Teamarbeit leicht gemacht: Das Exchange-Service des ZID

Seit August 2006 stellt der Zentrale Informatikdienst für Organisationseinheiten der Universität Wien neben dem bewährten Mailservice auch eine umfassendere Kommunikationsplattform zur Verfügung: Microsoft Exchange.

MS-Exchange ist eine so genannte *Groupware*, eine Software, die Arbeitsgruppen eine gemeinsame Nutzung verschiedener Daten erleichtert. Mit Hilfe eines entsprechenden Klientenprogramms lassen sich nicht nur eMail-Nachrichten bearbeiten, sondern auch mehrere Kalender führen, Kontakte erstellen bzw. organisieren sowie Aufgabenlisten und Notizen verwalten.

Alle diese Funktionen können – je nach Konfiguration der Zugriffsrechte – sowohl von einzelnen BenutzerInnen als auch von mehreren Personen gemeinsam verwendet werden. MS-Exchange ermöglicht darüber hinaus auch eine einfache Synchronisation mit diversen Handhelds. Im vergangenen halben Jahr haben sich bereits mehr als 700 Universitäts-MitarbeiterInnen für das Exchange-Service entschieden (siehe dazu auch Kasten *Das Exchange-Service des ZID: Was steckt dahinter?* auf Seite 32).

Eine Software – drei Einsatzmöglichkeiten

Auf Wunsch stellt der ZID jeder Organisationseinheit der Uni Wien einen eigenen Exchange-Bereich zur Verfügung (mehr darüber im Abschnitt *Anmeldung und Umstellung*). Dieser Bereich wird *Öffentlicher Ordner* genannt und ausschließlich von der Organisationseinheit selbst verwaltet. Der ZID nimmt keinerlei Einfluss auf die Struktur des öffentlichen Ordners oder die Vergabe der Zugriffsrechte, bietet aber selbstverständlich jegliche erforderliche Unterstützung bei der Umstellung auf bzw. der Anwendung von MS-Exchange (siehe *Informationen und Schulungen*).

In Bezug auf die Nutzung des Exchange-Service sind drei verschiedene „Ausbaustufen“ möglich:

1) Exchange ohne Groupware im eigentlichen Sinn:

Für jemanden, der bereits mit MS-Outlook vertraut ist, ist der Umstieg auf MS-Exchange ohne große Änderung der Nutzungsgewohnheiten möglich. Die Funktionsordner *Kalender, Aufgaben, Notizen* und *Adressen* können wie bisher verwendet werden. Einzig und allein der *Persönliche Ordner*, in dem alle Unterordner beheimatet sind, wird in der Exchange-Konfiguration von Outlook als *Postfach – Nachname Vorname* bezeichnet. Diese erste Art der Exchange-Nutzung – die alleinige Verwendung der persönlichen Daten – beinhaltet noch keine Groupware-funktionen, erweist sich aber bereits durch die zentrale Speicherung der Daten am Server und die verschiedenen Zugriffsvarianten (siehe weiter unten) als überaus nützlich: Es ist damit z.B. nicht mehr notwendig, Adressbücher auf verschiedenen PCs oder Notebooks manuell synchron zu halten.

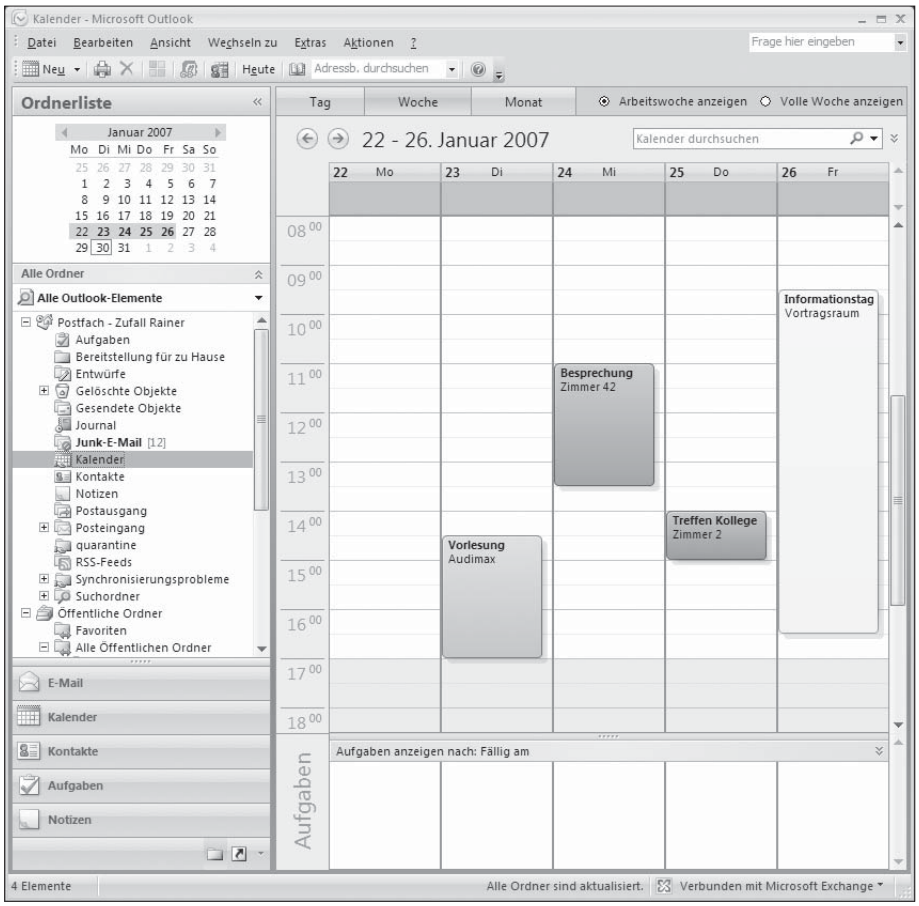


Abb. 1: Exchange-Kalenderfunktion (MS-Outlook 2007)

2) Freigabe von Ordnern des eigenen Postfachs:

Die zweite Stufe besteht darin, die Funktionsordner des eigenen Postfachs für andere Einzelpersonen freizugeben. Beispielsweise kann man KollegInnen den Zugriff auf den eigenen Kalender (siehe **Abb. 1**) erlau-

