7.1.1 Eine kurze Geschichte der Verzeichnisdienste

Die Geschichte des Mississippi beginnt in einem mickrigen Teich irgendwo im Norden Minnesotas, die Geschichte der globalen Verzeichnisdienste mit einem dürftigen Dokument namens X.500, *Data Networks and Open System Communications*. Zu den Personen der Handlung in der Geschichte der Verzeichnisdienste gehören Standardisierungsorganisationen und Anbieter in aller Welt. Eine der Hauptpersonen ist die ITU (*International Telecommunication Union*, Internationale Telekommunikationsvereinigung). Die ITU ist eine Agentur bei den Vereinten Nationen, die für interessierte Regierungen als Forum zur Erzielung eines Konsenses über globale Telekommunikationsangelegenheiten dient. Zu den Mitgliedern der ITU gehören Hersteller und Dienstleistungsbetriebe aus über 130 Ländern.

Der Teil der ITU, der sich insbesondere mit Empfehlungen für Verzeichnisdienste befasst, ist ITU-T (*Telecommunication Standardization Sector*, Abteilung Telekommunikations-Standardisierung). Der ITU-T hieß früher *Comité Consultatif International Téléphonique et Télégraphique* (CCITT). Er gibt Empfehlungen auf einer Reihe von Gebieten aus, von der Nachrichtentechnik über Messgeräte bis hin zu Faxeinrichtungen. Diese Empfehlungen werden in Serien zusammengefasst, die mit einem Buchstaben versehen sind. Die Serie V beispielsweise deckt die Datenkommunikation über Telefonnetzwerke ab und hat so berühmte Standards wie V.34, *Wideband Analog Modem Communication* (Breitbandkommunikation über analoge Modems), oder V.90, *Connecting Analog to Digital Modems* (Verbindung analoger und digitaler Modems), hervorgebracht. Die Serie X, zu denen auch die Empfehlung X.500 für Verzeichnisdienste gehört, befasst sich mit einer Reihe von Datennetzwerk- und Kommunikationstechnologien für offene Systeme wie beispielsweise den X.400-Nachrichtensystemen. Eine vollständige Liste aller ITU-Empfehlungen in englischer Sprache finden Sie unter *www.itu.int/publications/itu-t/itutx.htm*.

Der ITU-T setzt keine Standards, sondern spricht nur Empfehlungen aus. Zur Einsetzung eines internationalen Standards bedarf es der Zustimmung der ISO (*International Organization for Standardization*, Internationale Standardisierungsorganisation). Anders als die ITU, deren Mitglieder aus der Industrie stammen, setzt sich die ISO aus Mitgliedern nationaler Standardisierungsinstitute zusammen (aus Deutschland beispielsweise das Deutsche Institut für Normung). Die ISO-Website finden Sie unter *www.ISO.ch*. Das *ch* zeigt an, dass die Seite auf einem Schweizer Server liegt – nur für den Fall, dass Sie mit den Länderkürzeln nach ISO 3166 nicht vertraut sind.

> ***Die Herkunft der Bezeichnung »ISO«***
>
> *Vielleicht wundern Sie sich, dass das Akronym ISO nicht mit dem Namen* International Organization for Standardization *korrespondiert. Tatsächlich handelt es sich hierbei auch nicht um ein Akronym, vielmehr kommt die Bezeichnung vom griechischen Wort isos, das auf Deutsch gleich heißt. Der Name wurde verwendet, um ein Durcheinander von Akronymen zu verhindern, das bei der Übersetzung von* International Organization for Standardization *in die jeweilige Landessprache entstanden wäre.*

Die ISO ist für die Einrichtung von Standards in fast allen denkbaren Bereichen zuständig, von den Qualitätsstandards des ISO 9000 bis hin zu den genormten Papiergrößen des ISO 216. In der Netzwerkbranche am bekanntesten ist ISO 7498 (*Information Technology – Open System Interconnection – Basic Reference Model*), besser bekannt als OSI-Modell. ISO-Standards, die den Datenkommunikationsbereich betreffen, werden oft gemeinsam mit dem ITU-T veröffentlicht. Die X.500-Empfehlungen für Verzeichnisdienste finden sich als ISO 9594 (*Information Technology – Open System Interconnection – The Directory*) wieder. Da die ISO die Standards bestimmt, während der ITU-T nur Empfehlungen ausspricht, ist es eigentlich widersinnig, vom X.500-Standard zu reden; trotzdem hat sich diese Bezeichnung durchgesetzt, da die beiden Dokumente identisch sind. In diesem Buch wird die Bezeichnung »x.500/9594-Standard« verwendet.

