betrieb vorzubereiten; Deutschland beispielsweise will noch heuer damit beginnen.

Eine interessante Idee ist, ENUM auch für das Routing von Telefonnummern und für die Rufnummernmitnahme in der Telefonie einzusetzen (*Line Number Database: Welcher Telefonprovider ist für welche Nummer zuständig?*). Zumindest in letzterem Bereich könnte ENUM Konkurrenz bekommen: Die EU-Kommission beauftragte das ETSI (*European Telecommunications Standards Institute*; `www.etsi.org`) mit der Entwicklung einer Lösung für das Problem der Nummernportabilität. Als Antwort präsentierte dieses das Konzept eines so genannten *Universal Communications Identifier* (UCI), der in technischer Hinsicht viele Ähnlichkeiten mit ENUM aufweist, allerdings noch auf einige Feinheiten der Telefonie Rücksicht nimmt. Der augenscheinlichste Unterschied ist, dass mit UCIs alle Daten zu einer Telefonnummer (z.B. Gateways) nicht öffentlich abrufbar sind, sondern in eigenen, nur den Telekom-Konzernen zugänglichen Datenbanken gespeichert werden. Das kommt jenen Kritikern von ENUM entgegen, die befürchten, dass die ENUM-Daten aufgrund ihrer Öffentlichkeit von Spammern als Adress-Quelle missbraucht werden; bei der UCI-Lösung stehen die Daten aber für IP-Telefone wieder nicht zur Verfügung.

Mit ENUM ist es erstmals gelungen, eine definierte Grundlage für das Zusammenwirken von IP-Telefonie und „klassischer" Telefonie zu schaffen. Auch wenn ENUM vielleicht nicht alle Finessen abdeckt, die sich Techniker aus Telekom-Unternehmen wünschen – die pragmatische Vorgangsweise des IETF, simple und einfach zu realisierende Lösungen zu standardisieren, war bis jetzt erfolgreich und schafft die Basis dafür, dass Software- und Hardwarehersteller ENUM implementieren und dieser Technologie zum Erfolg verhelfen.

Andreas Papst ■

IPv6 im Uni-Datennetz

Der Zentrale Informatikdienst der Uni Wien ist bereits seit einigen Jahren an einer Reihe von Forschungs- und Pilotprojekten beteiligt, die sich mit dem Thema IPv6 beschäftigen.[1] Nachdem diese Tests weitgehend abgeschlossen sind, ist es nun an der Zeit, auf Basis der gewonnenen Erfahrungen IPv6 im Datennetz der Universität regulär einzusetzen. (Zur Beruhigung: Es handelt sich dabei um eine Erweiterung des Datennetzes, die keine Auswirkungen auf die bestehende IPv4-Infrastruktur hat. Für Institute bzw. AnwenderInnen, die an IPv6 nicht interessiert sind, ergeben sich daher keinerlei Änderungen.)

Adressen

Eine IPv6-Infrastruktur erfordert in erster Linie IPv6-Adressen für die einzelnen Rechner. Um zukünftig alle Internet-Services des ZID auch über IPv6 anbieten zu können, musste für die Uni Wien ein ausreichend großer Adressbereich reserviert werden. Die Internet-Standards[2] sehen hier für jeden Endkunden (auch für jeden Heimanwender mit Internetanbindung über Modem/ISDN, Kabel oder DSL) ein so genanntes */48-Prefix*[3] vor. Aufgrund ihrer rund 13000 Fernzugänge bekam die Universität Wien im Sommer 2004 den Adressbereich **`2001:62a::/31`** zugewiesen, aus dem der Bereich **`2001:62a:4::/48`** für das reguläre Datennetz (LAN) der Universität verwendet wird. Nachdem die wichtigsten Netzwerkkomponenten im Uni-LAN bereits IPv6 unterstützen, kann somit die gesamte Universität mit einer IPv6-Internetanbindung versorgt werden. Dies erfolgt über dieselbe LAN-Infrastruktur, über die auch IPv4 betrieben wird (*Dual Stack*). Dadurch ist es ohne zusätzliche Hardware möglich, Rechner gleichzeitig mit IPv4 und IPv6 zu versorgen.

