Orientierungshilfe

beim

Einsatz von Verzeichnisdiensten

erstellt vom Arbeitskreis „Technik“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Stand: September 2000

In der Arbeitsgruppe haben mitgewirkt:
Fr. Meyer zu Natrup (Berliner Datenschutzbeauftragter), W. Ernestus (Bundesbeauftragter für den Datenschutz)

1. Einleitung

In den letzten Jahren hat sich die Informationstechnologie sehr schnell weiterentwickelt. Dies gilt insbesondere im Bereich der Vernetzung und der offenen Kommunikationssysteme. Die verstärkte Nutzung neuer Kommunikationsformen wie E-Mail erfordert eine neue Art der Verbreitung der Kommunikationsadressen. Hierzu werden zunehmend elektronische Verzeichnisse eingesetzt. Da auf die Informationen in diesen Verzeichnissen von verschiedenen Stellen aus direkt zugegriffen werden kann und insbesondere beliebige Informationen gespeichert werden können, geht die Funktionalität weit über die bisherigen Möglichkeiten eines in Papierform vorliegenden Adress- und Telefonverzeichnises hinaus. Hieraus ergibt sich die Notwendigkeit, dass von der datenverarbeitenden Stelle festgelegt werden muss, welche Daten im Verzeichnis gespeichert werden. Zum Einsatz kommen sowohl ISO-konforme (X.500) Systeme als auch Industriestandards (z. B. Network Directory System, NDS).

Da in einem Verzeichnisdienst auch personenbezogene Daten gespeichert werden können, ist die Betrachtung datenschutzrechtlicher Aspekte notwendig. Im Verzeichnisdienst existieren verschiedene datenschutzrechtliche Probleme. Diese betreffen zum einen technische Aspekte, wie die sichere Übertragung personenbezogener Daten, zum anderen rechtliche Aspekte, wie Inhalt, Form und Zugriff auf Einträge. Im Vordergrund steht dabei, dass schutzwürdige Belange der verzeichneten Personen nicht beeinträchtigt werden.

Diese Empfehlung befasst sich mit den Möglichkeiten des datenschutzgerechten Einsatzes von Verzeichnisdiensten. Sie basiert auf dem Betrieb eines Verzeichnisdienstes in einer definierten **Netzwerkumgebung (Intranet) innerhalb der öffentlichen Verwaltung.** Die intranetübergreifende Verbindung mehrerer Verzeichnisse, z. B. über das Internet, wird nicht betrachtet. Des Weiteren wird die generelle Problematik der Systemverwaltung der beteiligten Rechnersysteme auch nicht mit einbezogen, da diese unabhängig von Verzeichnisdiensten sind.