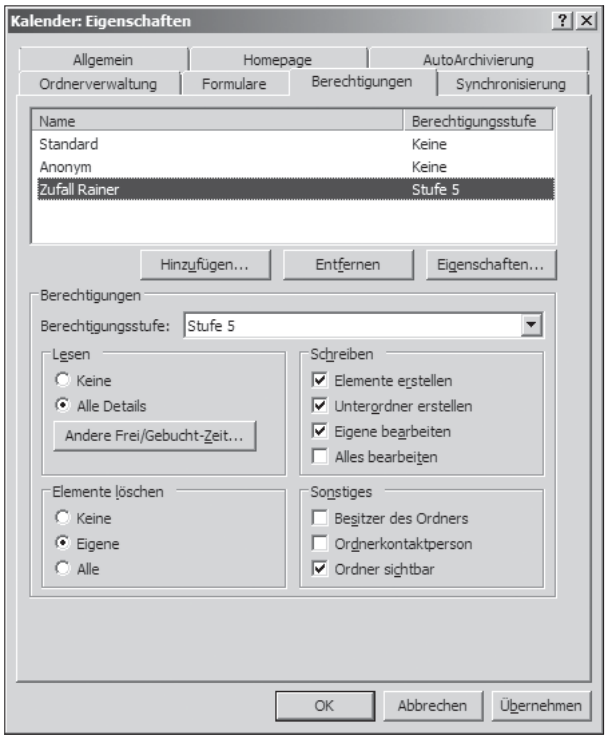


Abb. 2: Freigaben bearbeiten (MS-Outlook 2007)

ben, indem man mit der rechten Maustaste darauf klickt und unter dem Menüpunkt *Eigenschaften* die Registerkarte *Freigaben* entsprechend bearbeitet. Die Rechtevergabe erfolgt entweder über vordefinierte Stufen (von 0 bis 8), oder man setzt die gewünschten Eigenschaften nach Bedarf – z.B. lässt sich definieren, ob ein Berechtigter nur lesen oder auch Einträge erstellen darf (siehe **Abb 2**). Man kann Termine auch als *privat* kennzeichnen; dann ist für die Zugriffsberechtigten zwar ersichtlich, dass der Termin reserviert ist, die Details werden jedoch nicht angezeigt.

3) Verwendung des öffentlichen Ordners:

In der dritten Ausbaustufe der Exchange-Nutzung werden Kalender, Aufgaben, Notizen und Adressen nicht nur im eigenen Postfach angelegt, sondern auch – in beliebiger Struktur – im *Öffentlichen Ordner* der jeweiligen Organisationseinheit. Der öffentliche Ordner eignet sich z.B. für gemeinsame Projektpläne, Adresslisten oder Terminpläne für Besprechungszimmer; hier kann aber auch ein Mailordner mit einer eMail-Adresse (z.B. einer Service-Mailadresse) verknüpft werden.

Die Rechteverwaltung des öffentlichen Ordners wird vom Administrator der jeweiligen Organisationseinheit durchgeführt: Der Administrator kann entweder allen oder auch nur bestimmten MitarbeiterInnen Zugriff gewähren – sogar eine Freigabe für Angehörige anderer Organisationseinheiten ist möglich. Diese BenutzerInnen haben dann zwei entsprechend gekennzeichnete öffentliche Ordner.

Die Groupware-Funktionalität von MS-Exchange ist ein wichtiges Werkzeug, um Geschäftsprozesse transparent darstellen und effizient ausführen zu können. Daher ist es notwendig, spezielles Augenmerk auf den Umstellungsprozess und dessen Planung zu legen: Jeder bereits in der Planung berücksichtigte Geschäftsprozess muss nicht später aufwendig hinzugefügt werden. Nähere Informationen zum Umstellungsprozess finden Sie im Abschnitt *Anmeldung und Umstellung*.

Zugriffsvarianten

Der Zugriff auf den Exchange-Server der Universität Wien ist derzeit mit folgenden Klientenprogrammen möglich: **Outlook 2003 SP2** bzw. **Outlook 2007** (für Betriebssystem Windows XP SP2 oder neuer), **Entourage 2004** (Mac OS X) und **Evolution** (Linux). Das Service kann jedoch nicht nur vom eigenen PC aus genutzt werden:

- Der **Outlook Web Access** (`http://owa.univie.ac.at/`) erlaubt den Zugriff auf eMail-Nachrichten, Kalendereinträge, Kontakte und Aufgaben mittels Webbrowser und somit von praktisch jedem Rechner mit Internetanschluss aus (siehe **Abb. 3**). Nach Eingabe dieses URLs wird man auf die SSL-gesicherte Webseite des Exchange-Servers weitergeleitet; die Daten werden also verschlüsselt übertragen.

- Via **Outlook Mobile Access** (`http://oma.univie.ac.at/`) können die Daten auf dem Exchange-Server über ein mobiles Gerät ohne Exchange-Unterstützung (z.B. Mobiltelefon) oder über einen alphanumerischen Browser (z.B. w3m/lynx unter Unix) abgerufen und abgeglichen werden. Die Darstellungsmöglichkeiten sind dabei allerdings stark eingeschränkt.

- Wer ein Smartphone oder einen PDA mit Exchange-fähigem Betriebssystem besitzt, kann seine Daten mittels **Exchange Active Sync** über GPRS/UMTS oder WLAN direkt mit dem Server synchronisieren. Bei nicht Exchange-fähigen Geräten wie Nokia Communicator ist dies z.B. mit Hilfe der kommerziellen Drittanbieter-Software RoadSync (`www.dataviz.com/roadsync`) möglich. In beiden Fällen werden die Daten ebenfalls verschlüsselt übertragen. Mit aktuellen Windows Mobile PDAs ist es darüber hinaus bereits möglich, eingehende Nachrichten und Kalendereinträge via **PUSH-Dienst** ohne vorherige Synchronisation in Echtzeit zu erhalten.

Zusätzlich kann Ihr Konto am Exchange-Server auch für den IMAP-Zugriff freigeschaltet werden. Dadurch wird es möglich, mit einem beliebigen Mailprogramm eine IMAP-Verbindung zum Exchange-Server herzustellen, um eMail-Nachrichten zu bearbeiten. Neuere Versionen von Mac OS X erlauben dies auch mit dem Programm Apple Mail (wie Sie in Apple Mail einen Exchange-Account konfigurieren, ist unter `www.univie.ac.at/ZID/anleitungen-exchange/applemail/` beschrieben). Wenn Sie den IMAP-Zugang verwenden möchten, wenden Sie sich bitte per eMail an die Adresse `exchange.zid@univie.ac.at`.

Anmeldung und Umstellung

Wie eingangs erwähnt, steht das Exchange-Service des Zentralen Informatikdienstes nicht für einzelne UniversitätsmitarbeiterInnen, sondern nur für Organisationseinheiten zur Verfügung. Die Anmeldung zu diesem Service kann daher nur durch eine Organisationseinheit der Universität Wien (unter Angabe eines EDV-Verantwortlichen und/oder Fakultätsbetreuers) erfolgen.