Klienten

Die Zuweisung von IPv6-Adressen an die Arbeitsplatzrechner erfolgt derzeit mittels *Stateless Autoconfiguration*. Diese Methode wird inzwischen von allen gängigen Betriebssystemen unterstützt und hat den Vorteil, dass die Verteilung sehr einfach und ohne manuelle Konfigurationsänderungen des PCs funktioniert (*Plug & Play*). Die auf solche Weise vergebenen IPv6-Adressen werden nach der Norm EUI64 gebildet und enthalten daher auch die MAC-Adresse des jeweiligen Rechners, was die Fehlersuche bei Problemen erheblich erleichtert. Einzig die Eintragung von DNS-Namen zu den IPv6-Adressen ist bei Arbeitsplatzrechnern auf Grund des administrativen Aufwands derzeit nicht vorgesehen.

Zu beachten ist, dass sehr viele Internet-Applikationen IPv6 bevorzugen, sobald dieses Protokoll am betreffenden PC aktiviert wurde. Das kann mitunter zu Fehlern führen, wenn die Zieladresse nur über IPv4 erreichbar ist. Für erste Versuche mit IPv6 steht das Datentankstellen-Netz des ZID zur Verfügung (siehe `www.univie.ac.at/ZID/pns/`). In diesem Netz erhält man – ebenfalls über *Stateless Autoconfiguration* – neben einer IPv4- auch eine IPv6-Adresse zugewiesen und kann nach erfolgter Anmeldung die IPv6-Verbindung ins Internet testen.

Server des ZID

Der erste Schritt beim Aufbau eines IPv6-Netzwerks ist es, das Nameservice (DNS, siehe `www.univie.ac.at/ZID/dns/`) IPv6-fähig zu machen. Dies umfasst neben dem Eintragen von IPv6-Adressen in das DNS – was ausschließlich von der Software der Nameserver abhängig ist und auf allen DNS-Servern des ZID bereits seit geraumer Zeit unterstützt wird – auch die Erreichbarkeit der Nameserver via IPv6. Letzteres wurde sowohl für die Nameserver der Uni Wien als auch für zwei DNS-Server der `.at`-Topleveldomain im Sommer 2004 realisiert. Diese Nameserver sind seither unter folgenden IPv6-Adressen erreichbar:

- für `.at`:
  NS2.UNIVIE.AC.AT `2001:628:453:4302::53`
  NS-US1.NIC.AT `2001:4f8:4:b::202`

- für die Domain `univie.ac.at` (mit allen Subdomains):
  NS3.UNIVIE.AC.AT `2001:62a:4:303::53`
  NS4.UNIVIE.AC.AT `2001:62a:4:304::53`
  NS5.UNIVIE.AC.AT `2001:628:402:1:204:acff:fede:2319`

Die Server NS3.UNIVIE.AC.AT und NS4.UNIVIE.AC.AT sind innerhalb des Uni-LAN auch als rekursive Nameserver über IPv6 verwendbar. Damit ist für IPv6-fähige Rechner im Datennetz der Universität Wien im Prinzip keine parallele IPv4-Verbindung mehr nötig; alle Schlüsselfunktionen des Netzwerks werden von der IPv6-Infrastruktur unterstützt.