2. Verzeichnisdienste

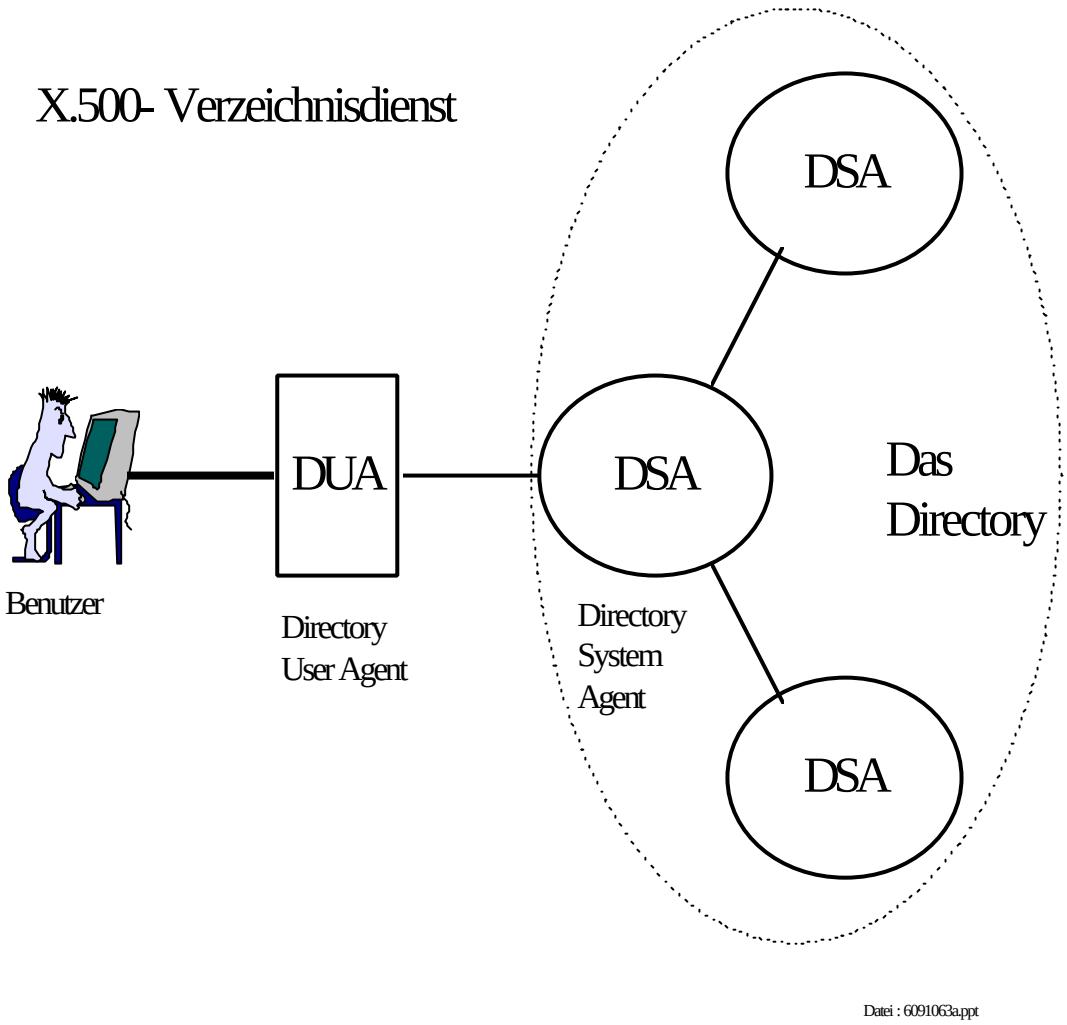
2.1 Verzeichnisdienst: X.500

X.500 (ISO-9594) ist ein von der Comité Consultatif International Télégraphique et Téléphonique (CCITT) [1] und der International Standardization Organization (ISO) erarbeiteter Standard, der einen global verteilten Verzeichnisdienst – **den Verzeichnisdienst** – beschreibt. Er kann als ein in vielen Aspekten erweitertes elektronisches Telefonbuch, dass neben Telefonnummern auch andere Kommunikationsadressen, z. B. E-Mail-Adressen, enthält, betrachtet werden.

Darüber hinaus können relativ beliebige Informationen über Organisationen, deren Mitarbeiter, Rechner, Peripheriegeräte und verfügbare Dienste, also das gesamte Spektrum aller im Kontext von vernetzten Computer- und Kommunikationssystemen vorkommenden Elementen, enthalten sein.

Die Benutzer des Directory-Systems können sowohl menschliche Benutzer als auch Anwendungsprogramme sein. Bei der Interaktion mit dem Directory greift der Benutzer über einen *Directory User Agent* (DUA) auf die Directory-Informationen zu. Dabei sieht die Verzeichnisnorm das *Directory Access Protocol* (DAP) als Zugangsprotokoll vor. Aufgrund der Komplexität hat sich dieses allerdings am Markt nicht durchgesetzt, sondern wurde teilweise (insbesondere in den Endgeräten) durch das **Lightweight Directory Access Protocol (LDAP)** als stark vereinfachtes Zugriffsprotokoll ersetzt. Das Directory besteht aus mehreren kooperierenden *Directory System Agents* (DSA), die auf verschiedenen Rechnern realisiert sein können[1].

