February 2005

Sicherheitsmodelle für Kooperationen

Robert Schmaltz
Universität Göttingen

Philipp Goos
Universität Göttingen

Svenja Hagenhoff
Universität Göttingen

In: Ferstl, Otto K, u.a. (Hg) 2005. *Wirtschaftsinformatik 2005: eEconomy, eGovernment, eSociety*; 7. Internationale Tagung Wirtschaftsinformatik 2005. Heidelberg: Physica-Verlag

ISBN: 3-7908-1574-8

Sicherheitsmodelle für Kooperationen

Robert Schmaltz, Philipp Goos, Svenja Hagenhoff
Universität Göttingen

Zusammenfassung: In diesem Beitrag werden zwei Möglichkeiten der Ausgestaltung rollenbasierter Sicherheitsmodelle auf ihre Eignung zum Festlegen und Überwachen von Zugriffsrechten in kooperativ genutzten IT-Systemen überprüft. Anhand vorher erarbeiteter Kriterien wird verdeutlicht, dass sich synergieorientierte Anforderungen besser durch ein zentrales Modell abbilden lassen, spezifische Anforderungen der Kooperationspartner jedoch eher durch ein dezentrales Modell realisiert werden können.

Schlüsselworte: Kooperationen, Zugriffsschutz, Sicherheitsmodelle

1 Einleitung

Unter den heutigen Wettbewerbsbedingungen sind die unternehmenseigenen Ressourcen und Fähigkeiten vielfach nicht ausreichend, um erfolgreich im Wettbewerb bestehen zu können. So muss zunehmend auch auf unternehmensexterne Ressourcen zurückgegriffen werden, um Wettbewerbsvorteile zu erzielen. Diese Ressourcen werden vermehrt im Rahmen von Kooperationen beschafft. Dabei laufen eng verknüpfte, mehrstufige Wertschöpfungsprozesse ab, die mehrere Partner umfassen.

Um eine effiziente Durchführung von Prozessen über die Grenzen der kooperierenden Unternehmen hinaus zu ermöglichen, sollte die eingesetzte IT in technisch und wirtschaftlich sinnvoller Weise integriert werden. Im Rahmen dieser Integration müssen die Kooperationspartner auch Nutzern aus Partnerunternehmen einen begrenzten Zugriff auf interne IT-Systeme gewähren. Dabei entsteht ein Spannungsfeld zwischen der Einbindung von Partnern und dem Schutz internen Knowhows. Für die Festlegung und Überwachung der erforderlichen Zugriffsrechte bietet sich der Einsatz von Sicherheitsmodellen an. Um die potenziell divergierenden Sicherheitsbedürfnisse der Partner angemessen zu berücksichtigen, ist der Einsatz rollenbasierter Modelle sinnvoll, da sich diese gegenüber herkömmlichen Ansätzen insbesondere durch verbesserte Flexibilität und Effizienz auszeichnen. Ziel des vorliegenden Beitrages ist es, die Eignung rollenbasierter Sicherheitsmodelle für kooperativ genutzte IT-Systeme zu untersuchen. Dazu werden in Kap. 2 zunächst die wesentlichen Grundlagen von Kooperationen und Sicherheitsmodellen

sowie die wichtigsten Eigenschaften des rollenbasierten Zugriffsschutzes vorgestellt. In Kap. 3 werden dann die Anforderungen und Besonderheiten des Zugriffsschutzes in Kooperationen ermittelt. In Kap. 4 folgt ein Vergleich von zentralen und dezentralen Sicherheitsmodellen für Kooperationen und Kap. 5 enthält ein zusammenfassendes Fazit.

2 Grundlagen

Im folgenden Kapitel werden die wesentlichen begrifflichen Grundlagen von Kooperationen, Sicherheitsstrategien und -modellen geklärt. Zudem wird der Begriff der rollenbasierten Zugriffskontrolle eingeführt.

2.1 Unternehmenskooperationen

Die klassische Betriebs- und Volkswirtschaftslehre geht von nur zwei möglichen Koordinationsformen zum Erbringen einer Leistung aus: dem Markt und der Hierarchie [Coas37, S. 390] [Stru99, S. 30]. Gerade in den letzten Jahren entstehen jedoch zunehmend Kooperationen, die Eigenschaften der beiden Koordinationsformen vermischen.

