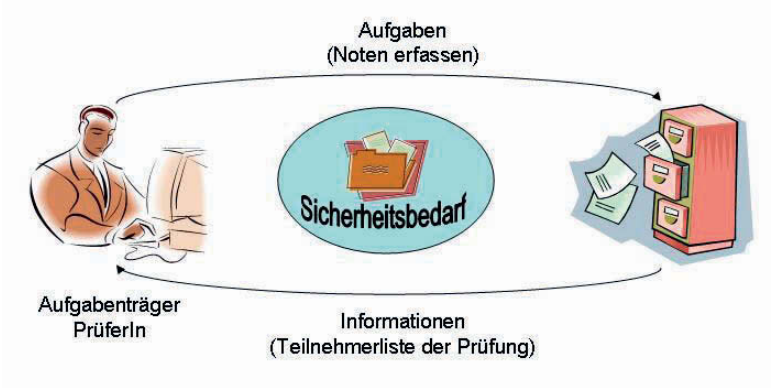
Autorisierung in Informationssystemen – woher kennt die Anwendung mich und meine Rolle?

von Dipl. Wirtsch. Inf. Gerlinde Fischer

7. Einleitung

Ein Prüfer hat nach Ende der Prüfungszeit u. a. die Aufgabe, Noten für unterschiedliche Prüfung zu erfassen. Dazu benötigt er Informationen, welche Studierenden an welcher Prüfung teilgenommen haben. In dieser Situation entsteht ein Sicherheitsbedarf, denn ein Prüfer darf nur die Informationen der Studierenden sehen, die bei ihm auch eine Prüfung abgelegt haben. Abbildung 1 stellt dieses Szenario dar.

Abbildung 1: Sicherheitsbedarf bei der Erfassung von Noten



Ein Aufgabenträger, z. B. ein Prüfer, benötigt zur Erledigung seiner Aufgaben Informationen, die im betrieblichen Informationssystem gespeichert sind. Dabei muss auf der einen Seite gewährleistet werden, dass einem Aufgabenträger alle notwendigen Informationen zur Verfügung stehen und auf der anderen Seite, dass er keine Informationen

erhält, für die er keine Autorisierung hat. Dies sicherzustellen ist eine Anforderung der Informationssicherheit.

Die Informationssicherheit wird u. a. durch die Grundfunktionen Authentifizierung und Autorisierung umgesetzt. Die Authentifizierung identifiziert den Aufgabenträger, z. B. den Prüfer, der sich an einem Computer, einem Netzwerk oder einem Anwendungssystem anmeldet. Nach der notwendigen und vorgelagerten Authentifizierung überprüft die Autorisierung die Berechtigungen des angemeldeten Aufgabenträgers in seiner Rolle, z. B. als Prüfungsausschussvorsitzender, und entscheidet, auf welche Informationen er zugreifen darf.

Obwohl Authentifizierung und Autorisierung schon seit einigen Jahrzehnten Gegenstand der Forschung sind, ergibt sich immer wieder neuer Forschungsbedarf durch sich ändernde Nutzungsszenarien und Weiterentwicklungen, wie z. B. die Verbreitung des Internets, einen hohen Grad an Vernetzung oder der Nutzung von Webservices (vgl. Feng et al. 2004, S. 357; Lehmann 2007, S. 1; Linkies und Off 2006; Strembeck und Neumann 2004, S. 393). Jeder technologische Fortschritt in der Informationstechnik bringt neue Sicherheitsbedrohungen, die neue Sicherheitslösungen erfordern. Dabei verändert sich die Technologie oftmals schneller als neue Informationssicherheitslösungen entwickelt werden können (Gasser 1988, S. 8).

Im vorliegenden Beitrag wird zunächst anhand ausgewählter Rollenkonzepte herausgearbeitet, wie sich die Rolle in das betriebliche Informationssystem, in dem Informationen verarbeitet werden, einordnen lässt. Danach werden Grundlagen der Informationssicherheit und Authentifizierung erläutert. Anschließend werden die Grundlagen und die Konzeption des auf einem rollenbasierten Zugriffskontrollmodell basierenden Autorisierungssystems FN2RBAC vorgestellt. Nach einer Zusammenfassung wird ein Ausblick auf den weiteren Forschungsbedarf gegeben.

2. Rollen im Konzept des betrieblichen Informationssystems

Für die Konzeption und Implementierung von Autoriserungssysteme für Anwendungssysteme hat sich das rollenbasierte Zugriffskontrollmodell während der letzten 15 Jahre zu einem weit verbreiteten Modell entwickelt (Coyne und Weil 2008, S. 84). **Rolle** ist dabei das zentrale Element dieses Zugriffskontrollmodells. Rolle ist zudem ein häufig verwendeter Begriff in den verschiedenen Disziplinen der Computerwissenschaft, z. B. Workflow-Systemen, Softwareentwicklung und Datenbanken. Außerhalb der Computerwissenschaft ist er z. B. präsent in den Sozialwissenschaften und der Organisationstheorie. Bedauerlicherweise gibt es keine gemeinsame Übereinstimmung über die verschiedenen Semantiken des Begriffes Rolle, die alle Nutzungen einschließt (vgl. Boella et al. 2007, S. 81; Neumann und Strembeck 2001, S. 58). Somit bezeichnet der Begriff Rolle in Abhängigkeit von Wissensgebieten zum Teil unterschiedliche, manchmal divergierende Sachverhalte (vgl. Thomas und Biddle 1966, S. 23; Lehmann 1999, S. 316; Crook et al. 2002, S. 11).

Zunächst wird die Verwendung des Begriffs Rolle in den verschiedenen Wissensgebieten vorgestellt und ein zusammenfassendes Rollenkonzept entwickelt. Nach einer Einführung in das betriebliche Informationssystem (IS) erfolgt die Einordnung der Rolle in das Konzept des IS.

2.1 Rollenkonzepte

Im Folgenden wird eine Systematisierung des Begriffs Rolle anhand von fünf ausgewählten Rollenkonzepten vorgenommen (vgl. Süßmilch-Walther und Gilleßen 2003, S. 4–16; Walther 2005, S. 6–15). Durch die verschiedenen Anwendungsgebiete lassen sich folgende Rollenkonzepte beschreiben:

- kompetenzorientiertes Rollenkonzept
- organisationsorientiertes Rollenkonzept
- aufgabenorientiertes Rollenkonzept

- verhaltensorientiertes Rollenkonzept
- berechtigungsorientiertes Rollenkonzept

Die daraus entstehende Abgrenzung der einzelnen Rollenkonzepte kann nicht als vollständig disjunkt betrachtet werden. Es bestehen durchaus Gemeinsamkeiten in Begrifflichkeiten und Themen. Allen Konzepten gemeinsam ist, dass die Rolle mehreren Aufgabenträgern, die dabei die Stellvertretung untereinander übernehmen können, zugeordnet wird. Der konkrete Aufgabenträger wird dabei erst zur Laufzeit ermittelt.

Im kompetenzorientierten Rollenkonzept werden Qualitätsanforderungen an eine Rolle definiert, die sich auf die vier Kompetenzarten Fach-, Methoden-, Sozial- und Medienkompetenz beziehen. Die Rolle verknüpft hierbei Aufgaben und Verantwortlichkeiten und beschreibt eine Grundmenge von Qualitätsanforderungen hinsichtlich Fähigkeiten und Kompetenzen, die eine Person besitzen muss, um bestimmte Aufgaben zu erfüllen (vgl. van der Aalst und van Hee 2002, S. 353; Frings und Weisbecker 1998, S. 19f; Graf 2002, S. 48). Eine Rolle definiert Erfahrungen, Kenntnisse und Fähigkeiten, die für die Durchführung von Aufgaben notwendig sind. Eine Rolle kann für mehrere Aufgaben zuständig sein, aber auch mehrere Rollen für eine Aufgabe (Frings und Weisbecker 1998, S. 19). Die Rolle **Prüfer** erfüllt u. a. die Aufgaben „Noten von Prüfungen zu erfassen“ und „Lehrveranstaltungen erzeugen“. Die Rolle **Student** und **Prüfungsamt** können beide die Aufgaben „Student zu einer Prüfung anmelden“ erledigen. Alle Aufgabenträger, die über ihre Rolle für die Bearbeitung einer bestimmten Aufgabe qualifiziert sind, können diese ausführen und sind damit austauschbar (Reichert und Dadam 2000, S. 26).

