DIPLOMARBEIT

Titel der Diplomarbeit

„Wiederherstellung einer homogenen Information Security Policy aus proprietär gewachsenen Berechtigungsverwaltungen in einer großen öffentlichen Institution“

Verfasser

Harald Wöhrnschimmel

angestrebter akademischer Grad

Magister der Sozial- und Wirtschaftswissenschaften (Mag. rer. soc. oec.)

Wien, 2008

Studienkennzahl lt. Studienblatt:	A 175
Studienrichtung lt. Studienblatt:	Wirtschaftsinformatik
Betreuer:	Univ.-Prof. Dipl.-Ing. Dr. techn. Thomas Grechenig

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die den benutzten Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Wien, am 27.11.2008 ----------

Name

Danksagung

Mein herzlicher Dank gilt all jenen Personen, welche durch ihre persönliche und fachliche Unterstützung zum Gelingen dieser Diplomarbeit beigetragen haben. Insbesondere erwähnen möchte ich Univ.-Prof. Dipl.-Ing. Dr. techn. Thomas Grechenig und Mag. Dr. Brigitte Brem vom Institut für Rechnergestützte Automation der Technischen Universität Wien für deren Hilfsbereitschaft und Ausdauer während der Fertigstellung der Arbeit. Ebenso seien jene Kollegen und Freunde erwähnt, die mir bei Detailfragen hilfreich zu Rate gestanden sind.
Und ein besonderer Dank gilt meinen Eltern für die moralische Unterstützung und die finanzielle Ermöglichung meiner Ausbildung.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Mit dem Fortschreiten der automatisierten Datenverarbeitung findet eine immer größer werdende Anzahl von unterschiedlichen EDV-Systeme Einzug in moderne Unternehmen. In jedem dieser Systeme werden Daten generiert beziehungsweise weiter verarbeitet, wobei im Normalfall ein vitales Interesse besteht, diese Daten vor unbefugtem Zugriff zu schützen. Aufgrund der meist proprietären Berechtigungsverwaltungen der einzelnen Systeme resultiert jedoch das Problem, dass es im laufenden Betrieb an Transparenz mangelt, jederzeit alle vergebenen Berechtigungen auf Vorgaben der IT-Sicherheit prüfen zu können. Durch die dabei entstehende Grauzone ergibt sich ein reales Sicherheitsrisiko. Im Folgenden wird auf Basis bestehender theoretischer Grundlagen eine praktische Lösung erarbeitet, mit dessen Hilfe sicherheitsrelevante Vorgaben der Berechtigungsverwaltung analysiert und kontrolliert werden können.

1.1 Ausgangssituation

In jedem System, in denen Mitarbeiter Tätigkeiten verrichten sollen, müssen diese auch über alle zur Erfüllung ihrer Aufgaben erforderlichen Berechtigungen verfügen. Dabei gilt grundsätzlich das Konzept der Least-Privilege beziehungsweise das „need-to-know“-Prinzip [1], wonach jeder Berechtigte exakt über jene Berechtigungen verfügen muss, die er zur Erfüllung seiner Tätigkeiten benötigt. Eventuelle Überberechtigungen von Mitarbeitern ist einer jener Aspekte, welche im Zuge dieser Arbeit aufgezeigt werden müssen. Ein weiterer Schwerpunkt der Analyse ist die Kontrolle allgemeiner relevanter Sicherheitsvorgaben und deren Einhaltung im laufenden Betrieb.
Die vorliegende Arbeit entstand im Zuge eines realen Projektes und beinhaltet neben der praktischen Umsetzung auch eine wissenschaftliche Auseinandersetzung mit dem zugrunde liegenden Themenbereich.

1.2 Systemumfeld

Der Ursprung dieser Arbeit liegt in evidenten Bedürfnissen der IT-Abteilung eines österreichischen Großunternehmens im Finanzsektor. Hauptbetätigungsfeld dieser ist, für einen reibungslosen Betrieb der unternehmenseigenen Infrastruktur zu sorgen. Dazu gehört das Netzwerk, Clients und Server ebenso wie alle angebotenen Applikationen. In dem Unternehmen sind rund 1000 Mitarbeiter beschäftigt, wobei ein Großteil jener über einen IT-Arbeitsplatz verfügt. Wie auch schon das Tätigkeitsfeld des Unternehmens zeigt, spielen elektronische Daten im laufenden Betrieb eine wesentliche Rolle. Einerseits gibt es eine Vielzahl an elektronischen Kommunikationswegen mit dem Zweck des externen Datenaustausches. Ein weiterer Faktor ist die Datenverarbeitung und die interne Speicherung beziehungsweise Archivierung der Daten.
Zentraler Bestandteil ist ein unternehmensumfassendes Local Area Network (LAN) mit Anbindung einiger Zweigstellen im In- und Ausland. Eingebunden in das Netzwerk

sind etwa 700 Clients. Dazu zählen herkömmliche Desktop Computer ebenso wie Notebooks aber auch vermehrt ThinClients. Diese ThinClients dienen neben der Ein- und Ausgabe lediglich zur Anbindung an Terminalserver. Für zentrale Dienste im Netzwerk stehen rund 150 Server zur Verfügung. Davon übernimmt jedoch nur ein Teil die Funktionen im laufenden Produktivbetrieb. Die verbleibenden Server dienen als Ausfallssysteme beziehungsweise als Testserver.
Als Netzwerkbetriebssysteme dienen sowohl die Produkte von Windows als auch von Novell. Bei der Anmeldung am Netzwerk erfolgt simultan eine Authentifizierung gegen ein Active Directory und ein eDirectory, wodurch der Benutzer Zugriff auf die jeweiligen verwalteten Ressourcen erhält. Nach erfolgreicher Anmeldung werden dem Mitarbeiter eine Auswahl von insgesamt rund 200 verwalteten Applikationen angeboten – gemäß den speziellen Erfordernissen des Mitarbeiters. Diese sind teilweise lokal am Computer installierte Bürosoftware wie Microsoft Office, beziehungsweise Tools wie der Acrobat Reader. Darüber hinaus existieren in dem Unternehmen einige Produkte mit Client/Server Architektur. Zu den Bedeutendsten im Unternehmen gehört die betriebswirtschaftliche Software von SAP beziehungsweise ein Aktenverwaltungssystem und eine Archivlösung für Langzeitspeicherung der Daten.
Als Unternehmen im Finanzsektor sind Information und Wissen bedeutendte Werte. Wesentlicher Gesichtspunkt ist Sicherheit, sowohl hinsichtlich System- als auch Netzwerkausfällen als auch hinsichtlich Schutz vor unbefugte Datenzugriffe. Die technische Verantwortung für die Sicherheit der Daten im Unternehmen trägt die IT-Abteilung. Die Verantwortung für Berechtigungen, insbesondere bei Software mit Client/Server Architektur, liegt oftmals dezentral. Gemäß dem Prinzip der Data-Ownership, wo der Ersteller beziehungsweise Besitzer von Daten für die Berechtigungsfestlegung zuständig ist, liegt die organisatorische Verantwortung innerhalb der jeweiligen Fachabteilung. Wie im Kapitel 3.1 beschrieben, kommt es bei der Einführung einer neuen Applikation zur Bildung eines initialen Berechtigungsmodells in Beteiligung von Systembetreuern, Abteilungsverantwortlichen, Systemverantwortlichen und gegebenenfalls Fachleuten von externen Firmen. Die Umsetzung dieser erfolgt während der Inbetriebnahme des Produktes. Im laufenden Betrieb erfolgen Änderungen von Berechtigungen nach elektronischer Anforderung und Genehmigung des Verantwortlichen durch die zentrale Berechtigungsverwaltung.

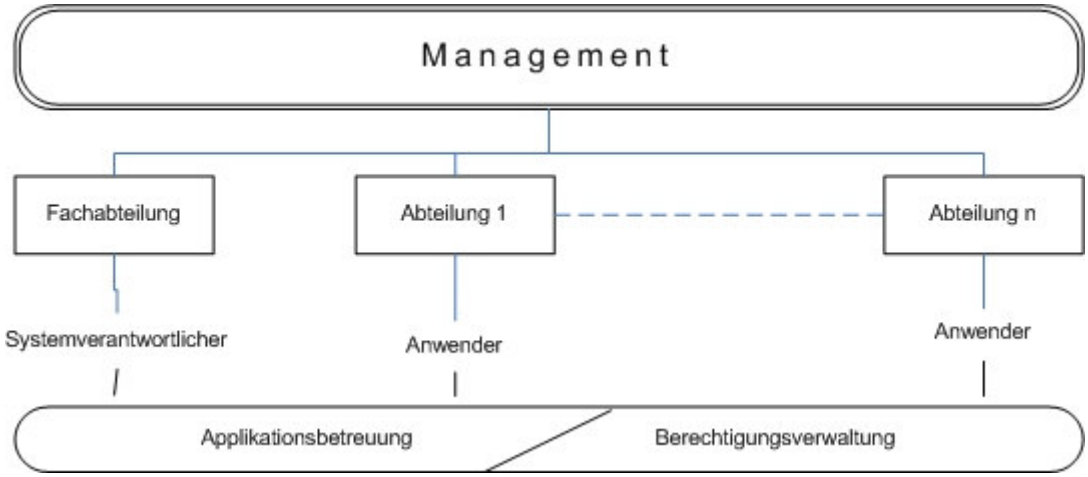

Abbildung 1: Akteure

Abbildung 1 zeigt Verantwortlichkeiten innerhalb des Unternehmens. Der Systemverantwortliche, meist in einer Fachabteilung, ist für alle Berechtigungen innerhalb eines speziellen Systems verantwortlich und der jeweilige Abteilungsleiter für alle abteilungsinternen Daten sowie Systemberechtigungen seiner Mitarbeiter. Die Applikationsbetreuung und die Berechtigungsverwaltung haben generell für die Einhaltung übergeordneter Sicherheitsrichtlinien zu sorgen.

1.3 Das Sicherheitsproblem

Genau hier entsteht der initiale Bedarf dieses Projektes. Die Verwaltung der vergebenen Berechtigungen erfolgt meist proprietär in der entsprechenden Applikation selbst. Eine Vielzahl möglicher Ursachen im laufenden Betrieb können Eingriffe in die Berechtigungsverwaltung erfordern, wie zum Beispiel:

- Namenswechsel bei Hochzeit
- Abteilungswechsel bei Jobrotation
- Dauerhafter Abteilungswechsel
- Kündigung des Mitarbeiters
- Änderung des Aufgabenbereiches
- Temporäre Berechtigungen für Praktikanten

All diese Änderungen erfordern einen sichergestellten, korrekten Informationsfluss aus der entsprechenden Abteilung hin zur Berechtigungsvergabe. Im Falle von fehlenden Berechtigungen ist die Chance ungleich höher, dass dieser Informationsfluss zustande kommt. Der gegenteilige Fall von zu vielen Rechten ebenso wie ein Irrtum bei der

Administration führen hingegen zu einem nicht einschätzbaren Sicherheitsrisiko. Wie sich am Beispiel eines Abteilungswechsels gut darstellen lässt, wird die Leitung der neuen Abteilung sehr rasch eventuell erforderliche Berechtigungen für den neuen Mitarbeiter beantragen. Ob der Mitarbeiter jedoch noch über spezielle Berechtigungen in anderen Systemen verfügt, die aus seiner bisherigen Tätigkeit resultieren, lässt sich nur sehr schwer feststellen. Vielmehr besteht aus Sicht der Beteiligten auch kein expliziter Anlass, diesem Umstand nachzugehen.
Prinzipiell obliegt es entweder der Sicherheitsabteilung oder dem Systemverantwortlichen, auch im laufenden Betrieb die Einhaltung von Sicherheitsrichtlinien zu prüfen. Über die jeweiligen systemeigenen Administrationsoberflächen ist es jedoch oftmals nicht zumutbar, vergebene Berechtigungen auszulesen und auf Plausibilität zu prüfen. Und ein Export der Berechtigungsdaten scheitert meist schon daran, dass in machen Systemen keine Exportschnittstelle implementiert ist. Selbst im Fall eines funktionierenden Exportes stellt sich immer noch das Problem, dass die erhaltenen Informationen der proprietären Verwaltungen meist nicht „human readable“ und somit für weitere Analysen unbrauchbar sind.

1.4 Ziel dieser Arbeit

Ziel ist es, Sicherheitsrisken in proprietären Berechtigungsverwaltungen auf ein Minimum zu reduzieren. Dies soll dadurch erreicht werden, dass alle für die Richtigkeit von Berechtigungen zuständigen Personen eine Möglichkeit geboten wird, diese auch zu kontrollieren. Bei der Art der Darstellung ist darauf Rücksicht zu nehmen, dass die prüfende Person grundsätzlich in drei unterschiedlichen Funktionen zuständig sein kann.
So sind Systemadministratoren beziehungsweise Systemverantwortliche für alle vergebenen Berechtigungen innerhalb eines Systems verantwortlich, unabhängig von der Abteilung der Berechtigten. Aus Sicht eines Abteilungsleiters hingegen sind wiederum alle Berechtigungen seiner Mitarbeiter von Interesse, unabhängig vom jeweiligen System. Zusätzlich obliegt dem Abteilungsleiter in der Funktion des Besitzers auch die Verantwortung hinsichtlich der Daten auf dem Abteilungslaufwerk. Personen der IT-Sicherheit soll neben einer visuellen Darstellung weiters eine Möglichkeit geboten werden, systematische Prüfungen in Form von Regeln durchführen zu können.
Die Auswertung der jeweiligen Berechtigungsdaten soll in periodischen Abständen erfolgen. Die Ergebnisse sollen den jeweiligen Verantwortlichen im Intranet zur Einsicht angeboten werden.

1.5 Methodische Vorgehensweise

Erster Schritt ist eine Erhebung, welche Systeme für die Analyse von Bedeutung sind. Von zentralem Interesse sind dabei die beiden Verzeichnisdienste als Referenz, da alle

Benutzer in den jeweiligen Systemen auch über eine Netzwerkberechtigung verfügen müssen. Danach müssen die Möglichkeiten geprüft werden, ob und wie auf die jeweiligen Berechtigungsdaten der Systeme zugegriffen werden kann.
Die Entwicklung einer systemübergreifenden Struktur erfolgt auf Basis der aus den Systemen ausgelesenen Berechtigungsdaten gemeinsam in Einbezug der theoretischen Grundlagen, auf welche Konzepte die Berechtigungsstrukturen beruhen können. Als angestrebter Datentyp wird eine XML-Datei gewählt, deren Validität anhand einer DTD-Datei überprüft werden kann. Zur Generierung der einzelnen XML-Dateien ist eine herstellerseitige Anpassung der systemeigenen Exportschnittstelle ebenso wie die Entwicklung eines spezifischen Parsers denkbar.
Über eine einheitliche Importschnittstelle werden diese Informationen in einer zentralen Datenbank abgelegt, wo sie zu weiteren Analysen zur Verfügung stehen. Anschließend folgt die Schaffung von Analysemöglichkeiten in Form einer webbasierenden Darstellung und einer Möglichkeit, auf Anomalien als Set von Regeln prüfen zu können. Die Entwicklung erfolgt als evolutionäres Prototyping, wo eine schrittweise Erweiterung entsprechend dem Feedback nach ausgiebigen Testszenarien erfolgt. Aufgrund der strikten Trennung von Daten und Layout ist der Aufwand bei der Erweiterung um zusätzliche zu analysierende Applikationen minimiert.

1.6 Aufbau der Arbeit

Erster Schwerpunkt der Arbeit ist eine Zusammenstellung bekannter Mechanismen und Modelle, welche in Berechtigungsstrukturen Anwendung finden könnten. Diesbezüglich erfolgt in Kapitel 2 eine Auflistung relevanter Zugriffskontrollmechanismen und Sicherheitsmodelle, wie wir sie auch in den im Zuge dieser Arbeit analysierten Systemen vorfinden werden. Anschließend folgt eine allgemeingültige Definition von Sicherheitsrichtlinien entsprechend dem Standard ISO/IEC 27001:2005 [2].
Kapitel 3 startet mit der Betrachtung, wie im konkreten Unternehmen jene Sicherheitsrichtlinien entstehen, welche in den jeweiligen Systemen durchgesetzt werden sollen. Danach werden die Berechtigungsverwaltungen vier repräsentativer Systeme nach deren strukturellen Eigenheiten untersucht und kategorisiert und in Folge aufgezeigt, welche Sicherheitsrichtlinien jeweils durchzusetzen sind.
Mit dem Wissen über die jeweiligen Berechtigungsstrukturen erfolgt in Kapitel 4 eine systemübergreifende Analyse und die Bildung einer Datenstruktur, in welcher alle betrachteten Berechtigungen der Einzelsysteme abgebildet werden können.
Die praktische Umsetzung in Kapitel 5 reicht von der Generierung der uniformen Berechtigungsdaten hin bis zur Entwicklung und Strukturierung der zentralen Datenbank und den Algorithmen zur Darstellung der jeweiligen Zugriffsberechtigungen. Weiters beschrieben ist die Wahl der verwendeten Technologie mit Begründung und Beispielcode.

Abschließend folgt in Kapitel 6 eine detaillierte Erfahrungsanalyse sowohl aus Entwickler- als auch aus Kundensicht und in Kapitel 7 eine Zusammenfassung mit gezogenen Schlussfolgerungen und Zukunftsperspektiven.

1.7 Themenabgrenzung

Die vorliegende Arbeit verfolgt eine Minimierung des Sicherheitsrisikos nach dem „Least-Privileges“-Prinzip, welches als einer der Grundprinzipen schon in frühen Werken der IT-Sicherheit erwähnt wurde (siehe zum Beispiel [3]). Dies besagt, dass alle in Systemen berechtigte Personen exakt so viele Berechtigungen besitzen, wie sie für die Verrichtung ihrer Arbeit unbedingt benötigen – nicht mehr und auch nicht weniger. Die Analyse der Berechtigungen erfolgt durch Vergleich des Sollzustandes in Form von Sicherheitsrichtlinien und dem Istzustand anhand der Auswertung der in den Systemen vergebenen Berechtigungen.
Nicht Umfang der Arbeit sind alle potentiellen Angriffe auf die zu schützenden Daten durch Übernahme einer fremden Identität im System, durch Belauschen gewährter Zugriffe berechtigter Personen aber auch alle anderen Versuche, sich auf nicht zulässige Art und Weise Zugriff auf die Daten zu verschaffen. Die bei den jeweiligen Sicherheitsmodellen angeführten Kritikpunkte dienen lediglich zum Aufzeigen bekannter systembedingter Schwachstellen und einer entsprechenden Sensibilisierung für einen eventuellen Einsatz in der Praxis.
Die Kumulierung der Berechtigungsdaten erfolgt lediglich aus dem Zweck der Analyse und Darstellung. Alle administrativen Eingriffe müssen in der Berechtigungsverwaltung des jeweiligen Systems durchgeführt werden.

2 Sicherheitsrelevante Grundlagen

In diesem Kapitel werden alle relevanten theoretischen Grundlagen proprietärer Berechtigungsverwaltungen dargestellt. Ausgangsbasis sind hierfür die unterschiedlichen Zugriffskontrollmechanismen. Anschließend werden Sicherheitsmodelle angeführt, die es ermöglichen, auch in komplexen Strukturen aus einer Vielzahl an Mitarbeitern und Daten mit unterschiedlichem Sicherheitsbedarf eine in sich schlüssige Berechtigungsverwaltung zu etablieren. Dies bildet die zugrundeliegenden Theorie der im anschließenden Kapitel durchgeführten praktischen Analyse in vier Systemen.
Anschließend folgt eine theoretische Beschreibung zur Bildung von Sicherheitsrichtlinien, wie sie aus strategischem Blickwinkel entworfen die Basis der Berechtigungsverwaltungen darstellen.

2.1 Das Sicherheitsproblem

Oberstes Ziel ist Vertraulichkeit. Gemäß Definition bedeutet Vertraulichkeit:

> *„the property that information is not made available or disclosed to unauthorized individuals, entities or processes"*
> (ISO/IEC27001:2005 [2])

Eine deutschsprachige Definition findet man unter anderem auch in [4]. Erster Sicherheitsmechanismus ist die Implementierung einer Authentifizierung. Dadurch kann die auf das System zugreifende physische Person identifiziert und einer abstrakten Person innerhalb des Systems zugeordnet werden. Die Zugriffskontrolle entscheidet nun, welche effektiven Berechtigungen dieser Person besitzt (Abbildung 2).

Abbildung 2: Authentifizierung

Jedes der in dieser Arbeit betrachteten Systeme verfügt über eine eigene, autarke Berechtigungsverwaltung. Wie die folgende Darstellung unterschiedlicher Ebenen der Zugriffskontrolle zeigt, können Zugriffe auf manche Ressourcen mehr als eine Authentifizierung erfordern.

2.2 Ebenen der Zugriffskontrolle

Ziel jedes Zugriffes sind letztendlich Informationen, die in unterschiedlichster Form als Datei vorliegen. Dazu zählen reine Datendateien ebenso wie Programmdateien, wo Zugriffe vom jeweiligen Betriebssystem kontrolliert werden. Erfolgt der eigentliche Informationszugriff mittels einer speziellen Applikation, so ist meist zusätzliche eine interne Kontrollinstanz implementiert. Insgesamt bieten sich gemäß [5] vier verschiedene Ebenen (Abbildung 3), in welchen Zugriffskontrollen möglich sind:

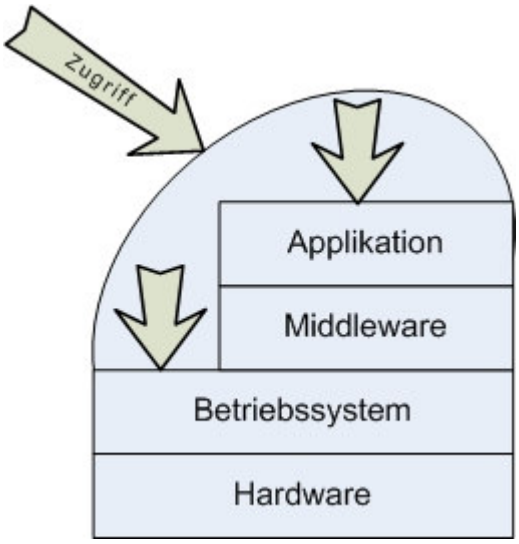

Abbildung 3: Ebenen der Zugriffskontrollen

Die jeweiligen Ausprägungen können wie folgt beschrieben werden:

- Die Möglichkeiten der Zugriffskontrolle auf Anwendungsebene sind am Vielfältigsten. Komplexe Sicherheitsrichtlinien, Benutzerrollen, Aktivitäten und spezielle Authentifizierungsarten sind individuell gestaltbar und lediglich vom Design der Applikation abhängig.
- Mechanismen der Middleware sind zum Beispiel auf Ebene von Datenbankzugriffen aber auch programmtechnisch vorgegebene Einschränkungen aus Sicht der Datenintegrität wie zum Beispiel Gegenbuchungen in Buchhaltungsprogrammen.
- Die Middleware benötigt wiederum Ressourcen des Betriebssystems. So erfolgt beispielsweise die Kontrolle der Dateiberechtigungen aber auch der Zugriff auf

Systemressourcen wie zum Beispiel Kommunikationsports in der Betriebssystemebene.

- Eine Zugriffskontrolle auf Hardwareebene dient vorwiegend zum Schutz vor Angriffen durch Ausführung von schadhaftem Programmcode.

Ausgehend von der Hardwareebene werden die Zugriffskontrollen mit steigender Ebene stets komplexer aber auch fehleranfälliger. Die in dieser Arbeit untersuchten Zugriffskontrollen beschränken sich auf die Betriebssystemebene in Form der Netzwerkbetriebssysteme Active Directory und eDirectory und auf die Anwendungsebene. Jeder Zugriff auf Ressourcen einer Anwendung erfordert eine vorhergegangene Authentifizierung auf Betriebssystemebene, weshalb der Benutzername im Betriebssystem in Folge als Referenz in der Berechtigungsanalyse verwendet wird. Für den Fall abweichender Benutzernamen in einem der betrachteten Anwendungen wird ein Mapping implementiert.

2.3 Grundlegende Arten von Zugriffen

Die Grundprinzipien der Zugriffskontrolle lassen sich am Besten am vereinfachten Beispiel der Betriebssystemebene veranschaulichen. Hier erfolgt die Kontrolle über Dateizugriffe, welche Programme ausgeführt werden können und wie ein Informationsfluss zustande kommen darf. In anderen Ebenen folgt die Zugriffskontrolle identen Prinzipien.
Für die weitere Darstellung vergebener Berechtigungen werden folgende Arten unterschieden:

r	*read, nur lesender Zugriff gestattet*
w	*write, lesender und schreibender Zugriff gestattet*
x	*execute, gestattet die Ausführung eines Programms*
-	*nicht berechtigt*

Voraussetzung für die Zuteilung der Berechtigung ist eine Authentifizierung im Betriebssystem.

2.4 Zugriffskontrollmechanismen

Mit Zugriffskontrollmechanismen bezeichnet man aus technischer Sicht Datenstrukturen, mit dessen Hilfe explizite Berechtigungen abgelegt und beliebig abgefragt beziehungsweise geändert werden können, unabhängig vom für die Implementierung verwendeten Datentyp.

2.4.1 Berechtigungsmatrix

Die verbreitetste Darstellung vergebener Berechtigungen erfolgt üblicherweise in Form einer Berechtigungsmatrix. Die Spalten entsprechen dabei dem Berechtigungsobjekt (Dateien, Programme,...), die Zeilen einzelnen Personen. Eine Matrix unter Berücksichtigung von Dateizugriffen und einem Buchhaltungsprogramm könnte zum Beispiel wie folgt aussehen:

	Betriebs-system	Buchhaltungs-programm	Buchhaltungs-daten	Auditdaten
Administrator	r w x	r w x	r w	r
Buchhalter	x	x	r w	-
Auditor	r x	r	r	r

Tabelle 1: Berechtigungsmatrix (nach [5])

Wie das Beispiel in Tabelle 1 zeigt, besitzt der Administrator nahezu universellen Zugriff auf das Gesamtsystem. Ausgenommen sind lediglich die Auditdaten, welche somit vor Manipulation durch den Administrator geschützt sind. Der Buchhalter benötigt die Berechtigungen um das Betriebssystem und das Buchhaltungsprogramm auszuführen, um weiters Buchhaltungsdaten verändern zu können. Der Auditor hat lesenden Zugriff auf alle Dateien.

Für einen normalen Betriebsablauf sind diese gesetzten Zugriffsberechtigungen ausreichend. Speziell bei einem Buchhaltungsprogramm könnte es jedoch zu Problemen kommen. Beispielsweise ist es eine Anforderung, dass Transaktionen „well-formed“ sind. So soll eine Abbuchung auf einem Konto einen Eingang auf einem anderen Konto zur Folge haben, was auch durch das Buchhaltungsprogramm sichergestellt werden kann.

Da jedoch sowohl der Administrator als auch der Buchhalter schreibenden Zugriff direkt auf die Buchhaltungsdaten haben, könnten Daten direkt über das Dateisystem und nicht nur über das Buchhaltungsprogramm manipuliert werden.[5]

2.4.2 Mehrstufige Berechtigungsmatrix

Als Abhilfe zu dem beschriebenen Problem kann eine mehrstufige Vergabe von Berechtigungen herangezogen werden, wie in folgender Matrix dargestellt wird:

	Betriebs-system	Buchhaltungs-programm	Buchhaltungs-daten	Auditdaten
Administrator	r w x	r w x	r	r
Buchhalter	r x	x	-	-
Auditor	r x	r	r	r
Buchhaltungs-programm	r w	r	r w	w

Tabelle 2: Mehrstufige Berechtigungsmatrix (nach [5])

Das Beispiel in Tabelle 2 zeigt, dass der Administrator universellen Zugriff am Betriebssystem und am Buchhaltungsprogramm besitzt. Hingegen hat er auf sämtliche Daten nur lesenden Zugriff. Der Auditor kann nach wie vor nur lesend auf alle Daten zugreifen. Einzig das Buchhaltungsprogramm ist berechtigt, Buchhaltungsdaten zu lesen und zu schreiben beziehungsweise Auditdaten zu schreiben. Somit ist sichergestellt, dass schreibende beziehungsweise verändernde Manipulation der Buchhaltungsdaten nur mittels Buchhaltungsprogramm erfolgen kann, in welchem detailliertere Berechtigungen aber auch Kontrollmechanismen implementiert sind.
Ein verbleibender Schwachpunkt ist, dass der Administrator aufgrund seiner schreibenden Berechtigung am Buchhaltungsprogramm sich auch auf die Buchhaltungsdaten Zugriff verschaffen könnte.

2.4.3 Mehrdimensionale Berechtigungsmatrix

Vor allem bei mehrfacher Verwendung ein und des selben Datenstammes für unterschiedliche Anwendungen stellt sich die Frage, welcher Benutzer darf mittels welcher Anwendung welche Operationen auf dem Datenstamm ausführen. Dies führt zur Bildung von dreidimensionalen Berechtigungsmatrizen.

