Alexander Tsolkas | Klaus Schmidt

Rollen und Berechtigungs-konzepte

Ansätze für das Identity- und Access Management im Unternehmen

PRAXIS

VIEWEG+ TEUBNER

‹kes›

Alexander Tsolkas | Klaus Schmidt

Rollen und Berechtigungskonzepte

Edition <kes>

herausgegeben von Peter Hohl

Mit der allgegenwärtigen Computertechnik ist auch die Bedeutung der Sicherheit von Informationen und IT-Systemen immens gestiegen. Angesichts der komplexen Materie und des schnellen Fortschritts der Informationstechnik benötigen IT-Profis dazu fundiertes und gut aufbereitetes Wissen.

Die Buchreihe Edition <kes> liefert das notwendige Know-how, fördert das Risikobewusstsein und hilft bei der Entwicklung und Umsetzung von Lösungen zur Sicherheit von IT-Systemen und ihrer Umgebung.

Herausgeber der Reihe ist Peter Hohl. Er ist darüber hinaus Herausgeber der <kes>– Die Zeitschrift für Informations-Sicherheit (s. a. www.kes.info), die seit 1985 im Secu-Media Verlag erscheint. Die <kes> behandelt alle sicherheitsrelevanten Themen von Audits über Sicherheits-Policies bis hin zu Verschlüsselung und Zugangskontrolle. Außerdem liefert sie Informationen über neue Sicherheits-Hard- und -Software sowie die einschlägige Gesetzgebung zu Multimedia und Datenschutz.

Konfliktmanagement für Sicherheitsprofis
Von Sebastian Klipper

Security Awareness
Von Michael Helisch und Dietmar Pokoyski

Mehr IT-Sicherheit durch Pen-Tests
Von Enno Rey, Michael Thumann und Dominick Baier

Der IT Security Manager
Von Heinrich Kersten und Gerhard Klett

ITIL Security Management realisieren
Von Jochen Brunnstein

IT-Sicherheit kompakt und verständlich
Von Bernhard C. Witt

IT-Risiko-Management mit System
Von Hans-Peter Königs

Praxis des IT-Rechts
Von Horst Speichert

IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz
Von Heinrich Kersten, Jürgen Reuter und Klaus-Werner Schröder

Datenschutz kompakt und verständlich
Von Bernhard C. Witt

Profikurs Sicherheit von Web-Servern
Von Volker Hockmann und Heinz-Dieter Knöll

www.viewegteubner.de

Alexander Tsolkas | Klaus Schmidt

Rollen und Berechtigungs-konzepte

Ansätze für das Identity- und Access Management im Unternehmen

Mit 121 Abbildungen

PRAXIS

VIEWEG+
TEUBNER

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

1. Auflage 2010

Lektorat: Christel Roß | Maren Mithöfer

Vieweg+Teubner Verlag ist eine Marke von Springer Fachmedien.
Springer Fachmedien ist Teil der Fachverlagsgruppe Springer Science+Business Media.
www.viewegteubner.de

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg
Druck und buchbinderische Verarbeitung: MercedesDruck, Berlin
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.
Printed in Germany

ISBN 978-3-8348-1243-8

Dieses Buch widme ich Susanne Slater, die eine große Bedeutung in meinem Leben hat.

Dieses Buch widme ich meiner lieben Familie, Franzi, Helen und Olivia. Es tut mir sehr leid, dass ihr in der Zeit der Erstellung dieses Buches weniger von mir hattet, und ich weniger von euch hatte. Dies sei nun wieder anders. ☺

Vorwort

Berechtigungen begegnen uns täglich in unserem Leben und jeder von uns besitzt eine Menge davon. Es sind Berechtigungen, Türen zu öffnen, Fahrzeuge zu führen oder in ein Land einzureisen. Auch im Unternehmen[1] und am Arbeitsplatz finden sich viele Berechtigungen für Dinge, die nur bestimmte Mitarbeiter[2] tun oder sehen dürfen. In diesem Buch konzentrieren wir uns auf IT-gestützte Berechtigungen im Unternehmen und deren unternehmensweite Organisation, Verwaltung und Steuerung.

Es wird zu sehen sein, dass das Thema Rollen- und Berechtigungskonzepte kein vorwiegend technisches Thema ist, obwohl es um IT-Berechtigungen geht und die Verwaltung und Steuerung natürlich mit Hilfe der IT erfolgt. Es sind vor allem die organisatorischen und konzeptionellen Teile, die über Erfolg und Misserfolg der Berechtigungsverwaltung entscheiden. Daher kommt der Planung der Berechtigungsorganisation eine besondere Bedeutung zu.

In *Kapitel 1* stellen wir zunächst die Grundelemente der Berechtigungsthematik vor, beginnend mit der Klärung, was eine Berechtigung ist und aus was sie besteht. Auch das Wesen von Rollen, Attributen oder Gruppen wird hier erläutert. Einsteiger lernen hier die Elemente kennen, mit denen später gearbeitet wird, aber auch für Profis ist vielleicht der eine oder andere interessante Aspekt dabei.

Kapitel 2 widmet sich dem Management von Identitäten und es wird erklärt, warum man nicht von Benutzern, sondern von Identitäten spricht. Dort wird auch klar, dass der Begriff Identity Management nicht eindeutig verwendet wird.

Ein wichtiges Element in der Berechtigungsthematik ist die Rolle. Aus diesem Grund behandelt *Kapitel 3* das Thema Rollenkonzept, darin geht es um die Fragen, warum Rollen sinnvoll sind und wie Rollen gefunden, organisiert und eingesetzt werden können. Für Fortgeschrittene werden auch komplexere Dinge wie Rollenhierarchien, Rollenebenen und Vererbung angesprochen.

Kapitel 4 stellt mit dem Standard der rollenbasierten Zugriffskontrolle (Role Based Access Control, RBAC) den eher theoretischen Überbau der Berechtigungssteuerung vor. Zugriffsbedingungen und -elemente lassen sich mathematisch beschreiben, und über Regeln können auf diese Weise vollständige Zugriffspolicies definiert werden.

---

[1] Wenn in diesem Buch von Unternehmen die Rede ist, sind damit gleichermaßen auch andere Organisationen, Behörden usw. gemeint.

[2] Wenn in diesem Buch die männliche Form der Bezeichnung einer Person gewählt wurde, so sind damit in gleicher Weise Frauen und Männer gemeint.