Nachdem nun alle wesentlichen Grundvoraussetzungen für den Betrieb von IPv6 gegeben sind, wird der ZID sukzessive alle Services, bei denen dies möglich ist, auch über das neue Protokoll anbieten. Bereits seit Sommer 2004 ist der Server FTP.UNIVIE.AC.AT über IPv6 erreichbar. Seit November 2004 verfügen auch die drei primären Mail-Exchanger für die `univie.ac.at`-Adressen über eine IPv6-Verbindung. Dadurch können von außen einlangende eMail-Nach-

---

1) Hintergrundinformationen zu IPv6 und den entsprechenden Projekten des ZID finden Sie im Artikel *IPv6 – Das Internetprotokoll der nächsten Generation* (*Comment 03/1,* Seite 35 bzw. unter `www.univie.ac.at/comment/03-1/031_35.html`).

2) siehe RFC 3177 (`http://ftp.univie.ac.at/netinfo/rfc/rfc3177.txt`)

3) Das sind 1.208.925.819.614.629.174.706.176 (= 2^{80}) IP-Adressen.

richten auch via IPv6-Transport zugestellt werden, was sich dann in der entsprechenden `Received:`-Zeile des Mail-Headers widerspiegelt – z.B.:

```
Received: from erasmus.terena.nl
(TERENA-tunnel-ipv6.Customer.surf.net
[IPv6:2001:610:ff:5::2])
by mx1.univie.ac.at (8.12.10/8.12.10) with
ESMTP id j0I8wNdT032167;
Tue, 18 Jan 2005 09:58:25 +0100 (CET)
```

IPv6 für Institute

In Instituts-Subnetzen kann IPv6 auf Wunsch des jeweiligen Instituts aktiviert werden. Die technischen Voraussetzungen hierfür sind im Wesentlichen dieselben wie für die Institutsfirewall und das DHCP-Service (siehe `www.univie.ac.at/ZID/datennetz/`). Sobald die IPv6-Anbindung existiert, ist es selbstverständlich auch möglich, die Institutsserver mit IPv6 zu betreiben. Für diese werden die IPv6-Adressen vom ZID direkt vergeben (kein EUI64) und in das DNS eingetragen, damit die Server auch bei einer Änderung der MAC-Adresse weiterhin unter derselben IP-Adresse erreichbar sind. Bei Servern ist natürlich besonders darauf zu achten, dass auch für IPv6-Zugriffe entsprechende Security-Maßnahmen getroffen werden müssen (Firewall usw.), um Angreifern keine „Schleichwege" in den vermeintlich sicheren Rechner zu bieten.

Bei Interesse bzw. Fragen wenden Sie sich bitte an die eMail-Adresse `netzwerk.zid@univie.ac.at`.

Ulrich Kiermayr ■

Virtual Private News (VPN)

Welcher VPN-Klient wofür?

Über das VPN-Service des Zentralen Informatikdienstes wurde bereits im *Comment 04/3* berichtet (VPN = *Virtual Private Network*; siehe `www.univie.ac.at/comment/04-3/043_23.html`). Derzeit gibt es drei verschiedene Möglichkeiten, um eine Verbindung zum VPN-Konzentrator des ZID aufzubauen; jedoch ist nicht jede Methode für jeden Zweck geeignet. Deshalb hier nochmals eine kurze Auflistung, welcher Klient wofür verwendet werden sollte:

1. WebVPN

Das WebVPN-Service (`https://univpn.univie.ac.at/`) ist auf das WWW-Protokoll HTTP(S) beschränkt und eignet sich daher einerseits dazu, von außerhalb der Universität auf Webseiten zuzugreifen, die nur innerhalb des Uni-Datennetzes zur Verfügung stehen (dies sind insbesondere Bibliotheksdienste und ähnliches). Da die Verbindung zwischen Browser und VPN-Konzentrator über das verschlüsselte Protokoll *Secure HTTP* (HTTPS) erfolgt, ist es darüber hinaus möglich, von außen über eine sichere Verbindung auf Webservices der Universität zuzugreifen, die kein HTTPS unterstützen: Nur die Verbindung vom VPN-Konzentrator zum jeweiligen Server wird im Klartext abgewickelt, die Verbindung vom Browser zur Uni Wien aber verschlüsselt.