2.4.4 Grenzen der Matrixdarstellung

Rein aus technischer Sicht können sowohl zwei- als auch dreidimensionale Berechtigungsmatrizen so wie beschrieben als zentrale Berechtigungsablage implementiert und gewartet werden. Mit steigender Anzahl der einzelnen Komponenten nimmt der Umfang der Matrix schnell unüberschaubare Größen an. So hat eine zweidimensionale Matrix bei 1000 Benutzern und 200 Programmen schon 200.000 Knotenpunkte zur expliziten Festlegung der Berechtigung.
Wobei die Problematik weniger bei der Performance liegt. Viel mehr leidet die Administrierbarkeit beziehungsweise steigt die Fehleranfälligkeit beim Festlegen und Ändern der Berechtigungen. Eine Verbesserung des Komforts kann beispielsweise durch die Bildung von Gruppen beziehungsweise Rollen erreicht werden, wobei Benutzer gleicher Berechtigung zu einem Objekt zusammengefasst werden, an welchem Änderungen einfach und für alle Benutzer zutreffend durchgeführt werden können. Ein anderer Ansatz ist die Aufspaltung der Gesamtmatrix einerseits spaltenweise in sogenannte Access Control Lists (ACLs), andererseits reihenweise in sogenannte Capabilities, auch Tickets genannt.

2.4.5 Gruppen und Rollen

Betrachtet man eine durchschnittliche Unternehmensstruktur, so lassen sich die Tätigkeiten eines Großteils der Mitarbeiter durch eine geringe Zahl an Kategorien darstellen. Teilweise spiegelt sich diese Einteilung im Organigramm des Unternehmens wider, wobei auch eine abteilungsübergreifende Kategorisierung möglich sein muss. Die Anzahl an Personen, welche durch ihre Aufgabe speziell festgelegte Berechtigungen benötigen (zum Beispiel Administratoren, Sicherheitsbeauftragte,...) reduziert sich dadurch auf ein überschaubares Maß.
Diese Kategorisierung wird durch die Einführung von Gruppen beziehungsweise funktionalen Rollen realisiert [5]. Mitarbeiter erhalten die erforderlichen Berechtigungen durch Mitgliedschaft in einem dieser beiden Kategorien.

	Betriebs-system	Buchhaltungs-programm	Buchhaltungs-daten	Auditdaten
Administrator	r w x	r w x	r w	r
Gruppe – Buchhalter	x	x	r w	-
Rolle - Auditor	r x	r	r	r

Tabelle 3: Matrix mit Gruppen und Rollen (nach [5])

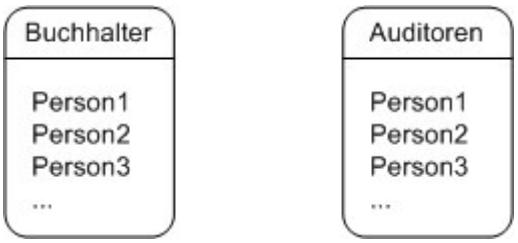

Abbildung 4: Gruppe bzw. Rolle

Tabelle 3 zeigt die Verwendung einer Gruppe beziehungsweise einer Rolle in einer Berechtigungsmatrix. Auf den ersten Blick scheint kein funktionaler Unterschied zwischen einer Gruppe und einer Rolle ersichtlich. So ist auch in einer Vielzahl an Systemen kein Unterschied in der Implementierung umgesetzt. Betrachtet man jedoch die dahinterliegenden Konzepte aus der Sicht von modernem Identity Management (IDM), so sind sehr wohl konzeptionelle Unterschiede erkennbar.

Gruppen

Einerseits können einzelne Benutzer durch Mitgliedschaft in einer oder mehreren Gruppen Berechtigungen erhalten. Andererseits ist es jedoch auch sehr wohl möglich, dem einzelnen Benutzer die erforderliche Berechtigung direkt zu erteilen. In der Berechtigungsprüfung ist es absolut irrelevant, ob der einzelne Benutzer die geprüfte Berechtigung nun durch Mitgliedschaft in einer Gruppe erhalten hat oder die Berechtigung dem Benutzer direkt zugeordnet wurde. Gruppen dienen somit lediglich zur Vereinfachung der administrativen Tätigkeit.

Rollen

Der Ausgangspunkt bei der Verwendung einer Rolle ist die Abbildung einer realen Rolle einer Person (zum Beispiel Buchhalter, Auditor,..) in der Berechtigungsverwaltung. Dieser eher theoretische Unterschied in der Betrachtungsweise führt jedoch zu der Eingrenzung, dass Benutzer erforderliche

Berechtigungen nur über ihre Rolle erhalten können, und niemals direkt berechtigt werden können.
In Folge kann die Verwendung von Rollen näher spezifiziert werden, sodass zum Beispiel ein und der selbe Benutzer nicht Mitglied zweier Rollen sein darf. So scheint es auch in der Realität wenig sinnvoll, die Funktion des Buchhalters und des Auditors mit einer Person zu besetzen.

2.4.6 Access Control Lists (ACLs)

Eine weitere Methode, komplexe Berechtigungsverwaltungen zu vereinfachen ist, eine einspaltige Berechtigungsmatrix beziehungsweise Liste mit direktem Bezug auf ein betroffenes Berechtigungsobjekt anzulegen [5].

	Buchhaltungs-daten
Administrator	r w
Buchhalter	r w
Auditor	r

Tabelle 4: Access Control List (nach [5])

Wie in Tabelle 4 dargestellt, können in einer ACL unterschiedliche Arten von Berechtigung festgelegt werden, wie „nur lesend“ oder „lesend und schreibend“. Ein anderer Ansatz von ACLs führt je nach Art der Berechtigung eine eigene Liste. Die Minimalvariante sind sogenannte Allow- und Deny-Listen, in denen festgelegt wird, welchen Benutzern der Zugriff gestattet und welchen er untersagt ist. Üblicherweise wird der Deny-Liste höhere Priorität eingeräumt, wodurch ein Benutzer in beiden Listen insgesamt keinen Zugriff erhält. In manchen Applikationen wie zum Beispiel der Apache Webserver kann die Reihenfolge der Abarbeitung dieser Listen in der Konfiguration festgelegt werden.
Durch diese dezentrale Verwaltung der Berechtigungen resultieren jedoch eine Vielzahl an Vor- beziehungsweise Nachteilen, teilweise begründet auf konzeptionelle Eigenheiten aber auch an der jeweiligen Implementierung.
Ein typisches Einsatzgebiet von ACLs sind Umgebungen, in denen Benutzern eines Systems die Möglichkeit geboten werden soll, Berechtigungen auf die eigenen Daten selbst zu verwalten. Generelle Sicherheitsrichtlinien und Zugriffsbeschränkungen werden zentral verwaltet, detaillierte Berechtigungen benutzerspezifisch am Berechtigungsobjekt festgelegt.
ACLs sind einfach zu implementieren jedoch leidet die Effizienz, da die Berechtigungsüberprüfung erst bei jedem tatsächlichen Zugriff auf ein

Berechtigungsobjekt geprüft werden muss. Anders als bei einem typischen Betriebssystem, wo eine Vielzahl an Berechtigungen schon beim Anmelden eines Benutzers ausgelesen und intern verwaltet werden.
Neben der Effizienz der Umsetzung ist ein weiterer wesentlicher Faktor die Transparenz gesetzter Berechtigungen. Aufgrund der dezentralen Verwaltung der Berechtigungen ist es nur mit hohem Aufwand möglich, diese benutzerbezogen zu analysieren beziehungsweise beim Stilllegen eines Benutzers dessen Berechtigungen in allen systemweit existierenden ACLs zu entfernen.

ACLs in Unix

Eine willkürliche Verwendung von ACLs ist sowohl in Unix als auch in dessen Linux-Varianten nicht vorgesehen. Dennoch entspricht die Berechtigungsverwaltung im Dateisystem durch Verwendung der Attribute rwx- für die Ressourcen owner, group und others einer vereinfachten ACL. Die Bedeutung der Attribute ist ident mit jenen bei den Berechtigungsmatrizen verwendeten und werden hintereinander in der Reihenfolge der berechtigten Ressourcen angeschrieben. Im Falle eines Verzeichnisses wird ein d (directory) vorangestellt.

drwxrw-r-- Herbert Webmaster

Bei obigen Beispiel handelt es sich um ein Verzeichnis, auf welches der Besitzer „Herbert“ voll berechtigt ist, Mitglieder der Gruppe „Webmaster“ zum Lesen und Schreiben berechtigt sind und alle anderen Benutzer lesend zugreifen dürfen.
Analog zur Berechtigung von Benutzern in Form von Personen, die sich am System anmelden, können auch Programme unter definierten Benutzern ausgeführt werden und es kann somit genau definiert werden, auf welchen Datenbereich das Programm welche Zugriffsart besitzt. [6]

ACLs in Windows NT

Analog zu Unix finden auch in Windows Umgebungen ACLs breite Verwendung. Mit jeder neuen Version von Windows werden laufend zusätzliche Neuerungen in der Berechtigungsverwaltung implementiert.
So wurden unter anderem die bekannten Attribute rwx- um zusätzliche Attribute wie ‚take ownership’, ‚change permission’ und ‚delete’ erweitert um die Flexibilität der Berechtigungsverwaltung zu steigern. Darüber hinaus kann ein Attribut nicht nur gesetzt sein (AccessAllowed) oder auch nicht (AccessDenied) – es kann weiters den Status ‚SystemAudit’ erhalten, wodurch eine Überwachung der Zugriffe aktiviert wird.
Aus technischer Sicht besitzt jede Ressource unter Windows einen sogenannten Sicherheitsdeskriptor, in dem die einzelnen Zugriffsrechte aufgelistet sind. Dieser Sicherheitsdeskriptor beinhaltet den Secure Identifier (SID) des Besitzers der Ressource und die eigentliche ACL. Diese ACL wiederum setzt sich aus einzelnen Datensätzen,

sogenannte Access Control Entries (ACEs), zusammen, die jeweils ein explizites Zugriffsrecht darstellen.
Jeder einzelne ACE besteht aus der SID des jeweiligen Benutzers bzw. der Gruppe, für die das Attribut gilt und einer detaillierten Beschreibung der Rechte.

<user="Herbert" user-sid="4711" guppe-sid="0815">

Der User namens Herbert wird eindeutig identifiziert anhand seiner User-SID „4711"und ist Mitglied einer Gruppe mit der Gruppen-SID „0815".

<ACL besitzer-sid="6789">
<AccessDenied sid="0815" op="W">
<AccessDenied sid="9922" op="R" op="W">
<AccessAllowed sid="4711" op="R" op="W">
</ACL>

Der Sicherheitsdeskriptor der dargestellten Ressource lässt erkennen, dass der Benutzer mit der SID „6789" der Besitzer der Ressource ist und über uneingeschränkte Rechte verfügt. Die in der ACL angeführten ACEs werden nun von oben beginnend zeilenweise abgearbeitet. Gemäß User-SID wäre der Benutzer „Herbert" zu Lese- und Schreibzugriffen berechtigt. Da jedoch die „AccessDenied" – Einträge vor den „AccessAllowed" – Einträge geprüft werden, resultiert aus dem ersten ACE für Mitglieder der Gruppe „0815" gesamt nur lesender Zugriff.
In Windows-Netzwerken können Berechtigungen auch zentral im Netzwerk verwaltet werden, wobei der Gültigkeitsbereich der Berechtigungen durch die sogenannte Domäne festgelegt wird. Zentral festgelegte Rechte haben Vorrang gegenüber lokalen Berechtigungen. Die Granularität möglicher Berechtigungen ist so fein, dass gezielt Tätigkeiten wie zum Beispiel Druckerinstallationen, Softwareupdates,... einzelner Benutzer im System erlaubt oder verboten werden können. Dem Benutzer gegenüber verbirgt sich die Berechtigungsverwaltung in ACLs und wird in Form der Windows-Registry als Verwaltungsinstrument angeboten.[7]

2.4.7 Capabilities

Eine weitere Möglichkeit, komplexe Berechtigungsmatrizen zu vereinfachen, ist die Zerlegung und Verwaltung der Berechtigungen unter Bezug auf den jeweiligen Benutzer (Abbildung 5). Diese Capabilities bilden sowohl systematisch als auch in analytischer Betrachtung dessen Vor- beziehungsweise Nachteile das Gegenteil von ACLs.

	Betriebs-system	Buchhaltungs-programm	Buchhaltungs-daten	Auditdaten
Buchhalter	x	x	r w	-

Tabelle 5: Capabilities (nach [5])

Um beispielsweise einer Vertretung an Stelle des Buchhalters die erforderlichen Berechtigungen zu erteilen, muss nur die jeweilige Capability übernommen werden. Hingegen ungleich unübersichtlicher ist eine Analyse, welche Benutzer beziehungsweise Gruppen Zugriff auf eine bestimmte Ressource besitzen. Dies kann vor allem bei sicherheitstechnischen Zwischenfällen von Bedeutung sein.
Als Vorteilhaft erwiesen sich Capabilities bei den Bestrebungen, betriebssysteminterne Vorgänge insofern abzusichern, als dass nicht alle Benutzertätigkeiten administrative Berechtigungen erfordern. Weitere Relevanz erzielen Capabilities mit steigender Verwendung von Zertifikaten, wo über die am Zertifizierungsserver ausgestellten Tickets benutzerspezifische Berechtigungen im Zielsystem zugeteilt werden.

Capabilities in Windows NT

Als Erweiterung zu den vorhin beschriebenen ACLs in Windows NT finden ab der Windows Version NT5 (2000) zusätzlich auch Capabilities Verwendung [7]. Dabei wird versucht, die jeweiligen Vorteile der beiden Systeme zielgerecht einzusetzen, wobei die existenten Berechtigungsstrukturen mittels ACLs teils ergänzt aber auch überschrieben werden.
Grundlegend wird die Verwendung von Gruppen forciert, Userprofile dienen als Berechtigungsablage und Richtlinien zur zentralen Steuerung von Berechtigungen mittels Active Directory. Der Einsatzbereich dieser Methoden findet jedoch vorwiegend innerhalb des Betriebssystems Anwendung, nicht jedoch zur Zugriffssteuerung auf Filesystemebene und ist daher für die in dieser Arbeit verfolgten Ziele nicht von Relevanz.

2.4.8 Directories

Eine vielfältigere wenngleich auch in der Administration anspruchsvollere Möglichkeit der Berechtigungsverwaltung ist die Verwendung von Verzeichnisdiensten beziehungsweise Directories. Als Mittel zur Abbildung der einzelnen beteiligten Komponenten und Berechtigungen stehen eine Vielzahl unterschiedlicher Objekte wie zum Beispiel Personen, Gruppen oder Ressourcen zur Verfügung. Die Anordnung dieser Objekte erfolgt in Form einer hierarchischen Baumstruktur. Abhängig vom jeweiligen Hersteller steht dem Administrator eine mehr oder weniger komfortable Benutzeroberfläche zur Verfügung.

Aufbau

Jedes Verzeichnis besitzt ein Wurzelelement, oftmals auch „root“ beziehungsweise „tree“ genannt, welches die Ausgangsbasis der Struktur bildet. Hierarchisch darunter erfolgt üblicherweise die Abbildung realer Unternehmensstrukturen wie zum Beispiel unterschiedliche Standorte, Abteilungen oder Organisationseinheiten.

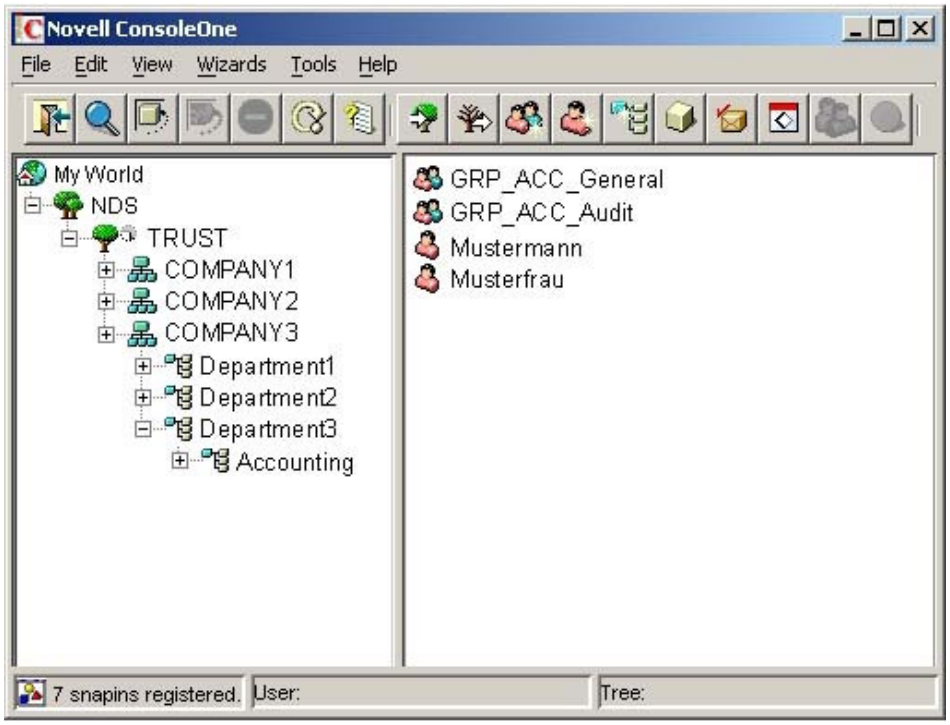

Abbildung 5: Verzeichnisbaum

Der realen Zugehörigkeit entsprechend erfolgt auch die Abbildung von Personen und Ressourcen des Unternehmens. Unabhängig davon können an beliebigen Stellen der Teilbäume weitere zur Verfügung stehende Objekte wie zum Beispiel Rollen abgebildet werden.

Objekte

Im Gegensatz zu bisher angeführten Berechtigungsverwaltungen, wo einer namentlich bezeichneten Person dezidiert Rechte zugeordnet wurden, entspricht in Directories eine Person einem komplexen Objekt mit einer Vielzahl an Eigenschaften, dessen Umfang vom jeweiligen Hersteller abhängen.

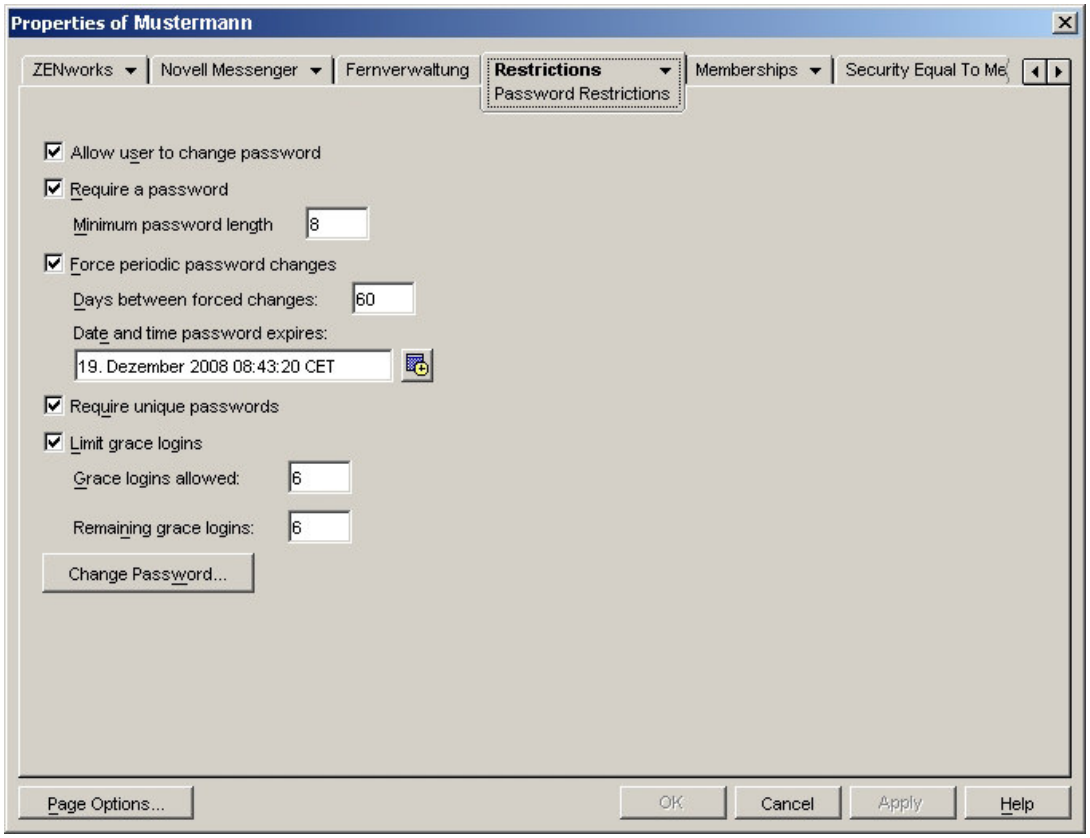

Abbildung 6: Objekt Person - Eigenschaften

Einige dieser Eigenschaften können vom Administrator vorgegeben werden, wie zum Beispiel Richtlinien hinsichtlich des verwendeten Passwortes (Länge, Wechselintervall,…), andere hingegen werden vom System generiert, wie zum Beispiel Datum und Uhrzeit der letzten Anmeldung der Person. Die Summe der einzelnen Eigenschaften nennt man Schema [8]. Durch Schemenerweiterung können beliebig zusätzliche Eigenschaften der Objekte definiert werden. So können auch im Directory verwaltete Ressourcen wie zum Beispiel Drucker oder Computer mit Standort und anderen Merkmalen versehen werden und bei Bedarf anhand dessen identifiziert werden.

Berechtigungen
Die eigentliche Zuordnung von Berechtigungen an Personen erfolgt vorzugsweise durch Mitgliedschaft einer Organisationseinheit, Gruppe oder Rolle. Schon durch die Position der Person in der hierarchischen Baumstruktur resultiert eine Gruppenzugehörigkeit. Üblicherweise ist eine Verschachtelung von Gruppen und Rollen untereinander uneingeschränkt möglich. Meist sind Rollen und Gruppen funktional ident und unterscheiden sich lediglich an ihren vordefinierten Eigenschaften. Für den Fall, dass es durch unterschiedliche Mitgliedschaften zu einem Konflikt bei einer konkreten Berechtigung kommt, gilt folgender Grundsatz:

Benutzerrecht bricht Rollenrecht bricht Gruppenrecht

Bei untereinander verschachtelten Gruppen und Rollen erben die Mitglieder die Berechtigungen, die dem übergeordnetem Objekt zugeteilt sind.

Implementierung
Technisch gesehen entspricht ein Directory einer relationalen Datenbank mit definierter Funktionsweise. Neben einem eventuellen proprietären Benutzerinterface zur Administration erfolgen Zugriffe üblicherweise anhand eines standardisierten Zugriffsprotokolls. Das ältere Directory Access Protokoll (DAP) wurde wegen seiner komplexen Spezifikation kaum verwendet. Dessen Weiterentwicklung, das Lightweight DAP (LDAP) hingegen findet weit verbreitete Anwendung. So können zum Beispiel viele aktuelle Mailprogramme auf ein zentrales Adressbuch mittels LDAP zugreifen und Email-Adressen abfragen. Auch schreibende Zugriffe erlaubt das LDAP, wodurch programmiertechnisch Änderungen im Directory durchgeführt werden können. Als Datenaustauschformat bieten die meisten Verzeichnisdienste eine standardisierte Import- beziehungsweise Exportschnittstelle für Daten im LDAP Data Interchange Format (LDIF) an. Der größte Vorteil eines Directorys liegt darin, dass in dieser übersichtlichen Baumstruktur durch unterschiedliche Gruppen- beziehungsweise Rollenmitgliedschaften die Berechtigungen einer Vielzahl unterschiedlicher Applikationen abgebildet werden können. Die jeweilige Applikation erfragt dabei mittels LDAP relevante Mitgliedschaften beziehungsweise direkt zugeordnete Eigenschaften der Person.

Die bekanntesten Produkte am Sektor der Verzeichnisdienste sind Microsofts Active Directory (AD) [9] und Novells eDirectory, vormals Novell Directory Service (NDS). Als kostengünstige Alternative sei das bei den meisten aktuellen Linux Distributionen inkludierte OpenLDAP erwähnt. Unabhängig von der Umsetzung zeichnet sich in Unternehmen ein starker Trend in Richtung eines zentralen Verzeichnisses (Metadirectory) zur Verwaltung personenbezogener Daten ab.

2.4.9 Role Based Access Control (RBAC)

Mittels Role Based Access Control (RBAC) wird dem Bestreben Rechnung getragen, Berechtigungen so granular und zweckmäßig wie möglich festzulegen. Jede Person soll über alle erforderlichen, jedoch keinesfalls mehr Rechte verfügen, als zum Ausführen ihrer Tätigkeit erforderlich sind. Durch Betrachtung der jeweiligen Aufgabe wird ein rollenbasiertes Abbild der Realität erstellt. Die einzelne Person wird dann einer oder mehreren Rollen zugeordnet, welche wiederum über entsprechende Rechte verfügen. Die Rechtevergabe erfolgt somit immer durch Rollenmitgliedschaft und nicht personenbezogen. Rollen lassen sich jederzeit beliebig hinzufügen, wodurch es ermöglicht wird, auch komplexe Berechtigungsstrukturen schrittweise aufzubauen.
Erste Entwicklungen in Richtung rollenbasierter Zugriffskontrolle erfolgten in den frühen 90er Jahren des vorigen Jahrhunderts [10]. 2004 folgte eine Standardisierung in Form der ANSI-Norm 359-2004. Das aktuelle Gesamtmodell besteht aus insgesamt vier einzelnen Versionen. Die Erste wird als Kernmodell bezeichnet und beschreibt die Grundfunktionen rollenbasierter Systeme. Die nächsten zwei Versionen setzen auf das Kernmodell auf und beschreiben jeweils eine funktionale Erweiterung. Die vierte Version repräsentiert eine Zusammenfassung der vorhergehenden Modelle.

Kernmodell
Das Kernmodell beschreibt die Basis dieser Berechtigungsverwaltung und besteht aus folgenden Komponenten:

- Rollen: Abbildungen von Tätigkeiten beziehungsweise Funktionen innerhalb des Systems.
- Rechte: Beschreiben, welche Operationen eine Rolle, an den mittels RBAC verwalteten Ressourcen, durchführen darf.
- Benutzer: Potentielle Anwender einer Rolle
- Sessions: Aktive Inanspruchnahme einer Rolle

Gemäß der in Abbildung 7 dargestellten Beziehungen können einer Rolle ein oder mehrere Rechte zugeteilt werden. Wobei eine dezidierte Berechtigung mehreren Rollen zugeordnet sein kann. Einem Benutzer werden genau jene Rollen zugeteilt, die er innerhalb des Systems ausüben darf. Wobei eine Rolle durch mehrere Benutzer ausgeführt werden kann.

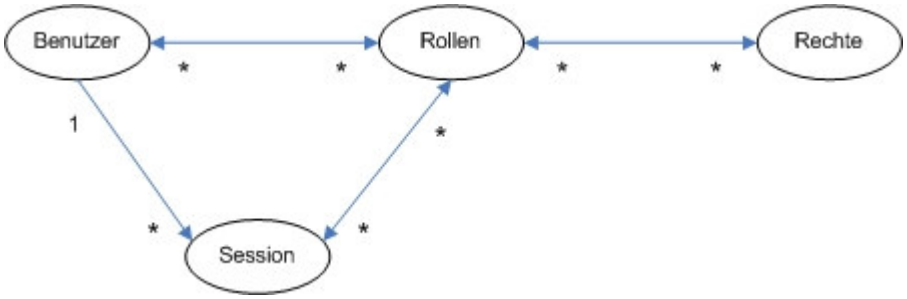

Abbildung 7: RBAC - Kernmodell

Eine Rolle erscheint bei erster Betrachtung funktional ident mit Gruppen aus vorhergehenden Modellen. Der wesentliche Unterschied liegt darin, dass der jeweilige Benutzer bei der Anmeldung am System eine Session aufbaut, bei der nicht automatisch alle zugeteilten Rollen aktiviert werden. Es entsteht eine selektive Inanspruchnahme einzelner Rollen. Die Zuordnung von Benutzern zu Rollen entspricht also nur der maximalen Möglichkeit an Berechtigungen. Die tatsächlichen Rechte sind von der in der aktuellen Session aktivierten Rollen abhängig. Zu beachten ist, dass je Benutzer mehrere Sessions aktiv sein können, jedoch entspricht eine Session genau einem Benutzer.[11]

Erweiterung 1

Das Grundmodell bietet ausreichend Möglichkeiten, jede denkbare Kombination von Berechtigungen an beliebige Rollen zuzuordnen. Schwachpunkt dieser autarken Rollen ist jedoch die Tatsache, dass bei marginal unterschiedlichen Berechtigungsanforderungen ähnlicher Rollen jede Rolle von Grund auf neu definiert werden muss. Die erste Erweiterung (Abbildung 8) schafft Abhilfe in Form der Implementierung einer Rollenhierarchie.