Unter einer Kooperation wird die Zusammenarbeit zwischen Unternehmen bzw. Unternehmensteilen verstanden [Rote90, S. 38]. Kooperationen werden durch zwei weitere Aspekte charakterisiert: das Verfolgen eines gemeinsamen, leistungswirtschaftlichen Sachziels und die rechtliche Selbständigkeit der Kooperationspartner [Wohl02, S. 11].

Durch die Zusammenarbeit mit Kooperationspartnern sollen Synergien realisiert werden. Sie umfassen mögliche Angebotserweiterungen durch das Bündeln von Ressourcen und Effizienzvorteile durch das Zusammenfassen administrativer Funktionen. Zudem erlauben Kooperationen den Partnern, sich auf ihre Kernkompetenzen zu konzentrieren. Um diese Synergien zu erreichen, ist eine enge Abstimmung und Verzahnung der Leistungserstellung erforderlich.

Das Erreichen von Synergien kann in einem Spannungsverhältnis zu den individuellen Zielen der Kooperationsteilnehmer stehen, die insbesondere eine Gewinnerzielungsabsicht auf Unternehmensebene verfolgen. Zur Gewinnerzielung ist es erforderlich, dass die Unternehmen ihre spezifischen Wettbewerbsvorteile bewahren können. So müssen die Kooperationspartner bestimmte Fähigkeiten und Ressourcen, wie Technologien, einzigartige Prozesse oder Kundendaten vor einem ungewollten Zugriff durch andere Kooperationsteilnehmer schützen. Dies bedeutet, dass die Sicherheit wettbewerbsrelevanter Informationen gewährleistet sein muss. Insgesamt lässt sich somit ein Spannungsverhältnis zwischen dem synerge-

tischen Kombinieren von Ressourcen und den Schutzbedürfnissen der einzelnen Partner feststellen.

Ein wichtiger Faktor für das Erzielen von Synergien in der gemeinsamen Leistungserstellung ist ein reibungsloser Informationsaustausch, der durch die Koppelung von IT-Systemen erreicht werden kann [StWu01, S. 370]. Auch in der gemeinsam genutzten IT müssen sich die oben genannten Schutzbedürfnisse widerspiegeln. Hierfür werden Sicherheitsstrategien und –modelle eingesetzt.

In fokalen Kooperationen, in denen ein Partner dominiert, können Sicherheitsstrategien von dieser zentralen Instanz vorgegeben werden. In polyzentrischen Kooperationen hingegen, in denen die Partner weitgehend gleichberechtigt sind, müssen die Teilnehmer nicht nur die Ausgestaltung der IT-Systeme, sondern auch die zu nutzende Sicherheitsstrategie gemeinsam festlegen. Dabei müssen die individuellen Anforderungen verstärkt berücksichtigt werden. Sicherheitsmodelle für diese Kooperationen bilden den Schwerpunkt der folgenden Betrachtungen, da durch die Berücksichtigung individueller Bedürfnisse neue Anforderungen an Sicherheitsmodelle gestellt werden, die in der Literatur bislang nur wenig Beachtung gefunden haben.

2.2 Sicherheitsstrategien und -modelle

Um den Schutz kritischer IT-Systeme zu gewährleisten, werden in vielen Organisationen explizite Schutzziele formuliert. Aus diesen Zielen kann eine Sicherheitsstrategie abgeleitet werden, in der die zu schützenden Objekte des Systems, die möglichen Nutzer und ihre Zugriffsrechte unabhängig von der Implementierung festgelegt werden. In einer Kooperation müssen deshalb die Schutzziele der einzelnen Partner zu einer Sicherheitsstrategie für die gemeinsamen IT-Systeme zusammengeführt werden. Dabei muss die Strategie flexibel bezüglich der unterschiedlichen Anforderungen sein und sowohl restriktive als auch offene Zugriffsschutzkonzepte für unterschiedliche Teile des Systems abbilden.