Das organisationsorientierte Rollenkonzept stellt die Aufbauorganisation in den Mittelpunkt der Betrachtung. In diesem Konzept werden Stellen mit ähnlichen organisatorischen Charakteristika wie Kompetenzen und Qualifikationen, die sich z. B. auf der gleichen hierarchischen Ebene oder in der gleichen organisatorischen Einheit befinden, zu Rollen

zusammengefasst (vgl. Galler 1997, S. 52; Rupietta und Wernke 1994, S. 143; Walther 2005, S. 11). Eine Rolle kann beliebig vielen Aufgabenträgern unabhängig voneinander zugewiesen werden, so dass Aufgabenträger mit gleichen Rollen in funktionsmäßiger, räumlicher und zeitlicher Art die Stellvertretung übernehmen können (vgl. Blümle 1975, S. 1888; Reichert und Dadam 2000, S. 27; Walther 2005, S. 11). Eine Rollenzuordnung ist nicht statisch: so kann ein Aufgabenträger im Laufe seines Arbeitslebens unterschiedliche Rollen einnehmen, aber auch zum gleichen Zeitpunkt mehreren Rollen zugeordnet sein (van der Aalst und van Hee 2002, S. 15). Durch dieses Konzept sind Prozess- und Organisationsdefinition voneinander getrennt. „Wenn ein neuer Mitarbeiter in das Unternehmen eintritt, muss man nicht die Prozessdefinition ändern, sondern" nur die entsprechende Rolle zuordnen (Walther 2005, S. 12).

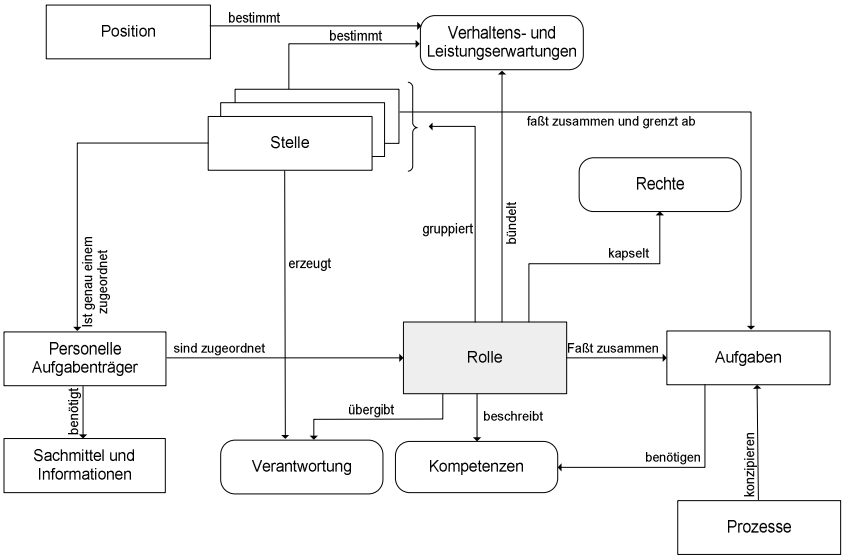
Im aufgabenorientierten Rollenkonzept stellt die Rolle eine Zusammenfassung von Aufgaben dar, die einem Aufgabenträger, der diese Aufgaben erledigen soll, zugeordnet werden können. Einem Aufgabenträger können auch mehrere Rollen zugeordnet werden (Esswein 1992, S. 8). Eine Rolle kann definiert werden als eine Menge von Funktionen, die mit einer speziellen Aufgabe verknüpft sind (Ahn und Sandhu 2000, S. 208).

Im verhaltensorientierten Rollenkonzept ist eine Rolle ein sozialwissenschaftlicher Begriff zur Kennzeichnung eines Systems von Verhaltensregeln, die meist durch Erwartungen definiert werden. Diese Erwartungen werden an den Inhaber einer bestimmten Position herangetragen (Alisch 2004, S. 2565). Die Verhaltensregeln und Erwartungen werden über die Rolle auf eine Person projiziert. In einem Unternehmen sind diese Verhaltens- und Leistungserwartungen in einer Stelle gebündelt und richten sich an einen potentiellen Aufgabenträger (vgl. Bokranz und Kasten 2001, S. 51; Schreyögg 2008, S. 102). Eine Stelle konkretisiert damit die Rollenerwartungen eines Unternehmens an einen Mitarbeiter (Picot et al. 1997, S. 167).

Im berechtigungsorientierten Rollenkonzept steht die Vergabe von Zugriffsrechten im Fokus (SAP 06.07.2007). Die Rolle kapselt hierbei Berechtigungen, Verantwortlichkeiten und Verpflichtungen innerhalb eines IS (Nyanchama und Osborn 1996, S. 131). Die Rolle bündelt dabei Zugriffsrechte, die sich auf Funktionen eines Anwendungssystems (AwS) beziehen. Diese Funktionen bestehen aus Objekten und ihren Operatoren. Anschließend werden diese Rollen den Aufgabenträgern zugeordnet. Vor Aufruf einer Funktion im AwS muss das Autorisierungssystem eine Rechteprüfung anhand der Parameter Aufgabenträger, Objekt und Operator durchführen und entscheiden, ob dem Aufgabenträger das Recht auf Zugriff eingeräumt wird.

Zusammenfassend lassen sich die unterschiedlichen Rollenkonzepte (Abbildung 2) wie folgt beschreiben: Rollen werden personellen Aufgabenträgern zugeordnet und kapseln die Berechtigungen, die ein Aufgabenträger erhalten soll. Aufgaben werden aus den Prozessen heraus konzipiert und werden in Stellen und/ oder Rollen zusammengefasst. Die Aufgaben werden über die beiden Konstrukte personellen Aufgabenträgern zugeordnet. Personelle Aufgabenträger benötigen zur Erledigung ihrer Aufgaben Sachmittel und Informationen. Eine Rolle beschreibt die notwendigen Kompetenzen zur Erledigung einer Aufgabe. Durch eine Rolle wird Verantwortung an einen Aufgabenträger übergeben. Eine Stelle erzeugt bei der Zuordnung zu einem Aufgabenträger Verantwortung. Stellen bzw. eine Position, die genau einem Aufgabenträger zugeordnet ist, bestimmt die Verhaltens- bzw. Leistungserwartungen für diesen Aufgabenträger.

Abbildung 2: Zusammenfassung der Rollenkonzepte nach (Walther 2005, S. 6–15)



Um eine Einordnung der Rolle in das betriebliche Informationssystem (IS) vornehmen zu können, wird im folgenden Kapitel zunächst das Konzept des IS vorgestellt, um anschließend ein ganzheitliches Rollenkonzept zu entwickeln.

2.2 Konzept des betrieblichen Informationssystems

Informationssysteme sind Systeme, die Informationen verarbeiten, z. B. erfassen, speichern und bereitstellen. Der Einsatz findet in Organisationen der Wirtschaft und Verwaltung statt und darüber hinaus durch die zunehmende Vernetzung auch überbetrieblich. Diese Informationssysteme werden als betriebliche Informationssysteme (IS) bezeichnet und betrachten den Zusammenhang zwischen Aufgaben und deren Zuordnung zu Aufgabenträgern (Ferstl und Sinz 2006, S. 1). Das IS beruht auf

Aufgabenobjekten des Typs Information, die für die Verrichtung einer Aufgabe notwendig sind oder bearbeitet werden müssen. Ein IS enthält eine Menge von Informationsverarbeitungsaufgaben, die durch Informationsbeziehungen verbunden sind. Die Menge aller Aufgaben zusammen mit den Informationsbeziehungen bilden die Aufgabenebene eines IS. Ein IS enthält daneben eine Menge von Aufgabenträgern[1], die durch Kommunikationssysteme verbunden sind. Die Aufgabenträger lassen sich in zwei Arten unterteilen:

- Maschinelle Aufgabenträger - Rechner, Rechnersysteme
- Personelle Aufgabenträger - Personen, wie Sachbearbeiter, Manager (Ferstl und Sinz 2001, S. 2f).

> „Die Menge aller Aufgabenträger bildet die Aufgabenträgerebene eines IS“ (Ferstl und Sinz 2006, S. 4).

Typischerweise ist bei der Durchführung betrieblicher Aufgaben eine Kooperation maschineller und personeller Aufgabenträger notwendig. Durch die Zuordnungsbeziehung zwischen Aufgaben und Aufgabenträgern wird der Grad der Automatisierung bestimmt.

- vollautomatisiert: Eine Aufgabe wird vollständig von maschinellen Aufgabenträgern durchgeführt.
- teil automatisiert: Personelle und maschinelle Aufgabenträgern führen eine Aufgabe gemeinsam aus.
- nicht automatisiert: Ausschließlich personelle Aufgabenträger sind an der Durchführung der Aufgabe beteiligt (Ferstl und Sinz 2001, S. 48).

> „Eine Informationsbeziehung zwischen zwei Aufgaben wird auf Aufgabenträgerebene bei unterschiedlichen Aufgabenträgern durch einen Kommunikationskanal zwischen diesen realisiert.“ (Ferstl und Sinz 2006, S. 4)

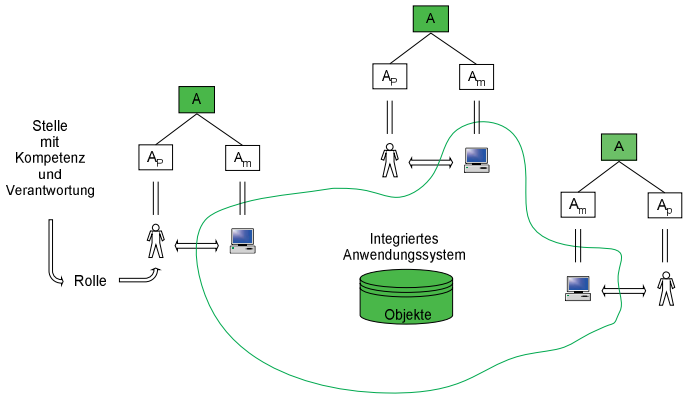
[1] Eine ausführliche Beschreibung des Begriffs Aufgabenträger findet sich in *(Schwarz H 1980)*.