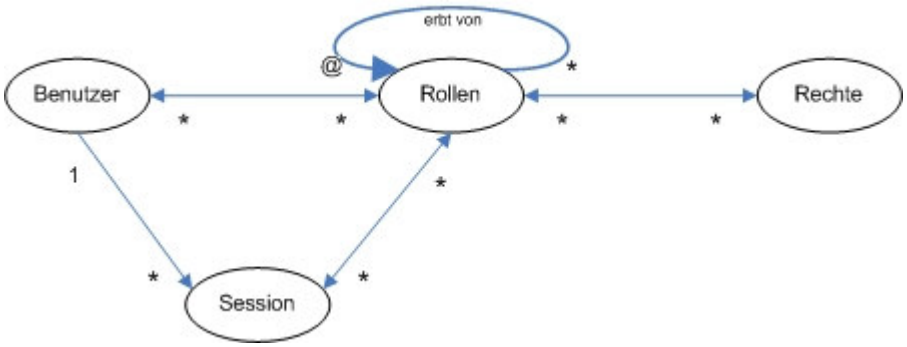

Abbildung 8: RBAC - Kernmodell mit Vererbung

Version 1 erlaubt somit, dass eine übergeordnete Rolle alle Berechtigungen mindestens einer untergeordneten Rolle übernehmen und erweitern kann. Dadurch wird es ähnlich eines Directorys unter anderem möglich, unternehmensinterne Strukturen abzubilden.
Aus Sicht der Berechtigungen entspricht die untergeordnete Rolle einer Teilmenge, übergeordnete Rollen verfügen in der Regel über zusätzlich vergebene Berechtigungen. Umgekehrt verfügen Benutzer einer übergeordneten Rolle über umfangreichere Berechtigungen und sind somit automatisch auch Benutzer der darunter liegenden Rolle.

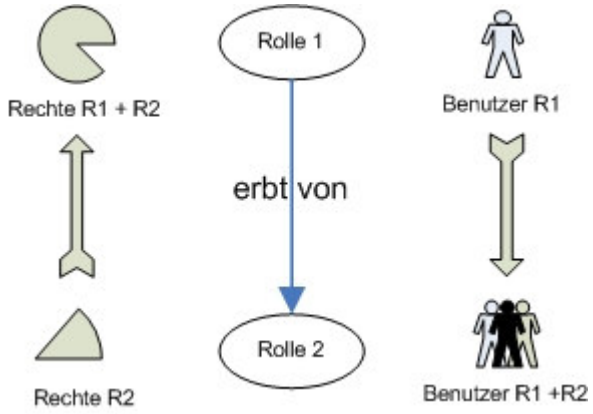

Abbildung 9: RBAC - Vererbungsregeln

Wie in Abbildung 9 dargestellt, ist Grundsätzlich eine uneingeschränkte Vererbung an Berechtigungen zwischen Rollen gestattet [12]. Manche Systeme verfügen jedoch über strukturelle beziehungsweise funktionale Einschränkungen, wie:

- Eine übergeordnete Rolle kann maximal eine andere Rolle beerben, wodurch die Komplexität überschaubar gehalten werden soll.
- Eine Baumstruktur mit genau einer Rolle maximaler Berechtigungen. (minimale Benutzer)
- Eine inverse Baumstruktur mit genau einer Rolle minimaler Berechtigungen. (maximale Benutzer)
- Eine Struktur mit jeweils einer Rolle minimaler und einer maximaler Berechtigungen und der verpflichtenden Eingliederung aller im System existierenden Rollen und Benutzer in diese Struktur.

Erweiterung 2

Die zweite , von der Version 1 unabhängige Erweiterung, ermöglicht die Festlegung von Einschränkungen hinsichtlich der Rollenverwendung. Hintergrund dafür ist die Trennung konfliktbehafteter Rollen. (SoD, Separation of Duties) Im einfachsten Fall erfolgt dies durch Festlegen einer Obergrenze maximaler gleichzeitig verwendeter Rollen. Mehr Flexibilität erhält man dadurch, indem explizit festgelegt wird, welche Rollen sich gegenseitig ausschließen.

Diese Einschränkungen können auf zwei unterschiedliche Arten festgelegt werden. Bei einer statischen Überprüfung ist es generell untersagt, einer Person zwei konfliktbehaftete Rollen zuzuordnen. Im dynamischen Fall ist die Zuordnung prinzipiell gestattet, man verbietet jedoch die gleichzeitige Verwendung innerhalb einer Session.

Gesamtmodell

Die beiden beschriebenen Erweiterungen der Grundform sind nicht vollständig kompatibel. Eine übergeordnete Rolle kann Berechtigungen anderer Rollen kombinieren (Version 1), welche sich jedoch durch eine Einschränkung (Version 2) gegenseitig ausschließen sollten und diese Vorgabe somit unwirksam wird. Das Gesamtmodell (Abbildung 10) selbst verfügt über keine weiteren Funktionen sondern ist nur eine konfliktfreie Vereinigung der beiden Erweiterungen.

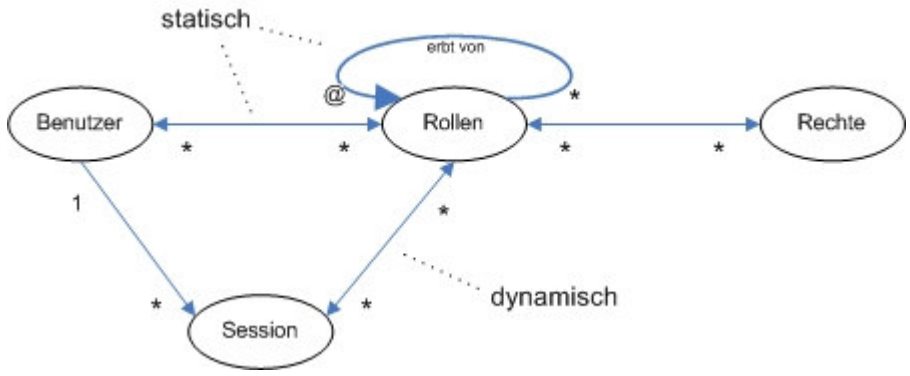

Abbildung 10: RBAC - Gesamtmodell

Sowohl in der Modelltheorie als auch aus Sicht der praktischen Umsetzung sind beliebige Erweiterungen des Konzeptes denkbar. So kann zum Beispiel die Zuordnung einer Rolle von zeitlichen Faktoren aber auch vom Eintreten eines bestimmten Ereignisses abhängig gemacht werden. Das daraus resultierende Gesamtmodell ergibt ein fein skalierbares, flexibles und zugleich mächtiges Werkzeug der Berechtigungsverwaltung.

2.4.10 Unterscheidungsmerkmale

Ein unabhängig vom gewählten Berechtigungsverwaltungssystems evidenter Aspekt ist die Granularität, mit der die Berechtigungen vergeben werden können. So kann zum Beispiel auf Betriebssystemebene exakt festgelegt werden, welche Mitarbeiter Änderungen in einer Datei machen können sollen und somit Schreibberechtigung auf die Datei benötigen. Soll jedoch innerhalb der Datei näher differenziert werden, welche Teilbereiche von welchem Mitarbeiter bearbeitet werden dürfen, so ist eine feinere Berechtigungseinteilung erforderlich, die auf Anwendungsebene implementiert werden muss. Aus administrativer Sicht ergibt sich jedoch dadurch das Problem, dass ein neuer Benutzer sowohl auf Betriebssystemebene für den generellen Zugriff auf die Datei als auch auf Anwendungsebene für den speziellen Teilbereich innerhalb der Datei berechtigt werden muss. In größeren Unternehmen sind dafür jedoch oftmals unterschiedliche Abteilungen beziehungsweise Mitarbeiter zuständig, dessen Koordination in der Praxis nicht immer hundertprozentig möglich ist.
Grundsätzlich kann man feststellen, dass mit höherer Ebene, in welcher die Berechtigung festgelegt wird, auch die Komplexität der Berechtigungsverwaltung und somit auch die Fehleranfälligkeit erhöht ist. Fehler durch falsch gesetzte Berechtigungen bieten aber eine ideale Möglichkeit für eventuelle Angriffe auf ein System.
Eine weitere denkbare Konsequenz komplexer Berechtigungssysteme ist das Unvermögen von Administratoren, exakt alle erforderlichen Berechtigungen zu erteilen, sei es aus mangelnder Ausbildung der Person aber auch aufgrund von Schwächen im Design der Berechtigungsverwaltung. Als Beispiele dafür seien der große Prozentsatz an Windows-Benutzern, die aus Einfachheit selbst für ihre alltägliche Tätigkeit am Rechner mit Administratorrechten ausgestattet sind, aber auch die vorwiegend linux-basierenden Webserver, die unter dem Benutzer „root“ ausgeführt werden, erwähnt. [13], [14]

2.5 Sicherheitsmodelle

Sicherheitsmodelle (Security Policy Models) bieten die Grundlagen zur Beschreibung oder Ausformulierung jener Sicherheitsrichtlinien (Security Policies), welche auf Basis der Zugriffskontrollmechanismen umgesetzt werden. Ausgangspunkte sind hierfür ebenfalls die Betrachtung von Mitarbeitern, Berechtigungsobjekte und die Art des lesenden Zugriffes beziehungsweise des schreibenden Informationsfluss.
Sicherheitsrichtlinien werden üblicherweise vom Management oder von Produktverantwortlichen festgelegt und definieren, welche Personen auf welche Daten welche Berechtigungen besitzen. Gemäß dem in Kapitel 1.6 erwähnte „Least-Privileges“-Prinzip sollen die Personen genau ausreichend Berechtigungen besitzen, die sie für ihre Tätigkeit benötigen. Diese Richtlinien sind üblicherweise strikt einzuhalten, wobei Abweichungen einen Sicherheitsalarm auslösen beziehungsweise zumindest dokumentiert werden sollen.

Eine Sicherheitsrichtlinie soll eine kurze aber prägnante Zielformulierung darstellen, unabhängig von den zur Implementierung zur Verfügung stehenden Schutzmechanismen. Sicherheitsmodelle bilden eine theoretische Grundlage als Hilfestellung bei der technischen Ausformulierung der Vorgaben.

2.5.1 Multilevel Security

Multilevel Security (MLS) ist die Klassifizierung von Daten anhand unterschiedlicher Geheimhaltungsstufen. Die ursprüngliche Entwicklung entsprang aus Bedürfnissen des Militärs und findet vermehrt in modernen Serversystemen Anwendung.

> *Daten (Geheimhaltungsstufen): offen - vertraulich – geheim – streng geheim*
> *Person (Freigabestufen): analoge Freigabestufen*

Je nach Modell ist der Zugriff ausgehend von der Freigabestufe der Person auf Daten festgelegter Geheimhaltungsstufen über definierte Zugriffsarten gestattet oder untersagt.

2.5.1.1 Bell-LaPadula Modell

Eine Richtlinie in diesem Modell besagt, dass Personen einer Freigabestufestufe nur auf Daten Zugriff besitzen, die in der selben oder in einer niedrigeren Geheimhaltungsstufe klassifiziert sind („no read up“)[15].

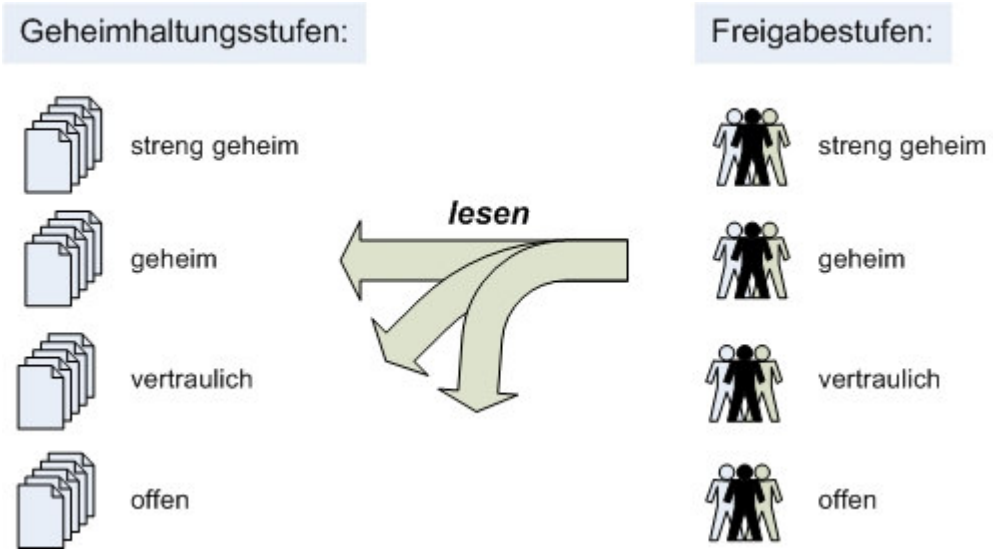

Abbildung 11: Bell-LaPadula Modell - lesen

Ein durch diese Richtlinie entstehender Effekt ist, dass ein Informationsfluss nur nach oben zulässig ist (Abbildung 11). Niedriger gestufte Personen haben keine Möglichkeit

auf Daten einer höheren Stufe zuzugreifen, außer diese Daten werden von einer autorisierten Person herabgestuft.
Eine weitere Richtlinie dieses Modells besagt, dass keine Daten in eine tiefere Stufe geschrieben werden dürfen („no write down“). Dadurch soll gesichert werden, dass Informationen von Personen einer höheren Freigabestufe nicht eigenmächtig in eine niedrigere Geheimhaltungsstufe übertragen werden.

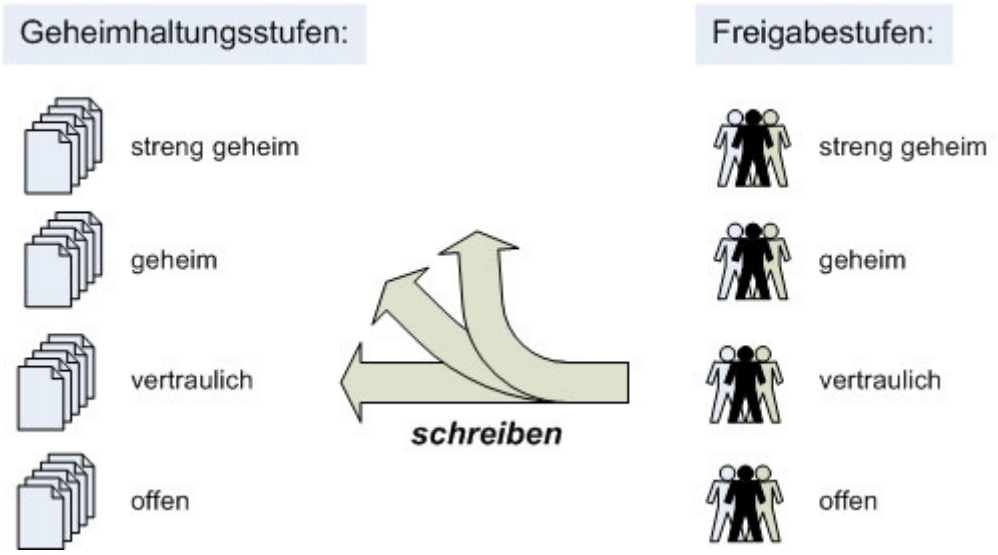

Abbildung 12: Bell-LaPadula Modell - schreiben

Aus sicherheitstechnischer Sicht bei der Umsetzung ist die zweite Richtlinie die Kritischere, da bei Verletzung dieser Regel ein herabstufen von Informationen ermöglicht wird.
In diesem Modell wird jedoch auch automatisch untersagt, dass Anweisungen in eine niedrigere Stufe gegeben werden können. Weiters entsteht dass Problem des blinden schreiben, da Daten zwar in eine höhere Stufe geschrieben werden dürfen, nicht jedoch gelesen.

2.5.1.2 System Z Modell

Das System Z ist weitgehend ident mit dem Bell-LaPadula Modell mit der Erweiterung, dass auf Anfrage temporär die Geheimhaltungsstufe von Daten durch einen Administrator herabgestuft werden kann. Motivation dafür ist, dass Personen von Grund auf mit so wenig wie möglich Berechtigungen ausgestattet werden und nicht sofort, wenn dieser Person für einen Zugriff Berechtigungen fehlen, diese sogleich hinaufgestuft werden.
Als Streitpunkt an diesem System wird immer angeführt, dass durch dieses Umstufen eindeutig Sicherheitsrichtlinien verletzt werden, wenn auch nur temporär, und somit

nicht als gesamtheitliches Sicherheitsmodell bezeichnet werden kann. Weiters ist aufgrund dieser erforderlichen Eingriffsmöglichkeit eine Implementierung in der Realität eher mühsam und aus sicherheitstechnischer Sicht fraglich.
Darüber hinaus gibt es noch eine Vielzahl weiterer Abwandlungen des Bell-LaPadula Modells, die vorwiegend bedarfsbezogen formuliert wurden und als eigenständige Modelle nicht von Bedeutung sind.

2.5.1.3 Biba Modell

Das Biba Modell wird weitläufig gerne als umgekehrtes Bell-LaPadula Modell bezeichnet [15]. Es besteht aus den selben Grundkomponenten jedoch mit genau entgegengesetzten Richtlinien. So dürfen Daten höherer Stufe gelesen werden und in niedrigeren Stufen geschrieben werden.
Dieses Modell dient vorwiegend der Integritätskontrolle von Daten, weniger der Kontrolle von Datenfluss. Wichtige Informationen können von Personen gelesen aber nicht verändert werden, geschrieben werden kann nur in nicht so sicherheitsrelevanten Bereichen. Anwendungsgebiete sind vorwiegend in der Steuerungs- und Messtechnik, wo Daten von extern nach fixen Richtlinien verarbeitet und ausgewertet werden sollen, nicht jedoch beliebig manipuliert werden können sollen.
Eine Optimierung aus Integritätskontrolle und Kontrolle des Datenflusses wäre eine Kombination von Biba und Bell-LaPadula Modell. Das Resultat wäre jedoch ein Modell, bei dem jede beteiligte Person genau nur auf jene Geheimhaltungsstufe Zugriff besitzt, die seiner Freigabestufe entspricht, was in der Praxis jedoch nicht von Relevanz ist.

2.5.1.4 Modellübergreifende Betrachtung

Das Konzept der Multilevel Security (MLS) eignet sich bevorzugt in Systemen, dessen angebotene Dienste laufend Angriffen ausgesetzt sind, wie zum Beispiel Webserver oder Firewalls. Sollte es einem Angreifer gelingen, über eine Schwachstelle Zugriff auf das Gesamtsystem zu erhalten, so sollen diese Zugriffe auf die entsprechende Anwendung begrenzt sein und keinesfalls eine komplette Übernahme des Systems zulassen.
Im Einsatzfall in Benutzersoftware haben Untersuchungen gezeigt, dass der Schwerpunkt hauptsächlich auf Datenintegrität gelegt wird und verwendete Sicherheitsmodelle grundlegend auf das des Biba Modells aufsetzen.

Kritikpunkte
Mit steigender Verbreitung dieser Sicherheitsmodelle kamen unterschiedliche Probleme sowohl aus konzeptioneller Sicht aber auch aus Sicht der Implementierung zum Vorschein:

- Ein konzeptioneller Schwachpunkt ist mit Sicherheit die Eigenschaft, dass Daten nur in „vertikaler “ Richtung anhand ihrer Geheimhaltungsstufe separiert werden

können, nicht jedoch in „horizontaler“ Richtung. Dadurch fehlt die Möglichkeit der Bildung von geschützten Datenbereichen, wie es zum Beispiel für Abteilungsdaten oder auch persönlichen Gesundheitsdaten erforderlich ist.

- Ein massives Problem ist die systemübergreifende Datenweitergabe. Selbst wenn auch im Zielsystem Multilevel Security (MLS) Verwendung findet, so kann nicht garantiert werden, dass die Anzahl bzw. Klassifizierung der Geheimhaltungsstufen vergleichbar ist mit jenen am Quellsystem. Ebenso muss bei der Datenübernahme aus einem Fremdsystem erstmals eine Klassifizierung durchgeführt werden.
- Die administrative Tätigkeit der Umsetzung dieser Sicherheitsmodelle setzt oftmals großes fachliches Wissen voraus, da das Konzept nicht direkt in gängige Berechtigungsverwaltungen abgebildet werden kann.
- Oftmals hat sich bei älteren Anwendungen herausgestellt, dass schon aus rein technischer Sicht eine Umsetzung gar nicht möglich ist, weshalb diese Anwendungen neu geschrieben oder zumindest maßgeblich überarbeitet werden mussten.
- Aus praktischer Sicht in der laufenden Administration zeigte sich im Problemfall die Gefahr der Überberechtigung. Das Erhöhen der Freigabestufe einer Person ist um ein vielfaches einfacher als das analysieren und eventuell erforderliche Anpassen von Geheimhaltungsstufen einzelner Daten.
- Kritisch ist weiters, dass es aus technischer Sicht für Entwickler oder Administratoren immer Zugriffsmöglichkeiten auf den kompletten Datenstamm aller Geheimhaltungsstufen geben muss.

Auch, wenn die Vielzahl der aufgezählten Probleme im ersten Moment abschreckend wirken mag, so profitiert zum Beispiel das Bell-LaPadula Modell durch seinen sehr simplen Aufbau. Und genau diese beobachteten Probleme waren auch mitverantwortlich dafür, dass laufend Verbesserung und Entwicklung an Sicherheitsmodellen betrieben wird. [15]

2.5.2 Multilateral Security

Multilateral Security setzt bei der Anforderung an, den Informationsfluss nicht in „horizontaler“ Richtung anhand Geheimhaltungsstufen zu kontrollieren, sondern in „vertikaler“ Richtung. Dies ermöglicht die Bildung geschützter Datenbereiche, wie es

zum Beispiel für sensible Patientendaten aber auch zur Abbildung organisatorischer Strukturen in Form von Abteilungsdaten erforderlich ist.

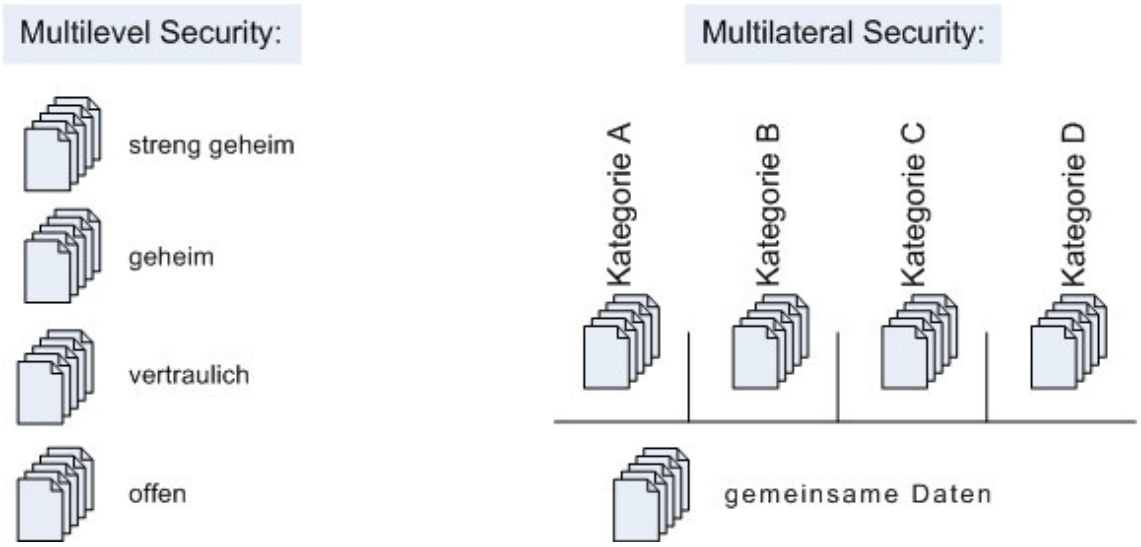

Abbildung 13: Multilateral Security

Oftmals ist der aktuelle Zugriffsbereich von äußeren Faktoren abhängig, was die Komplexität der Implementierung der einzelnen Sicherheitsmodelle maßgeblich erhöht aber auch fehleranfälliger macht. So sind Patientendaten generell vertraulich zu behandeln. Im Krankheitsfall ist es jedoch erforderlich, dass die behandelnden Ärzte Zugriff auf eine eventuelle Krankengeschichte des Patienten besitzen. Als weiteres Bespiel seien Unternehmensberater erwähnt, denen je nach aktuellen Kunden der Zugriff auf weitere Kundendaten untersagt sein sollte, um der Verwendung von Insiderwissen vorzubeugen.

2.5.2.1 Lattice Modell

Der Ursprung diese Modells liegt bei der amerikanischen Regierung, wo es üblich war, Daten nicht nur in Geheimhaltungsstufen einzuteilen sondern zusätzlich mit Code- beziehungsweise Schlüsselwörter zu versehen. So ist für den Zugriff auf die Daten nicht nur die erforderliche Freigabestufe sondern auch eine korrekte zusätzliche Abteilungs- beziehungsweise Gruppenmitgliedschaft erforderlich. In der Praxis zeigte sich jedoch, dass es bei freier Vergabemöglichkeit von Schlüsselwörtern und verbundener Anlage entsprechender Gruppen sehr schnell zu einem Wildwuchs kommt, der zu einem komplexen Netzwerk an effektiv gesetzten Berechtigungen führt.
Das Lattice Modell basiert somit grundlegend auf dem Bell-LaPadula Modell, ist jedoch um die Möglichkeit von Gruppenmitgliedschaften erweitert. Für den Datenstamm

bedeutet dies neben der Klassifizierung in Geheimhaltungsstufen die zusätzliche Zuordnung von ein oder mehreren Gruppen.

Datensatz („geheim“ („ Code A“))

Besitzt zum Beispiel ein Mitarbeiter Freigabestufe „geheim“, so ist es ihm primär gestattet, auf alle Daten der Geheimhaltungsstufe „geheim“ und darunter zuzugreifen. Sofern diese Daten weiters mit dem Codewort „Code A“ versehen sind, ist zusätzlich noch die Mitgliedschaft in der Gruppe „Code A“ erforderlich. Dies führt zu einem Netzwerk möglicher Berechtigungskombinationen.
Abteilungsdaten können somit einfacherweise durch Zuordnung des Abteilungsnamen als Schlüsselwort geschützt werden. Dies gleicht sozusagen einer Aufspaltung des Lattice Modells in einzelne Bell-LaPadula Modelle für jede Abteilung. Als dynamischen Ansatz der Berechtigungskontrolle könnte man beispielsweise implementieren, dass ab einer bestimmten Anzahl an Schlüsselwörtern die Geheimhaltungsstufe automatisch erhöht wird.

2.5.2.2 Chinese Wall

Ein weiterer Ansatz zur Verwaltung geschützter Datenbereiche ist das Chinese Wall Modell. Dessen Ursprung liegt im Finanzsektor und zielt auf die Vermeidung von Interessenskonflikten ab. So haben zum Beispiel Investmentbanker oder Unternehmensberater eine Vielzahl an Kunden ähnlicher Interessen. Ist ein Mitarbeiter nun mit den Belangen eines Kunden betraut, so darf er keinen Zugriff auf Daten anderer Kunden mit ähnlichem Betätigungsfeld besitzen. Somit haben bereits getätigte Zugriffe auf Daten Auswirkungen auf künftige Berechtigungen. Dies dient nicht nur dem Schutz der Daten einzelner Kunden, im Falle der Verwendung von Insiderinformationen im Wertpapierhandel kann es auch zu strafrechtlich relevanten Tatbeständen führen.