Die ISO ist die bedeutendste Standardisierungsinstitution der Welt, allerdings längst nicht die einzige. Viele Köche rühren im Standardisierungsbrei, was manchmal zu einer ziemlichen Schlammschlacht ausartet. Im Bereich der Datenkommunikation gibt es häufig Kontroversen zwischen der ISO und der IEC (*International Electrotechnical Commission*, Internationale Elektrotechnik-Kommission). Die IEC ist in den Bereichen Elektronik, Magnetik, Elektromagnetik, Elektroakustik, Telekommunikation und Energieerzeugung/-verteilung tätig und legt Terminologie, Symbole, Mess- und Leistungsstandards, Zuverlässigkeits-, Erscheinungs-, Entwicklungs-, Sicherheits- und Umweltstandards fest. Im Internet finden Sie die IEC unter *www.IEC.ch*, in Deutschland gibt es ein eigenes »Komitee der IEC«. ISO und ITU haben in Zusammenarbeit mit dem ITU-T Standards für Verzeichnisdienste veröffentlicht.

Ähnlich dem DIN in Deutschland gibt es auch in den USA eine große Standardisierungsinstitution namens ANSI (*American National Standards Institute*, Nationales Standardisierungsinstitut von Amerika) mit *sehr* vielen Beratungsgremien – nicht weiter verwunderlich in einem Land, in dem in Talkshows Millionen von Menschen regelmäßig tiefe Einblicke in ihr Sexualleben erlauben. Das Gremium mit dem größten Einfluss bei der Implementierung des X.500/9594-Standards ist die IETF (*Internet Engineering Task Force*, Spezialeinheit für Internettechnik). Die IETF ist ein Sammelsurium von Entwicklern, Forschern, Designern und völlig Wahnsinnigen aus allen betroffenen Bereichen, die Interesse an der Fortentwicklung des Internets haben. Spezielle Arbeitsgruppen der IETF stürzen sich in Scharen auf Internetprozesse, wobei sie einen Ablauf namens *Internet Standards Process* (Standardisierungsprozess für das Internet) gemeinsam nutzen; dabei handelt es sich um einen einzigartigen und etwas langatmigen Vorgang, der darin besteht, eine gute Idee erbarmungslos in Tausend Stücke zu hauen, die danach für den kollektiven Organismus leicht verdaulich sind.

Der Standardisierungsvorgang wird durch RFC-Dokumente (*Requested for Comments*, Bitte um Stellungnahme) erleichtert. Um einmal einen Eindruck davon zu geben, wie lange es dauern kann, bis neue Ideen zu Internetstandards geworden sind, sei erwähnt, dass von den Hunderten und Aberhunderten Ideen, die im RFC 2400, *Internet Official Protocol Standards* (Offizielle Protokollstandards für das Internet), erwähnt sind, bislang nur etwa drei Dutzend den erhabenen Status des »offiziellen Standards« erhalten haben. Der Rest drängelt sich noch immer im Genehmigungsprozess. Das allerdings hält die Anbieter nicht davon ab, bestimmte RFCs zu implementieren, die Bedingungen dieser RFCs hingegen sind frei wählbar (man beachte die subtile Widersprüchlichkeit dieser Formulierung). RFCs, Standards und als Standards gewünschte Dokumente, Entwürfe für das Internet und andere Arbeitspapiere findet man auf der Website der IETF (*www.IETF.org*) und verschiedenen gespiegelten Internetsites. Ich persönlich bevorzuge hierfür die Suchmaschine beim *Internet Engineering Standards Repository* unter *www.normos.org*.