Das dafür benötigte Formular ist unter **www.univie.ac.at/ZID/formulare/#fu** zu finden. Falls Sie nicht sicher sind, ob Ihre Organisationseinheit bereits für das Exchange-Service angemeldet ist, erkundigen Sie sich bitte bei Ihrem EDV-Betreuer bzw. beim Leiter Ihrer Organisationseinheit.

Nach Einlangen des Formulars richtet der ZID einen eigenen Exchange-Bereich für die jeweilige Organisationseinheit ein, weist dem angegebenen Administrator – d.h. dem EDV-Verantwortlichen bzw. Fakultätsbetreuer – die erforderlichen Berechtigungen für die Verwaltung dieses Bereichs zu und verständigt ihn darüber per eMail. Dies geschieht in der Regel innerhalb eines Arbeitstages nach Eintreffen der Anmeldung.

Der Umstellungsprozess dauert (je nach Vorkenntnissen von Administrator und BenutzerInnen) rund eine Woche: Auf Wunsch bietet der Zentrale Informatikdienst Präsentationen vor Ort an, in denen das Service und seine Anwendung vorgestellt werden. Die Mitarbeiter der Fakultätsunterstützung des ZID stehen auch gerne für detaillierte Gespräche zur Verfügung, um verschiedene Umstellungs- und Nutzungsvarianten zu diskutieren und abzuwägen: Wie bereits angesprochen, hat Exchange einen großen Einfluss auf die technische Unterstützung der Abbildung von Geschäftsprozessen; die Implementierung der Groupware sollte daher wohl durchdacht und sorgfältig geplant werden, um mühsame spätere Umstrukturierungen oder Erweiterungen zu vermeiden.

Nachdem die interne Rechtestruktur des Exchange-Bereichs (*„Wer darf welche Daten einsehen oder ändern?“*) ausschließlich von der Organisationseinheit selbst verwaltet wird, obliegt es dem zuständigen Administrator, interessierten MitarbeiterInnen den Zugang zum Exchange-Service zu ermöglichen, indem er ihre Mailbox-UserIDs in entsprechende Exchange-Konten umwandelt. Die tatsächliche Umstellung wird ebenfalls vom Administrator durchgeführt und besteht aus der Sicherung der vorhandenen, Exchange-relevanten Daten der teilnehmenden BenutzerInnen (Adressbücher, Kalender, Mailfolder, Projektdaten, ...) am Server, einschließlich allfälliger Umwandlung in ein geeignetes Dateiformat. Dieser Vorgang nimmt pro Arbeitsplatzrechner im Schnitt ca. eine Stunde in Anspruch, wobei der größte Teil der Zeit auf die Migration der Mailfolder entfällt. Auch hier ist der ZID gerne bereit, das Prozedere anhand von zwei bis drei exemplarischen Umstellungen genau zu erklären, um eventuelle Hürden oder Unklarheiten zu beseitigen.

Im Anschluss daran kann jeder teilnehmende Benutzer mit Hilfe der oben genannten Klienten auf sein Exchange-Konto zugreifen. Um eMail-Nachrichten über den Exchange-Server zu empfangen, muss er allerdings noch eine entsprechende Weiterleitung für seine Mailbox-Adresse einrichten, indem er unter **www.univie.ac.at/ZID/weiterleitung/** in der Webmaske die Option *Weiterleitung an den Exchange-Server* mittels Häkchen aktiviert.

Informationen und Schulungen

MS-Exchange als Groupware-Lösung ist eine komplexe Plattform mit großem Funktionsumfang, deren Verwendung eine eingehendere Beschäftigung mit der Thematik erfor-

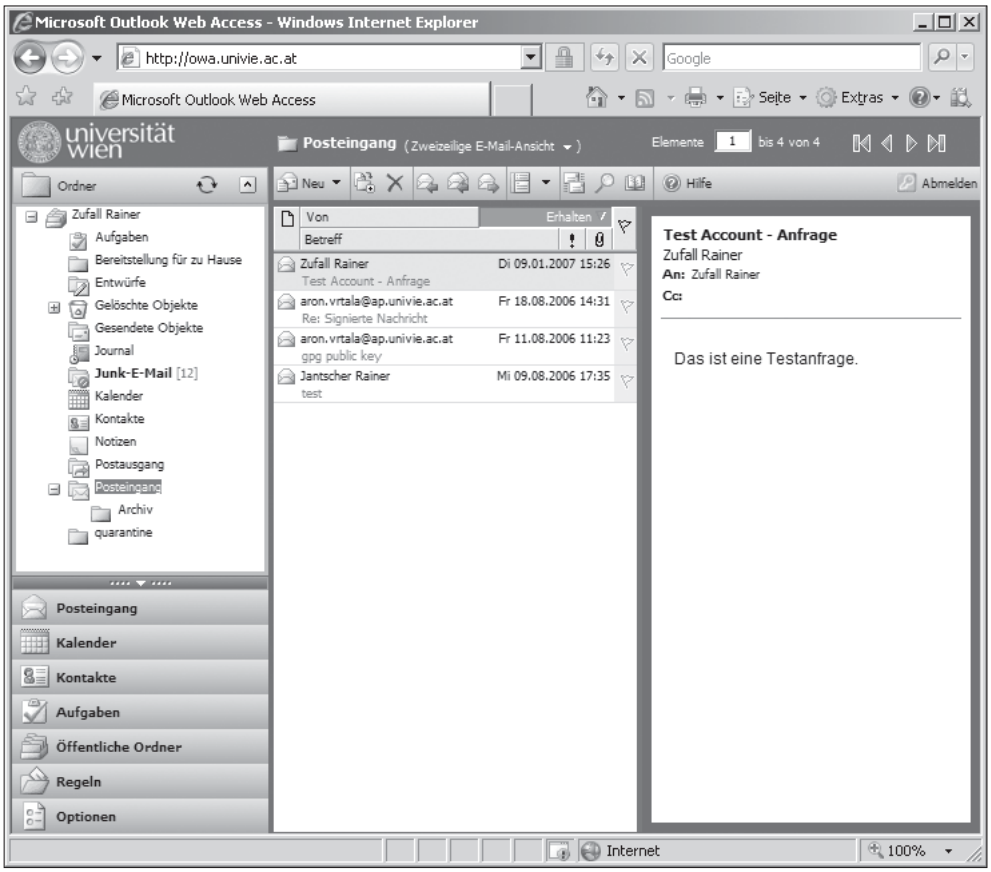


Abb. 3: eMail-Bearbeitung mittels Outlook Web Access

dert. Als Unterstützung für BenutzerInnen und AdministratorInnen bietet der Zentrale Informatikdienst deshalb folgende Services an:

Online-Hilfe (FAQs)

Nähere Informationen zum Exchange-Service, Anleitungen zur Einrichtung der diversen Klienten sowie Antworten auf häufig gestellte Fragen zum Thema sind auf der Webseite **`www.univie.ac.at/ZID/anleitungen-exchange/`** zu finden.

eMail-Ticketsystem

Alle eMail-Anfragen an die Mailadresse **`exchange.zid@univie.ac.at`** werden über ein Ticketsystem verwaltet, d.h. Sie erhalten eine automatische Antwort mit Ihrer Ticket-Nummer (z.B. `Ticket <URL: https://ticket.cc.univie.ac.at/rt/Ticket/Display.html?id=12345>`) und können jederzeit den aktuellen Bearbeitungsstand Ihrer Anfrage abrufen, indem Sie in der eMail-Nachricht auf diesen Link klicken. Sie müssen sich hierbei mit Ihrer Mailbox-UserID und dem dazugehörigen Passwort authentifizieren. Sollten Sie über keine Mailbox-UserID verfügen, können Sie sich selbstverständlich auch telefonisch über den Stand der Dinge informieren.