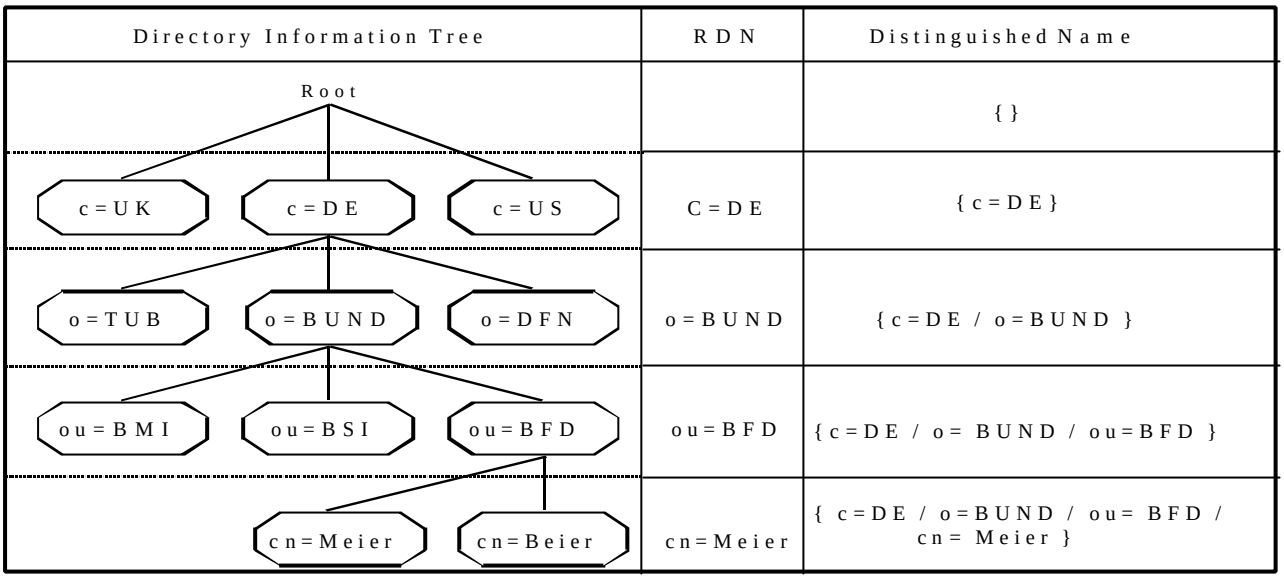
[1] Für die Kommunikation innerhalb des Directory-Systems wird das *Directory System Protocol* (DSP) verwendet.



Die Informationen, die das Verzeichnis bereitstellt, sind physikalisch über die DSAs verteilt, erscheinen jedoch für den Benutzer als eine logische Datenbasis. Die Gesamtheit aller Informationen über Objekte, die im Verzeichnis bekannt sind, wird als *Directory Information Base* (DIB) bezeichnet. Jedes Objekt wird darin durch einen Verzeichnis-Eintrag repräsentiert, der die für das Objekt relevanten Daten enthält.

Die Einträge der Datenbasis sind hierarchisch angeordnet. Die logische Sicht auf die Datenbasis erscheint als Baumstruktur[2]. Diese Baumstruktur bildet die Grundlage einer eindeutigen Namensgebung innerhalb des Verzeichnisses. Die Namen der Einträge werden gemäß einer mehrstufigen hierarchischen Namenskonvention gebildet. Ein Directory-Name (*Distinguished Name - DN*) setzt sich aus einer geordneten Folge einzelner Komponenten (*Relative Distinguished Name - RDN*) zusammen.

Datei: 6091063b.ppt



Die Namen von Einträgen der DIB sind eindeutig, d. h., jeder Name bezeichnet genau ein Objekt. Dieses wird dadurch erreicht, dass jede Namensgeberautorität (naming authority) innerhalb einer Hierarchiestufe unterschiedliche RDNs verwendet.