Man unterscheidet:

- Kommunikation C-C zwischen Rechner
- Kommunikation M-C zwischen Person und Rechnern und
- Kommunikation M-M zwischen Personen (Ferstl und Sinz 2006, S. 4).

Damit stellt sich die Frage, an welchen Stellen im IS ist eine Zugriffskontrolle notwendig? Teilautomatisierte Aufgaben (A) eines betrieblichen Informationssystems (IS) werden personellen und maschinellen Aufgabenträgern zugeordnet. Aufgaben für einen personellen Aufgabenträger (A_P) werden in einer Stelle zusammengefasst, die mit Kompetenz und Verantwortung ausgestattet ist. Der automatisierte Teil der Aufgaben wird von maschinellen Aufgabenträgern (A_m) durchgeführt. Diese werden zu einem integrierten Anwendungssystem (AwS) zusammengefasst.

Abbildung 3: Teilautomatisierte Aufgaben im IS



Die Objekte des AwS sind vor unerlaubten Zugriffen durch ein Autorisierungssystem zu schützen. Zur Verrichtung teilautomatisierter Aufgaben ist eine Mensch-Maschinen-Kommunikation erforderlich, da ein

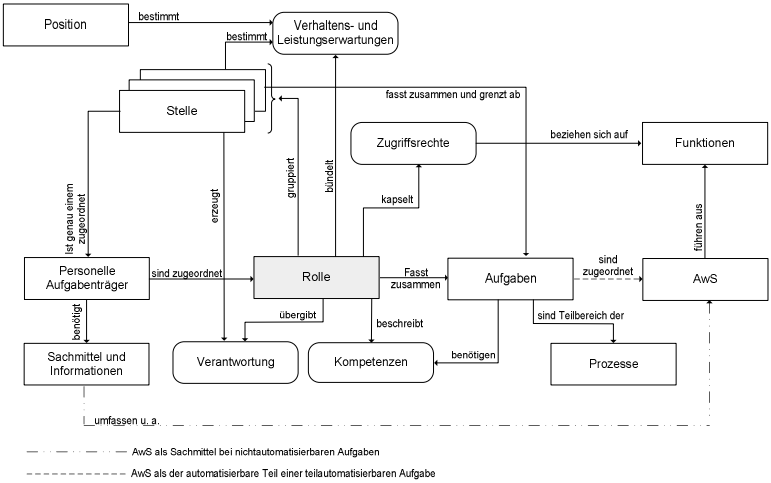
personeller Aufgabenträger mit einem maschinellen Aufgabenträger „kommuniziert“. An dieser Schnittstelle muss zur Gewährleistung der Informationssicherheit eine Authentifizierung und eine Autorisierung durchgeführt werden.

Zusätzlich zum Aspekt von teilautomatisierten Aufgaben besteht eine Mensch-Maschinen Kommunikation innerhalb eines IS, wenn ein Anwendungssystem als Sachmittel verwendet wird, um eine nicht automatisierbare Aufgabe zu lösen oder die dafür notwendigen Informationen im IS zu finden sind. Beide Aspekte werden in den folgenden Ausführungen berücksichtigt. Aus der organisatorischen Einbettung des personellen Aufgabenträgers und seiner Aufgaben lassen sich Rollen herleiten, die bei einer Mensch-Computer-Interaktion dafür sorgen, dass nur Objekte verfügbar sind, die ein personeller Aufgabenträger sehen bzw. bearbeiten darf.

2.3 Einordnung der Rolle in das betriebliche Informationssystem

Zunächst wird das im vorherigen Kapitel herausgearbeitete Rollenkonzept (siehe Abbildung 2) in Abbildung 4
um Anwendungssysteme und deren Funktionen erweitert, um anschließend eine Einordnung in das betriebliche Informationssystem vorzunehmen. Ein AwS kann in Funktionen zerlegt werden. Funktionen in diesem Sinne sind Elemente von Vorgängen, die funktional beschreibbar sind (Ferstl und Sinz 2006, S. 59–60). Diese Funktionen können als fachliche Objekte und den darauf wirkenden Operatoren betrachtet werden, z. B. Datenblatt des Studenten ausdrucken. Operatoren sind die nach außen gelegten Methoden, mit denen die Datenobjekte manipuliert und aufgerufen werden können. Die nach außen hin sichtbaren Objekte mit ihren Operatoren sind die Funktionen eines Anwendungssystems.

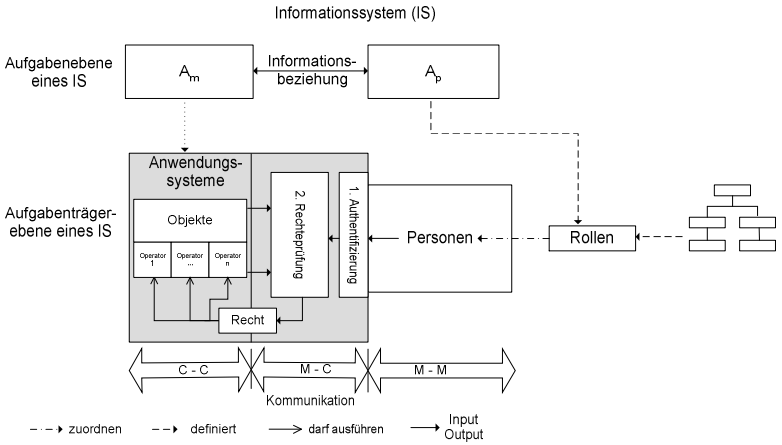
Abbildung 4: Einordnung des Anwendungssystem in ein ganzheitliches Rollenkonzept



Zugriffsrechte beziehen sich auf die extern aufrufbaren Funktionen, die in ihrer Gesamtheit das AwS darstellen. Diese Zugriffsrechte werden in Rollen gekapselt. Während der Laufzeit entscheidet das Autorisierungssystem, ob der Zugriff erlaubt ist oder nicht.

Die Einordnung von Authentifizierung und Autorisierung in das IS stellt Abbildung 5 dar. Rollen werden anhand der Aufgaben und der Organisationsstruktur innerhalb des IS ermittelt, Personen zugeordnet und beides in der Rechteverwaltung gespeichert. An der Schnittstelle M-C wird zuerst die Authentifizierung durchgeführt. Eine Person gibt zum Authentifizieren die Zugangsdaten an der Schnittstelle bekannt. Das Authentifizierungssystem überprüft die Identität. Nach erfolgreicher Authentifizierung findet die Rechteprüfung durch ein Autorisierungssystem statt. Es wird geprüft, ob der personelle Aufgabenträger die aufgerufene Funktion ausführen darf. Jeder Zugriff auf das Anwendungssystem erfolgt über die Rechteprüfung und wird dabei protokolliert.

Abbildung 5: Einordnen von Authentifizierung und Zugriffskontrolle in ein IS.



Authentifizierungs- und Autorisierungssysteme zusammen gewährleisten u. a. die Informationssicherheit. Im nächsten Kapitel werden Grundlagen der Informationssicherheit und insbesondere in Anwendungssystemen erläutert und ein kurzer Überblick über die Authentifizierung gegeben.

3. Informationssicherheit in Anwendungssystemen

Die Sachziele der Informationssicherheit, Vertraulichkeit, Integrität, Verbindlichkeit und Verfügbarkeit zu erfüllen und einen umfassenden Datenschutz zu gewährleisten, sind zentrale Aufgaben und Herausforderungen der Informationsgesellschaft und von strategischer Bedeutung für Unternehmen und Verwaltungen. Deshalb hat der Bereich der Informationssicherheit und insbesondere die Zugriffskontrolle in den letzen Jahren zunehmende Aufmerksamkeit in der Forschung erfahren (Zannone et al. 2006, S. 1; Junk und Mayer 2003, S. 5). Die Sicherheit der Daten in Anwendungssystemen wird zu einem notwendigen Bestandteil für eine integrierte, umfassende und unternehmensweite In-

formationssicherheit (Kern et al. 2004, S. 87), deshalb müssen sich Zugriffsrechte auf die Funktionsebene eines Anwendungssystems beziehen (Beresnevichiene 2003, S. 12).

> Die Informationssicherheit „ist und bleibt damit ein ‚Schlüssel' für die Zukunft der Informationsgesellschaft und dürfte – sowohl in Theorie als auch in der Praxis – weiter an Bedeutung gewinnen" (Sackmann 16.09.2008).

Bei der Diskussion um Informationssicherheit darf nicht übersehen werden, dass es eine hundertprozentige Sicherheit nicht gibt (Landwehr et al. 1984, S. 198).