Telefon-Hotline

Die Hotline der Fakultätsunterstützung des ZID ist montags bis freitags von 8:00 – 18:00 Uhr unter der Telefonnummer **+43-1-4277-141 40** erreichbar.

Schulungen

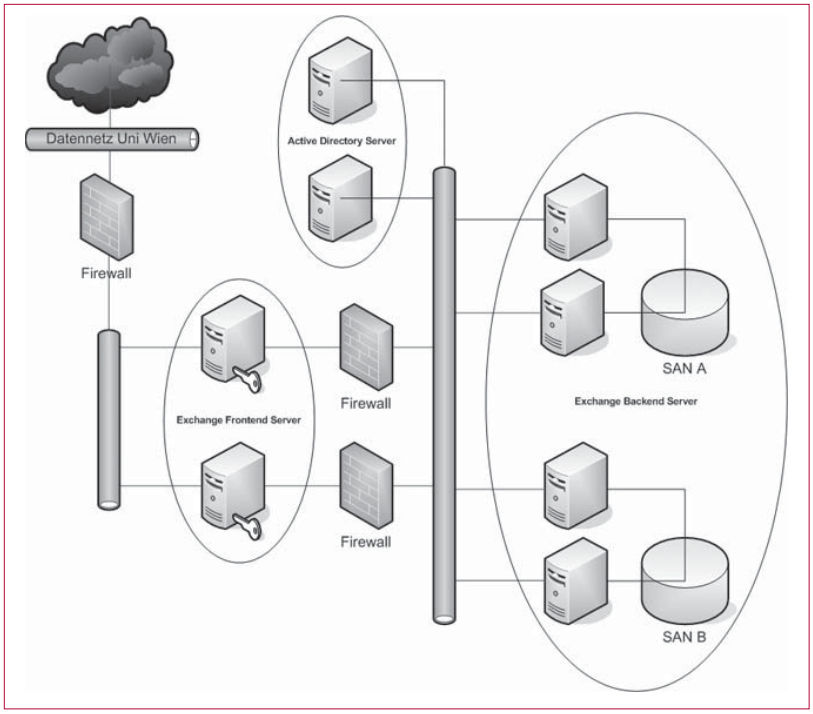
Bei Bedarf bietet der Zentrale Informatikdienst Schulungen für Exchange-BenutzerInnen, in denen vor allem die Anwenderseite von MS-Exchange näher vorgestellt wird. Darüber hinaus werden auf Anfrage auch Schulungen für EDV-Verantwortliche der Organisationseinheiten bzw. für FakultätsbetreuerInnen abgehalten, wobei hier das Hauptaugenmerk auf den administrativen Funktionen der Software liegt.

Rainer Jantscher & Stefan Just

Das Exchange-Service des ZID: Was steckt dahinter?

Um MS-Exchange als Service für alle UniversitätsmitarbeiterInnen anbieten zu können, muss die zugrunde liegende Server-Infrastruktur sowohl möglichst ausfallsicher sein als auch rasche Antwortzeiten gewährleisten – selbst bei hohen Zugriffszahlen. Diese Anforderungen werden mit Hilfe einer ausgeklügelten Hardware-Konfiguration erfüllt: Die Zugriffe der BenutzerInnen erfolgen auf zwei so genannte *Exchange Frontend Server*, die mittels *Network Load Balancing* eine dynamische Lastaufteilung der Anfragen auf die dahinter liegenden Datenbankserver durchführen. Diese Datenbankserver (derzeit vier) sind zu einem Cluster zusammengefasst und greifen über ein redundantes *Storage Area Network* (SAN) auf den jeweiligen Datenbankspeicher zu. Zwei *Active Directory Server*, die ebenfalls redundant ausgelegt sind, stellen die nötigen Benutzerdaten zur Verfügung und übernehmen die Passwort-Synchronisation der Mailbox-UserIDs. Darüber hinaus ist das System durch mehrere Firewalls vor unbefugten Zugriffen aus dem Netzwerk geschützt.

Diese Infrastruktur sorgt dafür, dass das Exchange-Service des ZID auch bei einem Ausfall einzelner Server uneingeschränkt verfügbar ist. Da das System bei Bedarf leicht um zusätzliche Server erweitert werden kann, sind auch keine Performance-Einbußen durch steigende Benutzerzahlen zu befürchten.



Exchange-Service des ZID – Hardware-Konfiguration

Audio- & Videostreams im Uni-Datennetz

Musik-Videoclips aus Pakistan, Nachrichten aus dem Nahen oder Fernen Osten, Berichte über neueste Forschungsergebnisse der Universität von Kalifornien oder Live-Übertragungen von Vorlesungen an der Université Pierre et Marie Curie in Paris – klingt das interessant für Sie? Nein? Gut, wir haben auch noch Live-Übertragungen aus dem irischen Parlament oder NASA TV. Neugierig geworden? Die Rede ist hier von diversen Audio- und Videostreams, die wir Ihnen seit kurzem im Datennetz der Universität Wien zur Verfügung stellen. Wie Sie in den Genuss dieses Augen- und Ohrenschmauses kommen, wollen wir Ihnen selbstverständlich nicht verschweigen.

Das Prinzip

Streaming ist eine Technik zur Datenübertragung via Internet (oder auch Intranet), mit der Dateien kontinuierlich – quasi „Stückchen für Stückchen" – übertragen und empfangen werden können. Der Vorteil dieser Technik gegenüber herkömmlichen Übertragungen ist, dass nicht auf das vollständige Herunterladen der Datei gewartet werden muss. Sie eignet sich deshalb besonders gut für das Übertragen von Multimedia wie Audio- oder Videodaten, da es sich hierbei in der Regel um große Datenmengen handelt. Dafür erfordert Streaming aber einen kontinuierlichen Datenstrom, ohne den keine lückenlose Übertragung sichergestellt werden kann. Um Audio- und Videodateien zu streamen, müssen diese zunächst in das beabsichtigte Ausgabeformat gewandelt und mittels eines Servers im Netzwerk angeboten werden. Man unterscheidet ganz allgemein zwischen Streaming auf Abruf (*On Demand*) und *Live Streaming*. Zur Wiedergabe der aus dem Netz gestreamten Daten ist ein so genannter *Player* erforderlich.