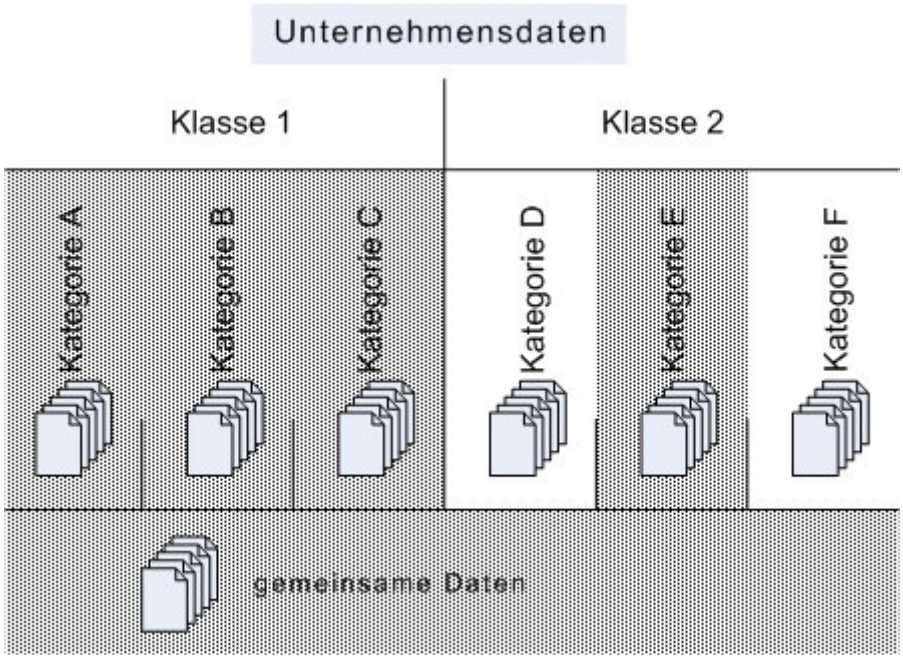

Abbildung 14: Chinese Wall

Je nach Branche der Kunden werden die Kundendaten in unterschiedliche Interessenskonfliktklassen unterteilt. Im Ausgangszustand besitzt jeder Mitarbeiter des Unternehmens vollen Zugriff auf die gesamten Kundendaten. Übernimmt nun ein Mitarbeiter die Betreuung eines Kunden, z.B. des „Kunden E“ in der „Konfliktklasse 2“, so darf dem Mitarbeiter künftig kein Zugriff auf Daten anderer Kunden der selben Konfliktklasse möglich sein. Unbeeinflusst bleiben hingegen die Zugriffsberechtigungen auf Kundendaten anderer Konfliktklassen beziehungsweise der gemeinsamen Daten.
In der Praxis zeigt sich, dass diese „Konfliktklassenregel“ meist nur temporäre Gültigkeit benötigt und mit einer Ablaufzeit versehen wird. Eine Umsetzung des Modells ohne manuellen administrativen Eingriffen ist jedoch nahezu undenkbar.

2.5.2.3 BMA Modell

Das BMA Model, benannt nach und entwickelt von der British Medical Association (BMA) steht stellvertretend für eine Vielzahl weiterer multilateraler Sicherheitsmodelle mit frei definiertem Regelwerk. Dabei gilt es einerseits, behandelnden Medizinern historische Untersuchungsdaten über die Krankengeschichte eines Patienten zu Verfügung zu stellen, andererseits die Privatsphäre des Patienten zu gewährleisten. Bestrebungen, persönliche Notfallsinformationen auf Smartcards zu speichern haben weitreichende Diskussionen hinsichtlich Datenschutz ausgelöst. Einerseits kann es im Notfall über Leben und Tod entscheiden, wenn dem Mediziner alle Informationen über eventuelle Unverträglichkeiten, Allergien oder aktuelle Krankheiten eines Verunfallten

zur Verfügung stehen. Die Tatsache, dass diese Informationen aber personenbezogen eventuell sogar auf der Smartcard selbst abgespeichert sind, löst verbreitet Unbehagen und Angst vor missbräuchlicher Verwendung aus.
Potentieller Risikofaktor für Datenschutzverletzungen ist hierbei die große Anzahl an Personen, denen Zugriff auf diese personalisierten Gesundheitsdaten ermöglicht werden muss. Sinnvoller Weise zählen dazu sämtliche Fachärzte respektive deren Praxisgehilfen. Weitaus größere Datenmengen können dementsprechend in Spitälern gesammelt und in Folge diskreditierend gegen unliebsame Personen verwendet werden oder aber auch missbräuchlich als Grundlage zur Risikofestlegung bei Gesundheitsversicherungen herangezogen werden.
Eine Verbesserung gelang mit Hilfe von Geheimhaltungsstufen analog zur Multilevel Security. Der Datenstamm eines Patienten durfte dafür nicht als Gesamtheit aller relevanten klinischen Daten gesehen werden sondern wurde in einzelne Informationseinheiten mit unterschiedlichen Zugriffsberechtigungen unterteilt. So wurden in frühen Entwicklungsstufen insbesondere Informationen über unheilbare Krankheiten wie zum Beispiel AIDS als höchst vertraulich eingestuft. Eine Weiterentwicklung in Richtung feiner festlegbarer Berechtigungen gelang durch Ersatz der Geheimhaltungsstufen durch Access Control Lists (ACLs). Dadurch kann auf Basis einzelner Personen festgelegt werden, auf welche Datenbereiche diesen welcher Zugriff gestattet ist.
Das Regelwerk des BMA Modells beinhaltet beispielsweise folgende Prinzipien (nach Ross Anderson [5]):

- Jede Informationseinheit muss über eine dezidierte ACL verfügen, mit welcher genau geregelt ist, welche Personen schreibend beziehungsweise lediglich lesend auf die Informationen Zugriff besitzen. Alle anderen Personen müssen durch das System am Zugriff gehindert werden.
- Der Zugriff auf Informationen kann nur mit Zustimmung des Patienten erfolgen. Im Falle einer Überweisung ist zusätzlich die Zustimmung des überweisenden Arztes erforderlich.
- Eine der Personen der ACL muss als Ansprechpartner ausgewiesen sein. Nur diese Person kann Änderungen an der ACL durchführen.
- Der Patient muss über Inhalt und Änderungen an der ACL laufend informiert werden und zustimmen, ausgenommen in Notfallsituationen oder gesetzlichen Ausnahmefällen.
- Niemand kann Daten ohne Wartefrist löschen.

- Alle Zugriffe, Änderungen und Löschungen von Informationen müssen mit Name, Datum und Uhrzeit protokolliert werden.
- Die Übernahme von Daten in andere Informationseinheiten ist nur möglich, wenn die Personen in der neu gültigen ACL eine Teilmenge der vorher gültigen ACL sind.
- Es ergeht gesonderte Information an den Patienten, sobald eine Person für den Zugriff berechtigt wird, die schon auf eine große Anzahl anderer Patientendaten berechtigt ist, um Datensammeln zu vermeiden.
- Gefordert sind vertrauenswürdige Computersysteme, welche die Patientendaten gemäß den angeführten Prinzipien verwalten und schützen.

Das Regelwerk des BMA Modells erfüllt weitgehend alle Ansprüche des Datenschutzes ebenso wie die Zielsetzung, historische Krankheits- beziehungsweise Behandlungsdaten eines Patienten für künftige Diagnosen und Auswertungen bereit zu stellen. Aufgrund des komplexen Aufbaues und der Verwaltungsmechanismen gestaltet sich die technische Umsetzung als sehr aufwendig und kostenintensiv. Eine weitere Hürde sind nationale Abweichungen im Regelwerk, die einen internationalen Austausch der Patientendaten erschweren.
Der größte Risikofaktor beim BMA Modell sind staatlich veranlasste statistische Auswertungen. Um repräsentative Daten erhalten zu können, müssen die Auswerter Zugriff auf eine entsprechend große Anzahl an Datensätzen besitzen. Verhindert werden soll jedoch das Auslesen aller vorliegenden medizinischen Daten zu einer bestimmten Person.
Eine denkbare Möglichkeit zur Wahrung der Anonymität ist die Trennung medizinischer Daten von Name und Anschrift der betreffenden Person. Dadurch sind zwar Abfragen anhand exakter Personendaten unterbunden ohne regionale beziehungsweise altersspezifische Auswertungen einzuschränken. Jedoch ist es weiterhin leicht möglich, aufgrund regionaler Einschränkung beim Wohnort und exaktem Geburtsdatum Rückschlüsse auf die genaue Identität der Person zu tätigen. Eine weitere Verbesserung erfolgt durch eine automatisierte Vorbearbeitung der Gesundheitsdaten, welche dann nur gruppiert in Altersklassen bzw. Regionen abgefragt werden können. Auch denkbar wären restriktive Beschränkungen für statistische Abfragen insofern, dass jede Abfrage eine Mindestanzahl an Ergebnissen liefern muss, da sonst die Abfrage als zu präzise und unzulässig gewertet wird. Dies sei nur als Denkanstoß zu verstehen und ist nicht Teil des eigentlichen Themas der Arbeit. Für weiterführende Informationen zum BMA-Modell siehe [16] beziehungsweise [17].

2.5.3 Modellerweiterungen

Unabhängig von den bisher erwähnten Modellen, Zugriffsberechtigungen abzubilden und in Regeln zu formulieren, resultieren zeitgleich klar definierte Wege, in denen ein Informationsfluss möglich ist. Darüber hinaus kann es jedoch als Erweiterung erforderlich sein, zusätzliche Regeln zur Kontrolle des Informationsflusses festzulegen. Ein typischer Anwendungsfall sind Sicherheitsmodelle im Buchhaltungs- beziehungsweise Bankenwesen. Diese basieren grundlegend auf multilaterale Sicherheitsmodelle, in denen die erforderlichen Berechtigungen in Abhängigkeit des Tätigkeitsbereiches festgelegt werden. Im Falle spezieller Transaktionen können jedoch über die erforderlichen Zugriffsberechtigungen hinaus weitere Bedingungen zu erfüllen sein. Von diesen seien in Folge die zwei gängigsten Varianten näher erläutert:

- Dual Control (Vier-Augen Prinzip): Für die Durchführung der Transaktion ist es erforderlich, dass mindestens zwei berechtigte Personen zeitgleich die Transaktion initiieren. Ein anschauliches Beispiel sind die aus Film und Fernsehen bekannten Szenen, in denen mindestens 2 US-Militärs für den Start einer Rakete mit nuklearen Sprengköpfen jeweils einen Schlüsselschalter betätigen müssen.

- Separation of Duties (Trennung der Zuständigkeitsbereiche) Dieses Prinzip spiegelt einen Workflow von mindestens zwei beteiligten Personen wider, welche für die Durchführung einer Transaktion jeweils eine Aktion ihres Gegenübers einholen müssen. Jede Bestellung von Bürobedarf in größeren Unternehmen folgt dieser Regel. Statt die Bestellung selbst auszulösen, muss der Mitarbeiter zuerst die Bestellung vom Vorgesetzten absegnen lassen und an den Einkauf weiterleiten. Die Warenannahme übernimmt das bestellte Material, liefert es an den Besteller intern weiter und übergibt die Rechnung an die Buchhaltung zur Verbuchung.

Diese zusätzlichen Regeln sind in machen Anwendungsfällen erforderlich und hilfreich, sind jedoch nicht Teil der Berechtigungsverwaltung bzw. Analyse und müssen in Form eines Workflows von der betreffenden Applikation abgebildet werden.

2.5.4 Auswahlkriterien

Die Auswahl eines Sicherheitsmodells für eine bestimmte Anwendung hängt von einer Vielzahl von Faktoren ab. Das Lattice Modell scheint in seiner Funktion zum Beispiel für Aktenverwaltungssysteme geeignet, da die Differenzierung anhand einer Beschlagwortung auch schon bei Akten in Papierform eine gängige Praxis war. Im Falle eines Archivs können alle Sicherheitsvorgaben abgebildet werden - soll jedoch ein

Informationsfluss kontrolliert werden, so stößt das Lattice Modell rasch an seine Grenzen. Es müssen zusätzliche Regeln gefunden werden oder aber auch die Datenweitergabe strikt an definierte Workflows gebunden werden.
Ein weiteres maßgebliches Unterscheidungsmerkmal ist, ob die Berechtigen wie zum Beispiel beim Chinese Wall Model zentral an einer Stelle verwaltet werden oder wie zum Beispiel beim BMA Model dezentral entsprechend vorgegebener Regeln vergeben werden können. Ersteres erfordert im Allgemeinen umfassendes Wissen über die Sicherheitsanforderungen und ermöglicht eine zentrale Kontrolle vergebener Berechtigungen. Eine dezentrale Berechtigungsvergabe ist hingegen einfacher zu warten, da zusätzlich erforderliche Berechtigungen von speziell dafür ausgewählten Personen vorgegebenen Regeln entsprechend jederzeit erteilt werden können. Die Daten der Zugriffskontrolle sind dabei oftmals direkt an die Information gekoppelt, wodurch eine zentrale Auswertung vergebener Berechtigungen nahezu unmöglich wird.
Die Vielfalt möglicher Modelle ist zu groß als dass man generell gültige Richtlinien zur Wahl eines Sicherheitsmodells festlegen kann. [5], [18]

2.6 Information Security Policies

Zum Schutz eigener Interessen und Ziele eines Unternehmens kommen unterschiedliche Sicherheitsvorgaben zum Einsatz. Die inhaltliche Beschreibung erfolgt in Form von Sicherheitsrichtlinien (Security Policies). Diese umfassen unter anderem den gesamten Bereich der Informationssicherheit, angefangen von physischen Zugangsbeschränkungen, bewusstseinsbildende Maßnahmen für Mitarbeiter bis zu Datensicherung oder Öffentlichkeitsarbeit. Ein für diese Arbeit relevanter Teilbereich davon ist die IT-Informationssicherheit. Genau genommen auch nur jener Teil davon, welcher Zugriffsberechtigungen auf elektronische Daten in den eingesetzten EDV-Systemen beschreibt.
Eine Sicherheitsrichtlinie ist üblicherweise ein Dokument mit einem Regelwerk, welches für die Erfüllung der Sicherheitsziele eingehalten werden muss.[19], [20]

2.6.1 Motivation und Ziele

Information und Wissen ist ein nicht zu unterschätzender Wert eines Unternehmens. Mitarbeiter benötigen im Zuge ihrer Tätigkeit Zugriff auf Daten und Informationen. Dabei muss auf folgende Aspekte Rücksicht genommen werden:

- Datenschutz: Einhaltung gesetzlicher und vertraglicher Vorgaben
- Vertraulichkeit: Informationen nur an berechtigte Personen
- Integrität: Schutz vor unberechtigter Änderung und Löschung
- Verfügbarkeit: Bei Bedarf abrufbar
- Authentizität: Information über die Identität des Anwender

Alle erforderlichen Maßnahmen zur Erfüllung dieser Sicherheitsziele werden in der Sicherheitsrichtlinie beschrieben.

2.6.2 Erstellung einer Policy

Unerlässlich für die erfolgreiche Entwicklung und Umsetzung einer Security Policy ist ein Rückhalt aus dem Management des Unternehmens. Grund dafür sind nicht nur die resultierenden Kosten sondern vor allem die Einführung meist unpopuläre Maßnahmen. Diese oft als lästig empfundenen Regeln machen sich aber spätestens beim ersten sicherheitstechnischen Zwischenfall bezahlt.
Aus praktischer Sicht unerlässlich ist eine Abwägung zwischen Sicherheit und Verwendbarkeit. Zu strikte Einschränkungen haben gegebenenfalls Auswirkungen auf die tägliche Arbeit des Mitarbeiters, wodurch ein aus sicherheitspolitischer Sicht kontraproduktives Bild beim Mitarbeiter entsteht. Praktische Hinweise für die Entwicklung von Security Policies findet man in [21] beziehungsweise [22].

Standard
Ein standardisierter Leitfaden zur Implementierung von Sicherheitsrichtlinien existiert in Form der ISO 17799 [23] beziehungsweise ISO/IEC 27001 [2], ein Text basierend auf dem British Standard 7799-1. Darüber hinaus gibt es eine Vielzahl öffentlicher Sicherheitshandbücher und Nachschlagewerke aber auch beratende Unternehmen, die bei der Entwicklung von Sicherheitsrichtlinien hilfreich sind.

Umfeldbeschreibung
Mit Hilfe der Sicherheitsrichtlinien sollen unternehmensweite Regeln eingeführt und angewendet werden. Unerlässlich dafür ist eine vorherige Analyse des Unternehmens und deren Struktur. Unter anderem sollten folgende Fragen geklärt werden:

- Welche Daten sollen geschützt werden?
- Welche Sicherheitsrichtlinien gibt es bereits?
- Kann der Grad der Umsetzung anhand Kennzahlen gemessen werden?
- Gibt es eine innerbetriebliche Kontrollinstanz?
- Gibt es Hilfestellung bei Sicherheitsproblemen?
- Sind die technischen Voraussetzung für die Umsetzung gegeben?
- Gibt es Konsequenzen für Zuwiderhandeln?

Erst nach Klärung dieser vorwiegend organisatorischen beziehungsweise technischen Fragen startet der Bildungsprozess einer Sicherheitsrichtlinie.

Beteiligte Bereiche

Technisch befinden sich interne elektronische Daten auf zentralen Datenspeichern, auf welche unternehmensweit zugegriffen werden kann. Im Entscheidungsprozess, welche Mitarbeiter auf welche Daten für welchen Zugriff berechtigt werden, gibt es mehrere beteiligte Unternehmensbereiche. [24], [25]

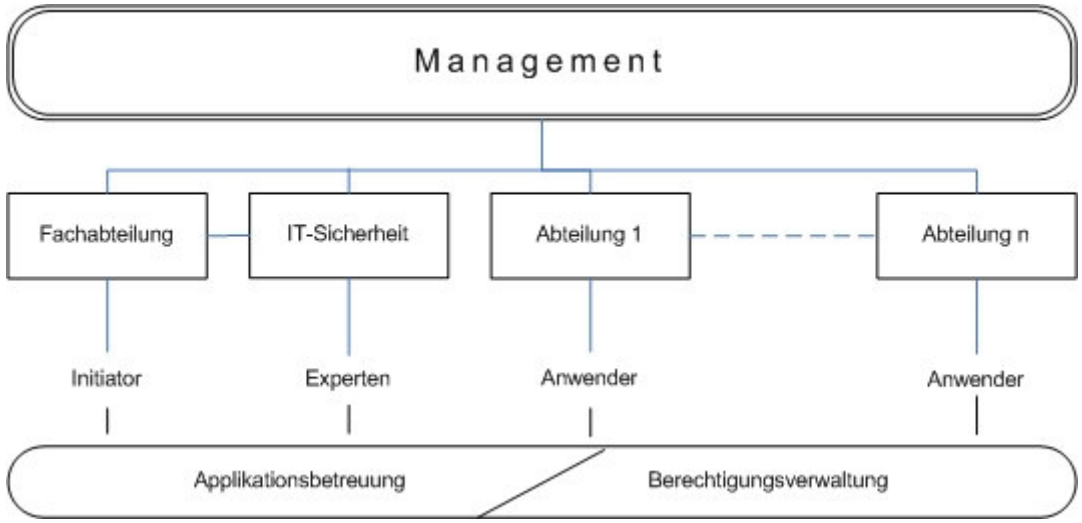

Abbildung 15: Unternehmensstruktur

Wie in Abbildung 15 dargestellt, ist die oberste und mächtigste Komponente das Management des Unternehmens, welchem die endgültige Entscheidung obliegt. Ein weiterer wichtiger Faktor ist der Besitzer der Informationen, also jene Person beziehungsweise Fachabteilung, welche diese Daten generiert oder sogar die gesamte Anwendung in dem Unternehmen etabliert hat. Sie hat aus fachlicher Sicht höchste Kompetenz, in welchen Bereichen des Unternehmens diese Daten auch von Nutzen sein könnten. Aus technischer Sicht steht weiters die IT-Sicherheit zur Verfügung. Dortige Experten verfügen über das nötige Fachwissen hinsichtlich Realisierbarkeit der Sicherheitsanforderungen. Zuletzt die Entscheidungsträger der weiteren Abteilungen des Unternehmens, welche letztendlich abteilungsintern festlegen, welche Personen für Berechtigungen genannt werden. In Abstimmung all diese beteiligten Unternehmensbereiche erfolgt die Bildung und Ausformulierung einer Sicherheitsrichtlinie.

Die Implementierung erfolgt durch die Applikationsbetreuer beziehungsweise Mitarbeiter der IT-Abteilung. Dabei müssen die Vorgaben der Sicherheitsrichtlinie mit den in der Anwendung zur Verfügung stehenden Mitteln der Berechtigungsverwaltung umgesetzt werden. Ebenso müssen die berechtigten Mitarbeiter informiert und unterwiesen werden.[26], [27]

2.6.3 Lebenszyklus

Ist eine Sicherheitsrichtlinie einmal in einem Unternehmen etabliert, unterliegt deren Einhaltung laufender Kontrolle und Überwachung, woraus regelmäßige Anpassungen resultieren.

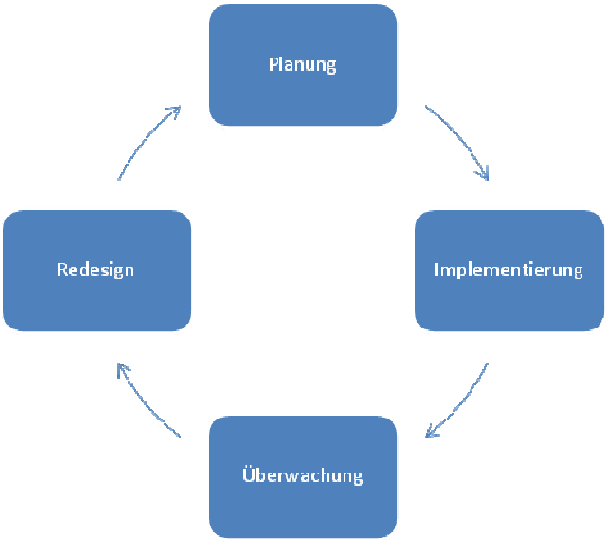

Abbildung 16: Lebenszyklus (PDCA-Modell) [28]

Das im BSI-Standard 100-1 [28] beschriebene PDCA-Modell (Plan, Do, Check, Act) findet sich auch im ISO/IEC 27001:2005 [2] wieder. Die initiale Planung und Implementierung bilden sozusagen die Grundlage dieses Kreislaufes. Eine Vielzahl unterschiedlicher Faktoren können im laufenden Betrieb eine Anpassung der Implementierung erfordern:

- Änderungen im Management
- Änderungen in der Unternehmensstruktur
- Änderungen des einzelnen Berechtigten
- Änderungen in der Anwendung
- Erkennung von Sicherheitsrisken
- Änderung der Sicherheitsanforderung

Vorgabe ist, dass zu jedem Zeitpunkt die in den Sicherheitsrichtlinien festgelegten Regeln der Zugriffskontrolle eingehalten werden.[29] Je nach Unternehmensgröße

obliegt diese Sicherheitsprüfung manchmal auch Mitarbeitern aus Fachabteilungen oder Sicherheitsbeauftragten, die nicht direkt mit der Anwendungsbetreuung beschäftigt sind. Daraus ergibt sich der Bedarf, auch technisch nicht versierten Mitarbeitern eine Möglichkeit zu bieten, aktuell vergebene Berechtigungen in einem System einzusehen.

Zusammenfassend sind die Sicherheitsrichtlinien (Information Security Policies) aus dem Bereich der elektronischen Datenverarbeitung aufgrund organisatorischer Gesichtspunkte gebildete Regeln, welche den Zugriff der Mitarbeiter auf unternehmensinterne Daten beschreiben. Basierend darauf geschieht die Auswahl eines im vorigen Unterkapitel beschriebenen Sicherheitsmodells beziehungsweise deren Konzepte der Multilateral und Multilevel Security. Die Umsetzung dessen erfolgt weiters in der Berechtigungsverwaltung des jeweiligen Systems. Technische Aspekte diesbezüglich wurden im Kapitel der Zugriffskontrollmechanismen abgehandelt. [30]

3 Systemumfeld

In diesem Kapitel folgt eine erste Betrachtung vier repräsentativer Systeme, in welchen die Berechtigungsanalyse durchgeführt wird. Dazu zählen die zwei bekanntesten Verzeichnisdienste, das Windows Active Directory (AD) und das Novell eDirectory gefolgt von der Geschäftsapplikationen SAP und das Langzeitarchivierungssystem EASY ARCHIVE von Easy Software. Nach einer kurzen, allgemeinen Systembeschreibung folgt eine Darstellung der jeweiligen Berechtigungsverwaltung aus praxisbezogener Sichtweise mit direktem Bezug auf Aspekte der vorangegangenen theoretischen Grundlagenanalyse. Weiters erfolgt eine Skizzierung der Information Security Policies, welche in den jeweiligen Systemen einzuhalten sind.
Zu allererst wird jedoch die Vorgehensweise beleuchtet, wie es in der Praxis eines Großunternehmens zur Entstehung und Erhaltung von Sicherheit kommt.

3.1 IT-Sicherheit

Information Security Policies (ISPs) im Unternehmen beschreiben formal, welche Personen oder Gruppen auf Daten im jeweiligen System zugreifen dürfen und in welcher Form dieser Zugriff gestattet ist. Die tatsächliche Zuordnung der Berechtigungen erfolgt auf Basis eines systemweit eindeutigen Benutzernamen und wird durch Abbildung der ISP in der systemeigenen Berechtigungsverwaltung umgesetzt (Abbildung 17).

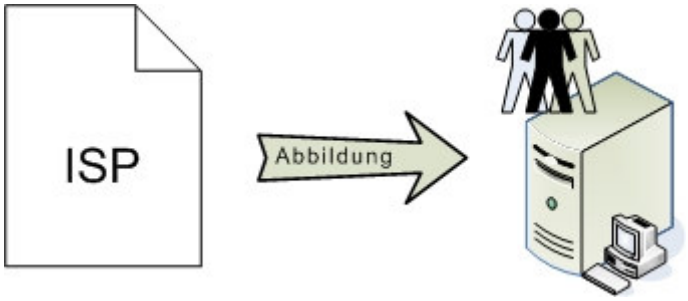

Abbildung 17: Umsetzung einer ISP

Voraussetzung für den Zugriff auf Ressourcen eines System ist die erfolgreiche Identifikation als in diesem System berechtigter Benutzer. [31], [32]

3.1.1 Authentifizierung

Der erste und für weitere Tätigkeiten unerlässliche Schritt der Identifikation geschieht bei der Anmeldung an einem Netzwerk-Client durch Eingabe von Benutzernamen und Passwort. Dadurch erfolgt simultan eine Authentifizierung sowohl an Microsofts Active Directory als auch an Novells eDirectory inklusive Übernahme der in diesen Systemen

zugeordneten Berechtigungen. Die in jedem weiteren System ebenfalls erforderliche Authentifizierung kann prinzipiell auf vier Arten erfolgen:

- In dem System ist die Eingabe eines von der Netzwerkanmeldung unabhängigen Benutzernamen und Passwort erforderlich. Die Berechtigungsverwaltung erfolgt vollkommen autark.
- Ein von der Zielanwendung unabhängiges System erkennt einen bevorstehenden Anmeldevorgang und befüllt automatisch Benutzername und Passwort in der Anmeldemaske des Zielsystems. Dieses Single Sign On (SSO) genannte System erfordert selbst auch eine einmalige Authentifizierung und muss mit Anmeldeinformationen der Zielsysteme erstbefüllt werden. Dies dient lediglich zur Steigerung des Komforts, die eigentliche Berechtigungsverwaltung erfolgt ebenso vollkommen autark.
- Die Zielanwendung prüft die Zugangsdaten mittels LDAP gegen einen der vorhandenen Verzeichnisdienste.
- Die Netzwerkanmeldung ist ausreichend. Die Authentifizierung im Zielsystem erfolgt durch Übernahme eines Kerberos-Tickets aus dem Netzwerk.

Die in den ersten beiden Punkten beschriebene Benutzer- und Berechtigungsverwaltung kommt vorwiegend in Klein- bis Kleinstanwendungen zum Einsatz. Vorteil dabei ist jedenfalls die völlige Unabhängigkeit vom Einsatzumfeld, da man nicht immer von der Existenz eines Zertifikatservers beziehungsweise eines zentralen Verzeichnisdienstes ausgehen kann. Nebenbei wird der Programmieraufwand auf ein Minimum reduziert.
Große Geschäftsanwendungen hingegen bieten meist neben deren interner proprietärer Berechtigungsverwaltung auch alternative Möglichkeiten, die sowohl Benutzern als auch Administratoren Erleichterungen bringen. So können zum Beispiel durch Einsatz einer Kerberos Authentifizierung die Anmeldeinformationen aus dem Netzwerk automatisch an die Anwendung weitergegeben werden, wodurch sich eine gesondert Anmeldung in der Zielanwendung erübrigt. Eine weitere Möglichkeit wäre, die Verwaltungsstrukturen der Berechtigungen innerhalb eines Systems in einem beliebigen Verzeichnisdienst abzubilden. Die Berechtigungsverwaltung erfolgt somit unter Zuhilfenahme der Benutzeroberfläche des jeweiligen Verzeichnisdienstes. Die Abfrage erfolgt über LDAP entweder mittels Synchronisation in die proprietäre Berechtigungsverwaltung der Anwendung oder im Ablauf direkt aus dem Verzeichnis.