In *Kapitel 5* geht es zur Sache, und der Weg von der Identität zu den Ressourcen wird mit Hilfe der in Kapitel 1 vorgestellten Elemente gestaltet. Schnell wird hier klar, dass es dazu ganz verschiedene Möglichkeiten gibt und dass es auf die Situation und die Strategie im jeweiligen Unternehmen ankommt, welche der bestehenden Möglichkeiten als passend zu betrachten ist.

Den Prozess des Berechtigens, also die Frage, wie kommt eine Identität zu den Berechtigungen, wird in *Kapitel 6* betrachtet, in dem sich alles um das Thema Provisioning dreht. Die einzelnen Arten von Provisioning, sei es das User-, Resource-, Server- oder Service Provisioning werden besprochen und die Anwendung von Regeln und Policies im Provisioning gezeigt.

Vor der Nutzung eines Systems bzw. einer Anwendung tritt oftmals mit dem Login eine erste, relativ globale Berechtigung auf, nämlich das System bzw. die Anwendung überhaupt „betreten" zu dürfen. *Kapitel 7* zeigt, welche Möglichkeiten für diese Authentifizierung zu finden sind, bevor in *Kapitel 8* die Autorisierung thematisiert wird, d.h. die Zugriffskontrolle im System bzw. der Anwendung.

Eine für viele Unternehmen spannende Sache ist das Thema Single Sign On, bei dem eine Identität mit dem Login Zugang zu allen Ressourcen bekommt, für die sie berechtigt ist. *Kapitel 9* beleuchtet die Ansätze zu diesem Konzept.

Mit *Kapitel 10* wird ein systemnahes Berechtigungskonzept mittels des Großrechnersicherheitssystem CA-ACF2 unter die Lupe genommen. Es wird beschrieben, wie man die Sicherheit mittels des von ACF2 bereitgestellten User Identification Strings –UID einer ganzen Organisation einfach abbilden kann.

Eine weitere, spannende Technologie im Bezug auf Berechtigungssysteme sind Meta Directories, denen *Kapitel 11* gewidmet ist. Dazu wird das Konzept von Verzeichnisdiensten erklärt und gezeigt, wie ein Meta Directory für die Berechtigungsverwaltung eingesetzt werden kann.

Den Trend, Berechtigungen nicht nur innerhalb des Unternehmens, sondern unternehmensübergreifend zu verwalten, greift *Kapitel 12* auf, in dem das Thema Identity Federation besprochen wird. Neben dem allgemeinen Konzept finden sich auch die technischen Protokolle wie SAML, SPML oder DSML, so dass verständlich wird, wie mit Hilfe von XML-basierter Kommunikation Berechtigungen systemunabhängig formuliert und verwaltet werden können.

Kapitel 13 schließt das Buch mit Betrachtungen zu den rechtlichen Rahmenbedingungen ab. Dabei werden wichtige rechtliche Grundlagen aufgezeigt, die nicht nur im Hinblick auf die Berechtigungsthematik Relevanz besitzen.

Neben den Autoren haben noch viele andere Personen Anteil an der Entstehung eines Buches, und so ist es auch bei diesem Buch. Das Seminar „Rollen- und Berechtigungskonzepte“ des Management Circle, geleitet vom Autor Klaus Schmidt, gab ihm den Anstoß zu diesem Buch, daher seien an dieser Stelle auch die Referenten Wolfgang Scholz von der FinanzIT und Christian Himmer von der Bayerischen Landesbank erwähnt.

Alexander Tsolkas hatte den Antrieb, dieses Buch zu veröffentlichen aus der betrieblichen Praxis, da er in vielen Firmen, die er beraten hat und berät, zum Teil unstrukturierte Zustände im Identitätsmanagement vorfand. Erwähnt sei Michael Louis Smith, ehemals EDS Xerox Account in Rochester, N.Y., USA, mit dem der Autor 1994 in 2 Monaten vor Ort ein Rollen- und Autorisierungskonzept für ganz Xerox USA/Mexiko für die Mainframes unter ACF2 erstellen durfte. Hilfreich für dieses Buch war auch die Planung des Rollen- und Berechtigungskonzepts im Rahmen des Sicherheits- und Betriebskonzeptes für das Outsourcing der Bürokommunikationssysteme Land Baden-Württemberg, erwähnt sei Herr Grell von der Staabsstelle für Verwaltungsreform BaWü, von dem ich viel gelernt habe. Weiterhin möchte ich gerne erinnern an Otto Schell von General Motors Europe und Dr. alias Doc. Hildebrandt, damals Opel Revision, mit denen der Autor das Berechtigungskonzept der damals größten SAP-Installation in Europa für GME mit korrigieren durfte. Auch der Job meiner letzten Festanstellung als CSO der Schenker AG, der es mir damals möglich machte, 5 ganze Jahre weltweit einen Einblick in die Sicherheit von Unternehmen zu gewinnen, trug zu diesem Buch bei.

Die Autoren möchten sich bei allen bedanken, die in Gesprächen und Diskussionen einen Beitrag zu diesem Buch geleistet haben. Allen, die Ratschläge erteilt, konstruktive Kritik geübt und Hinweise gegeben haben: Ein herzliches Dankeschön dafür. Lieber Johannes, ein spezielles Dankeschön an den „Rechtsgelehrten“ für den Review von Kapitel 15.

Unser Dank geht herzlichst an Fr. Dr. Roß vom Vieweg+Teubner Verlag für die Betreuung dieses Buchprojekts.

Neuhof und Riedstadt, im Frühjahr 2010

Klaus Schmidt

Alexander Tsolkas

Inhaltsverzeichnis

1 Elemente zur Berechtigungssteuerung

Eines der primären Ziele von unternehmensweiten Rollen- und Berechtigungskonzepten ist eine elegante und effiziente Berechtigungssteuerung. Die Grundlage für die Steuerung ist die Systematik, nach der die Berechtigungen organisiert und strukturiert sind. Die Strukturierung erfolgt mit Hilfe von Gestaltungs- oder Steuerungselementen, denen Identitäten und Berechtigungen zugeordnet werden.

Das primäre Ziel der Berechtigungssystematik ist es, einzelne Berechtigungen in größere Einheiten zusammen zu fassen, um sie damit schneller, übersichtlicher und eleganter zuordnen zu können. Mit einer durchdachten Gestaltung dieser Elemente lassen sich die erwähnten Steuerungsziele auch dann erreichen, wenn eine große Anzahl von Berechtigungen zu steuern ist oder die Berechtigungen miteinander verknüpft und/oder ineinander verschachtelt werden müssen.