Audio- & Videostreams: Eine kleine Auswahl

Research Channel
24h-Übertragung von Forschungsergebnissen, Vorlesungen, Interviews, Dokumentationen und Diskussionen weltweit führender Wissenschaftsinstitutionen (Programm unter `www.researchchannel.org`)

RAP – TV.RAP1, 2, 3 & 4
Multicast des Réseau Académique Parisien (Näheres unter `www.rap.prd.fr/services/tv.php`)

UCTV 4 By VBrick bzw. UCTV By VBrick
University of California Television sendet Forschungsergebnisse, Dokumentationen, Symposien und Vorlesungen der Universität von Kalifornien (`www.uctv.tv`).

UCTV International bietet div. internationale Sender:
- **Al Jazeera** (englischsprachiger Nachrichtensender aus dem Nahen Osten; `http://english.aljazeera.net/News`)
- **Bloomberg** (bekannter Finanz-Nachrichtensender; `www.bloomberg.com/media/tv/`)
- **DW-TV** (das offizielle deutsche Auslandsfernsehen der Deutschen Welle; `www.dw-world.de`)

VLC Media Player

Um sich die Audio- und Videostreams im Uni-Netz anhören/ansehen zu können, benötigen Sie einen Player, der den SAP/SDP-Standard unterstützt. Diverse Player erfüllen diese Anforderung. Wir legen Ihnen hierfür (aufgrund positiver Erfahrungen mit diesem Klienten) den ***VLC Media Player*** ans Herz, einen Multimedia-Player, den es für beinahe jede Plattform – sogar WinCE/PocketPC – gibt und der eine sehr breite Palette an Audio- und Videoformaten verarbeiten kann. Sie können den VLC Media Player (er ist Open Source-Software) unter `www.videolan.org/vlc/` kostenlos herunterladen. Wählen Sie dazu unter dem Punkt ***Download VLC*** Ihr Betriebssystem (z.B. Windows, Mac OS X). Sie gelangen nun auf die entsprechende Download-Seite. Wählen Sie das gewünschte Package aus und suchen Sie für dieses den geografisch naheliegendsten Download-Server (*Mirror*). Laden Sie das Installationspaket herunter, entpacken Sie es und installieren Sie es gemäß den Anleitungen des Installationsassistenten.

Danach starten Sie das Programm und wählen im Menü des VLC Media Player (Version 0.8.6a) ***Einstellungen – Einstellungen… – Wiedergabeliste – Diensterkennung***. Aktivieren Sie auf der Registerkarte *Diensterkennung* das Diensterkennungsmodul ***SAP-Ankündigungen***, indem Sie zuerst auf das leere Kästchen davor und dann auf die Schaltfläche ***Sichern*** klicken. Warten Sie nun bitte ca. eine Minute, bis die Änderung in Kraft tritt (Apple-User müssen das Programm eventuell neu starten). Klicken Sie dann im Menü ***Ansicht*** auf den Punkt ***Wiedergabeliste***. Die Wiedergabeliste öffnet sich in einem eigenen Fenster; wählen Sie dort die Option ***Datei – Diensterkennung***. Öffnen Sie die gewünschte Liste in der Wiedergabeliste, indem Sie sie mit einem Häkchen versehen. Die Liste wird nun angezeigt (Baumstruktur). Um einen Stream wiederzugeben, doppelklicken Sie auf den jeweiligen Listenpunkt, z.B. *Research Channel*. Wenn der Stream zur Zeit zur Verfügung steht (nicht alle Kanäle sind rund um die Uhr verfügbar), startet nun – eventuell mit ein paar Sekunden Verzögerung – die Wiedergabe im Player. **Achtung Windows-User:** Sie müssen den VLC Media Player in der Windows-Firewall freigeben! Wählen Sie hierzu (unter Windows XP) ***Start – Einstellungen – Systemsteuerung – Windows-Firewall***. Im Fenster *Windows-Firewall* wählen Sie die Registerkarte ***Ausnahmen*** und markieren unter *Programme und Dienste* das Kästchen vor ***VLC media player*** mit einem Häkchen. Bestätigen Sie Ihre Auswahl mit ***OK***.

Michaela Bociurko

Digitale Reichtümer

Was ist ein Digital Asset Management System und warum braucht die Universität Wien eines?

Jahrhundertelang wurden die Ergebnisse universitärer Lehre und Forschung fast ausschließlich in Papierform produziert. Es ist hauptsächlich Aufgabe der Bibliotheken, diese Schriften aufzubewahren, zu verwalten und zugänglich zu machen. In der langen Geschichte des wissenschaftlichen Bibliothekswesens haben sich hier erprobte Arbeitsweisen und Standards etabliert, sodass die Bibliotheken diese Aufgaben professionell und zuverlässig erfüllen.

Immer mehr Forschungsergebnisse und Lehrinhalte liegen jedoch ausschließlich in digitaler Form vor. Dabei kann es sich um die elektronische Form von Printmedien handeln (z. B. *Electronic Journals*), aber auch um Bilddaten, Audio- und Videomaterial, Softwareprodukte, Online-Lehrgänge aus Lernplattformen, Datenbanken und vieles andere.

Vielfach werden Online-Ressourcen jedoch nicht ganz ernst genommen: Was zählt, ist eine Publikation in einer renommierten Zeitschrift, alles andere ist bestenfalls schmückendes Beiwerk. Einerseits liegt das an einer gewissen Trägheit des Wissenschaftsbetriebes bei der Akzeptanz neuer Medien und wohl auch an wirtschaftlichen Interessen (z.B. der wissenschaftlichen Verlage); andererseits fehlt elektronischen Ressourcen tatsächlich noch einiges, was bei Zeitschriften und Büchern durch die lange etablierten Standards gegeben ist.

Ein Hauptproblem digitaler Ressourcen ist ihre Flüchtigkeit. Während sich an Gedrucktem kaum je etwas ändert, sind Webseiten und andere digitale Datenbestände ständig im Fluss. Eine direkte Konsequenz der Flüchtigkeit ist die mangelnde Zitierbarkeit. Es gibt genaue Regeln, wie wissenschaftliche Arbeiten zu zitieren sind. Findet man z.B. in einer Publikation das Zitat „A. Einstein, *Ann. Phys.*, 17(1905), pp. 891-921“, so mag es zwar vielleicht mühsam sein, die Originalarbeit in einer Bibliothek auszuheben, man kann aber sicher sein, die richtige Arbeit – in diesem Fall zu Einsteins spezieller Relativitätstheorie – zu finden.