Die Sicherheitsstrategie kann in Sicherheitsmodellen formal oder semiformal dargestellt werden. Die Modelle ermöglichen den Entwurf und die Analyse sicherheitsrelevanter Funktionen unabhängig von den Vorgaben einzelner Implementierungen. Zudem erlauben formale Sicherheitsmodelle, die Eigenschaften eines auf ihrer Basis implementierten Systems theoretisch zu überprüfen [SaCa01, S. 138]. Auch das Modell muss für den Einsatz in einer Kooperation die oben genannte Flexibilität aufweisen.

Die Umsetzung der Sicherheitsfunktionen auf der Basis des Modells kann dann auf unterschiedliche Weise erfolgen [Schi99, S. 125]. Im Fokus dieses Beitrags stehen die Sicherheitsmodelle, ihre konkrete Umsetzung wird hier jedoch nicht explizit betrachtet.

Der zentrale Aspekt der IT-Sicherheit, der in Sicherheitsmodellen abgebildet wird, ist die Autorisierung. Die Autorisierung bezeichnet das Prüfen der Zulässigkeit von Zugriffen auf Systemobjekte [TaSt02, S. 415]. In Kooperationen ist dieser Aspekt von besonderem Interesse, da der Zugriff auf Produktivsysteme durch externe Partner besonders sensibel ist. Etablierte Zugriffskontrollsysteme berücksichtigen die Anforderungen eines Zugriffsschutzes über Unternehmens- und Systemgrenzen hinaus jedoch nur am Rande [SaCa01]. Diese Problematik kann durch den Einsatz rollenbasierter Modelle gemildert werden.

2.3 Rollenbasierte Zugriffskontrolle

In Forschung und Praxis hat das Modell der rollenbasierten Zugriffskontrolle in jüngerer Zeit große Aufmerksamkeit erfahren [Sand01] [AoMi04] [DrMu+04]. Es wird auch als Role-Based Access Control (RBAC) bezeichnet und geht auf [SaCo+96] zurück. RBAC ist an dieser Stelle besonders geeignet, weil es flexibel bezüglich der abzubildenden Sicherheitsstrategie ist und unterschiedliche Ansätze abbilden kann [OsSa+00]. Im Gegensatz dazu geben die meisten traditionellen Modelle die umzusetzende Sicherheitsstrategie vor, indem sie entweder einen offenen Ansatz mit nutzerbestimmter Zugriffskontrolle (etwa im Zugriffsmatrix-Modell) oder einen geschlossenen Ansatz mit systembestimmter Kontrolle (etwa im Bell-Lapadula-Modell) verfolgen [Ecke03, S. 183].

RBAC basiert auf dem Grundgedanken, dass die Berechtigungen eines Nutzers von seiner Rolle in der Organisation abhängen. Daher wird in die Zuordnung von Nutzern zu Berechtigungen das Konzept der Rolle als Abstraktionsebene eingefügt.

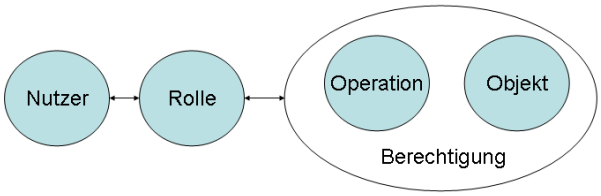

Abbildung 1: Grundkonzept der rollenbasierten Zugriffskontrolle

Den Rollen werden Berechtigungen zum Zugriff auf geschützte Objekte zugeordnet. Den Nutzern werden wiederum Rollen zugewiesen, die in Abhängigkeit von den ausgeübten Aufgaben aktiviert werden können. Nutzer können Zugriffe nur ausführen, wenn sie eine Rolle innehaben, die ihnen diesen Zugriff erlaubt. Die Rechtezuweisung erfolgt damit ausschließlich über Rollen [FeKu+03, S. 58]. Diese werden bei Ausübung der entsprechenden Tätigkeiten in Sitzungen (Sessions) aktiviert.