3.1.2 Security Management

Neben der technischen Betrachtung ebenso wesentlich ist die formale Betrachtung, welche Mitarbeiter prinzipiell innerhalb einer Anwendung oder auf Daten berechtigt werden sollen. Zentraler Koordinator hierfür ist das Security Management. Ziel des Security Management ist es, den Einsatz von Ressourcen im Unternehmen so zu gestalten, dass sowohl Vorgaben der internen Sicherheitspolitik als auch gesetzliche Rahmenbedingungen wie zum Beispiel das Datenschutzgesetz eingehalten werden. Dieses Ziel kann nur erfüllt werden, wenn sich alle Mitarbeiter des Unternehmens den sicherheitsrelevanten Vorgaben entsprechend verhalten. Die Aufgabe des Security Management umfasst somit den kompletten Bereich der Feststellung von Sicherheitszielen bis hin zur Ausformulierung und Kontrolle von Sicherheitsmaßnahmen zur Erfüllung dieser Sicherheitsziele. Dieser Sicherheitsprozess umfasst im wesentlichen folgende Schritte:

- Bildung einer Sicherheitspolitik
- Identifikation von Rollen und Verantwortlichen
- Risikomanagement
- Einführung von Sicherheitsmaßnahmen
- Management von Sicherheitsmaßnahmen

Die aus Sicht der Berechtigungsverwaltung relevanten Teilbereiche des Sicherheitsprozesses werden in Folge näher beschrieben.[23], [33], [19], [34]

3.1.3 Sicherheitspolitik

Die IT-Sicherheitspolitik als oberste Ebene der Sicherheitspyramide (Abbildung 18) definiert Richtlinien und Vorgaben zur Sicherstellung eines hohen Sicherheitsniveaus für alle Teilbereiche des Unternehmens. Sie beschreiben globale Sicherheitsstrategien auf abstrakter Ebene und werden in Abstimmung zwischen dem Security Management und der Unternehmensführung festgelegt.
Auf Basis der von der Unternehmensführung abgesegneten Sicherheitspolitik werden konkrete IT-Sicherheitsrichtlinien und IT-Sicherheitskonzepte erstellt. Dadurch ergibt sich eine gewisse Handlungsfreiheit des Security Managements, da konkrete Sicherheitsvorgaben, sofern sie der Sicherheitspolitik entsprechen, ohne expliziter Genehmigung von der Unternehmensführung umgesetzt werden können.

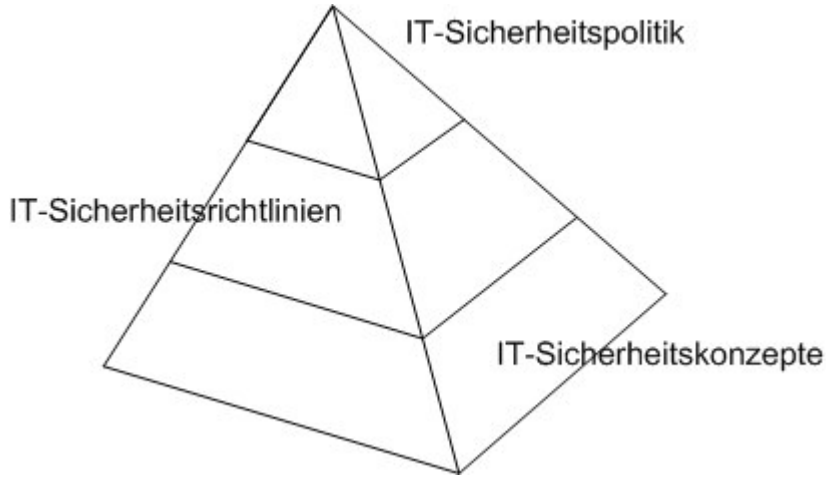

Abbildung 18: Sicherheitspyramide

Die Bildung der konkreten IT-Sicherheitsrichtlinien und IT-Sicherheitskonzepte erfolgt hingegen nicht mehr einzig vom Security Management sondern in Zusammenarbeit mit dem Security Forum. Wie in Abbildung 19 dargestellt ist dieses ein Gremium aus Personen der IT-Sicherheit, System Owner und gegebenenfalls Fachexperten zum Beispiel für die Berechtigungsverwaltung in speziellen Applikationen. [35], [1]

3.1.4 Rollen und Verantwortlichkeiten

Wesentlich bei der Bildung von Sicherheitsrichtlinien ist die Identifikation handelnder Mitarbeiter und Personen, da sie als Teilnehmer im Security Forum aktiv beteiligt sind. Aus Sicht der Berechtigungsverwaltung relevant sind insbesondere folgende zwei Akteure:

- Der System Owner oder fachliche Produktverantwortliche. Ihm obliegt die Gesamtverantwortung und somit auch die Verantwortung über die IT-Sicherheit einer Anwendung. Seine Aufgabe umfasst die Definition von Sicherheitsanforderungen, die Bildung und Einhaltung der Sicherheitsmaßnahmen, die Klassifikation der verarbeiteten Daten und die Vergabe von Benutzer- und Zugriffsrechten.
- Die Abteilungsleitung. Diese ist für Standardanwendungen und den Netzwerkzugriff innerhalb der jeweiligen Abteilung der System Owner. Für unternehmensumfassende Anwendungen obliegt der Abteilungsleitung die Verantwortung der Berechtigungsvergabe an explizite Mitarbeiter innerhalb der Abteilung.

3.1.5 Einführung von Sicherheitsmaßnahmen

Das Security Management in Zusammenarbeit mit dem Security Forum bilden nun konkrete IT-Sicherheitsrichtlinien und IT-Sicherheitskonzepte unter Berücksichtigung der unternehmensweiten Sicherheitspolitik.

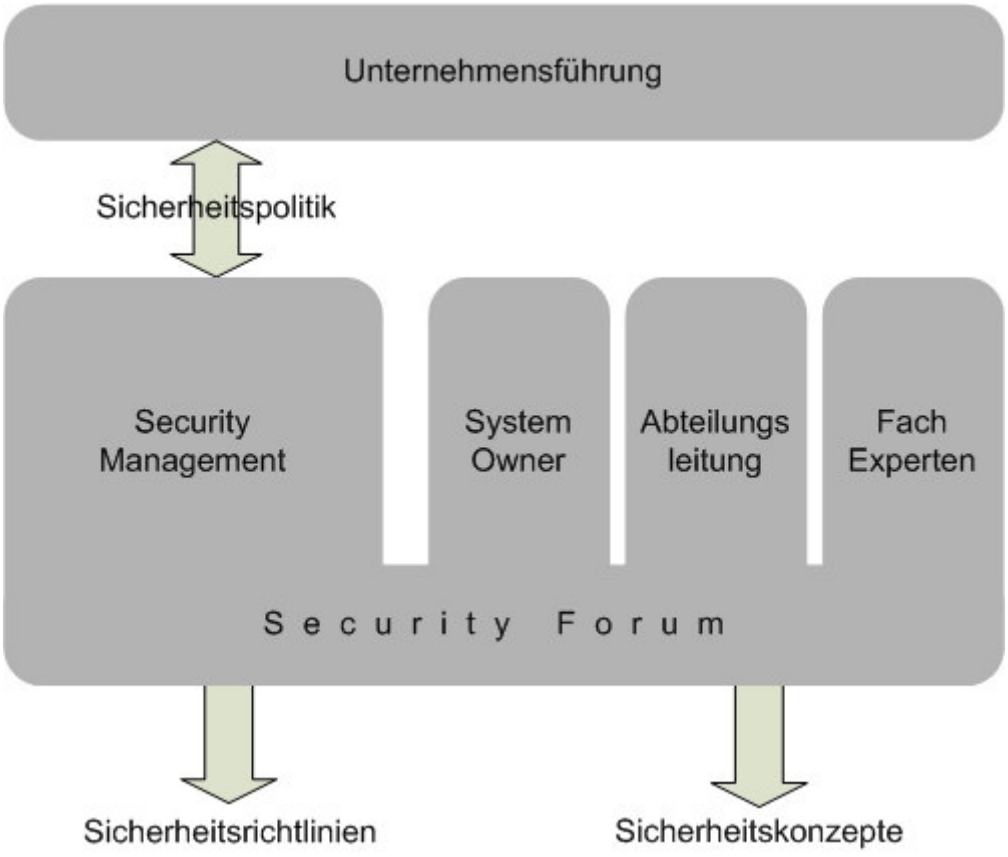

Abbildung 19: Entstehung von Sicherheitsmaßnahmen

Der System Owner trägt die alleinige Verantwortung. Er bewertet die Kritikalität einer Anwendung hinsichtlich folgender Faktoren:

- Vertraulichkeit: Wie vertraulich sind die in der Anwendung verarbeiteten Daten?
- Verfügbarkeit: In welchem Zeitraum muss das Gesamtsystem nach einem Totalausfall wieder funktionsfähig sein.
- Datenintegrität: Wie verlässlich sind die Daten?

Dieser Bewertungen bilden eine Entscheidungsgrundlage bei der Einführung einer Anwendung. Das Security Management beobachtet die Einhaltung der unternehmensweiten Sicherheitspolitik und eventuelle Fachexperten stehen beratend bei. Die

beschlossenen IT-Sicherheitsrichtlinien und IT-Sicherheitskonzepte werden in schriftlicher Form verfasst und an die Berechtigungsverwaltung beziehungsweise den Anwendungsbetreuer zur Umsetzung übergeben. [2], [36]

3.1.6 Management von Sicherheitsmaßnahmen

Eine IT-Sicherheitsmaßnahme ist nie ein statisches Dokument. Auch personelle Änderungen innerhalb des Unternehmens erfordern laufend Eingriffe in die Berechtigungsverwaltung und somit in den Wirkungsbereich der IT-Sicherheitsrichtlinien und IT-Sicherheitskonzepte. Falsch vergebene Berechtigungen können unter Umständen durch Protokollierung und regelmäßiger Auswertungen sicherheitsrelevanter Ereignisse identifiziert werden. Dabei ist ebenso wie bei einem erfolgreichen Angriff (Incident) schon ein unberechtigter Zugriff erfolgt. Auch liefern Protokollierungen in der Praxis umfangreiche Informationen, deren Auswertungen sich sehr schwierig gestalten.
Aus Sicht der Sicherheitspolitik sind regelmäßige Überprüfungen der IT-Sicherheitsmaßnahmen vorgesehen. Dabei ist die Einhaltung aller IT-Sicherheitsrichtlinien und IT-Sicherheitskonzepte auf Vollständigkeit und Korrektheit zu prüfen. Verantwortlich für diese Prüfungen ist der jeweilige System Owner, also der fachliche Produktverantwortliche beziehungsweise der Abteilungsleiter. Die Ergebnisse sind dem Security Forum mitzuteilen, wo etwaige Konsequenzen auf Sicherheitsmaßnahmen zu prüfen sind.
Genau an dieser Stelle im Sicherheitsprozess entspringt der Bedarf an der in dieser Arbeit beschriebenen Anwendung. Dem jeweiligen System Owner soll eine möglichst komfortable Möglichkeit geboten werden, aktuell vergebene Berechtigungen jederzeit abfragen und prüfen zu können. Diesbezüglich erfolgt anschließend eine Analyse relevanter Systeme, deren Berechtigungsverwaltung und Zugriffsmöglichkeiten auf die Berechtigungsinformationen.

3.2 Windows Active Directory

Das Active Directory ist der umfangreiche Verzeichnisdienst von Microsoft. Es bietet eine zentrale Verwaltung aller im Netzwerk befindlichen Ressourcen und ist weiters für die Authentifizierung des Benutzers am Computer beziehungsweise im Netzwerk mitverantwortlich. Durch Eingabe eines im Active Directory angelegten Benutzernamen in Kombination mit einem gültigen Passwort wird der Mitarbeiter eindeutig identifiziert und erhält Zugriff auf mittels Active Directory verwaltete Ressourcen. Als Zugriffskontrolle auf Betriebssystemebene sind primär alle benutzerbezogenen Informationen von Interesse. Als verwaltete Ressource werden vergebene Berechtigungen auf Datenserver analysiert.

3.2.1 Berechtigungsverwaltung

Wie schon der Name sagt, repräsentiert das Active Directory eine hierarchische Baumstruktur und ist Bestandteil von Microsofts Serverbetriebssystem. Als Verwaltungsoberfläche dient Microsofts Management Console, seit Windows 2000 in allen Windows Versionen enthalten. Mit Hilfe dieses universellen Verwaltungstools können je nach gestarteten Snap-In´s diverse administrative Tätigkeiten durchgeführt werden, demnach auch die Verwaltung aller Objekte in einem Active Directory. Die Ansicht der einzelnen Objekte in dieser hierarchischen Struktur ähnelt der des Windows Explorers.

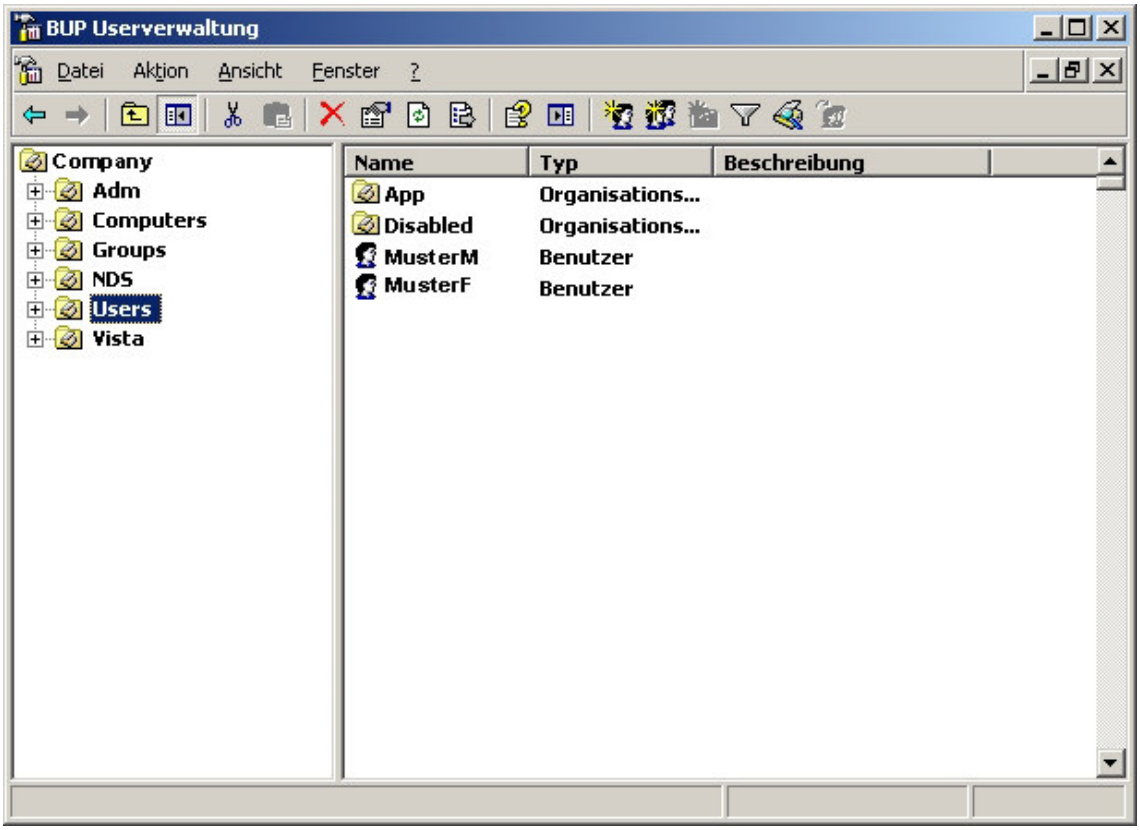

Abbildung 20: Active Directory

Abbildung 20 zeigt eine mögliche Baumstruktur, wie sie zur Verwaltung von Personen und Ressourcen in einem Netzwerk Anwendung findet. Im Fallbeispiel erfolgt zwar die primäre Benutzerverwaltung im eDirectory anhand der von Novell zur Verfügung gestellten Werkzeuge. Der Zugriff auf unter Windows verwaltete Ressourcen erfordert jedoch auch eine Authentifizierung im Active Directory, weshalb mit Hilfe einer automatischen Synchronisation ein Abgleich der Benutzerdaten erfolgt.

Die Zuteilung der Berechtigungen erfolgt primär auf Gruppen, weshalb neben Abteilungsgruppen eine Vielzahl an weiterer Gruppen für Projekte oder organisatorische Funktionen verwaltet werden. Der Hauptvorteil besteht darin, dass ein weiterer Mitarbeiter allein durch Mitgliedschaft in einer Gruppe alle erforderlichen Berechtigungen an diversen Ressourcen erhält.[37], [9]
Sämtliche Objekte, die im Dateisystem berechtigt werden, sind demnach mit Hilfe eines Verzeichnisdienstes verwaltet. Die effektive Zuordnung der Berechtigungen auf Objekte im Dateisystem erfolgt nun direkt am Berechtigungsobjekt, also auf das Verzeichnis oder auf die Datei am Datenserver. Durch einen Rechtsklick auf eine Datei oder ein Verzeichnis im Windows Explorer und Auswahl von „Eigenschaften – Sicherheit“ erhält man folgendes Fenster:

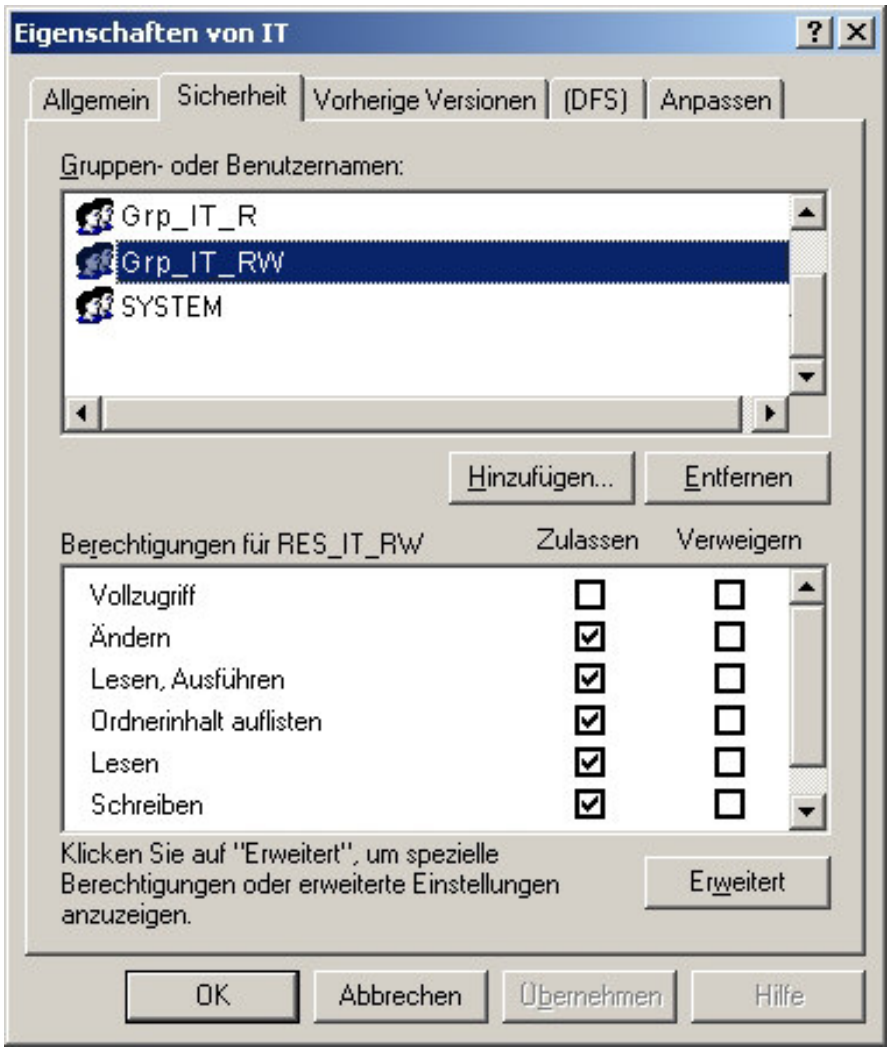

Abbildung 21: Berechtigungen an einem Verzeichnis

Im oberen Bereich des in Abbildung 21 dargestellten Dialogfensters sind alle berechtigten Benutzer und Gruppen angeführt. Nach Auswahl eines beliebigen Benutzers oder einer Gruppe werden im unteren Bereich die festgelegten Berechtigungen angeführt. Mittels der Schaltfläche „Hinzufügen“ beziehungsweise „Entfernen“ können nun die im Active Directory verwalteten Benutzer und Gruppen auf das jeweilige Objekt berechtigt werden, wobei die Art der Berechtigung im unteren Bereich definiert werden kann. Mittels der Schaltfläche „Erweitert“ können im folgenden Fenster noch nähere Details der Berechtigung festgelegt werden. Eine im Betrieb hilfreiche Funktion findet sich auf der Registerkarte „Effektive Berechtigungen“.

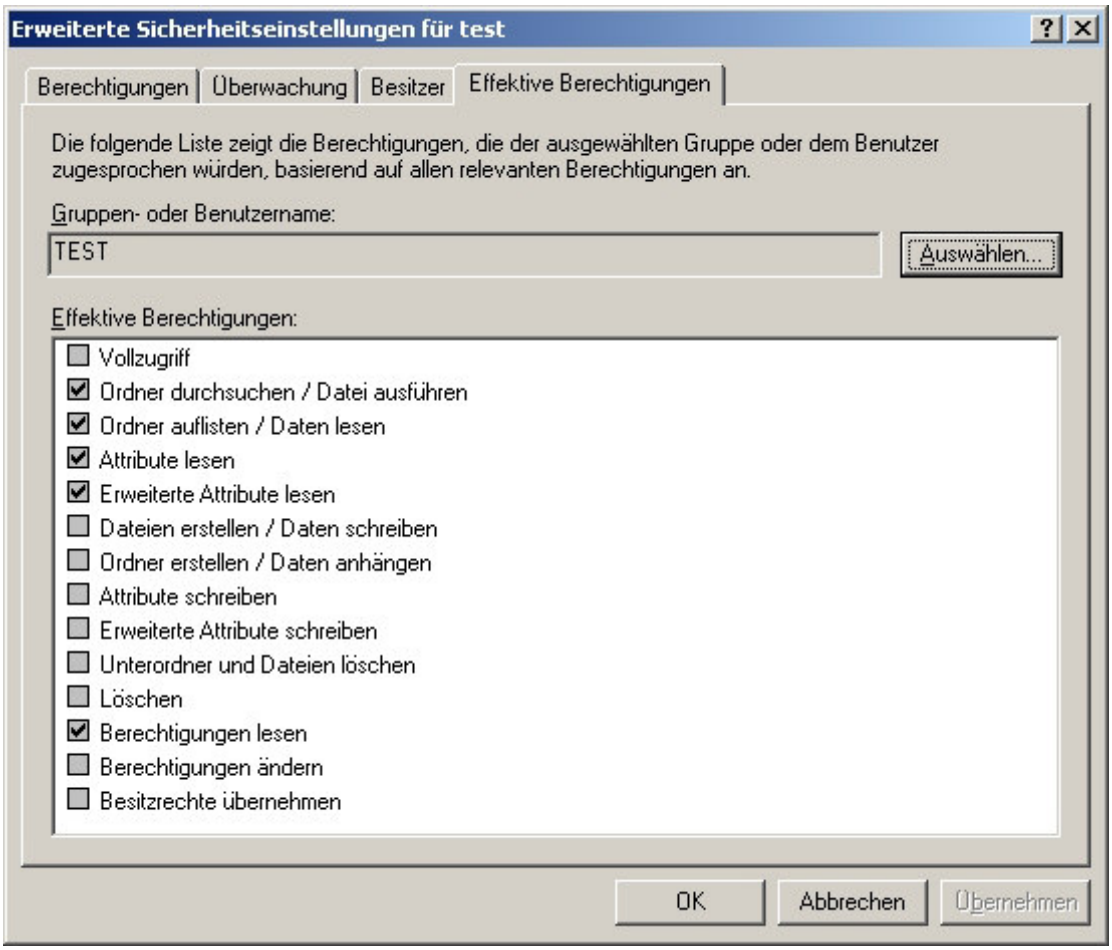

Abbildung 22: Erweiterte Sicherheitseinstellungen

Die Rechtevergabe erfolgt auf Gruppen, welche im Active Directory administriert werden. Um schnell zu überprüfen, ob sich eine bestimmte Person auch in der berechtigten Gruppe befindet, können in dem in Abbildung 22 dargestellten Fenster personenbezogen die effektiven Berechtigungen angezeigt werden. [38]

3.2.2 Information Security Policy

Die in diesem System verwalteten Daten sind Dateien auf Windows Servern. Aufgrund der großen Anzahl einzelner Berechtigungsobjekte wurde der Weg der „Data Ownership“ gewählt, was bedeutet, dass Änderungen der Berechtigungen einzig vom Eigentümer der Daten angefordert werden können. Dies muss in elektronischer Form erfolgen und wird aus Gründen der Nachvollziehbarkeit dokumentiert. Prinzipiell existieren folgende Arten von Datenbereiche:

- Home-Laufwerk: Jeder Mitarbeiter ist im Besitz eines eigenen Datenbereiches, auf den nur der jeweilige Mitarbeiter selbst Zugriff besitzt und somit Eigentümer dieser Daten ist. Aus organisatorischen Gründen werden an dieser Berechtigungsstruktur keine Änderungen durchgeführt.
- Gruppen-Laufwerk: Jede Abteilung verfügt über einen Bereich an Daten, Eigentümer ist die jeweilige Abteilungsleitung. Prinzipiell ist es möglich und in größeren Abteilungen oftmals erforderlich, das Abteilungslaufwerk in kleinere Bereiche mit unterschiedlichen Berechtigungen zu unterteilen. Die Zuordnung erfolgt wie beschrieben über eine eigene Gruppe, über welche sogar abteilungsfremde Mitarbeiter berechtigt werden dürfen. Technische Vorgabe ist, dass der Ort der Berechtigungsvergabe maximal in der zweiten Unterebene der Verzeichnisstruktur erfolgen darf.
- Projekt-Laufwerke: Eigentümer ist der Leiter des Projektes. Alle Änderungen erfolgen auf Anforderung mit Genehmigung des Projektleiters.

3.2.3 Berechtigungsauswertung

Die benutzerbezogenen Informationen werden mit Hilfe eines Scripts direkt über LDAP aus dem Verzeichnis ausgelesen. Die Zugriffsrechte am Datenserver sind direkt bei dem Objekt gespeichert. Es handelt sich dabei eindeutig um eine Access Control List (ACL). Microsoft bietet auch ein Tool zum Modifizieren und Auslesen der Berechtigungen für die Verwendung in der Kommandozeile an, Change Access Control List (CACLS.exe) Der Aufruf erfolgt mit Übergaben des Pfades des zu analysierenden Objektes als ersten Parameter. Der weitere Parameter „/T“ bewirkt ein rekursives Durchsuchen eines Teilbaumes und liefert alle gesetzten Berechtigungen aller im Teilbaum erhaltenen Dateien und Ordner. Der Output kann in eine Datei geschrieben und zur weiteren Analyse gespeichert werden. So liefert zum Beispiel die Abfrage der gesetzten Berechtigungen auf ein Gruppenlaufwerk namens IT folgende in Abbildung 23 dargestellte Informationen:

```
C:\>cacls G:\IT
G:\IT DOMAIN\GRP_IT_RW:(OI)(CI)C
      DOMAIN \GRP_IT_R:(Beschränkter Zugriff:)
                       READ_CONTROL
                       SYNCHRONIZE
                       FILE_GENERIC_READ
                       FILE_READ_DATA
                       FILE_READ_EA
                       FILE_READ_ATTRIBUTES
      VORDEFINIERT\Administratoren:(OI)(CI)F
      NT-AUTORITÄT\Authentifizierte Benutzer:(OI)(CI)(Beschränkter Zugriff:)
                                                    SYNCHRONIZE
                                                    FILE_EXECUTE
      DOMAIN \Admin:(OI)(CI)F
      NT-AUTORITÄT\SYSTEM:(OI)(CI)F
```

Abbildung 23: Auswertung von Dateiberechtigungen

Neben vordefinierten Systemgruppen und Benutzern, die unter anderem Datensicherungen durchführen, sind auf dieses Verzeichnis zwei Gruppen aus der Verwaltung im Active Directory explizit berechtigt, „DOMAIN\GRP_IT_RW“ und „DOMAIN\GRP_IT_R“.