Ganz anders verhält es sich bei Zitaten von Webinhalten und anderen digitalen Ressourcen. Hier haben sich noch keine verbindlichen Zitierregeln etabliert, die einfache Angabe von URLs ist unzureichend: Niemand garantiert, dass beispielsweise `www.univie.ac.at/comment/06-2/062_27.html` nach fünf Jahren noch immer existiert bzw. dass dort noch dasselbe Dokument zu finden ist wie zu dem Zeitpunkt, als es zitiert wurde.[1)] Besonders schwierig ist das Zitieren von dynamisch generierten Webseiten bzw. solchen, die sich sehr rasch ändern wie z.B. Wikis.[2)]

Es wurden verschiedene Lösungen für das Zitieren von Online-Ressourcen vorgeschlagen, z.B. den kompletten Inhalt von zitierten Webseiten auszudrucken und der Arbeit beizulegen. Andere kommen zu dem Schluss, dass Webzitate überhaupt unzulässig sind und nur auf Papier Gedrucktes wahren wissenschaftlichen Wert hat. Ich finde diese Schlussfolgerung absurd: Anstatt die Existenz von Online-Ressourcen zu ignorieren und deren wissenschaftlichen Wert zu leugnen, ist es vielmehr erforderlich, die Werkzeuge zu schaffen, mit denen digitale Daten die notwendigen Eigenschaften wie Beständigkeit, Auffindbarkeit und Zitierbarkeit erhalten – und genau das ist die Funktion eines *Digital Asset Management Systems* (DAMS).

Anforderungen an ein Digital Asset Management System

Langzeitarchivierung

Die Aufgaben und Herausforderungen bei der Aufbewahrung geschriebener und gedruckter Dokumente für künftige Generationen sind wohlbekannt. Trotz vieler schmerzlicher Verluste durch Brände, Kriege, Diebstähle oder einfach den „Zahn der Zeit“ ist eine beachtliche Anzahl an Schriften aus früheren Jahrhunderten erhalten, und das oft in einem bemerkenswert guten Zustand: Säurefreies Papier überdauert problemlos mehrere hundert Jahre, so manche Pergament-Handschrift aus dem frühen Mittelalter oder der Spätantike wirkt nach mehr als tausend Jahren so frisch, als hätte sie eben erst das Skriptorium verlassen. Große Bibliotheken verfügen über eigene Abteilungen für die Konservierung und Restaurierung ihrer Bestände.

Bei digitalen Objekten ist die Haltbarkeit des physischen Mediums vermutlich wesentlich kürzer als die Jahrhunderte, die Papier überdauern kann: Festplatten geben nach wenigen Jahren den Geist auf, Magnetbänder reagieren sehr empfindlich auf magnetische Einflüsse, was sie oft sehr schnell unlesbar macht. Viele digitale Medien (z.B. DVD) sind noch recht neu; über ihre Haltbarkeit ist wenig bekannt.[3)]

---

1) In diesem Fall versprechen wir, die URLs von *Comment*-Artikeln auf unbeschränkte Zeit beizubehalten und den Inhalt nicht nachträglich zu ändern – allerdings kann so eine Garantie von niemandem kontrolliert werden und ist daher von beschränktem Wert.

2) Wikipedia bietet für diesen Zweck die Option des so genannten Permanentlinks, bei der jede Version eines Dokuments gespeichert wird (siehe z.B. `http://de.wikipedia.org/w/index.php?title=Idiot&oldid=9847828`).

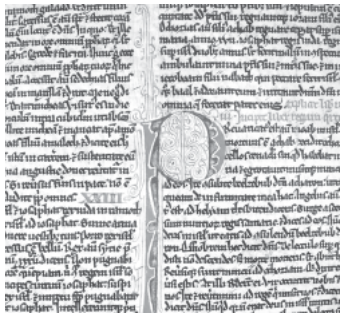
3) siehe dazu z.B. `http://www.heise.de/newsticker/meldung/85686`

Im Gegensatz zu Gedrucktem lassen sich digitale Objekte jedoch verlustfrei kopieren: Es besteht kein Unterschied zwischen Original und Kopie. Deshalb ist die Vergänglichkeit des physischen Mediums nur insofern ein Problem, als ein regelmäßiges Umkopieren auf neue Datenträger erforderlich ist. Beispielsweise findet sich auf dem Webserver der Universität Wien (`WWW.UNIVIE.AC.AT`) so manche Datei aus dem Jahr 1995, obwohl seither mehrmals die Hardware getauscht wurde (zuletzt bei der Übersiedlung der Daten in das *Storage Area Network*, vgl. Seite 16).

Die wahren Probleme der digitalen Langzeitarchivierung liegen anderswo: Einerseits brauchen digitale Objekte eine „Heimstätte“, die dauerhafter ist als die üblichen Webseiten, deren Lebenszeit selten mehr als ein paar Jahre beträgt. Andererseits muss sichergestellt werden, dass die verwendeten Datenformate auch in Zukunft noch lesbar sind.

Auch wenn viele ältere Datenträger wie Magnetband-Spulen oder 8-Zoll-Disketten physisch unversehrt sein mögen, so sind die Daten darauf nur mit enormem Aufwand zu lesen, weil es heutzutage fast überall an entsprechenden Geräten und Laufwerken fehlt. So manches Textverarbeitungsprogramm, das Mitte der Achtzigerjahre des vorigen Jahrhunderts populär war, ist inzwischen in Vergessenheit geraten, sodass Dokumente, die mit solchen Programmen geschrieben wurden, nur mehr mühsam zu entziffern sind.

Selbstverständlich kann heute niemand wissen, welche Formate noch in hundert Jahren lesbar sein werden. Durch die Beschränkung auf Standard-Formate, die zusätzlich noch möglichst *self-contained* sein sollen (d.h. bei denen alle erforderlichen Informationen wie z.B. die verwendeten Schriftarten im Dokument selbst enthalten sind), besteht zwar keine Garantie, aber immerhin eine hohe Wahrscheinlichkeit, dass auch unsere Urenkel sich noch an den digitalen Schätzen erfreuen können, die wir heute produzieren.



Verschiedene Speichermedien

Metadaten: Standards und Schnittstellen

Wollte man ein Buch in einer Bibliothek ins Regal stellen, aber nicht in den Katalog aufnehmen, so wäre dieses praktisch wertlos. Erst die Aufnahme von Autor, Titel, Verlag, Jahrgang, ISBN, Aufstellungsort usw. in den Bibliothekskatalog sowie die Erfassung von Kategorien und Schlagwörtern macht das Buch zum Bestandteil einer Bibliothek. Die fehlerfreie Katalogisierung und Beschlagwortung ist durchaus keine triviale Aufgabe und erfordert geschultes Fachpersonal.