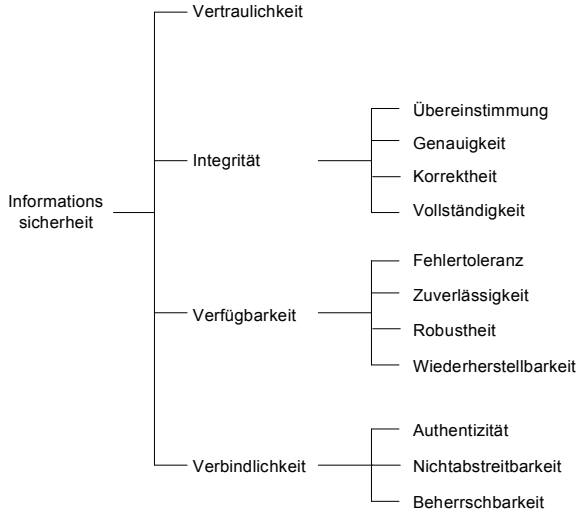
> Informationssicherheit „bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Gefährdungen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß beschränkt sind" (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2005, S. 42).

Durch die rasante Entwicklung in der Informationstechnologie können nicht alle in der Zukunft zu erwartenden Angriffe und Möglichkeiten erkannt und deren Auswirkungen abgeschätzt werden. Informationssicherheit ist ein dynamischer Prozess und ein dynamisches Betrachtungsobjekt, die Entwicklung neuer Sicherheitsmechanismen folgt laufend der technischen Entwicklung (Gasser 1988, S. 8; Sackmann 16.09.2008).

3.1 Ziele und Grundfunktionen der Informationssicherheit

Im Bereich der Informationssicherheit werden Begriffe zum Teil uneinheitlich benutzt. Eine ausführliche Taxonomie der deutschen Begriffe auf Grundlage ausgewählter internationaler Normen findet sich in (Pohl 2004; Schier 1999, S. 30–32). Als allgemeiner Konsens haben sich in der Literatur die folgenden vier Sachziele der Informationssicherheit herauskristallisiert: Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit (Pohl 2004, S. 679; Raepple 2001, S. 4). Die Sachziele Integrität, Verfügbarkeit und Verbindlichkeit werden in weitere Komponenten zerlegt. Abbildung 6 zeigt diese Komponenten im Überblick.

Abbildung 6: der Informationssicherheit mit ihren Komponenten nach (Pohl 2004, S. 680)



Vertraulichkeit ist der Schutz vor unberechtigtem Informationsgewinn, d. h. Informationen sind nur für Berechtigte zugänglich. Dabei muss auch der Schutz während der Übertragung von Information über Netzwerke gewährleistet werden. Vertraulichkeit beinhaltet keine weiteren Komponenten.

Integrität stellt die Genauigkeit, Korrektheit und Vollständigkeit von Informationen und Verfahren sicher. Daten werden nicht unberechtigt verändert, gelöscht oder zerstört. Daneben muss die Übereinstimmung zwischen tatsächlichem Wert eines Objektes und dem verarbeitenden bzw. gespeicherten Wert bestehen. Integrität setzt sich zusammen aus:

- **Datenintegrität:** Sie umfasst die Sicherstellung der Korrektheit, also Unversehrtheit von Daten. Die Daten müssen vor der unberechtigten Modifikation geschützt werden.

- **Systemintegrität:** Sie bezieht sich auf eine korrekte Funktionsweise eines AwS. Systemsicherheit ist die Voraussetzung für Datenintegrität.

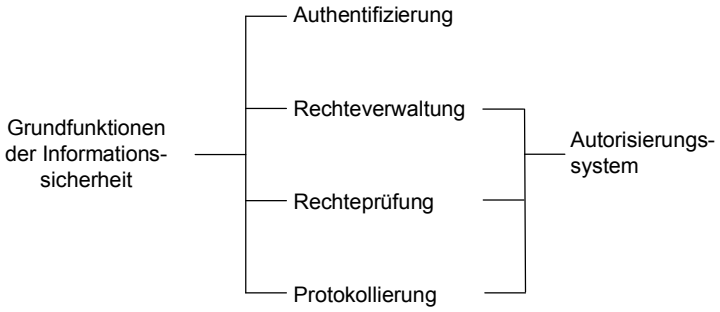
Verfügbarkeit stellt sicher, dass alle benötigten Daten sowie die zur Verarbeitung notwendigen Anwendungssysteme und Betriebsmittel jederzeit verfügbar und funktionsbereit sind, wenn ein autorisierter Nutzer zugreifen will. Die Komponenten der Verfügbarkeit sind: Zuverlässigkeit, Fehlertoleranz, Robustheit und Wiederherstellbarkeit. Diese müssen durch die Funktionssicherheit des AwS gewährleistet werden.

Verbindlichkeit ist die Eigenschaft eines Systems, zurechenbare, rechtsverbindliche Kommunikation zu unterstützen. Sie schützt den Sender gegen Täuschung und es gibt keine Möglichkeit des Abstreitens durch Sender und Empfänger. Durch Verbindlichkeit werden in einem Informationssystem alle versuchten und erfolgten Aktivitäten, wie Zugriffe von Subjekten auf Objekte, nachvollziehbar beschrieben. Dabei werden Aktivitäten Subjekten zugeordnet und es wird die Erkennung und Untersuchung von Angriffen ermöglicht. Grundlage für die Verbindlichkeit sind Authentizität, Nichtabstreitbarkeit und Revisionsfähigkeit (Eckert 2001, S. 5–9; Pohl 2004, S. 679–680).

Im Kontext der Informationssicherheit von Anwendungssystemen sind die Sachziele Vertraulichkeit, Integrität und Verbindlichkeit sicherzustellen. Die Informationssicherheit von Anwendungssystemen setzt voraus, dass die Systemintegrität bzw. Funktionssicherheit des AwS gewährleistet ist, d. h. Ist- und Soll-Funktionalität des AwS stimmen überein. Neben dem AwS selbst muss die Verfügbarkeit durch die Installation, die Einbettung in die Rechnerarchitektur und geeignete Notfallkonzepte sichergestellt werden. Die Informationssicherheit sichert darauf aufbauend, dass es zu keiner unautorisierten Informationsveränderung oder Informationsgewinnung kommen kann (Eckert 2008, S. 4–5).

Die Sachziele der Informationssicherheit werden durch die Grundfunktionen Authentifizierung sowie Autorisierung bestehend aus Rechteverwaltung, Rechteprüfung und Protokollierung (Audit) erreicht:

Abbildung 7: Grundfunktionen der Informationssicherheit (Pohl 2004, S. 682)



Die Authentifizierung übernimmt die Identitätsprüfung eines Subjektes und stellt die vorgegebene Identität sicher (Eckert 2008, S. 7). Sie überprüft die Echtheit einer Person, einer Organisation oder eines Programms. Um unerlaubte Zugriffe auf ein System zu verhindern, müssen Subjekte eindeutig identifizierbar sein. Die Authentifizierung legt nicht fest, welche Funktionen innerhalb eines Systems einem Subjekt zur Verfügung stehen. Das Thema der Authentifizierung ist Teil der Systemumgebung. Das Verfahren der Authentifizierung muss vom Autorisierungssystem vollständig getrennt sein, ist diesem zwingend vorgelagert und eine notwendige Voraussetzung für eine funktionierende Zugriffskontrolle (Essmayr et al. 2004, S. 132).

Die Rechteverwaltung bildet die Datenbasis für die Rechteprüfung zur Abwehr von Bedrohungen für die Informationssicherheit infolge von unautorisierten Zugriffen auf Objekte. Die Rechteverwaltung speichert Informationen über die zu schützenden Objekte und Operatoren und wird anhand der von der Sicherheitsstrategie festgelegten Richtlinien modelliert und implementiert. Sie hat sicherzustellen, dass alle Subjekte

und Objekte, für die Zugriffsbeschränkungen festgelegt sind, auch von der Rechteverwaltung erfasst wird (Eckert 2001, S. 92, 375).

Die Rechteprüfung überprüft bei jedem Zugriff, ob ein Subjekt s das Objekt o mit dem Operator op aufrufen darf und stützt sich auf die gespeicherten Daten der Rechteverwaltung. Die Rechteprüfung überprüft die Funktionen, die aufgerufen werden, führt die notwendigen Kontrollen durch und entscheidet anschließend, welche Funktionen ausgeführt werden dürfen. Zwischen der Rechteprüfung und der Ausübung des Zugriffsrechts darf keine weitere Aktion möglich sein (Eckert 2001, S. 92–93). Ist die Authentifizierung nur unzureichend gewährleistet, wird auch die Rechteprüfung als gescheitert angesehen.

Um eine nachträgliche Analyse der Zugriffe zu ermöglichen, müssen alle Zugriffe und ausgeführten Funktionen protokolliert werden. Im Anschluss an die Rechteprüfung wird die Protokollierung des Zugriffes vorgenommen, so dass, wenn notwendig, eine Verbindlichkeit hergestellt werden kann. Die Beweissicherung legt fest, welche Ereignisse und Informationen zu protokollieren sind. Die Identität eines Subjektes, die aufgerufenen Objekte mit den dazugehörigen Operatoren und der dazugehörige Zeitpunkt einer Aufrufanforderung sind mindestens zu protokollieren (Eckert 2001, S. 93).