Bevor in Kapitel 5 auf die Berechtigungsvergabe und -steuerung unter Verwendung dieser Elemente näher eingegangen wird, erscheint es sinnvoll, zunächst das Wesen und die Bedeutung dieser Elemente vorzustellen und ihre Funktionsweise zu erläutern. Dies ist die Aufgabe dieses Kapitels.

1.1 Berechtigung

Das elementarste Element für die Strukturierung von Berechtigungen ist die Berechtigung selbst. Berechtigungen schützen Ressourcen vor unbefugtem Zugriff, so dass nur demjenigen der Zugriff gestattet wird, der über die benötigten Berechtigungen verfügt. Da es sich sowohl beim Ausführen von IT-Funktionen als auch beim Aufrufen von IT-Inhalten um IT-Zugriffe handelt, spricht man auch von *Zugriffsberechtigungen*.

Möchte man zum Ausdruck bringen, dass es sich um eine Berechtigung handelt, die sich auf eine IT-Funktion bezieht, wird auch der Begriff *Ausführungsberechtigung* verwendet. Er besitzt noch eine weitere Bedeutung, denn mit diesem Begriff wird auch die Berechtigung zum Starten einer ausführbaren Datei (Programm oder Skript) bezeichnet.

Aufbau einer Berechtigung

Eine Berechtigung besteht aus zwei Komponenten:

1. *Zu berechtigendes Objekt*
   Die erste Komponente gibt an, welches Objekt mit der Berechtigung geschützt wird. Das Objekt kann entweder ein Inhalt sein, auf den über eine IT-Applikation zugegriffen wird, oder eine Funktion, die ausgeführt wird. Um den Bezug zu dem zu schützenden Objekt zu verdeutlichen, wird hierfür auch der Begriff Berechtigungsobjekt verwendet.
   Das Objekt selbst wird auch als *Ressource* bezeichnet, da es Funktionen und Inhalte

A. Tsolkas, K. Schmidt, *Rollen und Berechtigungskonzepte*, DOI 10.1007/978-3-8348-9745-9_1,

bereitstellt, die von den Identitäten (z.B. Benutzern) genutzt werden können. Ressourcen werden in *Funktionsressourcen* und *Inhaltsressourcen* unterschieden, je nachdem was durch die Ressource bereitgestellt wird. Eine Ressource kann dabei auch gleichzeitig Funktions- und Inhaltsressource sein, nämlich dann, wenn beides durch die Ressource bereitgestellt wird.

In prozessorientierten Betrachtungen findet man auch den Begriff *Berechtigungspunkt*. Er gibt an, wann (an welcher Stelle) man beim Arbeiten mit der Ressource auf die jeweilige Berechtigungsprüfung trifft. Der Berechtigungspunkt kann dabei eher global (z.B. beim Start einer IT-Anwendung) oder eher atomar sein (z.B. beim Aufruf einer einzelnen Funktion in einer IT-Anwendung), je nachdem wie fein der Schutz der Ressource gestaltet sein muss.

In der Realität hat man es nicht nur mit voneinander losgelösten Objekten zu tun, sondern auch mit hierarchisch angeordneten, d.h. über- und untergeordneten Objekten. So kann ein Telefon als Ganzes ein zu berechtigendes Objekt sein, aber auch jede Zifferntaste auf dem Telefon kann ein zu berechtigendes Objekt darstellen.

2. *Zu berechtigende Operation*
   Als zweite Komponente muss noch angegeben werden, welche Operation bzw. Aktion in Bezug auf das Berechtigungsobjekt mittels der jeweiligen Berechtigung freigegeben bzw. gesperrt werden soll. Während es bei einer Inhaltsressource wie z.B. einer Festplatte bzw. einem Dateisystem meist einen einheitlichen Satz von Operationen gibt, orientieren sich die Operationen bei Funktionsressourcen an der jeweiligen Funktionalität, so dass es dort keine Einheitlichkeit geben kann.

Anhand eines Beispiels sollen die Komponenten verdeutlicht werden (siehe Abbildung 1.1). Die **Ressource** im weiteren Sinne ist hier die TK-Anlage mit den angeschlossenen Nebenstellen. Im engeren Sinne ist die Ressource die Nebenstelle 746.

Im Hinblick auf das **zu berechtigende Objekt** bzw. den Berechtigungspunkt ergibt sich eine dreistufige Objekthierarchie. Die oberste Ebene bildet die TK-Anlage als Ganzes, die zweite Ebene besteht in der Nebenstelle 746, die dritte Ebene ist die jeweilige Verbindungsart (Verbindungen im Ortsnetz, zu Mobilfunknetzen usw.) in der Nebenstelle 746.

Innerhalb der Berechtigungsplanung muss entschieden werden, auf welcher Ebene die Berechtigungen verwaltet und gesteuert werden sollen bzw. müssen. Im Beispiel der TK-Anlage wird beispielsweise die Berechtigung für interne Gespräche in der Regel auf der Ebene der TK-Anlage gesteuert, d.h. sie wird global für jede Nebenstelle vergeben.

Die **zu berechtigende Operation** besteht darin, über die jeweilige Verbindungskategorie zu kommunizieren. Die Operation „kommunizieren" ist dabei keine atomare Operation. Sie kann weiter zerlegt werden in die Operationen „Verbindungen der jeweiligen Verbindungskategorie aufbauen", „Informationen austauschen" und „Verbindung abbauen". Es macht in den meisten Fällen bei einer TK-Anlage aber keinen Sinn, die Operationen auf dieser atomaren Ebene zu schützen, so dass die atomaren Operationen zusammengefasst und als eine einzige Operation behandelt werden.

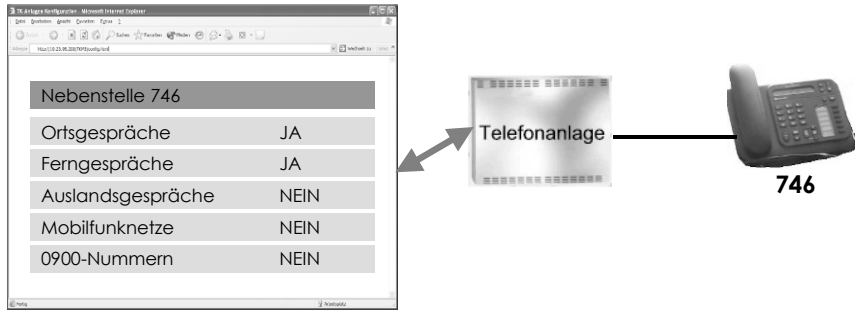

Abbildung 1.1: Berechtigungen in einer TK-Anlage

Das gezeigte Beispiel verdeutlicht die spezifischen Operationen bei Funktionsressourcen, denn die Operation „über eine Verbindungskategorie kommunizieren" wird man in dieser Form in anderen IT-Systemen nicht finden. Bei Inhaltsressourcen lassen sich dagegen einige, oft verwendete Operationen identifizieren. Berechtigungen für sensible Operationen wie das Löschen von Inhalten schließen oft Berechtigungen für weniger sensible Operationen mit ein, weshalb auch von Berechtigungsstufen gesprochen wird. Die meistgebrauchten Operationen im IT-Umfeld sind:

- *Entdecken (Detect)*
  Mit dem Besitz der Berechtigung zur Durchführung der Detect-Operation (kurz: Detect-Berechtigung) darf die Existenz des jeweiligen Objekts festgestellt werden, auf das sich die Detect-Berechtigung bezieht. Weitere Rechte sind damit nicht verbunden, d.h. das Objekt darf weder gelistet noch angezeigt werden.
- *Suchen (Search / Find)*
  Während bei der Detect-Berechtigung der Ablageort des Objekts genau bekannt sein muss, gestattet es die Search-Berechtigung, nach dem Objekt zu suchen. Auch eine unscharfe Suche kann möglich sein, so dass das Objekt auch dann lokalisiert werden kann, wenn der genaue Bezeichner des Objekts nicht bekannt ist. Die Search-Berechtigung schließt die Detect-Berechtigung mit ein.
- *Vergleichen (Compare)*
  Die Compare-Berechtigung gestattet es, Vergleiche durchzuführen. Das bekannteste Beispiel für ein Objekt mit Compare-Berechtigung ist das Passwort. Es darf nicht gelesen werden, aber eine Passwort-Eingabe darf mit dem gespeicherten Passwort verglichen werden. Desgleichen ist es mit der Compare-Berechtigung möglich, Vergleiche zwischen Objekten durchzuführen, z.B. zwei Dateien zu vergleichen und festzustellen, welche Datei mehr Speicherplatz verbraucht. Die Compare-Berechtigung schließt die Detect-Berechtigung mit ein.
- *Darstellen oder Zeigen (Show)*
  Während bei den vorhergegangenen Operationen das Objekt selbst noch relativ „im Dunkeln lag", gestattet es die Show-Berechtigung, das Objekt als Ganzes anzuzeigen. Es

darf beispielsweise in Listen und Verzeichnissen aufgeführt werden. Die Show-Berechtigung schließt die Search- und Compare-Berechtigung mit ein.

- *Lesen (Read)*
  Die Read-Berechtigung ist die erste Berechtigung, die einen Zugriff auf das Objekt gestattet. Ist das Objekt eine Datei, dann darf sie geöffnet und der Inhalt angezeigt und/oder ausgelesen werden. Weiterhin können Attribute und Verwaltungsinformationen des Objekts angezeigt werden. Die Read-Berechtigung schließt die Show-Berechtigung mit ein.
- *Hinzufügen (Add)*
  Bei den bislang beschriebenen Operationen blieb der Zustand der Inhaltsressource unverändert. Mit der Add-Berechtigung ist es nun jedoch möglich, neue Objekte in die Ressource aufzunehmen, z.B. eine neue Datei im Dateisystem abzulegen.
  Damit wird der Zustand der Ressource verändert. Dies ist besonders für die IT-Security von Bedeutung, denn mit der Add-Berechtigung entstehen Bedrohungen wie die Überflutung (Flooding) durch massenhaft angelegte Dateien oder die Blockierung (Blocking) durch einzelne, aber sehr umfangreiche Dateien.
  Die Add-Berechtigung schließt nur die Detect-Berechtigung mit ein, was zu der kuriosen Situation führen kann, dass ein Benutzer zwar in einem Dateiverzeichnis eine Datei anlegen kann, diese dann aber nicht lesen darf. Viele IT-Systeme fangen dies dadurch ab, dass sie der anlegenden Identität automatisch entsprechende Berechtigungen vergeben.
- *Ändern (Change / Modify)*
  Mit der Change- bzw. Modify-Operation beginnen die kritischen Operationen, denn mit dieser Operation können Inhalte manipuliert und zerstört werden. Die Change-Berechtigung gestattet es, die Inhalte der Ressource zu verändern. Es können neue Inhalte hinzugefügt und bestehende Inhalte weggenommen werden.
  Bei einer Datei ist es damit möglich, durch Wegnahme des gesamten Inhalts die Datei faktisch zu löschen, auch wenn keine Löschberechtigung für die Datei besteht. Aus diesem Grund wird die Change-Berechtigung oft mit der Löschberechtigung kombiniert, was zu der Operation „schreiben" (write) führt. Die Change-Berechtigung schließt die Read-Berechtigung mit ein.
- *Löschen (Delete)*
  Um ein Objekt als Ganzes vollständig zu entfernen, wird die Operation Delete (löschen) verwendet. Die Delete-Berechtigung schließt die Detect-Berechtigung mit ein.
- *Ausführen (Execute)*
  Die Execute-Operation wird verwendet, um ausführbare Inhalte wie Programme oder Skripte zu starten. Die entsprechende Execute-Berechtigung schließt die Detect- und oft auch die Show-Berechtigung mit ein.

Die weiter oben beschriebenen Komponenten einer Berechtigung lassen sich mit der folgenden Frage gut merken: „Welches Objekt soll genutzt und damit was getan werden?". Ist das Objekt in ein übergeordnetes Objekt eingebettet (z.B. wenn es sich bei dem Objekt um

eine Funktion einer Anwendung handelt), dann lässt sich die Frage zu „Welche Ressource soll genutzt und darin an welcher Stelle was getan werden?“ erweitern.

Die Berechtigung an sich sagt jedoch noch nichts darüber aus, *für wen* die Funktion bzw. der Inhalt freigegeben wird. Dies lässt sich erst dann sagen, wenn die Berechtigung einer Identität zugeordnet wurde. Dieser Schritt wird als Berechtigungsvergabe bezeichnet und in Kapitel 5 dargestellt.

Beispiel: UNIX-Dateisystem

Das UNIX-Dateisystem verwaltet die Dateien in einem UNIX-System. Jedes Objekt (Datei) wird über den Zugriffsschutzmechanismus des Dateisystems vor unbefugtem Zugriff geschützt. Jede Datei besitzt einen Eintrag im Dateikatalog und wird durch den Dateinamen im Dateisystem repräsentiert. Daraus ergibt sich, dass der Dateiname innerhalb eines Dateiverzeichnisses eindeutig sein muss.