Die ausgegebene Berechtigung kann folgende Bedeutung besitzen:

n	none – nicht berechtigt
r	read – Leseberechtigung
w	write – Schreibberechtigung
c	change – Berechtigungen ändern und read ,write
f	full – Vollzugriff
	…und spezielle Berechtigungen („FILE_READ_ATTRIBUTES“,…)

Die Gültigkeit des Access Control Entrie (ACE) bezieht sich auf:

OI	dieses Verzeichnis inklusive beinhalteter Dateien
CI	dieses Verzeichnis und Unterverzeichnisse
IO	nicht auf dieses Verzeichnis oder diese Dateien
-	nur dieses Verzeichnis
	…und beliebige Kombinationen obiger

Die Gruppe „DOMAIN\GRP_IT_RW“ besitzt demnach lesenden und schreibenden Zugriff auf das aktuelle Verzeichnis inklusive beinhalteter Dateien und vererbt diese Berechtigung auf alle Unterordner weiter. Die Gruppe „DOMAIN\GRP_IT_R“ hat spezielle Leseberechtigung explizit auf dieses Verzeichnis. Alle Mitarbeiter, die tiefer in der Verzeichnisstruktur berechtigt werden, müssen Mitglied dieser Gruppe sein, da

sie andernfalls zwar berechtigt sind aber für sie die Verzeichnisstruktur im Explorer nicht sichtbar ist. [39], [40]

3.3 Novell eDirectory

Das Novell eDirectory ist die Weiterentwicklung des Novell Directory Systems und ist sozusagen die Entsprechung des Active Directory. Es ist somit ebenfalls ein Verzeichnisdienst mit hierarchischer Baumstruktur. Die Authentifizierung im eDirectory erfolgt simultan zur Anmeldung im Active Directory bei der Anmeldung im Netzwerk. Als zweites Netzwerkbetriebssystem sind ebenso wie beim Active Directory alle personenbezogenen Informationen relevant.
Weiters werden im eDirectory Berechtigungen des NetWare Application Launcher (NAL) verwaltet. Novell bietet in diesem Instrument die Möglichkeit, Softwareinstallationen zentral zu verwalten und dem Mitarbeiter zur selbstständigen Installation am Client im Bedarfsfall anzubieten. Das Berechtigungsobjekt ist in diesem Fall das NAL-Objekt, welches die Installation eines Programms am Clientrechner durchführt. Aus technischer Sicht erstellt ein Administrator einen Snapshot einer sauberen Installation und importiert diese in die Verwaltung.
Ein kleines Clientprogramm prüft nach erfolgter Anmeldung, welche optionalen Installationen dem jeweiligen Benutzer angeboten werden. Die Zuweisung an Mitarbeiter erfolgt durch Mitgliedschaft in einer entsprechenden Benutzergruppe.

3.3.1 Berechtigungsverwaltung

Novell bietet als Werkzeug zur Verwaltung die ConsoleOne als eigenständiges Programm beziehungsweise in Form einer Weboberfläche. Für die Erstellung eines NAL-Objektes wird ein spezielles SnapIn benötigt. Die Berechtigungsverwaltung erfolgt durch Mitgliedschaft einer definierten Gruppe, welche in einem speziellen Container in der Berechtigungsstruktur gesammelt werden. Abbildung 24 zeigt ein Dialogfenster der ConsoleOne, in dem die Verwaltung der berechtigten Benutzer erfolgt.

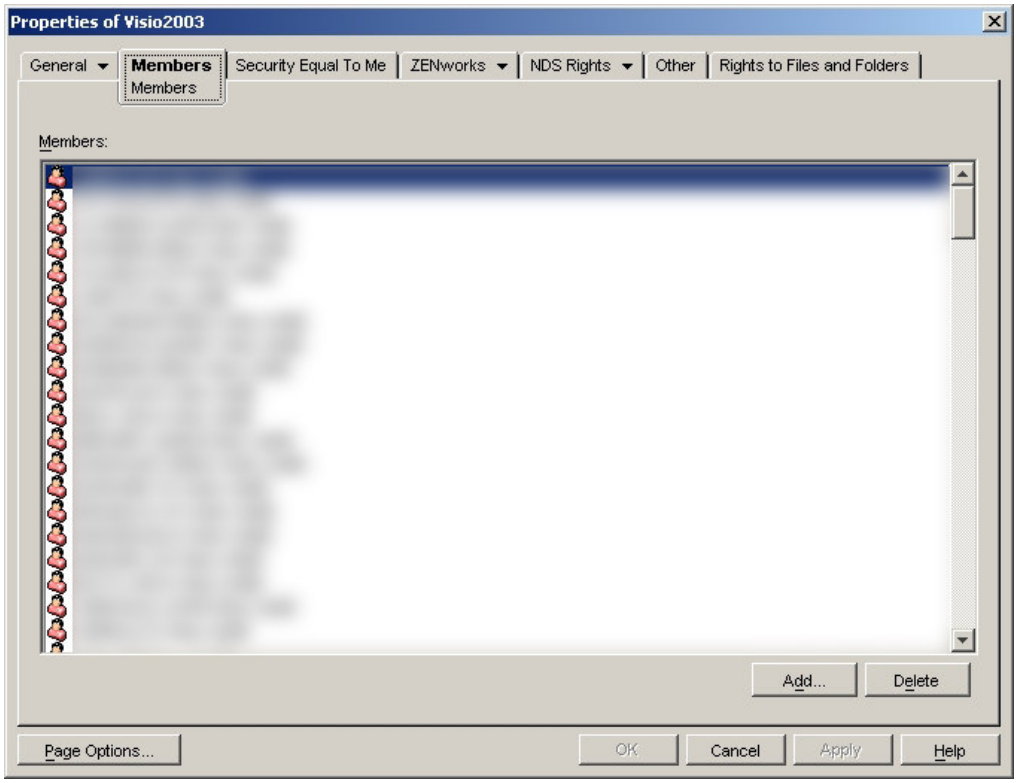

Abbildung 24: Mitgliedschaften einer NAL-Gruppe

Mit der Schaltfläche „Add“ können im Verzeichnis existierende Benutzer als Mitglieder in dieser Gruppe festgelegt werden. Die Verwaltung erfolgt ausnahmslos innerhalb eines Verzeichnisdienstes.[41]

3.3.2 Information Security Policy

Das System dient eigentlich als Hilfsmittel der IT-Abteilung und obliegt voll in deren Verantwortung. Alle erwünschten Berechtigungen können per elektronischer Anforderung beantragt werden. Die IT-Abteilung prüft eventuelle technische Voraussetzungen und vergibt mittels Mitgliedschaft in der entsprechenden Benutzergruppe die gewünschte Berechtigung. Der Mitarbeiter kann durch Aufruf des NAL-Objektes die gewünschte Installation am Client selbstständig starten. Nach erfolgreicher Installation verschwindet das NAL-Objekt vom Desktop des Mitarbeiters.
Ein Spezialfall sind lizenzpflichtige Programme. Da Programme, die mittels NAL-Objekt verteilt werden nicht zur Standardausstattung eines unternehmenstypischen Clients gehören, muss die Abteilungsleitung einer Kostenübernahme zustimmen. Die Verwaltung und gegebenenfalls der Nachkauf verbrauchter Lizenzen wird von der IT-Abteilung durchgeführt. Um die Weiterverrechnung der Lizenzkosten an die jeweilige Fachabteilung belegen zu können, sollen vergebene Berechtigungen in die Analyse aufgenommen werden.

3.3.3 Berechtigungsauswertung

Alle relevanten Berechtigungsinformationen befinden sich in einem Verzeichnisdienst, auf dem über LDAP zugegriffen werden kann. Somit können mit jeder beliebigen Programmiersprache, welche LDAP-Abfragen unterstützt, die Berechtigungen direkt aus dem Verzeichnis abgefragt werden und in eine valide XML-Datei geschrieben werden. [8]

3.4 Easy Archive

Das deutsche Unternehmen EASY SOFTWARE AG erstellt und vertreibt unterschiedliche Softwarelösungen im Bereich Dokumentenmanagement (DMS) und Archivierung. Je nach Umfang der Implementierung und der jeweiligen Importschnittstellen können gescannte Belege ebenso wie Emails, Office Dokumente aber auch Daten aus Enterprise Ressource Planning Systemen (ERP) wie zum Beispiel SAP an das EASY ENTERPRISE DMS übergeben werden (Abbildung 25). Innerhalb des Systems bestehen umfassende Möglichkeiten, Geschäftsprozesse in Form von Workflows abzubilden um Durchlaufzeiten zu optimieren. Unabhängig davon bietet die Komponente EASY ARCHIVE ein elektronisches Archivsystem zur komfortablen und revisionssicheren Ablage von Dokumenten aller Art.

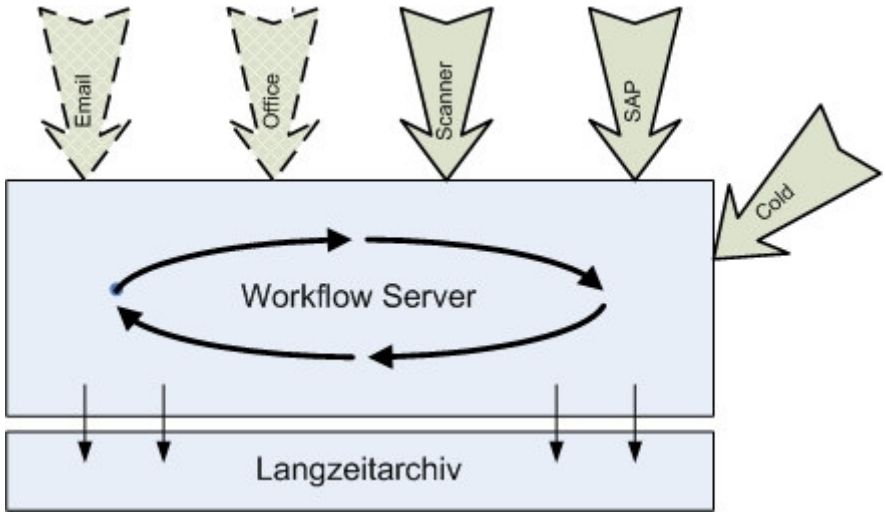

Abbildung 25: EASY Komponenten

Das implementierte System, an dem die Berechtigungsanalyse durchgeführt wurde, verwendet von den vordefinierten Importschnittstellen lediglich jene zu SAP und zu Dokumentscanner. Darüber hinaus wurde eine zusätzliche Schnittstelle zum Import beliebiger Datenfiles erstellt („Cold“). Verwendungszweck ist primär die Nutzung als

Langzeitarchiv, zur Abbildung von Workflows für Akten ist ein gesondertes System im Einsatz.

3.4.1 Berechtigungsverwaltung

Die Software wurde erst vor kurzem einem Update unterzogen, wobei sich wesentliche Teile im Konzept der Berechtigungsverwaltung geändert haben.

Version Alt:
Die Benutzerverwaltung der Zugriffskontrolle erfolgt ausschließlich systemintern. Mit Hilfe des optionalen Zusatzprogramms EASY Single Sign On (SSO) werden die Anmeldedaten automatisch an das System übergeben. Anhand des angemeldeten Benutzers erfolgt eine Zuteilung in ein oder mehrere Gruppen innerhalb des Systems.

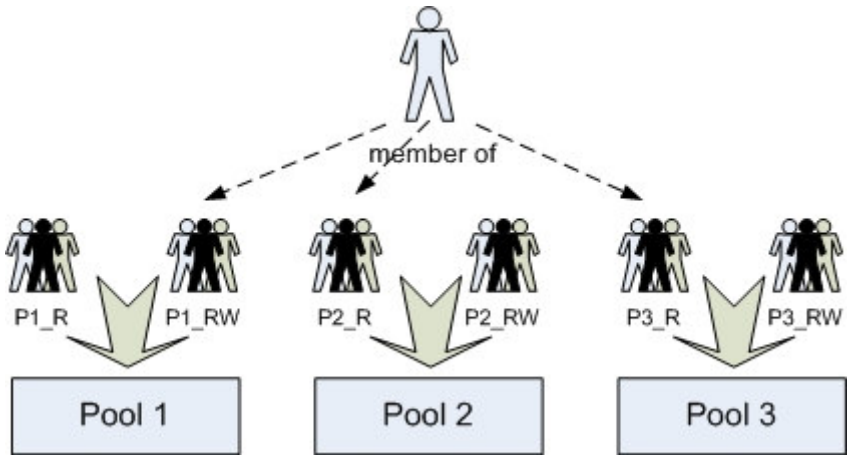

Abbildung 26: EASY Archive Alt

Wie in Abbildung 26 dargestellt, ist das Gesamtarchiv nach organisatorischen Aspekten in unterschiedliche, von einander getrennte Datenpools unterteilt. Jedem Datenpool ist eine Benutzergruppe mit Lese- und eine Gruppe mit Lese- und Schreibberechtigung zugeordnet. Nach erfolgter Anmeldung erfolgt eine Überprüfung der jeweiligen Gruppenmitgliedschaft und die Zuordnung der jeweiligen Berechtigungen auf den entsprechenden Datenpool.
Personen, welche Daten in das Archiv ablegen sollen, müssen der Gruppe mit Lese- und Schreibberechtigung zugeordnet sein. Im obigen Beispiel darf der angemeldete Benutzer in das Datenpool 1 archivieren und in den beiden anderen Pools recherchieren. Unabhängig davon existieren noch spezielle Benutzerkonten zur Administration beziehungsweise Rechtezuteilung.
Aus technischer Sicht entspricht die Berechtigungsverwaltung der einer Berechtigungsmatrix unter Verwendung von Gruppen. Durch die Trennung in

eigenständige, geschützte Datenpools ist ein multilaterales Sicherheitsmodell vorherrschend.

Version Neu

Erster Schritt ist ebenfalls eine Authentifizierung im System. Verfügt der bei Programmaufruf am Client angemeldete Benutzer über Berechtigungen im System, so erfolgt über LDAP eine automatische Kontrolle des Passwortes. Andernfalls erscheint eine Anmeldemaske zur manuellen Eingabe von Benutzername und Passwort. Die detaillierte Zuordnung effektiver Berechtigungen ist im Vergleich zur Vorgängerversion um einiges flexibler aber auch komplexer.

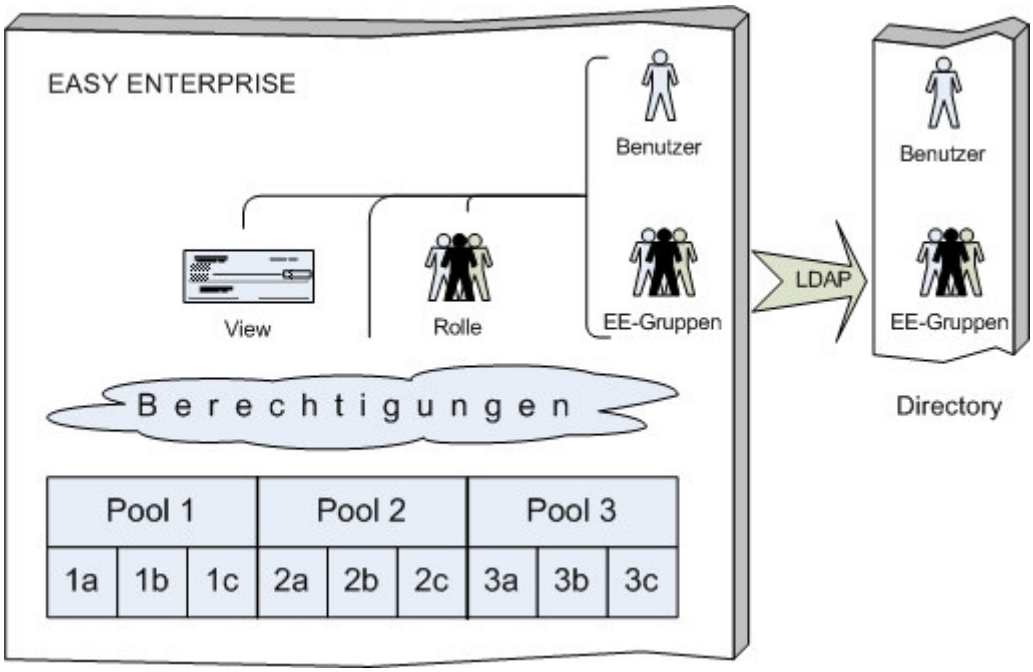

Abbildung 27: EASY Archive Neu

Abgesehen von Benutzern mit besonderen Berechtigungen (Administratoren,…) erfolgt die Berechtigungszuordnung primär durch Mitgliedschaft des Benutzers (oder einer vollständigen Organisationseinheit) in einer oder mehreren Gruppen. Aufgrund der technischen Möglichkeit der neuen Version, mittels LDAP Abfragen durchführen zu können, erfolgt die Verwaltung von Gruppen und deren Mitglieder im zentralen Verzeichnisdienst (Abbildung 27).

In der internen Berechtigungsverwaltung erfolgt unabhängig davon eine Verwaltung einzelner Rollen und die Zuordnung effektiver Berechtigungen auf Teile des Datenpools an die jeweiligen Rollen. Die Verwaltung der Rollen selbst erfolgt in einer hierarchischen Baumstruktur mit unterschiedlichen Arten der Vererbung. Erste wesentliche Unterscheidung ist nach der Art der Berechtigung der Rolle:

- Verweigerung einer Aktivität
- vererbbare Genehmigung einer Aktivität
- nicht vererbbare Genehmigung einer Aktivität

Je nach Art der Beziehung zwischen zwei Rollen ergeben sich folgende mögliche Szenarien der Vererbung von Berechtigungen:

- deny: übergeordnete Rolle vererbt Verweigerung nach unten
- allow: vererbbare Genehmigungen werden an untergeordnete Rolle übergeben
- allow: nicht vererbbare Genehmigungen werden an übergeordnete Rolle übergeben

Dadurch kann die Richtung des Rechteflusses unter Rollen beliebig zwischen „top-down“ und „bottom-up“ angepasst werden.
Die eigentliche Zuordnung von Berechtigungen an den einzelnen Benutzer erfolgt durch Zuordnung von Rollen aus der Baumstruktur an Gruppen, denen der Benutzer angehört. Definierbare Views sind ein weiteres Werkzeug, um Einschränkungen der Sichtbarkeit durchzuführen. Mittels sogenannter Content Related Permissions können sogar vom Inhalt einzelner Felder abhängig Einschränkungen festgelegt werden. Aus administrativer Sicht ist jedoch die Beschränkung anhand von Berechtigungen vorzuziehen. [42], [43]

3.4.2 Information Security Policy

Die Festlegung der Berechtigungsstruktur erfolgt nach Rücksprache mit den jeweiligen Fachabteilungen. So können in manchen Abteilungen alle Mitarbeiter auf alle Daten im abteilungseigenen Datenpool zugreifen. Für andere Abteilungen gelten unterschiedliche Vorgaben. Änderungen der Berechtigungsstruktur erfolgen auf elektronische Anforderungen der jeweiligen Abteilungsleitung.

3.4.3 Berechtigungsauswertung

In der bei der Entwicklung des Analysewerkzeuges aktuellen alten Version mit der proprietären Berechtigungsverwaltung von Benutzer und Gruppen war keinerlei Möglichkeit vorgesehen, Berechtigungsdaten zu exportieren. Die Firma EASY

SOFTWARE implementierte erst nach Auftrag im Zuge dieses Projektes eine Exportschnittstelle gemäß den aus dem Projekt resultierenden Vorgaben.
Für die neue Version erfolgt eine Auswertung der im Verzeichnisdienst verwalteten Teilbereiche der Berechtigungen über LDAP, wobei möglichst eine 1:1 Zuordnung der Gruppen aus dem Verzeichnisdienst an Rollen innerhalb des Systems angestrebt wurde.

3.5 SAP

SAP ERP, vormals SAP R/3, ist ein unternehmensweites Informationssystem, mit dessen Hilfe Daten aller geschäftsrelevanten Teilbereiche eines Unternehmens in Zusammenhang gebracht werden können. Der modulare Aufbau dieser Gesamtlösung entspricht meist der üblichen Unternehmensstruktur. Einzelne Module können zwar unabhängig voneinander eingesetzt werden, aufgrund der hohen funktionalen Abhängigkeit der einzelnen Teilbereiche eines Unternehmens existiert sehr wohl aus informationstechnischer Sicht eine Abhängigkeit der Module untereinander.
Für die Berechtigungsanalyse betrachtete Teilbereiche sind nach alter Notation SAP R/3, BW (Business Warehouse), EC (E-Procurement), HR (Human Ressources) und DW, ein branchenspezifisches Modul. [44]

3.5.1 Berechtigungsverwaltung

Voraussetzung für einen Zugriff auf Systemdaten ist eine Authentifizierung. Dies erfolgt durch Eingabe eines Benutzernamens und einem Passwort und der Auswahl des erwünschten Zielsystems innerhalb SAP. Ohne Single Sign On (SSO) Lösung von Drittherstellern sind diese Eingaben bei jeder Anmeldung manuell durchzuführen. Die Haltung berechtigter Benutzer erfolgt im sogenannten Benutzerstamm. Die Zuordnung von Berechtigungen an die jeweiligen Benutzer erfolgt in Form eines sogenannten Berechtigungsprofils. Eine Gesamtübersicht, wie Berechtigungen in SAP festgelegt werden können, ist in Abbildung 28 dargestellt.

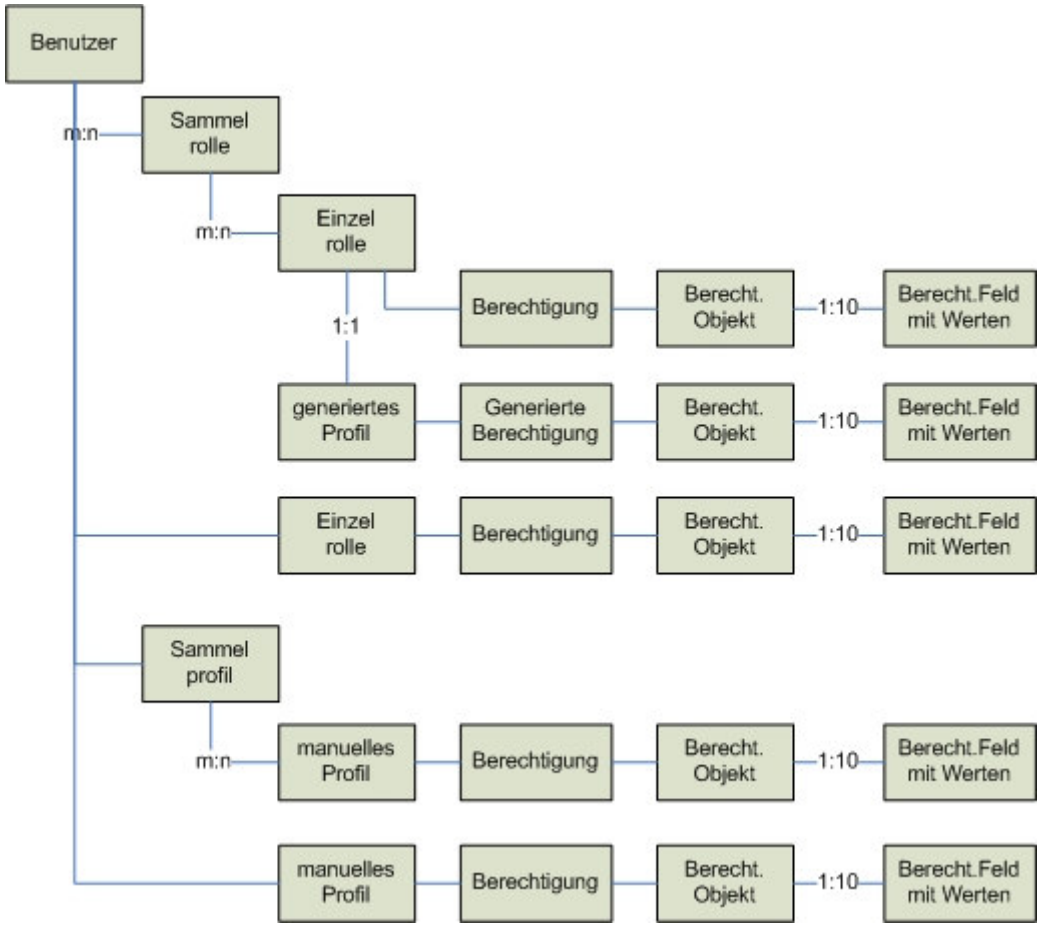

Abbildung 28: SAP-Berechtigungskonzept im Überblick nach [45]

Berechtigungsobjekte können mit Vorbedingungen verknüpft sein und ermöglichen die Kontrolle, eine Aktivität durchzuführen. Eine Berechtigung ist die Ausprägung eines Berechtigungsobjektes, an der die Aktivität praktisch durchgeführt werden kann. Die eigentliche Berechtigungszuordnung an einzelne Benutzer erfolgt über Rollen oder Profile. Dabei unterscheidet man:

- Einzelrolle als einfachste Form einer Berechtigung.
- Berechtigungsprofil, mit dem Profilgenerator aus einer Einzelrolle generiert und um benutzerspezifische Einstellungen erweiterbar, entspricht der technischen Abbildung einer Rolle.
- Sammelrolle oder Sammelprofil als Zusammenfassung einzelner Rollen oder Profile.

Die Verwendung des Profilgenerators ermöglicht eine Delegierung administrativer Tätigkeiten auf Berechtigungen, Berechtigungsprofile und Benutzerstammdaten. Rollen

und Profile können beliebig verschachtelt werden und repräsentieren eine hierarchische Baumstruktur. Die Haltung der Benutzerdaten erfolgt in einer Datenbanktabelle. [46], [47]

3.5.2 Information Security Policy

Aufgrund der hohen Anzahl an Berechtigungsobjekten und Aktivitäten innerhalb des Systems ist es nahezu unmöglich, eine zentrale Berechtigungsverwaltung durchzuführen. Lediglich tiefgreifende, strukturelle Eingriffe werden nach elektronischer Anforderung von einem zentralen Systembetreuer durchgeführt. Die feinere Berechtigungsvergabe erfolgt gemäß dem auch von SAP präferierten „Brückenkopf-Prinzip“. Dabei werden in allen Abteilungen und organisatorischen Einheiten einzelne Personen speziell technisch geschult. Diese Brückenköpfe verfügen zusätzlich in ihrem Tätigkeitsbereich über einen guten Überblick über den Bedarf erforderlicher Berechtigungen und übernehmen Verantwortung und Durchführung der dezentralen Berechtigungsverwaltung.

3.5.3 Berechtigungsauswertung

Der Export von innerhalb SAP festgelegten Berechtigungen erzeugt eine CSV-Datei mit einer umfangreichen Auflistung aller Benutzer und deren zugeordneter Rollen beziehungsweise Profile. [45]

4 Systemübergreifende Repräsentation

Wie sich gezeigt hat, zeichnet sich jede der betrachteten Berechtigungsverwaltungen sowohl aus praktischer Sichtweise als auch anhand theoretischer Aspekte durch spezifische Eigenheiten aus. Dennoch ist ein Datenmodell zu entwickeln, mit dessen Hilfe sich die relevanten Berechtigungsinformationen aller betrachteten Systeme abbilden lassen.
Als strategische Vorgehensweise werden die unterschiedlichen Berechtigungsverwaltungen auf Gemeinsamkeiten untersucht.

4.1 Bestandteile des Modells

Bei analytischer Betrachtung der jeweiligen Systeme lassen sich folgende übergreifende Gemeinsamkeiten feststellen:

4.1.1 Benutzer

In jedem System existierend sind Benutzer. Sie sind das kleinste Objekt, welchem Berechtigungen zugeteilt werden können. Im Falle der Verzeichnisdienste dienen diese Benutzer zur Anmeldung am Netzwerk und verfügen über eine Vielzahl an definierten Eigenschaften, die zum Beispiel Aufbau und Gültigkeit von Passwörtern festlegen. Benutzer in anderen Systemen sind primär komplett unabhängig von den für den Netzwerkzugriff vergebene Benutzernamen. Aus Gründen der Übersichtlichkeit werden jedoch meist idente Bezeichnungen vergeben. Andernfalls muss bei der Auswertung ein Mapping der Benutzernamen durchgeführt werden.

4.1.2 Gruppen

In komplexeren Systemumfeldern hat sich die Verwendung von Benutzergruppen als vorteilhaft herausgestellt. Diese bieten insbesondere zwei Erleichterungen:

- Lange Listen einzelner Benutzer am Berechtigungsobjekt vermindern die Übersichtlichkeit in der Berechtigungsverwaltung
- Hat eine reale Mitgliedschaft, zum Beispiel in einer Abteilung, eine Vielzahl diskreter Berechtigungen zur Folge, so ist es um ein Vielfaches einfacher, einen weiteren Benutzer als Mitglied einer Gruppe hinzuzufügen als dem Benutzer explizit alle resultierenden Berechtigungen zuzuordnen.

In den Verzeichnisdiensten sind Gruppen elementare Bestandteile. Aber auch in anderen betrachteten Berechtigungsverwaltungen ist das Hilfsmittel einer Gruppe implementiert. Im Zuge der Analyse hat sich gezeigt, dass Rollen und Gruppen in ihrer Verwendung funktional ident sind. Somit erfolgt eine absolute Gleichstellung von Rollen und Gruppen in der weiteren Analyse.

4.1.3 Berechtigungsobjekte

Ein weiterer fixer Bestandteil jeder Berechtigungsverwaltung sind jene Objekte, auf welche der Zugriff reglementiert werden soll. Angefangen von Dateien und Verzeichnissen bis zu Softwareinstallationen oder Unternehmensdaten können die zu schützenden Informationen unterschiedlichste Ausprägung annehmen. Aus funktionaler Sicht besteht jedoch kein Unterschied zwischen den jeweiligen Berechtigungsobjekten. Die am Beginn der Analyse herangezogenen Berechtigungsdaten bezogen sich auf Softwareinstallationen mittels Novell Application Launcher (NAL), weshalb in weiterer Folge für Berechtigungsobjekte das Synonym „Anwendung“ (Application) Verwendung findet.