Eine Herausforderung bei der Gewährleistung der Informationssicherheit im AwS ist die höhere Komplexität der Zugriffkontrolle im Gegensatz zur Zugriffskontrolle in Betriebssystemen. In Betriebssystemen gibt es viele Subjekte, viele Objekte, jedoch nur wenige Operatoren, wie z. B. „lesen“ oder „schreiben“. Bei der Zugriffskontrolle im AwS gibt es viele Subjekte, viele Objekte und viele verschiedene Operatoren. Autorisierungssysteme für Anwendungssysteme sind zudem oftmals anwendungsspezifisch und damit proprietär gestaltet (Kern et al. 2004, S. 88f).

3.2 Grundlagen der Authentifizierung

Unter Authentizität eines Subjekts wird die Echtheit und Glaubwürdigkeit verstanden, die anhand seiner eindeutigen Identität und seiner charakterisierenden Eigenschaften überprüfbar ist. Mit der Authentifizierung wird ein Subjekt mit einer eindeutigen Kennung verbunden. Es muss die Authentifizierungsinformation, z. B. Passwörter von den Identifikationsinformationen getrennt aufbewahren, da Passwörter geheim, die Kennungen aber öffentlich sind (Gasser 1988, S. 23). Die Authentifizierung überprüft mit geeigneten Methoden die Korrektheit der behaupteten Identität eines Gegenübers und ermittelt damit die Quelle einer Anfrage. Die Authentifizierung ist der Autorisierung vorgeschaltet und muss durch die Systemarchitektur sichergestellt werden (Essmayr et al. 2004, S. 129).

Eine Authentifizierung kann an Hand verschiedener Merkmale durchgeführt werden. In der Praxis werden zur Authentifizierung folgende drei Merkmale verwendet: Kenntnis spezifischen Wissens (Passwort), persönlicher Besitz (Chipkarte), Biometrie: Überprüfung eines bestimmten Merkmales oder Verhaltens, z. B. körperliches Merkmal (Fingerabdruck) oder typische Bewegungsmuster (Tastenanschlag). Darüber hinaus existieren Kombinationen der oben genannten Merkmale, beispielsweise eine Chipkarte (Besitz) zusammen mit einem PIN (Passwort) oder ein Ausweis zusammen mit biometrischen Merkmalen (Eymann 2004, S. 10; Müller 2005, S. 173ff).

Verfahren, die eine Authentifizierung mit Hilfe von Wissen realisieren, sind unter anderem Passwort, PIN, Einmalpasswort, Challenge-Response und One Time PIN Token (SecureID) (Eckert 2001, S. 307–321; Eckert 2008, S. 442). Häufig wird eine Authentifizierung mittels Passwort durchgeführt (Müller 2005, S. 174). Bekannteste Vertreter der Verfahren, die einen Besitz überprüfen, sind Chipkarten oder Smartcards, daneben gibt es noch Magnetstreifenkarte, Krypto-Token, Schlüs-

sel, RFID-Karte, Zertifikate[2] (Eymann 2004, S. 10; Müller 2005, S. 173). Biometrie bezeichnet zusammenfassend die Überprüfung persönlicher Merkmale oder persönliches Verhalten. Verfahren für die Überprüfung durch Biometrie finden derzeit enormen Aufschwung. Beispiele sind Fingerabdruck, Gesichtserkennung, Tastaturanschlag, DNA, Stimme, Handlinienstruktur und Augen-Netzhaut-Identifizierung.

Aus den verschiedenen Authentifizierungsverfahren wird das am häufigsten in der Praxis anzutreffende Passwortverfahren als Beispiel für die Authentifizierung durch die Kenntnis spezifischen Wissens beschrieben. Ein Subjekt authentifiziert sich mittels eines Passwortes, durch Austausch eines Geheimnisses, an einem Rechner, zwischen Arbeitsplatzrechner und Server oder in einem Netzwerk. Das System, das eine Authentifizierung vornimmt, hat die Passwörter sicher zu verwalten. Es werden kryptographische Methoden eingesetzt, um Passwörter zu verschlüssseln und damit sicher zu speichern.

Abbildung 8: Eingabedialog für Kennung und Passwort im ZUV-Portal der Universität Bamberg

[2] Eine verteilte Authentifizierung über Zertifikate wird in dieser Arbeit nicht behandelt, dazu wird auf die Literatur verwiesen (Rieger S 2007).

Um einen Mindeststandard an Sicherheit zu gewährleisten, sind u. a. folgende Anforderungen an Passwörter zu stellen: Mindestlänge acht Zeichen, kein Eigenname oder eigene Vor- oder Nachnamen, mindestens ein Sonderzeichen, möglichst viele unterschiedlichen Zahlen und Buchstaben und eine geringe Anzahl von Fehlversuchen beim Login (Eckert 2001, S. 309–310).

Nach der Authentifizierung am Arbeitsplatzrechner kann bei der Weitergabe der Passwörter in Netzwerken das Konzept der Einmal-Passwörter verwendet werden oder bei der Authentifizierung von Chipkarten das Challenge-Response-Verfahren verwendet werden[3].

4. Konzeption eines Autorisierungssystems

Nach einer erfolgreichen Authentifizierung wird durch das nachgelagerte Autorisierungssystem entschieden, welche Anwendung und welche Berechtigungen innerhalb einer Anwendung einem Aufgabenträger zur Erledigung seiner Aufgaben zur Verfügung stehen.

4.1 Grundlagen eines Autorisierungssystems

Ausgangspunkt jedes Autorisierungssystems bildet die Sicherheitsstrategie.

> Sicherheitsstrategie ist die Formulierung von „Schutzzielen und allgemeinen Sicherheitsmaßnahmen im Sinne offizieller Vorgaben eines Unternehmens oder einer“ Verwaltung (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2005, S. 8(Glossar)).

Die Sicherheitsstrategie beinhaltet Gesetze und Regeln, die definieren, wie eine Organisation ihre Informationen sicher verwaltet (Eckert 2001, S. 13). Um aus der Sicherheitsstrategie und der Geschäftspolitik heraus

[3] Für ein vertiefendes Studium über die Funktionsweise von Einmal-Passwörtern (Haller NM, Metz C et al. 1998) und des Challenge-Response-Verfahrens (Eckert C 2001, S. 320–323; Rankl W, Effing W 2002, S. 221–223) wird auf die Literatur verwiesen.

ein Autorisierungssystem zu entwickeln, wird dieser Vorgang in drei Abstraktionsebenen eingeteilt.

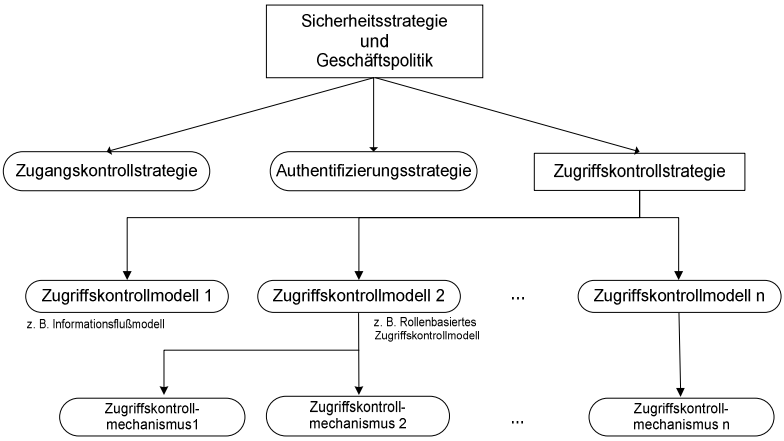
- Zugriffskontrollstrategie
- Zugriffskontrollmodelle
- Zugriffskontrollmechanismen

Die allgemeine Sicherheitsstrategie und die Geschäftspolitik beeinflussen die Zugangskontrollstrategie, Authentifizierungsstrategie und die Zugriffskontrollstrategie. Abbildung 9 zeigt den Weg von der Sicherheitsstrategie zum Zugriffskontrollmechanismus. Die Zugriffskontrollstrategie definiert auf abstrakter Ebene die Zielsetzung, Vorgehensweise und das Entscheidungsverfahren bei der Umsetzung der Zugriffskontrolle (Seufert 2001, S. 30). Die Zugriffskontrollstrategie sollte nicht entsprechend der technischen Sicherheitskonzepte beschrieben werden, sondern die Sicherheitsstrategie des Unternehmens reflektieren. Der Zugriffskontrollmechanismus führt die Rechteprüfung anhand der in der Rechteverwaltung gespeicherten Informationen durch und erlaubt oder verbietet einen Zugriff.

Um die große Lücke der Abstraktion zwischen Strategie und Mechanismus zu schließen, wurden formale Zugriffskontrollmodelle entwickelt. Für alle drei hier genannten Zugriffskontrollstrategien haben sich in Laufe der Zeit verschiedene Zugriffskontrollmodelle mit zahlreichen Varianten herausgebildet.

> „Die Untersuchung komplexer Systeme erfolgt im Allgemeinen nicht direkt durch Eingriff in das System, sondern indirekt anhand eines geeigneten Modells“ (Ferstl und Sinz 2006, S. 20).