Jeder Eintrag im Directory besteht aus mehreren Informationen (Attributen). Ein Attribut wird durch einen Attributtyp und einen bzw. mehrere Attributwerte definiert. Ein Beispiel hierfür ist ein Personeneintrag, der folgendes Aussehen haben könnte:

Name des Eintrags (DN): {c=DE / o=Berliner Datenschutzbeauftragter / ou=Bereich Informatik und Organisation / cn=Meier}

Attributtyp	Attributwert(e)
Name	Manni
Nachname	Meier
Postanschrift	Musterstr, 1000 Musterstadt
Telefonnummer	+49 099 12345678
	+49 099 11223344
Faxnummer	+49 230 99999999
E-mail	mzn@muster.de
favourite drink	Sekt extra dry

[2] Die Directory Information Base stellt sich somit als *Directory Information Tree* (DIT) dar.

Die im Verzeichnis gespeicherten Daten müssen gegen unautorisierten Zugriff geschützt werden. Hierzu wurde in der Norm X.509 die Sicherung der im Verzeichnis durchgeführten Kommunikation beschrieben. Die dargestellten Verfahren unterscheiden zwischen schwacher und starker Authentifizierung. Die schwache Authentifizierungsprozedur basiert auf dem eindeutigen Namen (DN) und einem Passwort. Die starke Authentifizierung arbeitet mit einem asymmetrischen Kryptosystem (z. B. dem RSA-Algorithmus).

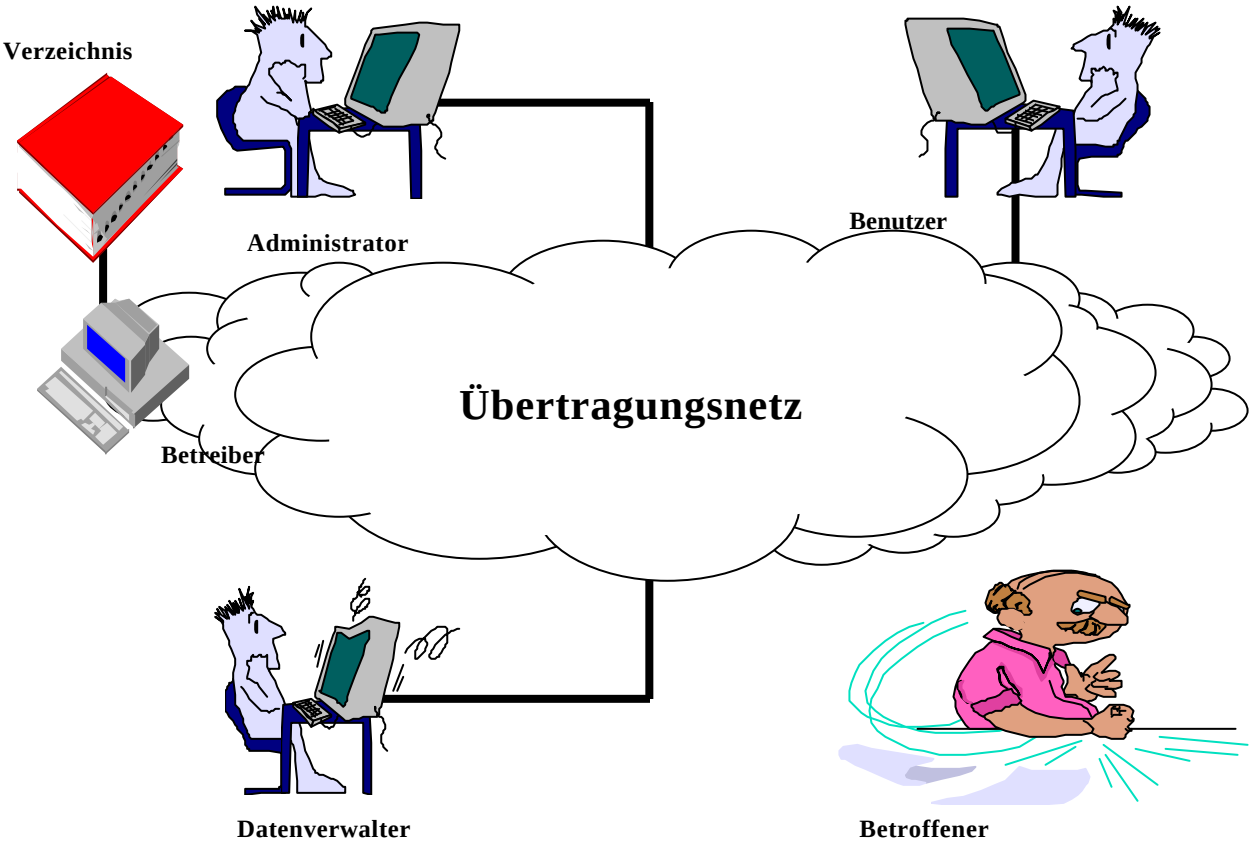
Für die Zugriffskontrolle existiert ein generelles Zugriffskontroll-Modell, das die Anwendung einer bestimmten Sicherheitspolitik (security policy), die jedoch nicht durch das Verzeichnis vorgeschrieben wird, erlaubt. Als Basis wird ein Zugriffskontroll-Schema definiert, das auf Zugriffskontroll-Listen (Access Control Lists, ACL) basiert. Über die Zugriffskontroll-Listen wird festgelegt, wer auf welche Daten in einem Eintrag in welcher Weise (beispielsweise lesend, schreibend) zugreifen kann. Die Normung des Zugriffskontrollmechanismus erfolgte im X.500-Standard erst 1993.