2. VPN über Windows XP

Um auch andere (nicht webbasierte) Services nutzen zu können, für die der Zugriff auf das Universitätsdatennetz beschränkt ist, kann man den Windows XP-eigenen VPN-Klienten verwenden (eine Anleitung finden Sie unter `www.univie.ac.at/ZID/anleitungen/vpn-winxp/`). Damit ist es möglich, von außen auf beliebige IP-basierte Dienste zuzugreifen. In diesem Fall wird die Verbindung nicht verschlüsselt; daher ist dies nur dann sinnvoll, wenn keine Verschlüsselung vom Klienten zum VPN-Konzentrator benötigt wird (z.B. weil der Dienst an sich schon Verschlüsselung auf der gesamten Strecke bietet).

3. VPN mit Cisco-Klient

Für alles andere – insbesondere dann, wenn eine verschlüsselte Verbindung vom Klienten in das Datennetz der Uni Wien notwendig ist – sollte man den VPN-Klienten von Cisco verwenden, der unter `www.univie.ac.at/ZID/vpn/` für Windows, MacOS X, Linux und BSD/Solaris zur Verfügung steht. Dieser unterstützt eine starke Verschlüsselung sowie sichere Authentifizierung und bietet somit maximale Sicherheit im Netzwerk.

Zugriff auf die Max Perutz Library

Um auch den MitarbeiterInnen jener Institute, die nicht in der Dr.-Bohr-Gasse angesiedelt sind, den Zugriff auf die *Max Perutz Library* (Online-Journale zum Thema Biotechnologie) zu ermöglichen, bietet der ZID ab sofort ein Web-VPN-Service dafür an. Das Einstiegsportal ist unter **`https://vbc-journals.univie.ac.at/`** weltweit erreichbar.

Welche Institute auf das Service zugreifen dürfen, entscheidet die Universitätsbibliothek; die MitarbeiterInnen jener Institute können sich dann mit ihrer Mailbox-UserID auf dieser Webseite anmelden. Dadurch erhalten sie denselben Zugriff auf die Online-Journale, der bisher nur für die Institute in der Dr.-Bohr-Gasse verfügbar war.

Ulrich Kiermayr ■

WLAN-SECURITY@HOME

Schöne neue (Funk)welt

Zeitungslesen am Frühstückstisch – passé? Mitnichten. Das vertraute Rascheln von Papier wurde lediglich von einer eintönig summenden CPU-Kühlung abgelöst. Das Gegenüber verbirgt sich nicht mehr hinter unordentlich gefaltetem Druckwerk, sondern hinter einem aufgeklappten anthrazitfarbenen Notebookdisplay. Im Falle diverser Unmutsäußerungen des Tischnachbarn verbleibt selbigem der Rückzug samt Kipferl, Kaffee und WWW hinaus auf die Veranda. Schönwetter vorausgesetzt. Beziehungsweise ins Wohnzimmer auf die Couch. Ganz nach Belieben. Das erst kürzlich eingerichtete heimische WLAN macht's möglich. Schließlich handelt es sich hierbei um ein *Wireless Local Area Network,* also ein drahtloses lokales Netzwerk, das an Stelle von Kabeln ein Funksystem zur Datenübertragung nutzt.

Waren WLANs einst vorwiegend professionellen Anwendern vorbehalten, so haben sie indes längst auch ihren Siegeszug in private Haushalte angetreten. Komfort, erhöhte Mobilität sowie sinkende Preise von WLAN-Technologien spielen dabei eine nicht unerhebliche Rolle. Auch der technische Aufwand zur Realisierung eines solchen heimischen Funknetzes hält sich in Grenzen: Nach Installation eines Accesspoints oder Routers und Ausstattung des Rechners mit einer Funknetzkarte (viele neuere Marken-Notebooks sind bereits serienmäßig damit ausgerüstet) können sich BenutzerInnen bereits innerhalb der Reichweite des Funkadapters oder der Basisstation mit ihrem Notebook frei bewegen.