Die IETF und ihre zahlreiche Anhängerschaft kann viele der durch ISO und IEC gesetzten Standards und der ITU-Empfehlungen umgehen, falls sie es für nötig hält, nützliche Protokolle zur Norm zu machen. Ein Beispiel dafür ist das LDAP-Protokoll (*Lightweight Directory Access Protocol*). LDAP ist eine abgespeckte Version des X.500-Verzeichnisdienstes. Es stellt die Basis für Active Directory, für Netscape-Verzeichnisdienste und andere Verzeichnisdienstprodukte dar. LDAP ist eine Ausgeburt des Internets; es gibt keinen LDAP-Standard, der von der ISO abgesegnet ist und keine diesbezügliche Empfehlung seitens der ITU. Active Directory implementiert die aktuellste LDAP-Version, wie sie unter RFC 2251, *Lightweight Directory Access Protocol v3*, beschrieben ist. Diese RFC erweitert und vertieft die ursprünglich unter RFC 1777, *Lightweight Directory Access Protocol*, beschriebene LDAP-Spezifikation.

Obwohl LDAP keine exakte X.500-Implementierung darstellt, stammt doch ein grundlegender Teil von X.500 ab. Aus diesem Grunde soll zunächst der X.500-Standard einer genaueren Betrachtung unterzogen werden, bevor wir uns dem LDAP-Protokoll zuwenden.

7.1.2 Der X.500-Standard

Es war das Ziel der ITU-Empfehlung X.500 bzw. des ISO/IEC-Standards 9594, das babylonische Sprachengewirr zwischen Datenbankbeständen zu beenden und eine einheitliche Methodik für Speicherung, Verteilung und Zugriff auf Benutzerinformationen zu schaffen. Ein mit dem X.500/9594-Standard kompatibler Verzeichnisdienst verfügt über einen verteilten Speicher, der praktisch alle nützlichen Informationen über die Benutzer eines Informationssystems und die zu Grunde liegende Infrastruktur beinhaltet.

Wichtig ist die *verteilte* Natur des Informationsspeichers in einem Verzeichnisdienst, da der Sinn und Zweck des Verzeichnisses letztendlich darin besteht, jedem autorisierten Benutzer Zugang zu den Daten zu geben, wo immer auch im Netzwerk er sich befinden möge. Dies mit einer einzigen Datenbank, die auf viele Server repliziert wird, im großen Stile zu realisieren, ist quasi unmöglich. In einem X.500-Verzeichnisdienst verfügen die Server deswe-

gen über Teile der Gesamtinformation und verwenden ein kompliziertes Geflecht aus Verweisen und Zeigern, um Benutzer genau zu dem Server zu geleiten, auf dem die gesuchte Information liegt.

Der Rahmen für den verteilten Informationsspeicher in einem Verzeichnisdienst entspricht den funktionalen Grenzen der implementierenden Organisation. Gut aufgebaute Verzeichnisdienste findet man in Universitäten ebenso wie bei Regierungsbehörden, Großunternehmen, Vereinen und internationalen Telekommunikationskonzernen. Für den Kegelclub oder die Skatrunde wäre die Einführung eines Verzeichnisdienstes wahrscheinlich etwas übertrieben, aber rein strukturell spräche nichts gegen einen solchen Einsatz. Man würde einen Verzeichnisdienst auch kaum zur Organisation der örtlichen Videothek verwenden; es handelt sich hierbei also nicht um ein konventionelles Datenbanksystem. Aber wenn die Videothek einer Kette angeschlossen wäre und dreitausend Videotheken samt Personal zu verwalten wäre, die über ein Netzwerk miteinander verbunden wären, dann könnte man einen Verzeichnisdienst durchaus in Betracht ziehen.

Das Wunderbare an X.500 ist die flexible Art und Weise, wie es die Verwaltung des Informationsspeichers aufsplittert. Eine Organisation mit sehr strengen Unternehmensrichtlinien, die die Computernutzung regeln, und drakonischen Strafen bei Verletzung dieser Richtlinien kann einen X.500-Verzeichnisdienst ebenso einsetzen wie der Kreisverband der Kleingärtner, bei dem praktisch keinerlei Nutzungsrichtlinien vorhanden sind. Diese Flexibilität wird mit hoher Komplexität erkauft; ein wesentlicher Faktor dabei ist ein Dickicht aus Nomenklaturen voll obskurem Computerslang und den berüchtigten »Drei-Buchstaben-Abkürzungen« (DBAs). Die durch diese Termini und Akronyme bezeichneten Vorgänge tauchen leider recht häufig in den Dokumentationen über LDAP und Active Directory auf, insofern sollte man sich doch einen KÜB (Kurzen Überblick) verschaffen (siehe Abbildung 7.1).