Ähnliche Anforderungen gibt es bei der Erfassung digitaler Objekte: Zusätzlich zum Objekt selbst (beispielsweise eine Bilddatei) muss eine Beschreibung des Objekts mit Daten wie Autor, Datum der Erstellung usw. abgespeichert werden. Diese Art von Zusatzinformationen bezeichnet man als *Metadaten*.

Bei der Beschreibung digitaler Ressourcen muss ein Kompromiss gefunden werden: Einerseits ist größtmögliche Einheitlichkeit und Standardisierung gewünscht, was z.B. für globale Suchfunktionen unerlässlich ist. Andererseits ist hohe Flexibilität erforderlich: Verständlicherweise sind für die Beschreibung von digitalisierten archäologischen Funden ganz andere Metadaten erforderlich (z.B. Fundort) als etwa bei NMR-Spektren von chemischen Verbindungen (z.B. chemische Formel, verwendetes Messgerät).

Der wichtigste Metadaten-Standard, der 1994 definiert wurde und sich bereits weitgehend durchgesetzt hat, ist der so genannte *Dublin Core*-Standard.[4] Der Name „Core“ deutet bereits an, dass es sich dabei um die Kern-Elemente von Metadaten handelt, die noch durch beliebige Zusatzinformationen erweitert werden können. Zu den 15 Elementen des Dublin Core gehören beispielsweise eine eindeutige Identifikation des Objektes, die auch die Zitierbarkeit sicherstellt, die Art des Objekts (Bild, Text, physisches Objekt usw.) und Personen (Autor, Herausgeber).

Besonders wichtig ist das Einhalten von Standards, wenn Daten zwischen mehreren Systemen ausgetauscht werden sollen oder eine gemeinsame Suchfunktion über mehrere Sammlungen von Objekten gewünscht ist. Wer beispielsweise eine Bilddatenbank aufbaut, ohne sich um Metadaten-Standards zu kümmern, mag sich dadurch anfangs einiges an Arbeit ersparen, ohne einen Verlust an Funktionalität zu bemerken. Das rächt sich jedoch, sobald einmal ein Wechsel der Software erforderlich wird oder eine Vereinigung mit anderen Datenbanken gewünscht ist: Durch Standard-Formate kann man sich in diesen Fällen aufwendige Migrations-Programme ersparen.

Die Bedeutung von Standard-Formaten für die Langzeitarchivierung wurde bereits erwähnt; dasselbe gilt selbstverständlich auch für Metadaten.

Suchen und Finden, Pflegen und Betreuen

Es ist nicht damit getan, digitale Objekte für künftige Generationen ins Archiv zu stellen und dort virtuell verstauben zu lassen: Mindestens genau so wichtig ist der praktische Nutzen für die Gegenwart. Dazu gehört eine effiziente Suchfunktion, wobei durchaus auch Objekte gefunden werden können, die sich physisch anderswo befinden. In einem solchen Fall verwaltet das DAMS nur die Metadaten, anstelle des eigentlichen Objekts enthält es nur einen Verweis, wo dieses zu finden ist.

Weiters gehören zu einem solchen System Werkzeuge, die die Verwendung der digitalen Objekte in Forschung und Lehre ermöglichen. Zwar ist ein DAMS primär kein *Content Management System* (CMS) und auch keine Lernplattform (*Learning Management System*, LMS), aber die Funktionen dieser Systeme überschneiden sich teilweise. Welche Werkzeuge benötigt werden, hängt stark von der Art der Objekte ab: Bei Bilddateien sind das etwa Funktionen wie Generieren verschiedener Qualitätsstufen und Auflösungen, verschiedene Methoden von Darstellung und Projektion usw.

Eine wichtige Komponente sind auch die Hilfsmittel bei der Erfassung und Pflege von Daten: Möglichst automatisierte Generierung von Metadaten aus den Daten selbst[5], Methoden des *Ingest*, also der massenweisen Übernahme von Daten aus anderen Systemen, Hilfsmittel bei der Qualitätskontrolle usw.

Rechteverwaltung

Die Problematik von Urheber- und Verwertungsrechten digitaler Ressourcen ist ein schwieriges Feld, wo es noch viele ungelöste Fragen gibt. Meistens sind daran drei Parteien beteiligt: die Urheber (Autoren, Künstler, Forscher); die Inhaber der Verwertungsrechte, die von den Urhebern an diese mehr oder minder freiwillig abgetreten wurden (Verlage, Auftraggeber von Forschungsprojekten, Verwertungsgesellschaften)[6]; die Öffentlichkeit bzw. der Kundenkreis, der auf die digitalen Ressourcen zugreifen und diese nutzen will. Es ist Aufgabe des Gesetzgebers, einen gerechten Ausgleich zwischen den einander widersprechenden, mehr oder minder berechtigten Interessen der drei Beteiligten zu schaffen – eine Aufgabe, die er wohl noch nicht ganz zur allgemeinen Zufriedenheit gelöst hat.

Es gibt ein breites Spektrum von Meinungen zur digitalen Rechteproblematik. Am einen Ende der Skala stehen die Befürworter des *Open Access*-Gedankens, die die Meinung vertreten, dass universitäre Forschung von der Öffentlichkeit durch Steuermittel bezahlt wurde und dass daher die Öffentlichkeit das Recht habe, ohne Einschränkungen und weitere Kosten die Ergebnisse dieser Forschung zu nutzen. Am anderen Ende stehen die Verfechter eines restriktiven *Digital Rights Management*, die den öffentlichen Zugang zu digitalen Ressourcen so weit wie möglich einschränken und bei jeder Nutzung bei den Rechteverwertern – seltener bei den Urhebern – die Kasse klingeln lassen wollen.

Antworten auf diese Fragen zu finden, ist nicht Aufgabe eines Digital Asset Management-Projekts; es gibt vielmehr eigene Arbeitskreise, die sich mit der Rechteproblematik beschäftigen. Wichtig ist jedoch, dass ein DAMS über ein differenziertes System von Zugriffs- und Bearbeitungsrechten verfügt und alle gewünschten Lizenzmodelle abbilden kann.

Digital Asset Management an der Universität Wien

Das erfolgreiche Projekt UNIDAM (siehe `http://unidam.univie.ac.at/`) ist ein Digital Asset Management System, das durch eine Initiative der Philologisch-Kulturwissenschaftlichen Fakultät aufgebaut wurde. Zu den ersten Anwendern gehörte das Institut für Kunstgeschichte mit Bilddatenbanken; seither sind viele weitere Inhalte dazugekommen. UNIDAM steht zwar prinzipiell allen Universitätsinstituten zur Verfügung, wurde aber speziell für die Bedürfnisse der Philologisch-Kulturwissenschaftlichen Fakultät ausgewählt und erfüllt daher nicht alle Anforderungen an ein universitätsweites System.