Sicherheit?

Da Funknetze jedoch bekanntlich nicht vor physischen Barrieren wie den heimischen vier Wänden „Halt machen", sollte nicht außer Acht gelassen werden, dass für den sicheren Betrieb eines WLANs andere Voraussetzungen gelten als dies bei verkabelten Geräten bzw. Netzen der Fall ist. So wird oft bereits bei der Konzeption/Neuerrichtung eines WLANs verabsäumt, entsprechende zusätzliche Sicherheitsvorkehrungen zu treffen. Immer wieder belegen Untersuchungen deren mangelhafte Absicherung. Beispielsweise fand laut *heise* ein Rostocker Wissenschaftler heraus, dass in Deutschland fast jedes vierte drahtlose Computernetz völlig ungeschützt sei vor Angriffen. Der weit angelegte Test der Fachzeitschrift *c't* in Hannover, Berlin und München kam gar zu dem Schluss, dass jedes zweite WLAN „sperrangelweit offen" stünde. Diese Zahlen auf österreichische Verhältnisse zu übertragen, erscheint einzelnen Quellen[1)] zufolge sogar noch optimistisch. Und auch wenn die konkreten Zahlen regional und von Studie zu Studie variieren: Faktum bleibt, dass viele WLANs, sei es nun aus Unwissenheit oder Leichtfertigkeit der Betreiber, oder auch aus geringer Fürsorge der Hersteller (fehlende Dokumentationen, unbedachte Voreinstellungen), jeglichem Missbrauch und Mitgebrauch Tür und Tor öffnen.

Manche BenutzerInnen vermeinen auch, dass ihre Daten ohnehin nicht so „schützenswert" seien, als dass sich ein solcher Aufwand lohne. Nur: Ad 1 ist der Aufwand das private WLAN ein wenig sicherer zu gestalten gar nicht so groß, und ad 2 wird dabei außer Acht gelassen, dass es sich hierbei nicht nur um eine Frage der Datensicherheit handelt. So stellt – neben der Gefahr des missbräuchlichen Abhörens, Abfangens bzw. Manipulierens von Daten (*Data Privacy*) – auch die unberechtigte Mitbenutzung des Internetzugangs (*Unauthorized Access*) einen nicht zu unterschätzenden Risikofaktor dar. Bei bestehendem Volumen- oder Zeittarif können „Schwarz-Surfer" WLAN-BetreiberInnen teuer kommen – und: Bei Missbrauch ihrer Dienste (und somit ihrer Identität) für kriminelle Zwecke sind auch strafrechtliche Folgen (oder zumindest deren „Nebenwirkungen" wie etwa Einvernahmen, Hausdurchsuchungen, …) nicht gänzlich auszuschließen.

Wie schützen?

1. Allgemeine Überlegungen

Gewöhnlich lassen sich bereits im Vorfeld einige sicherheitsfördernde Maßnahmen treffen. „Ein kluger Kopf sorgt vor" und informiert sich bereits vor einem Neuerwerb darüber, welche Schutzfunktionen das jeweilige Gerät bietet. Fragen wie *Welche Verschlüsselung unterstützt der Router*, *Hat er einen MAC-Filter bzw. eine Firewall* und *Lässt sich der ESSID-Broadcast unterbinden* können eventuell bei der Auswahl behilflich sein. Auch bei der Aufstellung des Gerätes kann durch geschickte Positionierung des Routers/Accesspoints bereits bis zu einem gewissen Grad verhindert werden, dass Nachbarn oder Passanten an Ihrem WLAN mitpartizipieren.