2.2 Network Directory System (NDS)

Das Network Directory System (NDS) ist ein von Novell entwickelter Verzeichnisdienst. Es wurde als verteilte Datenbank konzipiert und ist für die Verwaltung von Netzwerken geeignet. NDS verwaltet Informationen über alle Komponenten im Netzwerk, z. B. Benutzer, Benutzergruppen und Drucker. Ein NDS-Objekt besteht aus einer Vielzahl von Informationen – Properties genannt – und den dazugehörenden Daten, die diese Properties haben können. Es existieren Objekte, mit deren Hilfe eine Baumstruktur ähnlich wie bei X.500 aufgebaut werden kann. Für jedes Objekt können Zugriffsberechtigungen vergeben werden. Dieses wird über Access Control Lists realisiert. Die Funktionalität von NDS umfasst weniger die Bereitstellung der Telefonbuch Funktionalität, sondern eher die Verwaltung von allen Objekten in großen Netzwerken.

3. Komponenten und Beteiligte

Ein Verzeichnisdienst stellt in der Regel nur eine Unterstützungsfunktion innerhalb eines anderen Verfahrens oder Dienstes bereit, beispielsweise von Kommunikationsadressen, Telefonnummern und öffentliche Schlüssel bei der Telekommunikation. Allerdings sind auch Lösungen vorstellbar, in denen die Verzeichnisdienste die Verwaltung und Organisation von anderen Datenbestände übernehmen. In der Regel werden heute Verzeichnisdienste zur Verwaltung der Objekte in großen Netzwerken (Intranet) eingesetzt (Administration). In beiden Fällen werden für den Betrieb des Dienstes gewisse Grundkomponenten – ein Übertragungsnetz, Knotenrechner, eine verteilte Datenbank etc. – benötigt. Auch treten in allen Fällen die gleichen Beteiligten auf, die entweder den Betrieb des Verzeichnisses sicherstellen oder als Betroffener mitwirken.



4. Problemdarstellung Datenschutz

In Verzeichnisdiensten wird der eindeutige Teilnehmername (Distinguished Name, DN) definiert. Dieser Name dient als Adresse im Verzeichnis, mit der Personen gefunden werden können. Um das Verzeichnis in einer benutzerfreundlichen Weise zu organisieren, wird zur Identifizierung eine Kette von Namen und Namensteilen verlangt. Dies führt dazu, dass eine Person eindeutig identifiziert werden kann. In Verbindung mit der Möglichkeit, beliebige Informationen zu einer Personen zu speichern, erwachsen hieraus besondere datenschutzrechtliche Gefahren. Hierbei ist insbesondere die einfache Zusammenführung bisher getrennt gespeicherter Daten zu sehen. Die Verbindung von verteilt vorliegenden Informationen und eventuell existierender Kopien (Repliken) können zu Probleme hinsichtlich der Aktualität der Daten führen[3]. Dies stellt insbesondere für die datenschutzrechtlichen Anforderungen bei der Berichtigung und Löschung ein Problem dar.