4.2 Modell der Berechtigungsinformationen

Zur künftigen Unterscheidung der einzelnen Berechtigungsdaten in der zentralen Datenbank werden sie einem übergeordneten Objekt „System“ entsprechend deren Ursprungssystem zugeordnet. Die Komponenten je System lassen sich wie folgt darstellen:

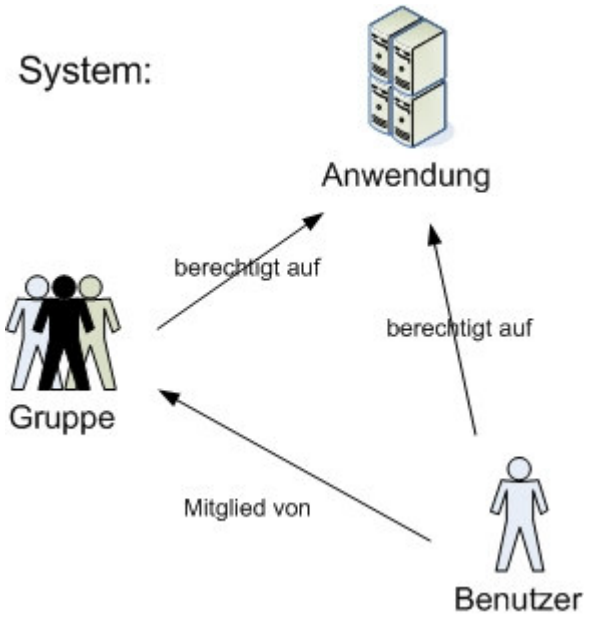

Abbildung 29: Benutzer – Gruppe – Anwendung

Wie Abbildung 29 zeigt, kann jeder Benutzer Mitglied einer oder mehrere Gruppen sein oder auch direkt auf eine oder mehrere Anwendungen berechtigt sein. Jede Gruppe kann auf eine oder mehrere Anwendungen berechtigt sein und diese Berechtigungen an ihre Mitglieder weitergeben.

4.3 Konzeptuelle Datenrepräsentation

Nach einer formalen, systemunabhängigen Beschreibung der jeweiligen Berechtigungskomponenten gilt es nun, diese Informationen auch in einer sinnvollen Datenstruktur zur elektronischen Weiterverarbeitung abzubilden.

4.3.1 XML als Beschreibungssprache

Um möglichste Plattform- und Anwendungsunabhängigkeit zu erzielen, wurde eine Beschreibung der Komponenten mittels Extensible Markup Language (XML) [48] gewählt. Hierarchisch strukturiert und durch XML-Tags gekennzeichnet sollen die Daten in Form von Textdateien gespeichert und zur Weiterverarbeitung abgelegt werden können. Abbildung 30 stellt die angestrebte XML-Struktur dar.

```
<system>
      <application/>
      <group/>
      <user/>
</system>
```

Abbildung 30: XML-Grundstruktur

In dieser Struktur lassen sich alle beteiligten Komponenten auflisten. Um weiters Mitgliedschaften der Benutzer in Gruppen beziehungsweise die jeweiligen Berechtigungen von Gruppen und Benutzer auf Applikationen abbilden zu können, müssen zusätzlich Referenzen eingeführt werden (Abbildung 31).

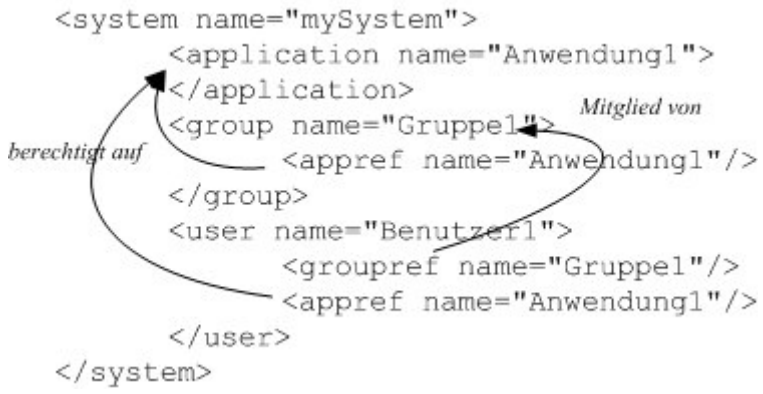

Abbildung 31: XML-Beziehungen

Bevor nun die jeweiligen Berechtigungsdaten der einzelnen Systeme inhaltlich in diese XML-Struktur überführt werden, soll eine Möglichkeit entwickelt werden, diese Daten formal auf Korrektheit zu prüfen.

4.3.2 DTD, Dokumenttypdefinition

Eine Dokumenttypdefinition (DTD) beschreibt mittels einer Grammatik das erwünschte einheitliche Format der XML-Datei. Die DTD-Datei wird zentral über einen Webserver zur Verfügung gestellt und kann jederzeit jederorts zur Validierung einzelner XML-Dateien herangezogen werden. Die entsprechende Dokumentenbeschreibung der angestrebten XML-Struktur ist in Abbildung 32 dargestellt.

```
<!ELEMENT system (application*, group*, user*)>
<!ELEMENT application (appdata?, description*)>
<!ELEMENT group (groupdata?, description*, appref*)>
<!ELEMENT appref EMPTY>
<!ATTLIST appref name CDATA #REQUIRED>
<!ELEMENT user (userdata?, description*, groupref*, appref*)>
<!ELEMENT groupref EMPTY>
<!ATTLIST groupref name CDATA #REQUIRED>
<!ELEMENT appref EMPTY>
<!ATTLIST appref name CDATA #REQUIRED>
```

Abbildung 32: Dokumenttypdefinition – DTD

Neben den jeweiligen Komponenten der Berechtigungszuteilung und deren Beziehungen untereinander beinhalten die einzelnen Berechtigungsverwaltungen eine Vielzahl zusätzlicher, wesentlicher Informationen, weshalb die Grundstruktur der XML-Datei um eine Vielzahl weiterer Elemente und Attribute erweitert wird.

4.4 Umfassende Datenrepräsentation

Nachstehend folgt eine inhaltliche Kurzbeschreibung der erweiternden Informationen in der angestrebten XML-Datei:

- Das Element „system“ erhält neben Namen und einer freien Beschreibung auch Informationen über das Exportdatum beziehungsweise den Gültigkeitszeitraum der Berechtigungsinformationen.
- Die jeweilige „application“ erhält neben optionalen Beschreibungsmöglichkeiten einen verpflichtenden, eindeutigen Namen, auf welchen gegebenenfalls aus „group“ beziehungsweise „user“ referenziert werden kann.

- Da referenzieren auf das Element „group“ ebenfalls möglich sein muss, ist auch ein verpflichteter, eindeutiger Name erforderlich. Darüber hinaus können schon anhand der Gruppen Informationen zu Benutzeranmeldungen verwaltet sein, insbesondere hinsichtlich Verhalten bei erkannten Eindringversuchen.
- Der Benutzeraccount „user“ beinhaltet neben einer detaillierten Beschreibung der zugeordneten Person alle relevanten sicherheitstechnischen Informationen hinsichtlich Sperren, Passwortvorgaben, letzter erfolgreicher Anmeldung oder auch Gültigkeit. Manche Systeme erfordern darüber hinaus rein userbezogene Berechtigungsbeschreibungen, weshalb dem Element „user“ diverse systemspezifische Unterelemente zugeordnet wurden.

Die vollständige Dokumenttypdefinition ist als Anhang beigefügt.

5 Praktische Umsetzung

Die praktische Umsetzung gliedert sich prinzipiell in drei Phasen. Erster und wesentlichster Schritt ist, die zu analysierenden Berechtigungsdaten der jeweiligen Systeme in das vorgegebene Datenformat zu überführen. Anschließend folgt die konzeptionelle Entwicklung und praktische Implementierung der zentralen Datenbank. Im dritten Schritt werden die gesammelten Daten analysiert und den verantwortlichen Personen zur Kontrolle zur Verfügung gestellt.

5.1 Generierung der Berechtigungsdaten

Je nach den technischen Gegebenheiten in den Quellsystemen unterscheidet sich die Vorgangsweise, die Berechtigungsinformationen zum Import in die zentrale Datenbank aufzuarbeiten.

5.1.1 Microsoft Active Directory

Mittels Microsoft Active Directory werden die Zugriffsrechte der Mitarbeiter auf Dateien auf dem zentralen Datenserver verwaltet. Die Berechtigungsinformationen werden dabei in Form einer Access Control List (ACL) mit dem jeweiligen Ordner oder der jeweiligen Datei im Dateisystem abgelegt.
Wie schon bei der Systembeschreibung erwähnt, können die Berechtigungsinformationen mit Hilfe des Kommandozeilentools CACLS.exe rekursiv aus dem Dateisystem ausgelesen und in eine Textdatei geschrieben werden. Die Umwandlung in das geforderte XML-Format erfolgt durch Konvertierung der Datei. Ein Visual Basic Script (VBS) liest die Berechtigungsinformationen aus der Textdatei aus und erzeugt unter Verwendung des XMLWriter-Objektes eine neue Datei im angestrebten Format. Die Validierung der XML-Datei gegen die DTD erfolgt ebenfalls im Script, wodurch eine zum Import fertige Datei aller Berechtigungsdaten vorliegt.

5.1.2 Novell eDirectory

Im eDirectory werden neben den Berechtigungen zur Softwareinstallation mittels NAL auch alle Benutzeraccounts für die Netzwerkanmeldung und alle Gruppenzugehörigkeiten verwaltet. Diese umfassenden Informationen werden mit Hilfe eines PERL-Script über LDAP aus dem Verzeichnis ausgelesen und in eine DTD-konforme XML-Datei geschrieben.

5.1.3 EASY Archive

Die ursprüngliche Version von EASY Archive besitzt eine rein proprietäre Berechtigungsverwaltung. Der Zugriff auf Berechtigungsinformationen ist nur über die integrierte Verwaltungsoberfläche möglich, Exportmöglichkeit ist keine vorgesehen. Im Zuge dieser Arbeit wurde von der Herstellerfirma eine Exportschnittstelle beauftragt, welche alle Berechtigungsdaten schon als valide XML-Datei ausgibt.

5.1.4 SAP

Die Berechtigungsinformationen in SAP können systemspezifisch als CSV-Datei exportiert werden. Ein eigenes PERL-Script wandelt diese Informationen in eine DTD-konforme XML-Datei um. In einer weiteren Ausbaustufe des Projektes wird auch in SAP eine Exportschnittstelle für Berechtigungsdaten in dem vorgegebenen Datenformat implementiert.

5.1.5 Weitere Systeme

Aufgrund des modularen Aufbaus und einer einheitlichen Importschnittstelle aller Berechtigungsdaten im definierten XML-Format können jederzeit Berechtigungsdaten aus weiteren Systemen in die Datenbank importiert werden. Voraussetzung ist lediglich eine bestandene Validierung gegen die vorgegebene DTD-Datei.

5.2 Proof of Concept

Die Entwicklung der zentralen Datenbank wird mit Microsoft Access durchgeführt. Es bietet neben den relevanten Funktionen einer Datenbank weiters eine komfortable Unterstützung von Abfragen und eine einfach zu implementierende graphische Oberfläche zur Interaktion für den Benutzer. Im ersten Schritt bildet Access eine autarke Anwendung. Für die Produktivnahme wurden die internen Datentabellen aus Access gegen Tabellen einer Oracle-Datenbank getauscht.

5.2.1 Datenbankmodell

Das grundlegende Datenmodell, wie in Abbildung 33 angeführt, beschreibt jenen Teil der Datenbank, in welchem die einzelnen Berechtigungsdaten der Systeme gespeichert werden. Anforderungen bei der Auswertung erfordern eine zusätzliche Erweiterung des Modells. Dabei ist dem Umstand Rechnung zu tragen, dass auch nur tatsächlich für die Daten beziehungsweise für das System verantwortliche Personen Einsicht auf die darin vergebenen Berechtigungen erhalten.

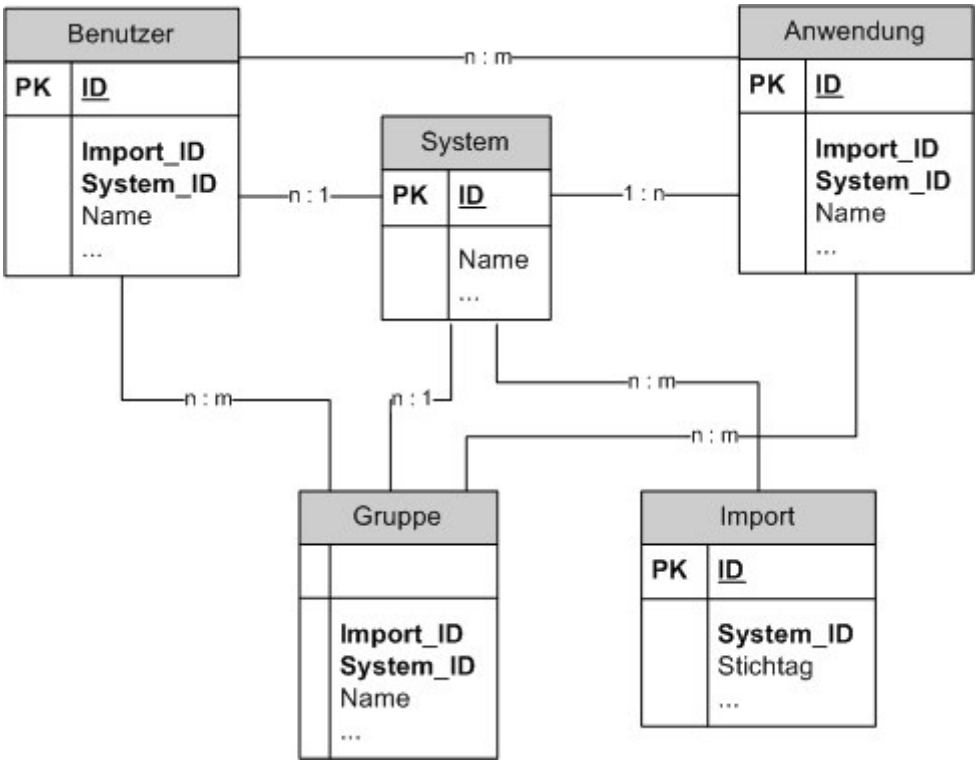

Abbildung 33: ER-Diagramm

Die Beschreibung der Berechtigungen erfolgt mittels der Objekte „Benutzer“, „Gruppe“ und „Anwendung“, wobei jeweils eine n:m-Beziehung unter den Objekten besteht. Zusammengefasst werden diese Berechtigungsinformationen mit Hilfe eines „System“, entsprechend dem Quellsystem, aus welchem die Daten stammen. Um Daten eines Systems zu mehreren Zeitpunkten verwalten zu können, wurde das Modell um den „Import“ erweitert.

5.2.2 Datenimport

Ein eigenes Benutzerinterface bietet die Möglichkeit, Datenimporte durch Auswahl der zu importierenden XML-Datei durchzuführen und zu verwalten.

5.2.3 Analysemöglichkeiten

Technisch bieten eine Vielzahl von Programmiersprachen über Open DataBase Connectivity (ODBC) eine Zugriffsmöglichkeit auf die in der Access Datenbank abgelegten Daten. Die einfachste Art zur Erstellung und Verwaltung von Abfragen ist die mit den von Access gebotenen Mitteln. Dadurch können Anomalien der Berechtigungsdaten effizient analysiert werden.

Für die Visualisierung können mittels einer geeigneten serverseitigen Programmiersprache direkt über ODBC die relevanten Informationen ausgelesen und zur webbasierenden Darstellung aufgearbeitet werden.

5.3 Finale Umsetzung

Aufgrund der großen Datenmengen und den daraus resultierenden Performanceeinbußen wird in der finalen Version die Datenhaltung in einer Oracle Datenbank durchgeführt. Die Verwaltung der Systemdaten erfolgt weiterhin über Access, in welches die jeweiligen Tabellen der Oracle Datenbank verknüpft wurden.

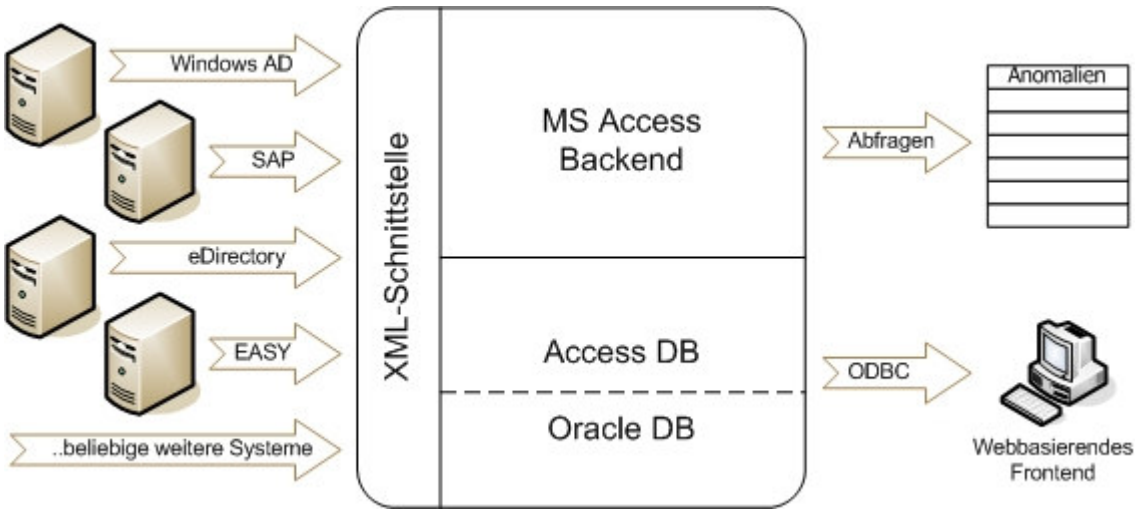

Abbildung 34: Darstellung - Gesamtsystem

Ein weiteres Kriterium ist, dass auch nur ausgewählten Personen Berechtigungsdaten der einzelnen Systemen zur Verfügung gestellt werden sollen. Aus diesem Grunde werden in der Datenbank sogenannte „Ansichten“ eingeführt, mit dessen Hilfe personenspezifisch festgelegt werden kann, für welche Mitarbeiter welche Daten aus dem System dargestellt werden.

5.3.1 Systematische Berechtigungsanalyse

Schon während der Entwicklung der zentralen Datenbank beziehungsweise beim Aufbereiten der jeweiligen Berechtigungsdaten werden laufend die Informationen auf inhaltliche Plausibilität geprüft. Deshalb, und auch mit der Absicht, den jeweiligen System Owner bereinigte Berechtigungsdaten zur Verfügung stellen zu können, werden als erster Schritt laufend Analysen auf Anomalien durchgeführt. Dabei werden mit Hilfe der Access eigenen Mitteln unterschiedlichste Abfragen erstellt und deren Ergebnisse auf Sinnhaftigkeit untersucht. Einige Beispiele untersuchter Anomalien wären:

- Die letzte Netzwerkanmeldung ist sehr lange zurück, was auf fehlende Aktualität des Accounts schließen lässt.

- Es hat noch nie eine Netzwerkanmeldung stattgefunden, wobei der Benutzer schon vor längerer Zeit angelegt wurde.
- Accounts, welche entweder bewusst oder durch Passwortfehleingaben zur Netzwerkanmeldung gesperrt sind.
- Benutzer, deren Passwortvorgaben nicht den unternehmensweiten Richtlinien entsprechen (Länge, Wechselintervalle,…).
- Benutzer, die sich zwar im Netzwerk authentifizieren können, aber darüber hinaus über keine zugeordneten Berechtigungen verfügen.
- Im Gegensatz dazu Benutzer, welche in einzelnen Systemen über Berechtigungen verfügen aber keine Netzwerkanmeldung durchführen dürfen.
- Berechtigungen, die im Dateisystem benutzerbezogen vergeben wurden, und nicht über Gruppen.
- Berechtigungen eines Mitarbeiters, die auf ein Home-Laufwerk eines anderen Mitarbeiters beziehungsweise auf ein Abteilungslaufwerk einer anderen Abteilung vergeben wurden.

Insgesamt wurden eine Vielzahl unterschiedlicher Anomalien aufgezeigt und analysiert. Insbesondere bei spezifischen Eigenschaften von Accounts lassen sich die Ursachen auf eine Fehlkonfiguration zurückführen und wurden korrigiert. Andere Anomalien beruhen auf systemspezifischen Anforderungen wie zum Beispiel Administratoren oder Testaccounts in einzelnen Systemen. Diese wurden auf Korrektheit überprüft und als erforderliche Ausnahmen festgehalten.

5.3.2 Dezentrale Datenvisualisierung

Der modulare Aufbau bedingt, dass alle Berechtigungsdaten der einzelnen Systeme vor dem Import als valide XML-Dateien vorliegen. Der erste und einfachste Ansatz einer Visualisierung der Daten ist, die XML-Datei mittels Extensible Stylesheet Language Transformation (XSLT)[49] direkt in eine HTML-Datei zu überführen. Dadurch können zwar keine komplexen Analysen durchgeführt werden, es ist jedoch ein geeignetes Mittel zur Visualisierung einfacher Gruppenmitgleidschaften beziehungsweise Referenzen zu Anwendungen. Im Anhang B befindet sich zur Veranschaulichung eine valide XML-Datei und im Anhang C eine XSLT-Datei, mit dessen Hilfe eine HTML-Datei erzeugt wird, in der alle Anwendungen aufgelistet werden inklusive aller Personen, die darauf referenzieren. Das Layout ist in einer Cascading Style Sheets (CSS)-Datei im Anhang D festgelegt.

5.3.3 Webbasierendes Frontend

Als Frontend zur Darstellung der einzelnen Berechtigungsdaten der Systeme für die jeweiligen System Owner wird eine webbasierende Anwendung entwickelt. Als Datenquelle dient die Oracle Datenbank, als serverseitige Programmiersprache zur Erzeugung der HTML-Ausgaben werden Java Server Pages (JSP) verwendet. Die Verwaltung einzelner „Ansichten“ und die Berechtigungsvergabe an den jeweiligen System Owner erfolgt in der Access Anwendung.
In der Aufarbeitung für die Darstellung im Browser müssen die unterschiedlichen Ansichten auf die Daten berücksichtigt werden, je nach dem, ob der Betrachter ein „Owner“ eines Systems ist oder über die Rolle des Abteilungsleiters zum System Owner aller Abteilungsdaten und Verantwortlichkeiten seiner Mitarbeiter wird. Die Weboberfläche ist technisch in zwei Frames unterteilt und wird aus Gründen der Anschaulichkeit in zwei Schritten erklärt:

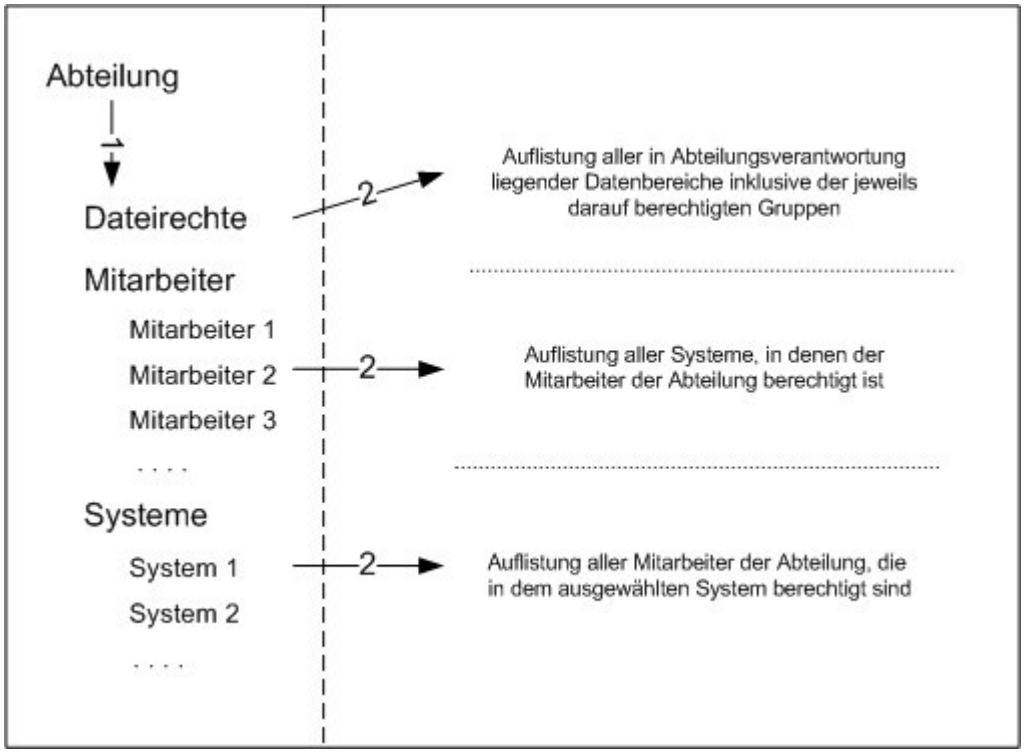

Abbildung 35: Weboberfläche aus Sicht eines Abteilungsleiters

Abbildung 35 zeigt das Frontend aus sicht eines Abteilungsleiters. Dabei ist von Interesse, welche Personen auf Abteilungsdaten Zugriff besitzen beziehungsweise über welche Berechtigungen abteilungsinterne Mitarbeiter in den einzelnen Systemen verfügen. Die Auswahl der Dateirechte in liefert eine Darstellung aller Datenbereiche in Abteilungsverantwortung und welche Gruppen darauf berechtigt sind. Bei auffallenden

Konstellationen, wie zum Beispiel die Gruppenmitgliedschaft eines nicht der Abteilung angehörigen Mitarbeiters wird die entsprechende Gruppe farblich hervorgehoben. Durch Auswahl der Gruppe werden die zugehörigen Mitglieder für nähere Analysen angezeigt.
Die Bereiche Mitarbeiter und Systeme beschreiben den selben Informationsbereich - einmal aus der Sicht, welche Berechtigungen ein Mitarbeiter der Abteilung in den unterschiedlichen Systemen besitzt, andererseits, welche Mitarbeiter der Abteilung in einem System berechtigt sind.

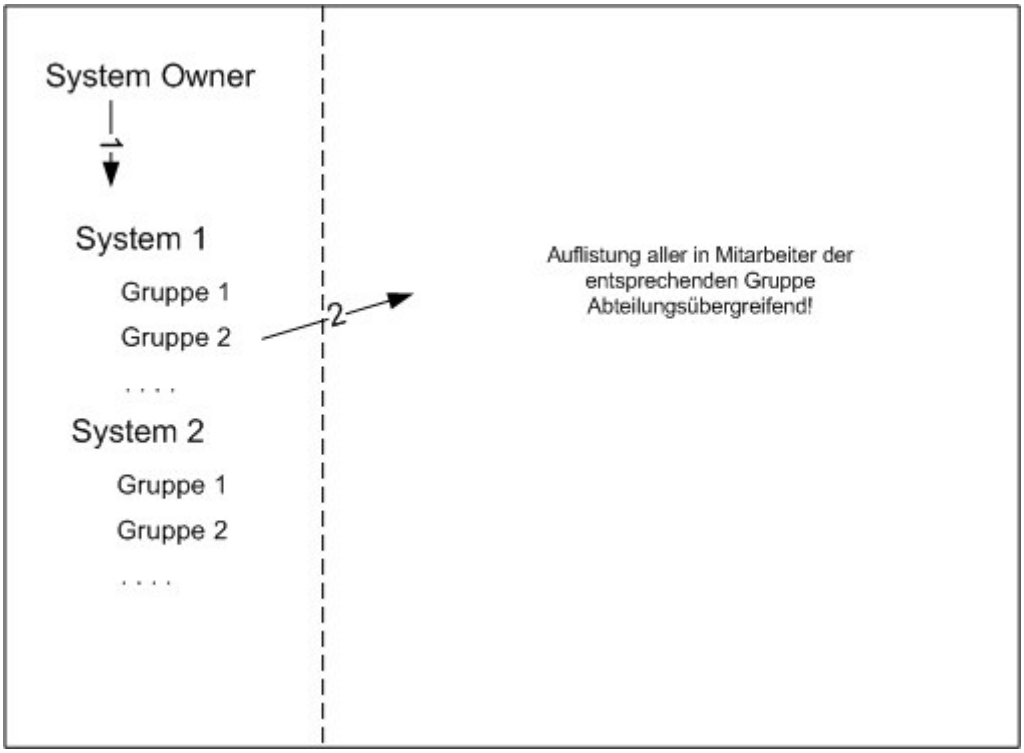

Abbildung 36: Weboberfläche aus Sicht eines System Owner

Der System Owner sieht , wie in Abbildung 36 dargestellt, alle in dem jeweiligen System existierenden Gruppen und deren entsprechende Mitglieder. Im Unterschied zum Abteilungsleiter werden dem System Owner jedoch abteilungsübergreifend alle Mitarbeiter aufgelistet.