Optimieren können Sie den Standort des Gerätes, indem Sie mit Ihrem Notebook (und am besten mit einer speziellen Antenne) die Reichweite des Routers/Accesspoints an verschiedenen Plätzen testen. Das Funkspektrum soll dabei so wenig wie möglich (oder besser: überhaupt nicht) öffentlich zugängliche Bereiche tangieren (von einer Positionierung an einer straßenseitigen Wand wäre demnach beispielsweise abzuraten). Weiters sollte das Gerät stets abgeschaltet werden, wenn es nicht benötigt wird. Auch damit reduziert sich die Wahrscheinlichkeit, dass sich jemand in Ihrer Abwesenheit Ihres Funknetzes „bedient".

1) Glaubt man an die Repräsentativität der Karten, die Wardriver (siehe Kasten auf Seite 35) hierzulande erstellen, so liegt die Anzahl unverschlüsselter Funknetze in Österreich sogar noch deutlich höher als in Deutschland.

2. WEP & WPA

Um eine (annähernd) ähnliche Sicherheit des Datenaustausches wie beim Kabel zu erreichen, wurde ursprünglich für WLANs die Funktion WEP (*Wired Equivalent Privacy*) entwickelt. Es handelt sich bei WEP um einen Teil des internationalen Standards IEEE 802.11, der von Herstellern in ihre 802.11-Hardware integriert wurde und so weite Verbreitung fand. WEP dient zur Datenverschlüsselung und Authentifizierung in Wireless LANs. Primäres Ziel ist es, Benutzerdaten vor einem möglichen „Lauschangriff" zu schützen. In gewissem Sinne schützt WEP sogar zweifach: So werden zum einen übertragene Daten durch Verschlüsselung geschützt, zum anderen ist eine Verbindung zum Accesspoint/Router nur möglich, wenn der Schlüssel bekannt ist.

Soviel zur Theorie. In der Praxis entdeckten Experten in dem Verfahren schon bald eine Reihe von Sicherheitslücken, so dass eine stete Weiterentwicklung vonnöten war. Mitte 2004 wurde von dem standardbildenden Gremium der internationalen Ingenieursgemeinschaft IEEE der neue Standard IEEE 802.11i für kabellose Netze ratifiziert. Teile dieses Standards kamen bereits unter der Bezeichnung WPA (*WiFi Protected Access*) als Übergangslösung zum Einsatz, um den Sicherheitslecks im Verschlüsselungsverfahren WEP zu begegnen. Mit WPA gelang es – obgleich es selbst die eine oder andere Achillesferse aufweist – zahlreiche bekannte WEP-Sicherheitsprobleme auszumerzen. Es ist demnach WEP vorzuziehen, vorausgesetzt Accesspoint/Router und Netzwerkkarte unterstützen bereits WPA. Sollte dies nicht der Fall sein, muss ohnehin auf WEP zurückgegriffen werden. Hier gilt: Je länger der Schlüssel, umso besser. Ab 128 Bit gilt WEP schon als relativ sicher. Mehr über Verschlüsselungsverfahren erfahren Sie z.B. im Artikel *Grundbegriffe der Krytographie*, *Comment 00/3*, Seite 20.

☞ ***Tipp:*** *Wichtig: Aktivieren Sie die Standard-Verschlüsselung WEP oder WPA an Ihrem Accesspoint/Router und an Ihrer WLAN-Karte. Folgen Sie hierfür den Anweisungen in der jeweiligen Bedienungsanleitung.*

3. „Starke" Passwörter

Wird ein neues Gerät gekauft, ist dieses mit einem Defaultpasswort ausgestattet, also einem auf dem Gerät werkseitig eingestellten Standardpasswort. Dieses sollte vom frischgebackenen Besitzer unbedingt umgehend geändert werden. Leider finden sich immer wieder Fälle, in denen das Defaultpasswort belassen wurde. Ein Angreifer muss dann lediglich die Standardpasswörter des jeweiligen Netzwerkkomponenten-Herstellers eruieren. Da es hierfür entsprechende Listen im Internet gibt, stellt dies kein schwieriges Unterfangen dar.