Abbildung 9: Von der Sicherheitsanforderung zum Zugriffsmechanismus nach (Seufert 2001, S. 30)



Dies gilt ebenso für die Untersuchung von Zugriffskontrollsystemen. Ein Zugriffskontrollmodell[4] (access control model) ist ein formales Modell oder ein Beschreibungsrahmen, mit dessen Hilfe eine Zugriffskontrollstrategie spezifiziert werden kann, um diese automatisiert durchführen zu können. Zugriffskontrollmodelle werden auf einer Abstraktionsebene beschrieben, um eine große Vielseitigkeit bei der Implementierung in unterschiedlichen Computerumgebungen zu ermöglichen. Ein Zugriffskontrollmodell kann eine oder mehrere Zugriffskontrollstrategien unterstützen (Osborn et al. 2000). Ein Zugriffskontrollmodell kann sowohl die Rechteverwaltung als auch die Rechteprüfung umfassen.

Im Laufe der Zeit wurden mehrere Zugriffskontrollmodelle entwickelt und untersucht. Wie in Kapitel 2 dargestellt, eignet sich das Konzept der Rolle und damit das rollenbasierte Zugriffskontrollmodell zur Bündelung der Zugriffsrechte, um ein aufgabenorientierten Autorisierungs-

[4] „Access control model“ wird in dieser Arbeit mit Zugriffskontrollmodell übersetzt, in der Literatur, z. B. in (Seufert SE 2001, S. 35), findet sich auch der Begriff Zugriffskontrollansatz.

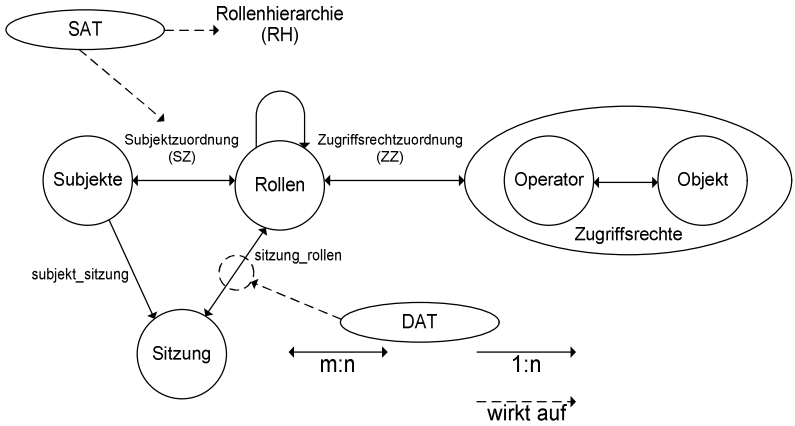
system umzusetzen. Dieses ausgewählte Zugriffskontrollmodell wird im folgenden Kapitel kurz vorgestellt.

4.2 Rollenbasiertes Zugriffskontrollmodell

Die Entitäten und deren Beziehungen des Kernmodells des rollenbasierten Zugriffskontrollmodells (RBAC) sind in
dargestellt. Das Kernmodell umfasst folgende Basiselemente: Nutzer bzw. Subjekte, Rollen, Objekte, Operatoren, Zugriffsrechte und Sitzung.

Nutzer oder Subjekte sind im Kernmodell als personelle Aufgabenträger (siehe Kapitel 3.1) definiert. Rollen definieren im Kernmodell eine Beziehung zwischen Subjekten und Zugriffsrechten. Eine *Rolle* ist eine Funktion innerhalb des Kontextes einer Organisation, die Autorität und Verantwortung an das zugeordnete Subjekt überträgt (ANSI INCITS 359-2004 01.03.2004, S. 3).

Abbildung 10: Komponenten des rollenbasierten Zugriffskontrollmodells



Die Objekte und die Operatoren hängen allein von dem zu schützenden Anwendungssystem ab und bestimmen das zu implementierende Auto-

risierungssystem (ANSI INCITS 359-2004 01.03.2004, S. 3). In einem Anwendungssystem, wie z. B. dem Prüfungsverwaltungssystem „FlexNow", ist ein Objekt ein Datenblatt eines Studenten und die Operatoren, die darauf angewendet werden können, sind: „bearbeiten", „drucken" und „lesen".

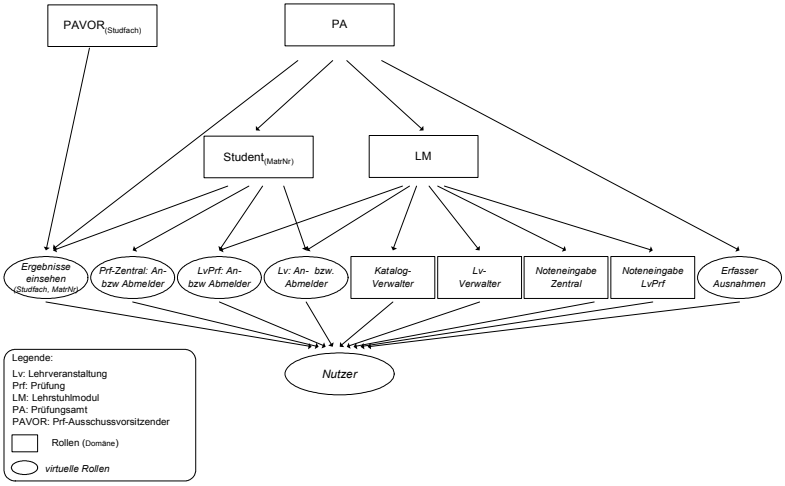
Zugriffsrechte sind Genehmigungen, eine *Operation* auf einem oder mehreren von einem auf RBAC aufbauenden Autorisierungssystem geschützten *Objekten* ausführen zu dürfen (ANSI INCITS 359-2004 01.03.2004, S. 3). Ein RBAC-Zugriffskontrollmodell funktioniert nach dem Erlaubnisprinzip, d.h. ist ein Recht nicht vorhanden, wird der Zugriff verweigert.

Zentrales Konzept des RBAC ist die Rollenbeziehung, dabei formuliert die Rolle die umzusetzende Zugriffskontrollstrategie. Zwischen Subjekten und Rollen (*Subjektzuordnung)* und zwischen Rollen und Zugriffsrechten (*Zugriffsrechtzuordnung)* besteht eine sogenannte m:n-Beziehung. Einem Subjekt kann mehr als eine Rolle zugeordnet sein und einer Rolle können mehrere Subjekte zugeordnet werden. Dies liefert eine hohe Flexibilität bei der Zuordnung von Zugriffsrechten zu Rollen und Subjekten zu Rollen, um den Zugang zu Ressourcen zu kontrollieren (ANSI INCITS 359-2004 01.03.2004, S. 4).

Eine *Sitzung* ist eine Verbindung zwischen einem Subjekt und der aktivierten Teilmenge von Rollen, die einem Subjekt zugeordnet sind und bildet genau ein Subjekt mit allen aktivierten Rollen ab. Ein Subjekt kann beliebig viele Sitzungen eröffnen. Die daraus verfügbaren Zugriffsrechte sind die von den aktivierten Rollen über alle Sitzungen hinweg aktivierten Zugriffsrechte (ANSI INCITS 359-2004 01.03.2004, S. 4). Das Kernmodell alleine reicht oftmals nicht aus, um ein umfassendes Autorisierungssystem implementieren zu können. Daher sieht auch der Standard bereits die Rollenhierarchie und die Aufgabentrennung als Erweiterung vor.

Die Rollenhierarchie (RH) erweitert das Kernmodell (ANSI INCITS 359-2004 01.03.2004, S. 5). Die Rollenhierarchie ist eine Möglichkeit, um eine organisatorische Beziehung von Autorität und Verantwortlichkeit wiederzuspiegeln (Ferraiolo et al. 2001, S. 234). Rollenhierarchien definieren eine Vererbungsbeziehung zwischen Rollen (ANSI INCITS 359-2004 01.03.2004, S. 235).

Abbildung 11: Rollenhierarchie in einem Autorisierungssystem eines Prüfungsverwaltungssystems



Zusätzlich kann die Aufgabentrennung orthogal zur Rollenhierarchie hinzugefügt werden. Das Konzept der Aufgabentrennung wird benötigt, um Strategien zur Verhinderung von Interessenskonflikten durchzusetzen. Zudem dürfen kritische Aufgaben in einem Unternehmen nicht

von ein und derselben Person ausgeführt werden.[5] Es gibt zwei Kategorien von Rollenbeschränkungen:

- eine statische (SAT) und
- eine dynamische Aufgabentrennung (DAT).

Bei einer statischen Aufgabentrennung wird bereits bei der Subjektzuordnung verhindert, einem Subjekt konfliktäre Rollen zuzuordnen. Bei einer dynamischen Aufgabentrennung können Subjekten bei der Subjektzuordnung konfliktäre Rollen zugeordnet werden, diese aber nicht gleichzeitig in derselben Session aktiviert werden, damit findet der Ausschluss der Aktivierung der Rollen zur Laufzeit statt (Kuhn 1997, S. 24).