Gemäß dem bereits dargestellten Aufbau von Berechtigungen, bestehen auch UNIX-Berechtigungen aus den beiden Komponenten Objekt und Operation. Wie Abbildung 1.2 zeigt, ist das Objekt die Datei, die durch den Dateieintrag repräsentiert wird. Als Operationen stellt das Dateisystem die drei Operationen read, write und execute zur Verfügung.

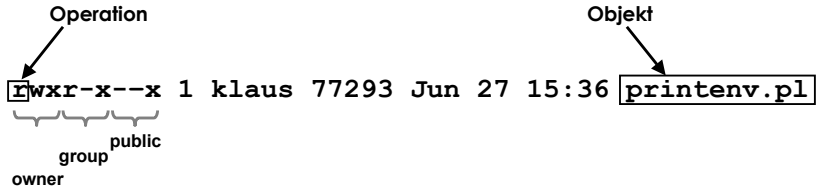

Abbildung 1.2: Berechtigungen im UNIX-Dateisystem

Um die Berechtigungen besser strukturieren bzw. steuern zu können, sind im UNIX-Dateisystem drei technische Rollen vorgesehen (zum Begriff der technischen Rolle siehe Abschnitt 1.2.2):

- *Owner*
  Als Besitzer einer Datei wird zunächst die Identität angesehen, die die Datei erzeugt bzw. im Dateisystem anlegt. Die Eigentümerschaft kann mit der Systemfunktion change owner (chown) nachträglich auf eine andere Identität übertragen werden. In der Regel verfügt der Besitzer über die umfangreichsten Berechtigungen zu einer Datei.
- *Group*
  Im UNIX-Dateisystem kann eine Datei einer Gruppe zugeordnet werden. Für die Mitglieder der Gruppe lassen sich zu der Datei eigene Zugriffsberechtigungen festlegen. In UNIX ist die Verwendung der Gruppen die einzige Möglichkeit, um Berechtigungen zu

strukturieren. Das muss beim Aufbau des Berechtigungswesens und bei der Abbildung der Gestaltungselemente berücksichtigt und entsprechend realisiert werden.

- *Public*
  Die Bezeichnung „public" (öffentlich) ist etwas irreführend, denn sie suggeriert, dass jedermann gemäß der vergebenen Berechtigungen zugreifen kann. Das ist jedoch nicht der Fall. Der Begriff Public meint vielmehr: „Alle authentifizierten Benutzer des Sytems".

Beispiel: Zugriffskontrollliste

Eine Zugriffskontrollliste (Access Control List, ACL) ist eine Zusammenfassung von Berechtigungen, die sich auf ein gemeinsames Objekt beziehen. Als Beispiel wird hier die Zugriffsverwaltung einer frühen Verzeichnisdienstimplementierung gezeigt (zu Verzeichnisdiensten bzw. Meta-Directory siehe Kapitel 11).

In Abbildung 1.3 sieht man links oben eine Dateneinheit (Eintrag) im Sinne einer elektronischen Visitenkarte im Verzeichnisdienst. Darunter sind die Berechtigungen zu sehen, die die Zugriffskontrollliste bilden. Die Komponenten Objekt und Operation sind auch hier zu finden. Zusätzlich zur Berechtigung wird in der Zugriffskontrollliste auch vermerkt, wer diese Berechtigung ausüben darf.

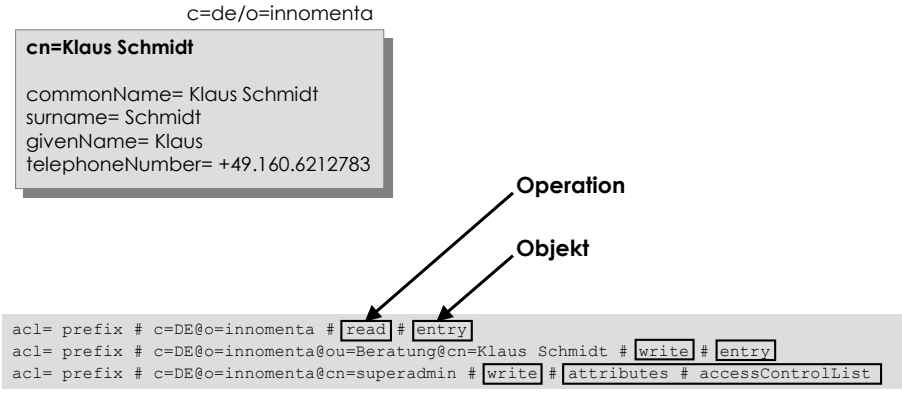

Abbildung 1.3: Zugriffskontrollliste

Die erste Zeile in der Zugriffskontrollliste berechtigt alle Benutzer, deren Verzeichnisdienst-Name mit „c=de/o=innomenta" beginnt (z.B. alle Mitarbeiter der Firma Innomenta), zum Lesen des dargestellten Eintrags. Den Eintrag ändern darf nur Klaus Schmidt selbst (Zeile 2). Änderungen an der Zugriffskontrollliste hingegen darf nur der Administrator vornehmen (Zeile 3).

Arten von Berechtigungen

In der einfachsten und konkretesten Form ist eine Berechtigung eine **binäre Berechtigung,** d.h. sie bezieht sich auf genau ein Objekt und eine Operation. Binäre Berechtigungen werden deshalb auch als Einzelberechtigungen bezeichnet. Die Berechtigung „Ortsgespräche führen" in der Nebenstelle 746 der TK-Anlage ist ein Beispiel für eine solche binäre Berechtigung. Entweder eine Identität besitzt diese Berechtigung und darf zugreifen oder eben nicht.

Die Tatsache, dass eine binäre Berechtigung nur diese zwei Zustände kennt (darf / darf nicht) und sich nur auf ein Objekt und eine Operation bezieht, wird für die Berechtigungsprüfung genutzt. Komplexe Berechtigungen, die sich beispielsweise auf mehrere Operationen beziehen, werden vor der Prüfung in binäre Berechtigungen aufgelöst und die Prüfung dann gegenüber den binären Berechtigungen durchgeführt.

Das gleiche gilt für die anderen Gestaltungs-/Steuerungselemente wie z.B. Profile. Diese werden zunächst auf Berechtigungen zurückgeführt und münden in viele einzelne, binäre Berechtigungen, auf deren Grundlage der Zugriff gestattet oder verweigert wird.