Vom Projektzentrum Lehrentwicklung, das großes Interesse an einem System zur Verwaltung und Archivierung digitaler Lehrinhalte hat, ging die Initiative aus, ein universitätsweites DAMS zu schaffen. Gemeinsam mit der Universitäts-

4) `www.dublincore.org`, siehe auch `http://de.wikipedia.org/wiki/Dublin_Core`

5) Ein Beispiel für Metadaten, die in den Daten selbst enthalten sind, sind die so genannten EXIF-Einträge, die in praktisch allen von Digitalkameras generierten Bilddateien enthalten sind und Angaben zur Aufnahme wie Datum und Uhrzeit, Kameramodell u.a. enthalten. Eine komfortable Upload-Funktion eines DAMS wird diese Metadaten automatisch extrahieren.

6) Im Unterschied zu den Verwertungsrechten ist das Urheberrecht ein unveräußerliches Recht und bleibt auf jeden Fall beim Urheber eines Werkes.

bibliothek, die einen dringenden Bedarf an einem System zur Verwaltung digitaler Ressourcen hat, sowie dem ZID, in dessen Kompetenz die technische Betreuung eines solchen Systems fällt, wurde Ende 2005 zu diesem Zweck ein Arbeitskreis gegründet.

Im März 2006 wurde ein Fragebogen an alle Institute versandt. Diese Umfrage brachte vor allem zwei wichtige Erkenntnisse: Einerseits das enorme Interesse an Langzeitarchivierung, andererseits eine überraschend große Menge an nicht-digitalen Beständen, die digitalisiert werden oder in absehbarer Zeit digitalisiert werden sollen. Anhand der Ergebnisse dieser Umfrage wurden verschiedene am Markt verfügbare Produkte evaluiert.

Evaluierung

Digital Asset Management ist eine noch relativ junge Disziplin, deshalb ist hier die Auswahl an Softwareprodukten nicht allzu groß. Von allen untersuchten Produkten kamen vier in die engere Wahl, wobei auch Institutionen besucht wurden, in denen sie bereits zum Einsatz kommen:

- **DigiTool**: Das bei weitem erfolgreichste kommerzielle DAM-Produkt ist DigiTool (`www.exlibrisgroup.com/digitool.htm`) der israelischen Firma ExLibris, die auch das an der Universität Wien eingesetzte Bibliothekssystem Aleph entwickelt hat. DigiTool wird beispielsweise von der Österreichischen Nationalbibliothek verwendet.

- **Fedora**: Mehrere interessante Projekte benutzen das Open Source-DAMS Fedora (`www.fedora.info`), z.B. die Encyclopedia of Chicago (siehe `http://www.encyclopedia.chicagohistory.org/`) und die Geisteswissenschaftliche Fakultät der Universität Graz (siehe `http://gams.uni-graz.at/`).

- **EasyDB**: Es wurde auch untersucht, ob die im UNIDAM-Projekt eingesetzte Software EasyDB (`www.programmfabrik.de/de/EasyDB`) für ein universitätsweites DAMS in Frage käme, was aber wegen mangelnder Unterstützung wichtiger Aspekte wie Langzeitarchivierung und Einhaltung von Standards nicht der Fall ist.

- **DSpace**: Das Open Source-Produkt DSpace (`www.dspace.org`), das unter anderem an der Universität Edinburgh zum Einsatz kommt, konnte bei einer Präsentation nicht überzeugen.

Fedora

Letztlich standen ein kommerzielles (DigiTool) und ein Open Source-Produkt (Fedora) zur Auswahl. Die Kostenunterschiede fielen bei der Entscheidungsfindung kaum ins Gewicht: Zwar entfallen bei Fedora die durchaus beträchtlichen Lizenzkosten, doch ist mit höherem Personalaufwand zu rechnen, um zusätzliche Features zu implementieren und das System an individuelle Bedürfnisse anzupassen.

Obwohl DigiTool durchaus allen Anforderungen entsprach (vor allem die Bedürfnisse der Universitätsbibliothek erfüllt es vorbildlich) und auch bei der Präsentation an der Österreichischen Nationalbibliothek keinen schlechten Eindruck machte, ging Fedora eindeutig als Sieger hervor.

Der große Vorteil von Fedora ist die Flexibilität: Die Kernfunktionen von Fedora beschränken sich auf die eines *Repository*, in dem die digitalen Objekte abgelegt werden. Über genormte XML-Schnittstellen (die so genannten *Web Services*) wird auf die Objekte zugegriffen. Solange diese Normen eingehalten werden, kann der Zugriff auf die Ressourcen völlig frei gestaltet werden. Diese Flexibilität ist bei einer großen und heterogenen Universität, wo verschiedene Institute und Forschungsbereiche die unterschiedlichsten Anforderungen haben, von essentieller Bedeutung.

Implementierung eines universitätsweiten Digital Asset Management Systems

Im Dezember 2006 wurde dem Rektorat ein Projektplan vorgelegt, in dem die Auswahl von Fedora empfohlen wurde und genügend Personalressourcen für Projektmanagement und Leitung sowie für die Programmierung von Zusatzfeatures zu Fedora vorgesehen waren. Dieser Projektplan wurde auch bewilligt, sodass Anfang 2007 mit der Umsetzung begonnen werden konnte.

Die ersten Pilotprojekte sollen gemeinsam mit drei Fakultäten bzw. Zentren (Informatik, Physik, Translationswissenschaften) durchgeführt werden. Die DLE Bibliotheks- und Archivwesen wird das Digital Asset Management System nicht nur betreiben, sondern auch mit eigenen Inhalten befüllen. Es ist damit zu rechnen, dass das DAM-Projekt der Uni Wien noch heuer zu ersten Ergebnissen führt, die allerdings nicht notwendigerweise öffentlich zu bestaunen sein werden – je nach gewählten Zugriffsrechten werden manche Inhalte frei zugänglich sein, andere jedoch nicht.

Der Erfolg des Projektes hängt in erster Linie von den Inhalten ab: Hochwertiger Content – z.B. Digitalisierungsprojekte, Forschungsergebnisse, die Sie als Aushängeschild der Öffentlichkeit präsentieren wollen, Lehrinhalte von Lernplattformen, die Sie für die Zukunft aufbewahren wollen – ist stets willkommen.

Peter Marksteiner

Falls Sie Interesse haben, am Digital Asset Management System der Universität Wien teilzunehmen, kontaktieren Sie bitte `dams.ub@univie.ac.at`.

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`