Neben diesen im Standard definierten Komponenten existieren mehrere Erweiterungen des Modells, um einen flexiblen Zugriffskontrollmechanismus zu entwickeln. Folgende ausgewählte Erweiterungen sind für eine Umsetzung notwendig. Das Konzept der Delegation von Zugriffsrechten an ein anderes Subjekt als Stellvertretung ist notwendig, um die Stellvertretung dezentral regeln zu können, z. B. möchte ein Lehrstuhlinhaber seinem Assistenten die Möglichkeit einräumen, die Ergebnisse für eine Prüfung einzutragen. Neben der Delegation ist die Domänenbeschränkung der Subjekte eine notwendige Erweiterung. Eine Domänenbeschränkung wird pro Rolle und Subjekt festgelegt. Dies bedeutet, dass Subjekte, die der gleichen Rolle angehören, zwar die gleichen Funktionen innerhalb eines Anwendungssystems aufrufen dürfen, aber die ausgelieferten Informationen je nach Zuständigkeitsbereich eines Subjektes unterschiedlichen Inhalts sind. Ein Prüfungsausschussvorsitzender benötigt für Beratungen und Entscheidungen den Prüfungsverlauf eines Studierenden, aber er darf laut Datenschutz nur Prüfungen und Informationen von den Studiengängen sehen, für die er zuständig ist.

Diese kurze Einführung in die Theorie der Autorisierung und des RBAC-Modells zeigt die Grundlagen für die Konzeption und Implemen-

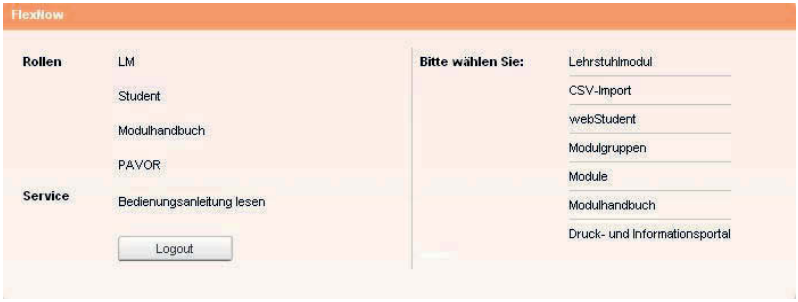
[5] Allgemeine Beschreibungen und Diskussionen zur Aufgabentrennung finden sind in (Brewer DF, Nash MJ 1989); (Clark DD, Wilson DR 1987); (Anderson R 2001, S. 166–199).

tierung des Zugriffskontrollmechanismus des Autorisierungssystems FN2RBAC. Im folgenden Kapitel wird anhand von FlexNow diese Konzeption aufgezeigt.

4.3 Konzeption der Autorisierung am Beispiel von „FlexNow“

Eine mögliche Umsetzung eines Autorisierungssystems zeigt der Aufruf von „FlexNow“ im ZUV-Portal der Universität Bamberg. Nach erfolgreicher Authentifizierung ist das Subjekt, z. B. der Prüfer, im Portal bekannt. Es stehen damit alle erlaubten Anwendungen und Rollen, wie zeigt, zur Verfügung.

Abbildung 12: Anzeige der Rollen und Anwendungauswahl innerhalb einer Sitzung



Auf der linken Seite werden alle Rollen angezeigt, die dem authentifizierten Subjekt in der Rechteverwaltung zugeordnet wurden. Auf der rechten Seite sind alle Anwendungen aufgelistet, die für die zugeordneten Rollen zur Verfügung stehen. Bei der Konzeption für die Autorisierung wurde die Entscheidung getroffen, dass implizit mit der Auswahl einer Anwendung auch die Rolle festgelegt wird. Es kann zu einem Zeitpunkt immer nur eine Rolle aktiv sein.

5. Zusammenfassung und Ausblick

Zurück zu der Ausgangsfrage: woher kennt die Anwendung mich und meine Rolle? Aufgabenträger benötigen zur Erledigung ihrer Aufgaben Informationen aus dem betrieblichen Informationssystem. Diese Informationen gilt es vor unberechtigter Nutzung zu schützen.

Um einen Aufgabenträger identifizieren zu können, werden Zugangsdaten gespeichert und eindeutig mit einem Aufgabenträger verbunden. Bei der Authentifizierung, einer Grundfunktion der Informationssicherheit, wird dieser Aufgabenträger durch Eingabe seiner Zugangsdaten ermittelt. Dadurch ist einer Anwendung bekannt, wer sich eingeloggt hat. Nach erfolgreicher Authentifizierung wird im zweiten Schritt geprüft, was einem Aufgabenträger im ausgewählten Kontext erlaubt ist

Sicherheitsadministratoren legen bei der Rechteverwaltung fest, welche Zugriffsrechte ein Aufgabenträger benötigt, um seine Aufgaben zu erfüllen. Zur Ermittlung der Zugriffsrechte existieren verschiedene Zugriffskontrollmodelle. Durch das Herausarbeiten der verschiedenen Rollenkonzepte und die Einordnung der Rolle in das betriebliche Informationssystem konnte aufgezeigt werden, dass sich methodisch aus den Aufgaben in einer Organisation Rollen ermitteln lassen. Diesen Rollen werden die benötigten Zugriffsrechte zugeordnet.

Damit eignet sich ein rollenbasiertes Zugriffskontrollmodell als Grundlage für die Entwicklung eines aufgabenorientierten Autorisierungssystems. Der Standard des rollenbasierten Zugriffskontrollmodells wurde um Konzepte wie Delegation und Domänenbeschränkung erweitert, um so eine größere Flexibilität zu erhalten.

Nachdem der Aufgabenträger identifiziert ist, können seine aktivierten Rollen in der Rechteverwaltung ermittelt werden. Vor Ausführung einer aufgerufenen Funktion im betrieblichen Informationssystem wird bei der Rechteprüfung ermittelt, ob einer dieser Rollen ein für diesen Funktonsaufruf äquivalentes Zugriffsrecht zugeordnet ist. Jeder Zugriff wird

zusammen mit der Information, ob dieser erlaubt ist oder nicht, protokolliert.

Das Thema Informationssicherheit und deren Umsetzung wird auch in Zukunft ein Forschungsgegenstand bleiben, z. B. besteht bei social networks wie „facebook“ im Bereich des Datenschutzes Handlungsbedarf.

Ein weiteres Thema ist eine Vereinheitlichung der Speicherung von Zugangsdaten für die Authentifizierung sowie von Zugriffsdaten der Rechteverwaltung möglichst übergreifend für alle Anwendungen in einem Unternehmen oder einer Verwaltung. Stichworte dazu sind unternehmensweites Ident- und Rollenmanagement. Viele im Einsatz befindliche Anwendungssysteme führen eine proprietäre Authentifizierung und Autorisierung durch. Dies führt zu einer Redundanz bei der Speicherung der notwendigen Daten. Dies bedeutet aber einen Mehraufwand bei der Kontrolle der Identität und der Zugriffe und erschwert die Überprüfung, wenn unzulässige Zugriffe erfolgt sind.

6. Literatur

Ahn G, Sandhu RS (2000) Role-based authorization constraints specification. ACM Transactions on Information SystemsSecurity 3(4):207–226.

Alisch K (2004) Gabler-Wirtschafts-Lexikon. [die ganze Welt der Wirtschaft Betriebswirtschaft, Volkswirtschaft, Recht, Steuern], 16. Aufl. Gabler, Wiesbaden

Anderson R (2001) Security engineering. A guide to building dependable distributed systems, New York

ANSI INCITS 359-2004 (01.03.2004) Role Based Access Control. American National Standard for Information Technology. http://www.cs.purdue.edu/homes/ninghui/readings/AccessControl/ANSI+INCITS+359-2004.pdf, Abruf am 2009-03-01

Beresnevichiene Y (2003) A role and context based security model. Technical Report Number 558. http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-558.pdf, Abruf am 2009-03-01

Blümle E (1975) Stellvertretung. In: Gaugler E (Hrsg) Handwörterbuch des Personalwesens. Poeschel, Stuttgart, S. 1887–1984

Boella G, van der Torre L, Verhagen H (2007) Roles, an interdisciplinary perspective. Applied Ontology 2(2):81–88

Bokranz R, Kasten L (2001) Organisations-Management in Dienstleistung und Verwaltung. Gestaltungsfelder, Instrumente und Konzepte, 3. Aufl. Gabler, Wiesbaden

Brewer DF, Nash MJ (1989) The Chinese Wall Security Policy. In: Proceedings of the IEEE Symposium on Security. IEEE Computer Society Press, S. 206–214

(2005) IT-Grundschutz-Kataloge (BSI05). Standardwerk zur IT-Sicherheit, Köln

Clark DD, Wilson DR (1987) A Comparison of Commercial and Military Computer Security Policies. In: Proceedings of the IEEE Symposium on Security and Privacy. IEEE Computer Society Press, S. 184–194

Coyne EJ, Weil T (2008) An RBAC Implementation and Interoperability Standard: The INCITS Cyber Security 1.1 Model. IEEE Security and Privacy 6(1):84–87. http://dx.doi.org/10.1109/MSP.2008.2