6 Projektergebnis

Im Zuge der praktische Umsetzung ergaben sich laufend neue Herausforderungen. Schon die Analyse der proprietären Berechtigungsinformationen erforderten eine enge Zusammenarbeit mit den jeweiligen Systemspezialisten. Zum Beispiel die in SAP vorgesehene Exportschnittstelle lieferte zwar alle Rollen und Gruppenzugehörigkeiten der Benutzer in Form einer CSV-Datei. Eine Interpretation effektiver Berechtigungen war dadurch noch nicht möglich. Es zeigte sich auch, dass oftmals schon zur störungsfreien Funktion einer Anwendung intern Berechtigungen gesetzt sein müssen, die mit den eigentlichen Berechtigungen der Mitarbeiter in keinem Zusammenhang stehen.
Weiters zeigte sich, dass in manchen Systemen mehrere Einzelberechtigungen vergeben werden müssen, um eine bestimmte Tätigkeit in dem betreffenden System ausführen zu können. Ein weiterer Sonderfall sind Systembenutzer, unter dessen Berechtigungen zum Beispiel Datensicherungen durchgeführt werden. All diese Informationen werden zwar in die zentrale Datenbank eingelesen. Im Sinne höchster Lesbarkeit mussten jedoch unterschiedliche Mechanismen bei der Aufbereitung der Daten eingeführt werden. So fassen beispielsweise abstrakte Labels mehrere Einzelberechtigungen zu einer anschaulichen Tätigkeit eines Mitarbeiters im System zusammen. Auch die Möglichkeit, Berechtigungen anhand spezieller Kriterien von der Analyse auszunehmen, führte zu einer Steigerung der Qualität der Ergebnisse.
All diese spezifischen Berechtigungen und Sonderfälle kamen erst bei der schrittweisen Umsetzung zum Vorschein. Wie damit umzugehen sei, konnten nur in reger Rücksprache mit den Systemverantwortlichen und der Sicherheitsabteilung festgelegt werden.

6.1 Zielüberprüfung

Hauptziel der Analyse war, den jeweiligen verantwortlichen Personen, sei es System Owner oder Abteilungsleitung, eine Möglichkeit zu bieten, auf benutzerfreundliche Art und Weise vergebene Berechtigungen einzusehen. Die hohe Anzahl an Änderungswünschen von Berechtigungen nach Produktivnahme des Systems belegt, dass durch diese Visualisierung eine Vielzahl an überflüssigen, beziehungsweise nicht mehr aktuellen Rechten identifiziert wurden. Durch die Bereinigung wurde ein Zugewinn an Sicherheit erzielt.
Auch der IT-Sicherheit wurde eine Möglichkeit geboten, allgemeine relevante Sicherheitsvorgaben und deren Einhaltung im laufenden Betrieb zu kontrollieren.
Aktueller Stand ist, dass die jeweiligen Berechtigungsdaten der Systeme einmal im Woche ausgelesen und aufgearbeitet werden. Eine Überprüfung der effektiven Berechtigungen ist somit jederzeit durchführbar.

6.2 Auswirkungen

Insbesondere der gleichzeitige Einsatz von Microsoft Active Directory und Novell eDirectory zur Verwaltung unterschiedlicher Ressourcen im Netzwerk erfordert zumindest für Standardbenutzer eine Koexistenz in beiden Verzeichnisdiensten. Analysen dahingehend leisteten wertvolle Vorarbeit für ein leicht zeitversetzt später gestartetes Projekt einer zentralen Benutzerverwaltung und Einführung eines Identity Managements (IDM).
Auch in Richtung der jeweiligen Systembetreiber wurden Zeichen gesetzt. Mit Hilfe dieser Anwendung entsteht sozusagen die Herausforderung, jederzeit auf eine saubere Berechtigungsverwaltung im betreuten System zu achten.

6.3 Schwachpunkte

Für eine lückenlose Überwachung der vergebenen Berechtigungen wäre eine laufende Protokollierung aller Änderungen innerhalb der Berechtigungsverwaltung erforderlich. Diese Funktion muss aber von der jeweiligen Anwendung unterstützt sein. Da die hier beschriebene Analyse nur Berechtigungsdaten zu bestimmten Zeitpunkten erfasst, kann keine lückenlose Kontrolle gewährleistet werden.
Ein weiterer Aspekt ist, dass Kontrollen auch tatsächlich durchgeführt werden müssen. Als Lösungsweg wurde diese Tätigkeit in relevante Stellenbeschreibungen übernommen.

6.4 Resümee

Mit Sicherheit konnte im Zuge des Projektes eine Sensibilisierung bei der Berechtigungsverwaltung und Kontrolle erzielt werden. Schon bei der Inbetriebnahme der ersten Testversionen wurden freiwillige System Owner in den weiteren Entwicklungsprozess involviert. Speziell für die Gestaltung der Weboberfläche konnte auf diese Art wertvolles Feedback gewonnen werden.
Das hohe Interesse der Testpersonen zeigte sich insofern, als dass rasch laufend Anfragen hinsichtlich korrekter Interpretation von dargestellten Berechtigungen erfolgte. Parallel dazu führte die IT-Sicherheit kontinuierlich Analysen auf Anomalien durch. Zahlenmäßig am häufigsten wurden Unregelmäßigkeiten hinsichtlich Passwortvorgaben wie zum Beispiel Wechselintervall oder Mindestlänge gefunden. Aus sicherheitstechnischer Sicht interessanter war das Auffinden schon lange nicht mehr verwendeter und auch nicht mehr benötigter Accounts. Diese stammen vorwiegend von Ferialpraktikanten oder externen Mitarbeitern, die nur vorübergehend im Unternehmen beschäftigt waren. Auch Abteilungswechsel oder Jobrotation konnten immer wieder als Ursache fehlerhafter Berechtigungen identifiziert werden. Generell kann man sagen, dass durch Modifikation der Rechte eines bestehenden Benutzers ein erhöhtes Gefahrenpotential für Fehlberechtigungen entsteht als bei Neuanlage des Benutzers.
Ein Spezialfall an Fehlberechtigungen sind Überberechtigungen einzelner Benutzer in bestimmten Bereichen. Hier hat sich gezeigt, dass vorwiegend Fehlfunktionen in

Anwendungen auslösend waren, indem als rasche Abhilfe bei der Fehlerbehebung, oftmals auch aufgrund von Druck von Außen, Berechtigungen abgeändert wurden und nie wieder korrigiert wurden.
Bezugspunkt in der Berechtigungsanalyse ist üblicherweise der Benutzername des Mitarbeiters, welcher für die Netzwerkanmeldung festgelegt wurde. In manchen Systemen ist es jedoch der Fall, dass ein unterschiedlicher Benutzername Verwendung findet. Um dennoch den Abteilungsleitern die korrekten Informationen zur Verfügung stellen zu können, musste ein Usermapping implementiert werden, wo unterschiedliche Benutzernamen unterschiedlicher Systeme in Relation zueinander gestellt werden können. Auch bei Mitarbeitern, die sich gerade auf Jobrotation befinden, wird dieser Mechanismus verwendet, da der Mitarbeiter in seiner temporären Funktion in der neuen Abteilung auch über unterschiedliche Berechtigungen in den jeweiligen Systemen verfügen muss als in seiner Stammabteilung von Nöten ist.
Im Laufe der Zeit wurden immer weitere Systeme in diese Berechtigungsanalyse aufgenommen. Das Angebot der Kontrollmöglichkeit der Berechtigungen wird von den System Owner auch weiterhin gerne angenommen. Auch Erweiterungswünsche auf in Verwendung befindliche B2B-Systeme wurden an die IT-Sicherheit herangetragen. Dies scheitert jedoch daran, da die Berechtigungsverwaltung dieser Anwendungen nicht im Einflussbereich der IT-Sicherheit liegt.
Die größte Nachfrage besteht an existierenden Berechtigungen auf Abteilungsdaten. Da manche Abteilungen sich gegenseitig ausschließende Tätigkeiten ausüben, darf keinesfalls ein Informationsfluss zwischen den Abteilungen existieren. Andernfalls wären sogar strafrechtliche Konsequenzen denkbar. Die IT-Sicherheit hat mittlerweile einen eigenen Prozess entwickelt, um nach einem Abgang eines Mitarbeiters aus einer Abteilung über alle Systeme übergreifend zu prüfen, ob der Mitarbeiter noch irgendwelche Berechtigungen auf Daten der Abteilung besitzt.
Zusammenfassend hat sich gezeigt, dass mit der Möglichkeit der Kontrolle auch das Interesse geweckt wurde. Das mit dem Projekt gestärkte Sicherheitsbewusstsein ist nur ein kleiner aber sehr wichtiger Punkt einer gelebten Sicherheitspolitik im Unternehmen.

7 Zusammenfassung

Tatsache ist, dass in jedem größeren EDV-System eine Berechtigungsverwaltung erforderlich ist. Ungelöst ist jedoch die Frage, welche Technik bevorzugt zur Verwaltung der Berechtigungen herangezogen werden soll. Diesbezüglich sind die jeweiligen Anforderungen zu Unterschiedlich, als dass man eindeutige Empfehlungen abgeben könnte.

Auch die Überschaubarkeit der Berechtigungen bildet einen nicht unwesentlichen Aspekt. Schon die Ausführungen und Möglichkeiten der Administratoroberfläche bestimmen, mit welchem Aufwand die Berechtigungen kontrolliert werden können. Ein weiterer Faktor ist die Möglichkeit, auch außerhalb der Anwendung auf die Berechtigungsinformationen zugreifen zu können. Dies kann entweder durch einen Export oder wie am Beispiel der Verzeichnisdienste über ein standardisiertes Protokoll direkt gegen die Berechtigungsverwaltung erfolgen.

Ein weiter wesentlicher Faktor ist die Flexibilität, Berechtigungen nach den vorgegebenen Sicherheitsrichtlinien abbilden zu können. Hierarchische Strukturen und die daraus resultierende Möglichkeit der Vererbung und die Bildung von Gruppen beziehungsweise Rollen tragen Maßgeblich zur Steigerung der selben bei.

Verzeichnisse würden alle erwähnten Aspekte nahezu perfekt erfüllen. Tendenziell bieten auch mittlerweile nahezu alle größeren Geschäftsapplikationen eine Anbindung an einen Verzeichnisdienst an. Ebenso der vermehrte Einsatz zentraler Identity Management Systeme (IDM) verweisen in diese Richtung.

Aus Sicht der Berechtigungskontrolle ergibt sich noch ein weiterer Sicherheitsaspekt. Ebenso die in dieser Arbeit beschriebene Berechtigungsanalyse ist nur in der Lage, einen IST-Zustand zum Zeitpunkt der Analyse abzubilden. Denkbar wäre, dass jemand vorübergehend über veränderte Berechtigungen verfügt. Sofern diese bis zum nächsten Zeitpunkt der Analyse wieder rückgängig gemacht wurden, können sie nicht erfasst werden. Auch wenn vom aktuellen Standpunkt aus gesehen ein Maximum der Anforderungen an Berechtigungsverwaltungen von Verzeichnisdiensten erfüllt werden, so zeichnet sich damit bereits eine neue Herausforderung ab: protokollierende Berechtigungsverwaltungen.

Literaturverzeichnis

[1] J. H. Saltzer and M. D. Schroeder, *The Protection of Information in Computer Systems*: IEEE, 1975.

[2] ISO/IEC 27001:2005, *Information technology -- Security techniques -- Information security management systems -- Requirements*. Genf, 2005.

[3] W. Ware, *Security Controls for Computer Systems*: RAND Corporation, 1970.

[4] T. J. Nagy and H. Wachmann, *Informationssicherheit und das Eisbergprinzip*: Eisberg-Group, 2004.

[5] R. J. Anderson, *Security Engineering: a guide to building dependable distributed systems*: Wiley Computer Publishing, 2001.

[6] R. Rosinski K. Rosen, J. Farber, *UNIX System V, Rel.4 Grundlagen und Praxis*: te-wi Verlag, 1993.

[7] B. Smith and B. Komar, *Windows Sicherheit – Die technische Referenz*: Microsoft Press, 2005.

[8] P. Kuo and J. Henderson, *Novell's Guide to Troubleshooting eDirectory*: Novell Press, 2005.

[9] S. Riemer, C. Kezema, M. Mulcare, and B. Wright, *Windows Server 2008 Active Directory Resource Kit*: Microsoft Press, 2008.

[10] D. F. Ferraiolo and D. R. Kuhn, *Role Based Access Control*: 15th National Computer Security Conference, 1992.

[11] R. Sandhu, D. F. Ferraiolo, and D. R. Kuhn, *The NIST Model for Role Based Access Control: Towards a Unified Standard*: Proceedings, ACM Workshopon Role Based Access Control, 2000.

[12] W.A. Jansen, *Inheritance Properties of Role Hierarchies*: 21st National Information Systems Security Conference, 1998.

[13] D. F. Ferraiolo, D. R. Kuhn, and R. Chandramouli, *Role-Based Access Control*: Artech House, 2003.

[14] D. Gollmann, *Computer Security*: John Wiley & Sons Ltd, 1999.

[15] E. Amoroso, *Fundamentals of Computer Security Technology*: Prentice Hall PTR, 1994.

[16] R. J. Anderson, *Personal Medical Information Security, Engineering, and Ethics*. Berlin: Springer, 2007.

[17] R. J. Anderson, *Security in Clinical Information Systems*: British Medical Association (BMA), 1996.

[18] F. S. Preiss, *Access Control Policy Editor and Analyzer for Policies on a Business Level*: Technische Universität Wien, 2007.

[19] W. Dohr, HJ. Pollirer, and E. Weiss, *Datenschutzrecht - DSG*: Manz, 2002.

[20] L. Willis, *Security Policies: Where to Begin*: SANS Institute, 2002.

[21] T. Jarmon, *A Preparation Guide to Information Security Policies*: SANS Institute, 2002.

[22] C. Kok Kee, *Security Policy Roadmap – Process for Creating Security Policies*: SANS Institute, 2001.

[23] ISO/IEC 17799:2005, *Information technology -- Security techniques -- Code of practice for information security management*. Genf, 2005.

[24] A. Calder and S. Watkins, *International IT Governance: An Executive Guide to ISO 17799/ISO 27001*: Kogan Page Limited, 2006.

[25] S. Canavan, *Information Security Policy – A Development Guide for Large and Small Companies*: SANS Institute, 2006.

[26] R. D. Lee, *Developing effective Information System Security Policies*: SANS Institute, 2001.
[27] R. Lehrbaum, *Managing Security Policies*: Technische Universität Wien, 2007.
[28] Bundesamt für Sicherheit in der Informationstechnik (BSI), *BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)*: Bundesamt für Sicherheit in der Informationstechnik (BSI), 2008.
[29] Bundesamt für Sicherheit in der Informationstechnik (BSI), *BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz*: Bundesamt für Sicherheit in der Informationstechnik (BSI), 2008.
[30] P. J. Kaleewoun, *An Overview of Corporate Computer User Policy*: SANS Institute, 2001.
[31] Informationssicherheitsbüro Bundeskanzleramt, Zentrum für sichere Informationstechnologie – Austria, *Österreichisches Informationssicherheits-handbuch*: Österreichische Computer Gesellschaft (BSI), 2008.
[32] W. H. Ware R. Turn, *Privacy and Security in Computer Systems*: RAND Corporation, 1975.
[33] ISO/IEC 27005:2008, *Information technology -- Security techniques -- Information security risk management*. Genf, 2008.
[34] R. Laurer, R. Borns, J. Strobl, M. Schütz, and O. Schütz, *Bankwesengesetz (BWG)*: Manz, 2006.
[35] D. Beer, R. von zur Mühlen, and P. Stürmann, *Informatik-Sicherheit für Sicherheitsverantwortliche und Führungskräfte*. Bonn: SIMEDIA GmbH, 1999.
[36] B. Guttman and E. A. Roback, *NIST Special Publication 800-12: An Introduction to Computer Security - The NIST Handbook - Computer Security*. Gaithersburg, 2005.
[37] J. M. Johansson, *Microsoft Server 2008 Security Resource Kit*. Redmond: Microsoft Press, 2008.
[38] S. Riemer, C. Kezema, M. Mulcare, B. Wright, and Microsoft Active Directory Team, *Windows Server 2008 Active Directory – Die technische Referenz*: Microsoft Press, 2008.
[39] M. Kuppinger, *Windows Server 2003 – das Handbuch*: Microsoft Press, 2003.
[40] H. Schmitzberger, *Datenauswertung der Rechtestrukturen unter Windows 2000 und deren Visualisierung*: Johannes Kepler Universität Linz, 2004.
[41] Novell Training Services, *Novell eDirectory Design and Implementation (Course 575)*: Novell, 2001.
[42] H. Maiwald, *EE.x FAQ*: EASY Software AG, 2008.
[43] EASY Software, *EASY ENTERPRISE.x Konfigurationsmanager*: EASY Software AG, 2008.
[44] F. Föse, L. Will, and S. Hagemann, *SAP NetWeaver AS ABAP System Administration*: SAP Press, 2008.
[45] IBM Business Consulting GmbH, *SAP Authorization System: Design and Implementation of Authorization concepts for SAP R/3 and SAP Enterprise Portals*: SAP Press, 2003.
[46] M. Linkies and F. Off, *SAP Security and Authorizations - Risk Management and Compliance with Legal Regulations in the SAP Environment*: SAP Press, 2006.
[47] SAP, *Berechtigungskonzept AS ABAP*: SAP AG, 2007.
[48] E. R. Harold, *XML in a nutshell*: O'Reilly, 2005.
[49] M. Bach, *XSL und XPath - verständlich und praxisnah*: LinkAddison-Wesley, 2000.

Anhang A - Zusammenfassung

Zugriffskontrolle ist ein wesentliches Sicherheitsmerkmal moderner Datenverarbeitung. Aktuelle EDV-Systeme bieten spezifische Möglichkeiten, Berechtigungen festzulegen. Die Entscheidung, welcher Benutzerkreis über welche Berechtigungen in einem System verfügt, kommt aus organisatorischer, beziehungsweise fachlicher Ebene und wird in Form von Sicherheitsrichtlinien festgehalten. Das Umsetzen und Administrieren obliegt in Folge technischem Fachpersonal. Aufgrund dieser physischen Trennung und oftmals fehlendem Fachwissen ist es den für die Berechtigungsfestlegung verantwortlichen Mitarbeitern schwer bis unmöglich, aktuell vergebene Berechtigungen zu kontrollieren. Ein einfacher Export und Weitergabe der Berechtigungsinformationen scheitert an den proprietären Zugriffskontrollmechanismen ebenso wie an den bei manchen Systemen gar nicht vorgesehenen Exportfunktionen.

Nach einer umfassenden und strukturierten Beschreibung aller erforderlichen theoretischen Grundlagen werden im Zuge dieser Arbeit unterschiedliche Berechtigungsstrukturen am Beispiel einiger Geschäftsapplikationen eines Großunternehmens analysiert und Gemeinsamkeiten gefunden. Diese bilden ein Schema einer vereinheitlichten Darstellung aller in den Systemen vergebenen Berechtigungen. Somit können nach entsprechender Aufarbeitung der einzelnen Berechtigungsdaten diese in einer einheitlichen Form in einer zentralen Datenbank abgelegt werden und für weitere Analysen und Visualisierungen den für die Richtigkeit der Berechtigungen verantwortlichen Personen zur Verfügung gestellt werden.

Anhang B - Abstract

Access Control is one of the crucial security features in modern computing. Today's information systems provide specific ways to define access rights. The decision, what right is granted to which user of a system is met on organizational or functional level and is described by information security policies. The implementation and administration shall be done by technical experts. Due to this physical separation and often lack of know-how it is hardly possible for the security staff in charge to know the actual rights. Since every system implements its own proprietary export or no export at all, comparison of access right information is very difficult. This also becomes an obstacle when rights are to be consolidated.

After a broad, structured description of relevant theoretical concepts this work will analyse and compare access control structures on hand of business applications of a large enterprise. This will lead to the composition of a schema of an uniform representation of the assigned rights. Using this schema a database is constructed where the security staff in charge is able to access and analyse the aggregated information.

This work provides a broad theoretical base in respect of access control.

Anhang C - Lebenslauf

Angaben zur Person

Name	**Wöhrnschimmel Harald**
Email	**fritztorrent@gmail.com**
Staatsangehörigkeit	**Österreich**
Geburtsdatum	**21.09.1970**

Bildungsweg

1976 – 1980	**21, Volksschule Ostmarkgasse**
1980 – 1984	**21, BRG Franklinstrasse**
1984 - 1990	**20, TGM, Nachrichtentechnik und Elektronik**
seit 1995	**Studium Wirtschaftsinformatik**

Berufliche Laufbahn

1991	**Servicetechniker einer Alarmanlagenfirma**
1991 - 1994	**Diagnosetechniker bei ALCATEL Strebersdorf**
1995 - 1999	**Freiberuflicher EDV – Trainer**
seit 2000	**Selbstständiger Dienstleister im EDV Bereich**

Zusätzliche Angaben

Bundesheer	**Abgeschlossen mit März 1991**
Sprachkenntnisse	**Deutsch, Englisch**
Führerschein	**A, B**

Anhang D - Vollständige Dokumenttypdefinition (DTD)

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!ELEMENT system (application*, group*, user*)>
<!--
name ............... name des systems, herkunft, plattform
exportdate ........ datum des exports
evalfrom .......... beginndatum des auswertungszeitraumes
evalto ............ enddatum des auswertungszeitraumes
info ............... anmerkung zur auswertung
encoding .......... ob attribut-wert urlencoded sind
-->
<!ATTLIST system
        name ID #REQUIRED
        exportdate CDATA #REQUIRED
        evalfrom CDATA #IMPLIED
        evalto CDATA #IMPLIED
        info CDATA #IMPLIED
>

<!-- ******** Im System existierende APPLIKATIONEN ******** -->

<!ELEMENT application (appdata?, description*)>
<!ATTLIST application
        name CDATA #REQUIRED
>

<!ELEMENT appdata EMPTY>
<!ATTLIST appdata
        shortname CDATA #IMPLIED
        longname CDATA #IMPLIED
>

<!--
<!ELEMENT description (#PCDATA)>
-->

<!-- * Im System existierende GRUPPEN inkl. Referenzen auf Applikationen: * -->

<!ELEMENT group (groupdata?, description*, accounts?, appref*)>
<!ATTLIST group
        name CDATA #REQUIRED
>

<!ELEMENT groupdata EMPTY>
<!ATTLIST groupdata
        shortname CDATA #IMPLIED
        longname CDATA #IMPLIED
        type CDATA #IMPLIED
        locked (true|false) "false"
>

<!ELEMENT description (#PCDATA)>

<!ELEMENT accounts EMPTY>
<!ATTLIST accounts
        detectintruder (true|false) "false"
        lockoutafterdetection (true|false) "false"
        loginintruderlimit CDATA #IMPLIED
        intruderattemptresetinterval CDATA #IMPLIED
        intruderlockoutresetinterval CDATA #IMPLIED
>
```

```
<!ELEMENT appref EMPTY>
<!-- applikationszugehoerigkeiten -->
<!ATTLIST appref
       name CDATA #REQUIRED
>


<!-- Im System existierende USER inkl. Referenzen auf Gruppen und Applikationen: -->

<!ELEMENT user (userdata?, description*, account?, password?, groupref*, appref*)>
<!-- eindeutiger bezeichner des users -->
<!ATTLIST user
       name CDATA #REQUIRED
>

<!ELEMENT userdata EMPTY>
<!--
fullname .......... langtext, naehere bezeichnung (deprecated - künftig: longname)
firstname ......... vorname
lastname .......... nachname
email..............emailadresse
department ........ abteilung
-->
<!ATTLIST userdata
       shortname CDATA #IMPLIED
       fullname CDATA #IMPLIED
       longname CDATA #IMPLIED
       firstname CDATA #IMPLIED
       lastname CDATA #IMPLIED
       email CDATA #IMPLIED
       department CDATA #IMPLIED
>

<!-- freie beschreibung des accounts -->
<!--
<!ELEMENT description (#PCDATA)>
-->
<!ELEMENT account EMPTY>
<!--
type ..................... type, kategorie des accounts
locked ................... ist konto gesperrt (in form true/false)
lastlogin ................ datum der letzten anmeldung
gracelogins ............ anzahl erlaubter fehlgeschl. loginversuche bis konto gesperrt
creationtimestamp ....... datum wann das konto erstellt wurde
concurrentconnections ... anzahl der erlaubten gleichzeitigen logins
expirationtime............ ende der gültigkeit des accounts
-->

<!ATTLIST account
       type CDATA #IMPLIED
       locked (true|false) "false"
       lockedbyintruder (true|false) "false"
       loginintruderattempts CDATA #IMPLIED
       lastlogin CDATA #IMPLIED
       logingracelimit CDATA #IMPLIED
       gracelogins CDATA #IMPLIED
       creationtimestamp CDATA #IMPLIED
       concurrentconnections CDATA #IMPLIED
       expirationtime CDATA #IMPLIED
>

<!ELEMENT password EMPTY>
<!--
required ..................... ist passwort erforderlich (in form true/false)
changeable ................... kann pwd vom user geaendert werden (in form true/false)
minlength .................... minimallaenge des passwortes
lifetime ..................... konkretes ablaufdatum des aktuell verwendeten passwortes
lastchange ................... datum des letzten passwortwechsels
passwordexpirationinterval ... generelle gueltigkeitsdauer des passwortes (in tagen)
-->
<!ATTLIST password
```

```
        required (true|false) #REQUIRED
        changeable (true|false) #REQUIRED
        minlength CDATA #IMPLIED
        lifetime CDATA #IMPLIED
        lastchange CDATA #IMPLIED
        passwordexpirationinterval CDATA #IMPLIED
>

<!ELEMENT groupref EMPTY>
<!-- gruppenzugehoerigkeiten -->
<!ATTLIST groupref
        name CDATA #REQUIRED
>

<!ELEMENT appref EMPTY>
<!-- applikationszugehoerigkeiten -->
<!ATTLIST appref
        name CDATA #REQUIRED
>

<!ELEMENT easyarchive EMPTY>
<!-- easyarchive wert -->
<!ATTLIST easyarchive
        value CDATA #REQUIRED
>

<!ELEMENT abc-flag EMPTY>
<!-- userrelated Properties  -->
<!ATTLIST abc-flag
        flag CDATA #REQUIRED
>
```

Anhang E – Auszug einer validen XML-Datei

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<?xml-stylesheet type="text/xsl" href="TRANSFORM.xslt"?>
<system name="easy" exportdate="2008-04-06" evalfrom="2008-10-01" evalto="2008-04-01">
        <application name="Klassenlotterie">
                <userref name="Mustermann"/>
                <userref name="Musterfrau"/>
        </application>
        <user name="Mustermann">
                <appref name=" Klassenlotterie "/>
        </user>
        <user name="Musterfrau">
                <appref name=" Klassenlotterie "/>
        </user>
</system>
```

Anhang F – XSL Transformation

```
<xsl:stylesheet
    version="1.0"
    xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
    xmlns:xlink="http://www.brainsick.at/formulare"
    extension-element-prefixes="xlink">

  <xsl:output
      method="html"
      indent="yes"
      encoding="UTF-8"/>

  <xsl:template match='/'>
    <html>
      <head>
        <title>Formulare</title>
        <link rel="stylesheet" type="text/css" href="STYLE.css"/>
      </head>
      <body>
        <div class="text">SMB Zugriffsanalyse</div>
        <table id="maintable" align="center" cellspacing="0" cellpadding="0">

          <xsl:apply-templates/>

        </table>
      </body>
    </html>
  </xsl:template>

  <xsl:template match="application">
              <tr>
                     <td class="border">
                            <xsl:value-of select="@name"/>
                     </td>

                            <xsl:apply-templates select="userref"/>

              </tr>
  </xsl:template>

  <xsl:template match="application/userref">
    <tr>
        <td class="entry">
              <xsl:value-of select="@name"/>
        </td>
    </tr>
  </xsl:template>

</xsl:stylesheet>
```

Anhang G – Layout als CSS-Datei

```
body {
  background-color: #F4E4FC;
  font-family: "Arial";
  link: #003300;
  vlink: #003300;
  alink: #003300;
}

#maintable {
        width: 600px;
        border-left-width: 3px;
        border-left-style: solid;
        border-right-width: 3px;
        border-right-style: solid;
        border-top-width: 3px;
        border-top-style: solid;
        border-bottom-width: 3px;
        border-bottom-style: solid;
        border-color: #1D054E;
        padding: 2px;
        border-spacing: 0px

}

.text {
  font-family: "Arial";
  font-size: 20pt;
  font-weight: bold;
  color: #1D054E;
  text-align: "center";
  padding: 5px;
}

.border {
        background-color:#BDAFD9;
        border-top-width: 1px;
        border-top-style: solid;
        padding-left: 4px;
}

.entry {
  font-family: "Arial";
  font-size: 11pt;
  padding-left: 15px;
}
```