Wertberechtigungen legen anhand eines Wertes fest, welche Operationen mit dem zu berechtigenden Objekt durchgeführt werden dürfen. Ein Beispiel hierfür sind die Werte für Berechtigungen im UNIX-Filesystem. Dort steht der Wert 7 für den Vollzugriff auf eine Datei. Die Ziffer 7 steht für die Summe aus 1+2+4, mit deren Hilfe die drei Operationen ausführen, schreiben und lesen kodiert werden, so wie es in Abbildung 1.4 zu sehen ist.

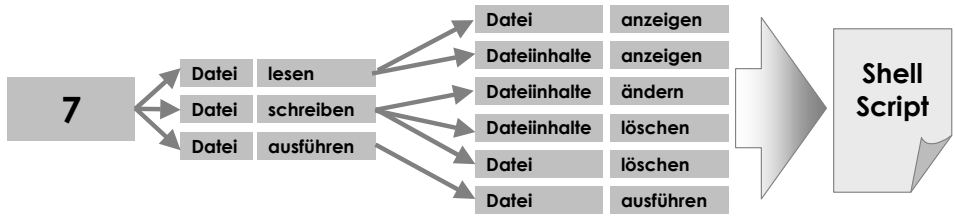

Abbildung 1.4: Von der Wertberechtigung zu den binären Berechtigungen der Ressource

Damit wird deutlich, dass sich mit Wertberechtigungen mehrere binäre Berechtigungen zusammenfassen lassen, ohne dass weitere Gestaltungs-/Steuerungselemente verwendet werden müssten.

Scope von Berechtigungen

Eine wichtiger Punkt in Bezug auf die Platzierung und Gestaltung von Berechtigungen ist die Frage, welche Zugriffe aufgrund einer Berechtigung freigegeben werden sollen. Man spricht in diesem Zusammenhang auch von der Granularität von Berechtigungen.

Ausgangspunkt für die Platzierung der Berechtigungen ist der Schutzbedarf der Ressource, der üblicherweise in einer Schutzbedarfsanalyse ermittelt wird. In diese Analyse fließen mehrere Faktoren ein, die die Wichtigkeit und Kritikalität der Ressource bzw. ihrer Funktionen und Inhalte determinieren (z.B. der Geschäftseinfluss).

Der Schutzbedarf wird hinsichtlich des Zugriffsschutzes innerhalb der Berechtigungsplanung umgesetzt. Dort wird festgelegt, wie fein (granular) der Schutz realisiert sein muss und welche Funktionen durch Berechtigungen geschützt werden müssen. Ebenso wird dort beschrieben, wie stark der Zugriffsschutz ausgeprägt sein muss, z.B. ob starke Authentifikationsmechanismen zum Einsatz kommen müssen.

Berechtigungsstufen

Eine Möglichkeit, Berechtigungen möglichst einfach vergeben zu können, besteht in der Verwendung von Berechtigungsstufen. Sie teilen die Spanne zwischen „über gar keine Berechtigung verfügend“ und „über alle Berechtigungen verfügend“ in mehrere Bereiche ein. In Abbildung 1.5 beziehen sich die Stufen ausschließlich auf die Operationen, es können aber auch einzelne Funktionen und Inhalte mit einbezogen werden.

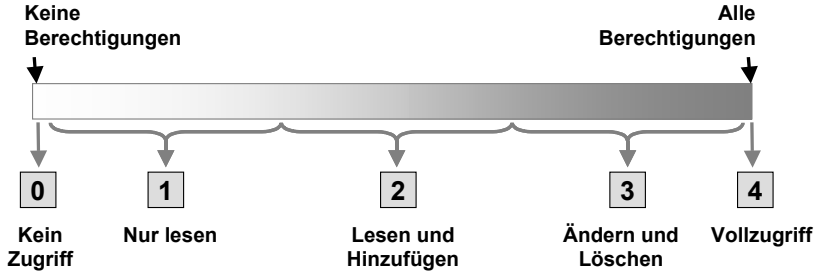

Abbildung 1.5: Berechtigungsstufen

Wenn die Berechtigungsstufen definiert sind, genügt es zur Berechtigungsvergabe, die Ziffer der Berechtigungsstufe anzugeben, die über ein berechtigungssteuerndes Element (eine Rolle, eine Gruppe usw.) an die Identität vergeben wird. Sollen verschiedene Kombinationen von Operationen möglich sein, so muss bei dem sich ergebenden Wert immer eindeutig sein, welche Operationen sich dahinter verbergen. Für jede Identität wird vermerkt, welche Berechtigungsstufe ihr zugeordnet ist:

Identität	Business-Funktion	Berechtigungsstufe
Susanne Kopp	Sachbearbeiterin	2
Klaus Schmidt	Manager	3
Alexander Tsolkas	Administrator	4

Der Vorteil der Verwendung von Berechtigungsstufen ist es, dass die Einzelberechtigungen nicht mehr in Erscheinung treten. Durch die Zuordnung einer Stufe ist bereits eindeutig festgelegt, über welchen Berechtigungsumfang die Identität verfügt. Dies vereinfacht die Berechtigungsvergabe.

Berechtigungsgrad und Berechtigungskette

Ist die Wahrnehmung einer Berechtigung abhängig von der Erlangung einer anderen Berechtigung, so spricht man von einer Berechtigung 2. Grades.

Im Beispiel der TK-Anlage ergibt sich für das Führen von Ferngesprächen beispielsweise:

1. Der Mitarbeiter muss berechtigt sein, die Nebenstelle 746 zu nutzen (Berechtigung 1. Grades).
2. Die Nebenstelle 746 muss so konfiguriert sein, dass für sie Ferngespräche freigeschaltet sind (Berechtigung 2. Grades).

Solange der Mitarbeiter nicht berechtigt ist, das Telefon an sich zu benutzen, sind die konfigurierten Verbindungskategorien irrelevant. Sie kommen erst dann zum Tragen, wenn die Berechtigung 1. Grades gegeben ist.

In der Praxis findet man oft die Situation, dass eine Berechtigung von mehreren anderen Berechtigungen abhängt. Nun könnte man das Prinzip des Berechtigungsgrades weiterführen und von Berechtigungen dritten, vierten oder fünften Grades sprechen. Sinnvoller erscheint es aber, in diesem Fall die gesamt Kette von aufeinander aufbauenden Berechtigungen zu betrachten, was zu dem Begriff der *Berechtigungskette* führt.