Darüber hinaus bieten sich zudem noch Verknüpfungsmöglichkeiten mit anderen elektronisch vorliegenden Daten, z. B. Telefonbuch auf CD-ROM, Adressbuch auf CD-ROM etc. Dieses ermöglicht die Erstellung von sehr detaillierten Profilen, deren Umfang nicht absehbar sind.

Üblicherweise wird der Verzeichnisdienst als Unterstützungsfunktion in bestehende Verfahren integriert. Damit muss sichergestellt sein, dass der Zugriff auf Informationen in Einträgen nur auf das für die Aufgabenerledigung Notwendige beschränkt wird.

Gefahren für das informationelle Selbstbestimmungsrecht erwachsen auch aus dem komplexen Zusammenspiel der verschiedenen Komponenten, die für den Betrieb des Verzeichnisdienstes benötigt werden. Jede Komponente für sich ist dabei einer Vielzahl von Bedrohungen ausgesetzt. Für jede einzelne Komponente kann dabei von den üblichen Bedrohungspotentialen ausgegangen werden, z. B. Manipulation der Einträge auf den Telekommunikationsleitungen, Zugriffe Unberechtigter (Mithören), Zerstörung der Infrastruktur, Einspielen alter Versionen des Dienstes, Virenbefall etc.

Neben diesen allgemeinen Bedrohungen gibt es allerdings auch verzeichnisspezifische.

Das Bedrohungspotential ist abhängig vom Verbreitungsgrad und den Zugriffsmöglichkeiten auf die Inhalte. Ein Beispiel ist die Einführung eines Verzeichnisdienstes in einem Intranet, in dem nur die Adressdaten der Mitarbeiter aufgenommen wurden und das ausschließlich zur Ver-

[3] Die Möglichkeit der Replikationen ist wesentlicher Bestandteil der Funktionalität eines Verzeichnisdienstes

besserung der internen Kommunikation dienen soll. Die Verbreitung der Adressen über das eigene Netz hinaus ist nicht vorgesehen. Damit ist das Verzeichnis als eine Art "hausinternes elektronisches Telefonbuch" zu bewerten. Die Bedrohung ist als sehr gering zu bewerten.

Verzeichnisdienste können durch Nutzung von systemimmanenten Replikationsmechanismen oder durch automatisiertes Abfragen zur Bildung von zeitabhängigen Profilen missbraucht werden. Dies sollte vor allem bedacht werden, wenn Verzeichnisdienste bereitgestellt werden, da die Auswerteverfahren und –werkzeuge dann nicht kontrollierbar sind.

4.1 Rechtliche Einordnung von Verzeichnisdiensten

Soweit ein Verzeichnisdienst nur im Intranet einer datenverarbeitenden Stelle angeboten wird, handelt es sich weder um einen Tele- noch einen Mediendienst. Es liegt somit kein „Angebot" i. S. d. §§ 2 Abs. 2 TDG bzw. MDSTV vor. Die Zulässigkeit derartiger Verzeichnisdienste richtet sich daher allein nach den allgemeinen datenschutzrechtlichen Bestimmungen für Dienst- und Arbeitsverhältnisse.

Wird der Verzeichnisdienst als Basis von Personalinformationssystemen genutzt oder gar ausgebaut, ist der Personalrat (und im Bereich der Privatwirtschaft der Betriebsrat) aufgefordert, durch Nutzung seiner Mitbestimmungsrechte und Abschluss von Dienst- und Betriebsvereinbarungen die Zusammenführung von Daten zu unterbinden bzw. zu kontrollieren.