- Informationen werden im X.500-Verzeichnis in einer DIB (Directory Information Base, Verzeichnisinformationsbank) gespeichert.
- Die DIB ist in Teile gegliedert, die in einer als DIT (Directory Information Tree, Verzeichnisinformationsbaum) bezeichneten hierarchischen Struktur angeordnet ist.
- Jeder Teilbereich der DIB ist auf einem Server abgelegt, der als DSA (Directory Service Agent, Verzeichnisdienstagent) bezeichnet wird.
- Ein Benutzer, der Verzeichnisinformationen benötigt, stellt seine Anfragen über eine Anwendungsschnittstelle namens DUA (Directory User Agent, Verzeichnisbenutzeragent).
- Ein DUA kommuniziert mit dem DAS über das DAP-Protokoll (Directory Access Protocol, Verzeichniszugriffs-Protokoll).
- Untereinander kommunizieren die DSAs über das DSP-Protokoll (Directory System Protocol, Verzeichnissystem-Protokoll).

erfolglos ausgeschöpft wären. Der DUA ist so programmiert, dass er in letzterem Fall Alternativen vorschlüge, z.B. babyrosa BMWs.

7.1.3 Warum LDAP und nicht X.500?

Einige reinrassige X.500-Verzeichnisdienste sind auf dem Markt erhältlich, aber nur wenige haben eine hohe Verbreitung erfahren. Das Problem dieser ursprünglichen X.500-Implementierungen liegt in dem durch die vielen Protokolle verursachten Datenverkehr. Stellen Sie sich eine Armee von DUAs vor, die alle über ISO DAP mit den DSAs reden, welche wiederum Anfragen an andere DSAs über DSP aussenden, während sie gleichzeitig ihre DIB auf andere DSAs in ihrer DMD über DISP replizieren … also wirklich, das kann doch nicht Ihr Ernst sein, oder?

In den frühen neunziger Jahren wollten ein paar findige Köpfe an der Universität Michigan einen Verzeichnisdienst aufbauen, um über 100.000 Studenten, die Angestellten und ihren Fachbereich zu verwalten. Angesichts der Komplexität von X.500 verwarfen Sie diesen Standard und erstellten ein Schema, das zwar an der X.500-Verzeichnisstruktur festhielt, als Protokoll jedoch das verbreitete TCP/IP-Protokoll anstelle von ISO verwendete und den Zugriff so rationalisierte. Ferner implementierten sie einen abgespeckten Referenzierungsmechanismus und ein flexibleres Sicherheitsmodell und verzichteten auf die Festlegung eines Replikations-Protokolls. Sie nannten dieses System LDAP (*Lightweight Directory Access Protocol). Der Rest ist Geschichte. Wenn Sie mehr darüber lesen wollen, werfen Sie mal einen Blick auf die Seite www.umich.edu/~dirsvcs.*

Als man bei Microsoft beschloss, das träge, registrierungsbasierte Sicherheitssystem des klassischen Windows NT durch einen echten Verzeichnisdienst zu ersetzen, die langwierige Entwicklung eines eigenen Verzeichnisdienstes jedoch scheute, entschied man sich zur Verwendung von LDAP. Und was – aus unserer Systemadministratorensicht – noch wichtiger war: Microsoft beschloss, diesen LDAP-Verzeichnisdienst mit zwei bewährten Technologien auszuliefern. Für die Datenbank verwendeten sie eine frisierte Version der ESE (*Extensible Schema Engine*, erweiterbare Schema-Engine), die seinerzeit mit Exchange eingeführt wurde. Microsoft zog ESE dem hauseigenen SQL Server vor, da SQL im Kontext eines LDAP-Verzeichnisses nicht effizient arbeitet. Andererseits war ESE ursprünglich als objektorientierte Datenbank konzipiert. Man könnte also durchaus anmerken, dass Exchange nichts anderes gewesen sei als eine dreijährige Betaphase für Active Directory; in einer gerechten Welt würden die Hunderttausende von Exchange-Administratoren, die an diesem Betatest teilgenommen haben, von Microsoft eine entsprechende (finanzielle) Anerkennung erhalten.