Bei der Berechtigungsplanung und Berechtigungsverwaltung ist es wichtig, auch die operativen Prozesse zu betrachten, in denen die Benutzer bzw. Identitäten die Berechtigungen nutzen. Es muss gewährleistet werden, dass eine vergebene Berechtigung auch wahrgenommen werden kann, d.h. alle vorher benötigten Berechtigungen müssen ebenfalls vergeben sein oder, falls sie das nicht sind, im Zuge der Berechtigungsvergabe mit vergeben werden.

Besonders dann, wenn das Prinzip des „Need to know“ umgesetzt werden soll, das heißt ein Benutzer nur über die Berechtigungen verfügen soll, die er für seine Tätigkeit benötigt, ist die Sicherstellung der Berechtigungsketten wichtig.

In vielen Fällen werden die Anwendungsprozesse nicht durchdacht, was dazu führt, dass spezielle Berechtigungskombinationen, die in bestimmten Arbeitssituationen benötigt werden, nicht zur Verfügung stehen. Die Folge ist, dass der Benutzer sich Fehlermeldungen gegenüber sieht, die er weder verstehen noch zuordnen kann, da die fehlende Berechtigung

nicht an der Stelle existieren muss, an der sich der Benutzer befindet, sondern an einer völlig anderen Stelle irgendwo in der Berechtigungskette.

Das ist nicht nur ärgerlich für den Benutzer, sondern auch für die Berechtigungsverwaltung, denn die Fehlersuche gestaltet sich u.U. schwierig und selbst dann, wenn fehlende Berechtigungen gefunden werden, können sie nicht so ohne weiteres vergeben werden, weil dadurch Seiteneffekte entstehen können, die wiederum dem „Need to know"-Prinzip widersprechen.

1.2 Rolle

Eines der wichtigsten Gestaltungs- und Steuerelemente für IT-gestützte Berechtigungen ist die Rolle. Entsprechend viel Raum nimmt die Beschäftigung mit Rollen in diesem Buch ein. So widmet sich mit Kapitel 3 ein ganzes Kapitel dem Rollenkonzept und dem Arbeiten mit Rollen innerhalb der Berechtigungsthematik.

Dort und in Kapitel 4 wird mit der Vorstellung des Prinzips der rollenbasierten Zugriffskontrolle (RBAC) auch gezeigt, warum Rollen für die Berechtigungsthematik so wichtig sind: Sie ermöglichen die Entkopplung der Berechtigungen von den Identitäten. Diese Möglichkeit ist so entscheidend, dass alle führenden Hersteller von modernen Softwaresystemen dazu übergegangen sind, dieses Prinzip in ihren Produkten abzubilden.

1.2.1 Business-Rolle

Eine Business-Rolle im Sinne des Berechtigungskonzepts beschreibt eine Funktion, die der Rolleninhaber für das Unternehmen ausübt. Die Funktion bezieht sich dabei entweder statisch auf ein bestimmtes Aufgabengebiet bzw. einen definierten Verantwortungsbereich oder dynamisch auf ein bestimmtes Tätigkeitsspektrum.

Für die Formulierung der Rollenbezeichnungen finden sich vier Varianten:

- *Orientiert an der Art der Funktion*
  Bei der Formulierung nach der Funktionsart steht nicht im Vordergrund, für welchen Bereich im Unternehmen der Rolleninhaber tätig ist, sondern auf welche Weise er tätig ist.
  Besteht die Funktion zum großen Teil darin, Beschlüsse zu treffen, dann könnte als Rolle „Entscheider" formuliert werden. Ob die Beschlüsse den Einkauf von Blechen oder die Vergabe von Dienstleistungen betreffen, ist bei dieser Formulierung unerheblich. Gleiches gilt für Rollen wie „Entwickler", „Projektleiter" oder „Manager".
- *Orientiert an dem Zuständigkeitsbereich*
  Diese Variante formuliert die Rolle danach, für welchen Bereich der Rolleninhaber zuständig ist. Der Bereich kann sich dabei direkt aus der Aufbauorganisation ergeben oder daraus abgeleitet werden. Beispiele für solche Bereiche sind der Einkauf, das Facility Management, das Controlling, usw.

Die Bezeichnungen der Rollen können in diesem Fall direkt von dem jeweiligen Bereich übernommen werden. Damit ergeben sich Rollen wie „Einkauf“ oder „Facility Management“.

- *Orientiert an der Bezeichnung des Funktionsträgers*
  Alternativ kann eine Rolle auch nach der Bezeichnung des Funktionsträgers benannt werden. Ein Beispiel ist die Rolle „Kassierer“ in einer Bank. Natürlich wäre hierfür auch eine Rolle „Bargeldverkehr“ denkbar, doch die Formulierung nach dem Funktionsträger ist in diesem Fall verständlicher.
  Die Funktionsträger-Variante wird häufig auch dann gewählt, wenn die Formulierung nach dem Funktionsbereich zu abstrakt wäre. So sind Rollenbezeichnungen wie „Verwaltung“, „Sachbearbeitung“ oder „Kontoführung“ ungeeignet, da sie zu abstrakt sind und es schwierig bis unmöglich ist, konkrete Berechtigungen zuzuordnen.
- *Orientiert an einem Geschäftsprozess oder einem Tätigkeitsablauf*
  Steht die Dynamik im Vordergrund, d.h. sollen vor allem die Prozesse durch Rollen abgebildet werden, so kann es sinnvoll sein, die Formulierung der Rollen an den Prozessbezeichnungen zu orientieren. Dadurch entstehen Rollen wie „Datenschutzaudit“ oder „Produktionsüberwachung“.

Abstrakte Rollen beschreiben auf allgemeine Art eine organisatorische Funktion. Die Rolle „Sachbearbeitung“ beschreibt als Beispiel eine abstrakte Funktion. Abstrakte Rollen sind für die Berechtigungssteuerung ungeeignet, da nicht klar ist, welche konkreten Tätigkeiten die Rolle enthält. Daher werden abstrakte Rollen vor allem im Rollenkonzept als Füllobjekte eingesetzt, um eine vollständige Hierarchie zu erhalten.

Für die Berechtigungssteuerung muss eine abstrakte Rolle durch weitere Unterteilung konkretisiert werden. Beispielsweise könnte der Rolle „Sachbearbeitung“ ein Zusatz hinzugefügt werden, auf welchen Bereich sich die Sachbearbeitung bezieht: „Sachbearbeitung Immobiliendarlehen“. Kann eine Rolle mit einzelnen Tätigkeiten unterlegt werden, die nicht weiter gegliedert werden müssen, so spricht man von konkreten bzw. **operativen Rollen**.