4.2 Veröffentlichung von Klarnamen

Grundsätzlich sollte allen Bediensteten, die keine herausgehobene Funktion innehaben, ein Wahlrecht dahingehend eingeräumt werden, ob sie mit ihrem Klarnamen oder mit einem selbstgewählten Pseudonym in ein über das Intranet abrufbares Verzeichnis eingestellt werden wollen. Dieses Modell könnte auch genutzt werden, um die Zusammenführung von verschiedenen Verzeichnissen zu unterbinden, wenn der Betroffene verschiedene rollenspezifische Pseudonyme wählt. Auf diese Weise könnten auch die Risiken einer unkontrollierten Sammlung personenbezogener Informationen durch Suchmaschinen begrenzt werden.

4.3 Beschäftigtendaten in Verzeichnisdiensten

Die Verarbeitung von Personaldaten ist im Bund und in den Ländern unterschiedlich geregelt. Zum Teil enthalten die allgemeinen Datenschutzgesetze einschlägige Bestimmungen, zum Teil wird die Verarbeitung in den Beamtengesetzen angesprochen, wobei einige Landesbeamtengesetze diese Regelungen im Tarifbereich für entsprechend anwendbar erklären. Das Bundesbeamtengesetz (BBG) enthält keine umfassenden Vorschriften über die Verarbeitung von Personaldaten, sondern lediglich Regelungen über die Datenerhebung und den Umgang mit Personalaktendaten. Inhaltlich stimmen alle Regelungen darin überein, dass Beschäftigtendaten verarbeitet werden dürfen, wenn dies u. a. zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht.

Soweit auf den Verzeichnisdienst nur Mitarbeiterinnen/Mitarbeiter der eigenen Verwaltung zugreifen können, dürfen die erforderlichen Angaben über sämtliche Mitarbeiterinnen/Mitarbeiter zur Verfügung gestellt werden. Erstreckt sich die Zugriffsmöglichkeit auch auf andere Stellen im jeweiligen Bundesland, dürfen Familienname, dienstliche Telefonnummer und Hinweise auf den Aufgabenbereich von solchen Personen in den Verzeichnisdienst aufgenommen werden, die den Anschluss aus dienstlichen Gründen nutzen müssen und bei denen die Erreichbarkeit zu ihrer dienstlichen Aufgabe gehört.

Unterschiedlich ist die Frage zu beurteilen, ob über diese Angaben hinaus die Amtsbezeichnung oder der Vorname in den Verzeichnisdienst eingestellt werden darf. Hier greifen unterschiedliche Regelungen in den einzelnen Bundesländer, so dass auf die gültige Rechtslage verwiesen wird.

Für Bedienstete, die in der Regel keinen unmittelbaren Kontakt außerhalb der eigenen Dienststelle haben (z. B. Angehörige interner Dienste, wie des Schreib- oder Botendienstes), ist die Bekanntgabe ihrer Daten nicht erforderlich. Deren Aufnahme in den Verzeichnisdienst wäre – soweit er über ein internes Verzeichnis hinausgeht – nur mit Einwilligung zulässig. Landesrechtliche Besonderheiten sind zu berücksichtigen.

Soweit die Auffassung vertreten wird, dass Name, Dienst-, Funktionsbezeichnung und Organisationseinheit von Bediensteten wegen ihres engen Bezuges zur amtlichen Tätigkeit nicht deren grundsätzlicher Verfügungsbefugnis und damit ihrem Recht auf informationelle Selbstbestimmung unterfallen (Amtswaltertheorie), ergeben sich keine anderen Ergebnisse.

Das Erfordernis, die genannten Daten für dienstliche Zwecke einzusetzen, dürfte sich regelmäßig auf das jeweilige Bundesland beschränken. Bei einer über den Landesbereich hinausgehenden Bereitstellung von Daten, beispielsweise bei einer Verbindung zweier öffentlicher Netze, empfiehlt sich – wie allgemein in Zweifelsfällen – der Abschluss einer Dienstvereinbarung.