Anfang November wurde ein Tool ins Netz gestellt, das auf jene WLAN-Funknetze abzielt, die WPA-PSK (*WiFi Protected Access, Pre-Shared Key*) in Kombination mit schwachen Passwörtern einsetzen. Mittels Brute Force- oder Wörterbuch-Attacke kann der WLAN-Angreifer das bei einer Client-Accesspoint-Verbindung benutzte Passwort ermitteln. Gefährdet sind nur WLANs, die schwache Passwörter (z.B. Orts- oder Personennamen bzw. gängige Begriffe) einsetzen. Die Wahl des Passwortes spielt demnach eine äußerst gewichtige Rolle. Es sollte eine möglichst komplexe, alphanumerische Zeichenfolge benutzt werden, wie beispielsweise *MIf:2Hu1Tf*. Weitere praktische Tipps zu diesem Thema finden Sie auch unter `www.univie.ac.at/ZID/passwort/`.

☞ ***Tipp:*** *Ändern Sie das Default-Passwort und wählen Sie stets „starke" Passwörter!*

4. (E)SSID

Bei dem so genannten SSID (*Service Set Identifier*) handelt es sich um den Namen des Funknetzes. Der SSID kann vom Administrator frei gewählt werden. Jeder Teilnehmer, der sich in das Netz einloggen möchte, benötigt diesen Namen für die Konfiguration seiner Netzwerkkarte. Beim Erwerb eines neuen Accesspoints oder Routers ist bereits werkseitig ein Netzwerkname (SSID) vorgegeben. Dieser sollte unbedingt geändert werden. Auch hier gilt selbiges zu beachten wie bei Passwörtern.

Von zahlreichen Accesspoints/Routern wird der SSID ständig gesendet, um den Geräten im Sendebereich mitzuteilen, dass hier ein Netzwerk existiert, mit dem sie sich verbinden können. Im Fachjargon bezeichnet man dies auch als *SSID Broadcast*. Leider bieten nicht alle Accesspoints/Router die Möglichkeit, das Senden der SSID zu unterbinden. Sollte Ihr Gerät dies jedoch unterstützen, machen Sie davon Gebrauch.

☞ ***Tipp:*** *Ändern Sie den SSID und deaktivieren Sie (falls möglich) dessen Broadcast!*

Warwalking, Wardriving & Warchalking

Unter Wardriving/Warwalking versteht man das systematische Aufspüren von WLANs mit Hilfe eines Autos bzw. per pedes. Zur notwendigen Ausstattung eines Wardrivers/Warwalkers zählen ein Notebook (oder auch ein PDA), zumeist eine spezielle Antenne sowie entsprechende Softwaretools, die man aus dem Internet herunterladen kann. Von A wie *AirJack* bis W wie *Wellenreiter* reicht die Palette diverser Programme, die den Wardriver/Warwalker befähigen, Wireless-Geräte aufzuspüren, deren Signalstärke zu berechnen, Verschlüsselungen oder schwache Passwörter zu knacken bzw. in andere Rechner einzudringen. Wurde ein offenes Funknetz gefunden, wird dieses manchmal auch vom Wardriver/Warwalker „markiert". Hiervon leitet sich auch der Begriff Warchalking her: Mit Kreide werden z.B. an Häuserwänden spezielle Symbole angebracht, die auf das gefundene WLAN und dessen Sicherheitsvorrichtungen hinweisen.

Wer nun mit Wardrivern eine neue Spezies aggressiver, auf dem Kriegspfad befindlicher Notebook-Besitzer assoziiert, dem sei verraten, dass sich der Begriff „War" eigentlich von *Wireless Access Revolution* ableitet und nicht unbedingt kriegsähnliche Szenarien beschwören möchte. Meist sind die Absichten dieser „Funknetz-Scouts" von äußerst friedlicher Natur, man begnügt sich mit dem bloßen Aufspüren und Kartographieren unverschlüsselter WLANs. Einen weitergehenden (illegalen) Zugriff auf die gefundenen Netzwerke und Rechner verbietet ein selbstauferlegter „Ehrenkodex". Natürlich unterwerfen sich nicht alle Wardriver diesen Regeln, wie in den meisten Bereichen gibt es auch hier vereinzelt schwarze Schafe.