Die Rollen im Unternehmen sind vergleichsweise stabil, da sie Ausdruck bestimmter Aufgaben sind. Die zuständigen Mitarbeiter sowie die möglichen Berechtigungen sind hingegen einem stetigen Wandel unterworfen. Daher kann mit der Bündelung der Rechte in Rollen eine erhebliche Reduktion des Administrationsaufwandes erreicht werden, weil die eher statischen Rollen-Rechte-Beziehungen bei Veränderungen der personellen Zuständigkeit nicht verändert werden müssen. Die Komplexität des Sicherheitsmodells wird zudem im Vergleich zu traditionellen Modellen, insbesondere nutzerspezifischen Zugriffskontroll-Listen, erheblich reduziert. Die Zahl der zu pflegenden Zuordnungen sinkt, da nicht mehr jedes Recht für jeden Nutzer einzeln angelegt werden muss. Stattdessen muss dem Nutzer nur noch eine Auswahl von Rollen zugewiesen werden, die aufgabenspezifische Bündel von Rechten enthalten und für alle Nutzer, die eine Aufgabe ausführen, gleich sind. Zudem erhöht die Nutzung von RBAC die Übersichtlichkeit des Sicherheitsmodells [FeKu+03].

Das mittlerweile als ANSI-Standard verabschiedete RBAC-Modell (ANSI INCITS 359-2004, vgl. [FeSa+01]) beinhaltet neben einem einfachen Rollenmodell zwei wesentliche Erweiterungen. Zum einen können Rollenmodelle hierarchisch geordnet werden, d. h. Rollen können die Rechte untergeordneter Rollen erben. Ergänzend können auch mehrfache Vererbungen definiert werden. Dies reduziert den Administrationsaufwand weiter, insbesondere bei komplexen Rollenhierarchien.

Neben den Vererbungen ist es zudem möglich, Rollenmitgliedschaften zu beschränken. Dabei können statische und dynamische Aufgabentrennungen definiert werden, d. h. die gleichzeitige Mitgliedschaft in einander ausschließenden Rollen bzw. deren gleichzeitige Aktivierung kann verhindert werden. Die Aufgabentrennung kann genutzt werden, um Interessenskonflikten vorzubeugen oder Genehmigungsmechanismen zu implementieren [Ecke03, S. 196].

Änderungen am Modell werden prinzipiell von einem zentralen Administrator vorgenommen. Das System kann um administrative Rollen ergänzt werden, mit denen die Zuweisung von Nutzern bzw. Privilegien zu Rollen an untergeordnete Administratoren delegiert werden kann [Sand98, S. 17]. Änderungen an einzelnen Rollen werden wiederum sofort für alle in der Rolle aktiven Nutzer gültig, was eine erhebliche Zeitersparnis bei der Rollenpflege bedeutet und die Fehleranfälligkeit des Systems senkt. In den konkreten Umsetzungen des Modells werden die Administratorentätigkeiten meist durch ein zentrales grafisches Werkzeug zur Wartung des gesamten Modells unterstützt [FeKu+03].

Das RBAC-Modell enthält keine grundsätzliche Festlegung bezüglich der Freigabe von Zugriffen. Insbesondere können sowohl diskretionäre, nutzerbestimmte Zugriffsregeln als auch systemweite, zentral verwaltete Beschränkungen abgebildet werden [OsSa+00, S. 85].

Aufgrund der Flexibilität hinsichtlich unterschiedlicher Sicherheitsstrategien und der Vereinfachung der Administration des Modells bildet RBAC die Grundlage für die in Kap. 3 diskutierten Sicherheitsmodelle.

3 Beurteilungskriterien für Sicherheitsmodelle in Kooperationen

Im folgenden Abschnitt werden zunächst die allgemeinen Anforderungen an Sicherheitsmodelle erörtert. Danach werden die speziellen Ziele des Zugriffsschutzes in Kooperationen erläutert, die als Grundlage für die daraus abgeleiteten weiterführenden Anforderungen dienen.

3.1 Allgemeine Anforderungen an Sicherheitsmodelle

Die IT-Sicherheit soll Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Daten garantieren [SaCa01, S. 138], [FeKu+03, S. 2]. Die Verfügbarkeit beruht primär auf den Eigenschaften der konkreten Implementierung (z. B. Fehlerfreiheit der Software und Redundanz der Hardware). Sie wird im Modell nicht berücksichtigt, da das Modell unabhängig von der Implementierung ist.