Es ist möglich, top-down zunächst die abstrakten Rollen zu formulieren und diese dann in operative Rollen zu verfeinern. Genauso möglich ist es, aus dem operativen Geschäft die operativen Rollen zu gewinnen und dann die abstrakteren Rollen im Sinne von Container-Objekten zu nutzen, um die operativen Rollen zusammenzufassen und ein geschlossenes Rollenkonzept zu erstellen.

Primärrollen (primary roles) besitzen direkten Einfluss auf die Geschäftstätigkeit und berühren unmittelbar die Wertschöpfungskette. Rollen, die parallel zu diesen Primärrollen existieren oder diesen zuarbeiten, nennt man **Sekundärrollen** (secondary roles) oder unterstützende Rollen (Support-Rollen).

Welche Business-Rollen im Unternehmen existieren und wie Tätigkeiten und Rechte den Rollen zugeordnet werden, wird durch das Rollenkonzept festgelegt, das in Kapitel 3 näher betrachtet wird.

Business-Rollen in der Berechtigungssteuerung

Die Business-Rolle ist, wie der Name schon andeutet, sehr nah an der Identität und ihrer geschäftlichen Funktion angesiedelt. Damit ist sie eines der besten Gestaltungselemente, wenn es darum geht, ganze Berechtigungsbündel tätigkeitsorientiert einer Identität zuzuordnen. Die Rolle ist dabei nur ein Mittler zwischen der Identität und den Ressourcen. Der Frage, wie Rollen innerhalb der Berechtigungssteuerung eingesetzt werden können, wird in Kapitel 5 weiter nachgegangen.

1.2.2 Technische Rolle

Technische Rollen beziehen sich auf die zu berechtigenden Objekte und nicht auf die Identitäten. Sie haben demnach mit den Benutzern und ihren geschäftlichen Tätigkeiten nichts zu tun. Technische Rollen werden in IT-Anwendungen eingesetzt, um Funktionen in der jeweiligen IT-Anwendung zu beschreiben und zu berechtigen.

Ein Beispiel für eine technische Rolle ist die Rolle „Systemverwalter" (root) in UNIX-Systemen. Die Rolle drückt zwar wie die Business-Rolle auch eine Funktion aus, jedoch bezieht sich diese Funktion ausschließlich auf das UNIX-System und nicht, wie bei der Business-Rolle, auf das Unternehmen.

Technische Rollen werden in den Systemen und Anwendungen mit Hilfe von technischen Benutzerkonten abgebildet. Durch die Anmeldung am System unter dem jeweiligen Benutzerkonto wird gegenüber dem System die damit verbundene technische Rolle übernommen, und die damit verknüpften Berechtigungen können genutzt werden.

Technische Rollen in der Berechtigungssteuerung

Im Gegensatz zur Business-Rolle ist eine technische Rolle nicht bei der Identität, sondern bei der Ressource angesiedelt. Eine technische Rolle kennt keine geschäftlichen Tätigkeiten von Identitäten, sie ist losgelöst von jeglicher organisatorischer Einbindung und betrachtet lediglich Benutzer des eigenen Systems.

Somit existiert eine technische Rolle als Mittler zwischen dem Systembenutzer und den Berechtigungen im System, wobei sie näher am Systembenutzer und dessen Funktion im System angesiedelt ist.

Die Verwendung von technischen Rollen in der Berechtigungssteuerung wird in Kapitel 5 näher beschrieben.

1.3 Attribut

Attribute sind einzelne Informationen, die einem Objekt hinzugefügt werden und die dazu verwendet werden, das jeweilige Objekt zu beschreiben oder zu charakterisieren. Um das Wesen von Attributen zu erläutern, greifen wir das Beispiel aus Abbildung 1.3 noch einmal auf. Das Objekt in der realen Welt ist eine Person, die durch die Information „Klaus

Schmidt" identifiziert wird. Der Name einer Person ist dabei keine Information, die eindeutig mit Merkmalen der Person abgeleitet wird, sondern sie ist eine von der Person selbst bzw. ihren Eltern bestimmte Information. Aus diesem Grund existieren meist mehrere Personen mit diesem Namen.

Das Objekt der realen Welt wird nun mit einem IT-Objekt in der IT abgebildet (siehe nachfolgende Abbildung). Als Technologie wird hier ein Verzeichnisdienst gewählt, in dem die Person mit einem Verzeichniseintrag geführt wird.

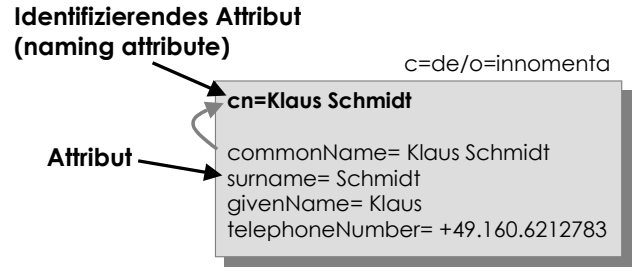

Abbildung 1.6: Attribute eines Objekts

Es ist meist nicht sinnvoll, das Objekt in seiner realen Komplexität abbilden zu wollen, daher werden einige, für den jeweiligen Zweck wichtige, Informationen ausgewählt und als Attribute in den Eintrag aufgenommen.

Attribute können völlig unterschiedliche Eigenschaften eines Objekts abbilden. Zu einer Person könnten neben alltäglichen Informationen wie Telefonnummer oder Geburtsdatum auch Neigungen (z.B. das Lieblingsgetränk), Gefühle (z.B. Träume), der Klang der Stimme (Stimmprobe), die visuelle Erscheinung (Foto, Video), Zugangsberechtigungen (Passworte, Zertifikate) und vieles mehr abgebildet werden.

Welche Attribute ausgewählt und aufgenommen werden, hängt davon ab, welche Anwendungen durch diese Attribute bedient werden sollen. Ein elektronisches Telefonbuch benötigt als Attribute nur den Namen, evtl. Zusatzattribute für die Eindeutigkeit des Namens (z.B. Abteilung) und die Telefonnummer. Eine Anwendung zur Hauspostzustellung benötigt zusätzlich den Standort und die Raumnummer.

Ebenso wie ein Objekt der realen Welt muss auch ein IT-Objekt identifiziert werden. Dies geschieht mit Hilfe eines Bezeichners (Identifier). Dazu wird ein Attribut des Objekts ausgewählt und zum identifizierenden Attribut (naming attribute) erhoben. In unserem Beispiel wird dafür ebenfalls der Name benutzt, es könnte aber auch eine andere Information verwendet werden. Wichtig dabei ist, dass das ausgewählte Attribut das Objekt eindeutig identifiziert.