5. Maßnahmen

Aus datenschutzrechtlicher Sicht sind beim Betrieb eines Verzeichnisdienstes technische und organisatorische Maßnahmen vorzunehmen, die geeignet sind, den aufgeführten Gefahren und Bedrohungen entgegenzuwirken.

Für die Komponenten, auf die der Verzeichnisdienst aufsetzt, sind hinreichende und angemessene technische und organisatorische Datenschutzmaßnahmen zu realisieren. Allgemeine Empfehlungen finden sich in entsprechenden Orientierungshilfen (z. B. Unix-Systeme, PCs, Mail-Systeme oder Datenträger) oder auch im BSI-Grundschutzhandbuch, im UNIX-Leitfaden des Hamburger Datenschutzbeauftragen und in Checklisten des Landesbeauftragten für den Datenschutz in Niedersachsen.

Über die grundlegenden Maßnahmen hinaus ist beim Einsatz von Verzeichnisdiensten Folgendes zu beachten:

- Der Verzeichniseintrag ist auf die notwendigen Angaben zu beschränken, beispielsweise E-Mail-Adresse, Telefonnummer, Faxnummer, öffentliche Schlüssel etc. Andere Informationen wie Hinweise auf Zuständigkeiten, Aufgabenbereiche, Tätigkeitsfelder, Arbeitszeiten, Örtlichkeiten etc. sollten, soweit nicht für die Aufgabenerledigung notwendig, nicht in das Verzeichnis aufgenommen werden.

- Die Zugriffsregelungen sind so eng wie möglich zufassen. Die Verantwortung hierzu muss eindeutig und durch eine hierfür verantwortliche Stelle vorgenommen werden. Grundsätzlich sollten starke Authentifizierungsmechanismen (Digitale Signatur, biometrische Verfahren) zum Einsatz kommen (siehe Kapitel 2.1). Produkte, die lediglich dem X.500-Standard entsprechen, sind nicht einzusetzen.

- Die Organisation des Verzeichnisdienstes muss so gestaltet werden, dass sicherstellt ist, dass die Einträge des Verzeichnisdienstes immer in möglichst zeitnaher Aktualität vorliegen. Dies schließt auch Kopien des Verzeichnisses (Repliken) ein.

- Die Neueinrichtung, Änderung und Löschung von Verzeichniseinträgen sowie die Erstellung und Verbreitung von Repliken sind zu Zwecken der Revision und Datenschutzkontrolle zu protokollieren. Sofern die Protokollierung kein Bestandteil des Produkts ist, muss eine ausreichende Protokollierung durch andere Komponenten, beispielsweise dem Betriebssystem, sichergestellt werden.

- Es ist zu prüfen, zu welchen Personen Angaben im Verzeichnisdienst zur Verfügung gestellt werden dürfen.

- Der Verzeichniseintrag ist auf die Angaben zu beschränken, die in der ausgeübten Funktion für die Nutzer des Verzeichnisses relevant sind.

- Vor "Veröffentlichung" des Eintrags im Verzeichnis müssen dem Betroffenen die Daten des Eintrags zur Einsichtnahme und/oder Korrektur vorgelegt werden. Anhand von Attributen ist eine Filterung der Verzeichniseinträge nach dem Gesichtspunkt der internen/externen Bereitstellung zu ermöglichen oder die Möglichkeit zu schaffen, dass die Betroffenen selbst eine Sperrung oder Freischaltung bestimmter Attribute vornehmen können.

- Zur Sicherung der Integrität sind bei der Übertragung grundsätzlich kryptographische Verfahren einzusetzen. Ist die Vertraulichkeit von Verzeichnisdaten zu gewährleisten, z. B. bei Abfragen oder Replikation über unsichere Leitungen, so sind auch hierfür geeignete kryptographische Methoden zu benutzen. Dazu stehen auch Werkzeuge außerhalb des Verzeichnisdienstes (etwa zur Verbindungsverschlüsselung) zur Verfügung.