Um Vertraulichkeit zu erreichen, müssen **objektspezifische Rechte** mit feiner Granularität vergeben werden können, um bspw. einzelne Dateien oder Felder in Datenbanken zu schützen. Andernfalls ist die Wahrscheinlichkeit sehr groß, dass Nutzer aufgrund zu pauschaler Vergaben zu viele Rechte erhalten.

Zudem müssen die Sicherheitsmechanismen vollständig sein, d. h. alle im System getätigten Zugriffe müssen überprüft werden, um ein Umgehen der Kontrollfunktionen zu verhindern. Um dies zu gewährleisten, ist eine **konsistente Gesamtsicht** des Sicherheitsmodells (als Grundlage der Sicherheitsmechanismen) erforderlich.

Weiterhin dürfen nur autorisierte Zugriffe durchgeführt werden. Das Modell muss also **entscheidbar** sein, um die Zulässigkeit von Anfragen feststellen zu können [SaCa01, S. 138].

Zur Sicherstellung der Integrität ist weiterhin eine **anwendungsspezifische Körnung** der Rechte erforderlich, unterschiedliche Befehle müssen also nach ihren Auswirkungen unterschiedlich behandelt werden [Ecke03, S. 179].

Weiterhin ist zu berücksichtigen, dass betrieblich eingesetzte IT-Systeme einem **Wirtschaftlichkeitskalkül** unterliegen. Auch der Aufwand für den Einsatz von Sicherheitsmodellen und -mechanismen muss in einem angemessenen Verhältnis zu ihrem Nutzen stehen. Folglich ist er bei der Auswahl und Gestaltung eines Sicherheitsmodells zu berücksichtigen.

3.2 Ziele des Einsatzes von Sicherheitsmodellen in Kooperationen

Sicherheitsmodelle in Kooperationen müssen zwei Bedingungen erfüllen, die in einem Spannungsverhältnis zueinander stehen. Zum einen müssen sie Synergien ermöglichen, was das übergeordnete Ziel einer Kooperation ist. Zum anderen müssen sie Schutz und Kontrolle gewährleisten, damit die Teilnahme an der Kooperation nicht die Ressourcen der einzelnen Partner gefährdet.

Für das Erzielen von Synergien im Rahmen der gemeinsamen Wertschöpfung müssen die Teilnehmer ihre IT-Infrastruktur für Partner zugänglich machen. In Entwicklungspartnerschaften lassen sich beispielsweise erhebliche Effizienzsteigerungen realisieren, wenn eine gemeinsame Daten- und Anwendungsbasis genutzt wird [StWu01]. Auch projektbegleitend genutzte Wissensmanagementanwendungen können Partnern zugänglich gemacht werden, um einen reibungslosen Informations- und Wissensfluss zu ermöglichen. Ziel ist es also, externen Nutzern Zugriff auf operative IT-Systeme zu gewähren.

Dabei besteht das Problem, dass die Partner die Zugriffsmöglichkeiten, die sie externen Nutzern einräumen, genau kontrollieren müssen. So ist beispielsweise bei Anwendungen aus dem F&E-Bereich sowie dem Wissensmanagement eine Kontrolle der Zugriffsmöglichkeiten wichtig, da die dort gespeicherten Explizierungen von Produkt- und Prozess-Know-how intellektuelles Kapital und eine Möglichkeit der Differenzierung im Wettbewerb darstellen [OeHa03, S. 23]. Diese sind zu schützen und sollten Dritten nur im für die Zusammenarbeit erforderlichen Maß zugänglich gemacht werden. Aus diesem individuellen Schutzziel leitet sich die Notwendigkeit ab, Zugriffe durch externe Nutzer zu kontrollieren und ggf. zu verhindern.