Crook R, Ince D, Nuseibeh B (2002) Towards an Analytical Role Modelling Framework for Security Requirements. In: Proc. of the 8 th International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ'02, S. 9 - 23

Eckert C (2001) IT-Sicherheit. Konzept - Verfahren - Protokolle. Oldenbourg, München

Eckert C (2008) IT-Sicherheit. Konzepte, Verfahren, Protokolle, 5., überarb. Aufl. Oldenbourg, München

Essmayr W, Probst S, Weippl E (2004) Role-Based Access Controls: Status, Dissemination, and Prospects for Generic Security Mechanisms. Electronic Commerce Research 4(1-2):127–156

Esswein W (1992) Das Rollenmodell der Organisation. Die Berücksichtigung aufbauorganisatorischer Regelungen in Unternehmensmodellen. Otto-Friedrich-Universität, Bamberg

Eymann T (2004) WI4 Sicherheit und Steuerung von Informationssystemen 4. Autorisierung. http://wi.oec.uni-bayreuth.de/fileadmin/download/04_II/wi_iv/ssit-04-autorisierung.pdf, Abruf am 2006-03-06

Feng X, Guoyuan L, Hao Huang, Li Xie (2004) Role-Based Access Control System for Web Services. In: CIT '04: Proceedings of the The Fourth International Conference on Computer and Information Technology. IEEE Computer Society Press, Washington, DC, USA, S. 357 - 362

Ferraiolo DF, Sandhu RS, Gavrila S, Kuhn DR, Chandramouli R (2001) Proposed NIST standard for role-based access control. ACM Transactions on Information Systems Security 4(3):224 - 274

Ferstl OK, Sinz EJ (2001) Grundlagen der Wirtschaftsinformatik, 4. Aufl. Oldenbourg, München

Ferstl OK, Sinz EJ (2006) Grundlagen der Wirtschaftsinformatik, 5., überarb. und erw. Aufl. Oldenbourg, München

Frings S, Weisbecker A (1998) Für jeden die Passende Rolle. it Management(7):18–25

Galler J (1997) Vom Geschäftsprozeßmodell zum Workflow-Modell. Gabler, Wiesbaden

Gasser M (1988) Building a secure computer system. Van Nostrand Reinhold, New York

Graf A (2002) Performance Measurement und Competency Management in der Praxis. HMD - Praxis Wirtschaftsinform.(227):46–55

Haller NM, et al. (1998) A One-Time Password System. RFC Editor, United States

Junk K, Mayer M (2003) Active Datamanagement. Säulen der Informationssicherheit. VDE-Verl., Berlin

Kern A, Kuhlmann M, Kuropka R, Ruthert A (2004) A meta model for authorisations in application security systems and their integration into RBAC administration. In: SACMAT '04: Proceedings of the ninth ACM symposium on Access control models and technologies. ACM, New York, NY, USA, S. 87 - 96

Kuhn DR (1997) Mutual exclusion of roles as a means of implementing separation of duty in role-based access control systems. In: RBAC '97: Proceedings of the second ACM workshop on Role-based access control. ACM, New York, NY, USA, S. 23 - 30

Landwehr CE, Heitmeyer CL, McLean J (1984) A security model for military message systems. ACM Trans. Comput. Syst. 2(3):198 - 222

Lehmann FR (1999) Fachlicher Entwurf von Workflow-Management-Anwendungen. Teubner, Stuttgart

Lehmann K (2007) Modelle und Techniken für eine effiziente und lückenlose Zugriffskontrolle in Java-basierten betrieblichen Anwendungen. Deutsche Nationalbibliothek, Frankfurt

Linkies M, Off F (2006) Sicherheit und Berechtigungen in SAP-Systemen, 1. Aufl. Galileo Press, Bonn

Müller K (2005) IT-Sicherheit mit System. Sicherheitspyramide und Vorgehensmodelel; Sicherheitsprozess und Katastrophenvorsorge; die 10 Schritte zum Sicherheitsmanagement, 2., verb. und erw. Aufl. Vieweg, Wiesbaden

Neumann G, Strembeck M (2001) Design and implementation of a flexible RBAC-service in an object-oriented scripting language. In: CCS '01: Proceedings of the 8th ACM conference on Computer and Communications Security. ACM, New York, NY, USA, S. 58 - 67

Nyanchama M, Osborn SL (1996) Modeling mandatory access control in role-based security systems. In: Proceedings of the ninth annual IFIP TC11 WG11.3 working conference on Database security IX : status and prospects. Chapman & Hall, Ltd., London, UK, UK, S. 129 - 144

Osborn SL, Sandhu RS, Munawer Q (2000) Configuring role-based access control to enforce mandatory and discretionary access control policies. ACM Transactions on Information Systems Security 3(2):85 - 106

Picot A, Dietl H, Franck E (1997) Organisation. Eine ökonomische Perspektive. Schäffer-Poeschel, Stuttgart

Pohl H (2004) Taxonomie und Modellbildung in der Informationssicherheit. Datenschutz und Datensicherheit 28(11):678–685

Raepple M (2001) Sicherheitskonzepte für das Internet. Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, 2., überarb. und erw. Aufl. dpunkt.verlag, Heidelberg

Rankl W, Effing W (2002) Handbuch der Chipkarten. Aufbau, Funktionsweise, Einsatz von Smart Cards, 4., überarb. und aktualisierte Aufl. Hanser, München

Reichert M, Dadam P (2000) Geschäftsprozessmodellierung und Workflow-Management - Konzepte, Systeme und deren Anwen-

dung. Industrie Management 16(3):23 - 27. http://dbis.eprints.uni-ulm.de/239/

Rieger S (2007) Einheitliche Authentifizierung in heterogenen IT-Strukturen für ein sicheres e-Science-Umfeld, 1. Aufl. Cuvillier, Göttingen

Rupietta W, Wernke G (1994) Umsetzung organisatorischer Regelungen in der Vorgangsbearbeitung mit WorkParty und ORM. In: Hasenkamp U, Kirn S, Syring Michael (Hrsg) CSCW - Computer supported cooperative work. Informationssysteme für dezentralisierte Unternehmensstrukturen, 1. Aufl. Addison-Wesley, Bonn, S. 135–154

Sackmann S (16.09.2008) IT-Sicherheit — Enzyklopaedie der Wirtschaftsinformatik. http://www.enzyklopaedie-der-wirtschaftsinformatik.de/wi-enzyklopaedie/lexikon/technologien-methoden/Informatik--Grundlagen/IT-Sicherheit, Abruf am 2009-04-01

SAP (06.07.2007) Rolle. SAP-Bibliothek - SAP DB. http://help.sap.com/saphelp_47x200/helpdata/de/48/8af5b0a54f11d2a97100a0c9449261/frameset.htm, Abruf am 2009-03-26

Schier K (1999) Vertrauenswürdige Kommunikation im elektronischen Zahlungsverkehr / Schier, Kathrin. http://deposit.ddb.de/cgi-bin/dokserv?idn=957624921, Abruf am 2009-03-26

Schreyögg G (2008) Organisation. Grundlagen moderner Organisationsgestaltung ; mit Fallstudien, 5., vollständig überarb. Aufl. Gabler, Wiesbaden

Schwarz H (1980) Aufgabenträger. In: Grochla E (Hrsg) Handwörterbuch der Organisation, 2., völlig neu gestaltete Aufl. Poeschel, Stuttgart, S. 217–224

Seufert SE (2001) Die Zugriffskontrolle. Eine Bestandsaufnahme relevanter Ansätze und deren Weiterentwicklung zu einem Konzept für die Ableitung von Zugriffsrechten aus der betrieblichen Organisation

Strembeck M, Neumann G (2004) An integrated approach to engineer and enforce context constraints in RBAC environments. ACM Transactions on Information Systems Security 7(3):392 - 427

Süßmilch-Walther I, Gilleßen S (2003) Ein Bezugsrahmen für Rollen in Unternehmungen. 1. Teil: Grundlagen, Abgrenzung und

Methodik. http://www.wissensnavigator.com/documents/Rollen1.pdf, Abruf am 2009-03-28

Thomas EJ, Biddle BJ (1966) Basic Concepts for Classifiying the Phenomena of Role. In: Biddle BJ, Thomas EJ (Hrsg) Role theory. Concepts and research. John Wiley & Sons, New York, S. 23–63

van Aalst der W, Hee van KM (2002) Workflow management. Models, methods, and systems. MIT Press, Cambridge, Mass.

Walther I (2005) Rollen- und Situationsmodellierung bei betrieblichen Dispositions- und Planungssystemen. http://www.opus.ub.uni-erlangen.de/opus/volltexte/ 2005/137, Abruf am 2009-03-28

Zannone N, Jajodia S, Wijesekera D (2006) Creating Objects in the Flexible Authorization Framework. In: Goos G, Hartmanis J, van Leeuwen J (Hrsg) Data and applications security XX. 20th Annual IFIP WG 11.3 Working Conference on Data and Applications Security, Sophia Antipolis, France, July 31 - August 2, 2006 ; proceedings. Springer-Verlag, Berlin, S. 1–14