Wardriver/Warwalker sind in vielen Regionen gut organisiert und bilden eigene Communities. Der Informations- und Erfahrungsaustausch findet über Foren oder Treffen statt. Einige Gruppen betreiben zudem ehrgeizige Projekte, wie etwa die *Wardriving Group Vienna* (`www.wgv.at`), die sich offensichtlich eine sukzessive Erfassung der verschlüsselten und unverschlüsselten WLANs aller österreichischer Regionen zum Ziel gesetzt hat. Wie kritisch man diesem „Hobby" auch immer gegenüberstehen mag – einen positiven Aspekt hat die Sache in jedem Fall: Und zwar das Sichtbarmachen von Sicherheitslücken und somit die Förderung eines stärkeren Problembewusstseins.

5. MAC-Filter

Filter machen sich eine Tradition elitärer Klubs zu Eigen: *Members only* heißt hier die Devise. Wer nicht auf der Liste steht, bleibt draußen. Die Aufnahme Ihrer „Mitglieder" nehmen Sie selbst vor – und zwar mittels Eintragung der MAC-Adresse aller zugriffsberechtigten Geräte. Die MAC-Adresse ist die vom Hersteller in die Netzwerkkarte eingebrannte, weltweit eindeutige Hardware-Adresse (z.B. `08:00:20:ae:fd:7e`), die es dem Router ermöglicht, den jeweiligen zugelassenen Rechner zu identifizieren.

Sollten Sie die MAC-Adresse Ihres Gerätes nicht kennen, können Sie diese unter Windows über die *Eingabeaufforderung* eruieren. (Bei Windows XP wählen Sie hierfür ***Start – Programme – Zubehör – Eingabeaufforderung***.) Geben Sie dort `ipconfig /all` ein. Unter den folgenden Informationen finden Sie auch die physikalische Adresse (= MAC-Adresse) Ihres Rechners.

☞ ***Tipp:*** *Beschränken Sie den Zugriff auf das Funknetz auf die bekannten Endgeräte!*

6. Remote Management

Zahlreiche Router bieten die Möglichkeit einer Fernwartung über das Internet, und bei einigen Herstellern ist diese Option bereits standardmäßig aktiviert. Es empfiehlt sich in diesen Fällen, die Funktion zu deaktivieren, da sie ohnehin selten benötigt wird und zudem die Gefahr besteht, dass Hacker sie als „Einstiegsportal" in Ihr Funknetz nutzen.

☞ ***Tipp:*** *Deaktivieren Sie die Fernwartung!*

Zum Abschluss

Freilich wollen wir uns hier keinen Illusionen hingeben – auch die sicherste Festung kann eingenommen werden. Und der beste Schutz für Ihre Data Privacy wäre ohnehin der Einsatz eines *Virtual Private Networks* (VPN), also einer TCP/IP-basierten Verbindung über öffentliche Leitungen, die über sicherere Protokolle hergestellt wird. Nur ist eine solche Lösung leider für die wenigsten privaten Nutzer praktikabel – zudem erfordert die Konfiguration eines eigenen VPN-Servers umfangreiches netzwerktechnisches Know-how.

Wer aber auf die Errichtung eines privaten „Fort Knox" verzichten kann und sich auch mit einem stabilen Schutzwall zufrieden gibt, der wird – mit einer ausgewogenen Kombination aus den oben genannten Maßnahmen – einen Großteil der unerwünschten Eindringlinge erfolgreich aus seinem Funknetz fernhalten und mit ruhigem Gewissen die Freuden des Äthers genießen können.

Michaela Bociurko ■