Insbesondere im Kontext schutzbedürftiger IT-Infrastrukturen wird dem Einsatz von Sicherheitsmodellen signifikanter Nutzen zugesprochen. Ein anwendungsübergreifendes Sicherheitsmodell ermöglicht eine transparente Verwaltung aller vergebenen Zugriffsrechte. Damit wird es möglich, einen Überblick über die sicherheitsrelevanten Nutzeraktivitäten zu gewinnen und diese auf ihre Übereinstimmung mit der Sicherheitsstrategie zu überprüfen [Ecke03, S. 141]. Zudem erleichtert der Einsatz insbesondere von rollenbasierten Sicherheitsmodellen bei einer entsprechenden Integration in die Anwendungen die Administration der Zugriffsrechte. Dies macht eine übergreifende Verwaltung der Zugriffe auf gemeinsam genutzte Systeme wünschenswert [Seuf02].

Aus diesen Zielen, dem Eröffnen von Synergiepotenzialen und dem Gewähren individueller Kontrollpotenziale, lassen sich Anforderungen an Sicherheitsmodelle für Kooperationen ableiten.

3.3 Anforderungen an Sicherheitsmodelle in Kooperationen

Soll ein Sicherheitsmodell kooperationsweit eingesetzt werden, so hat es zunächst die bereits diskutierten allgemeinen Anforderungen an den Zugriffsschutz zu erfüllen. Zudem bringen die kooperationsspezifischen Ziele weitere Anforderungen mit sich. Im Folgenden werden wesentliche, für typische Kooperationen gültige Aspekte aufgeführt. Diese können in synergiebezogene und sicherheitsorientierte Anforderungen unterteilt werden.

Synergieorientierte Anforderungen

Sollen Synergien erzielt werden, muss den Partnern der Zugriff auf interne Systeme gewährt werden. Dies ist nur bei angemessenen Sicherheitsmechanismen möglich. Die zu Grunde liegenden Modelle müssen dabei so gestaltet sein, dass der Aufwand für ihren Einsatz möglichst gering bleibt. Dies gilt auf der Nutzer- und der Administrationsseite. Um einen einfachen Zugriff zu ermöglichen, sind partnerübergreifende Nutzeridentitäten und eine konsistente Gesamtsicht erforderlich. Diese ermöglichen es, den Aufwand sowohl auf der Nutzer- als auch auf der Administrationsseite zu reduzieren.

Partnerübergreifende Nutzeridentitäten: Zugreifende Nutzer müssen zunächst authentifiziert werden. Dies kann gewährleistet werden, indem in jedem Partnersystem Nutzeridentitäten und Authentifizierungsmechanismen gepflegt werden. Dies ist jedoch mit sehr hohem Aufwand verbunden. Um ihn zu verringern, benötigt man Identitäten und Beschreibungen der Nutzer, die über die Grenzen der Verantwortungsbereiche hinweg austauschbar sind. Dann können die einzelnen Systeme potenzielle Nutzer identifizieren, ohne dass eine mehrfache Verwaltung der Nutzerdaten nötig ist. Dazu müssen Beschreibungssysteme definiert werden, die von allen Kooperationspartnern anerkannt werden [LoPr+03] und einen Austausch der Authentifizierungen mit geringem Aufwand erlauben.

Eine systemübergreifende Verwaltung der Authentifizierungsdaten ermöglicht es weiterhin, die Authentifizierung der Nutzer an einer Stelle zu konzentrieren (Single Sign On). Damit können Nutzer nach einmaliger Anmeldung, etwa an einem System ihres Arbeitgebers, ohne erneute Überprüfung auch Zugriff auf für sie relevante Partnersysteme erhalten. Damit werden auch auf der Nutzerseite potenzielle Hemmnisse für die übergreifende Systemnutzung verringert.

Konsistente Gesamtsicht: Neben der Administration der Nutzeridentitäten ist auch die Pflege der Rechte einzelner Nutzer zu berücksichtigen. Der dafür notwendige Aufwand verringert sich, wenn das Modell eine zentrale Übersicht über Nutzer, Rollen und Berechtigungen ermöglicht. Hierdurch können neuen Nutzern alle relevanten Berechtigungen schnell und einfach zugänglich gemacht werden.

Weiterhin wird es möglich, Erfordernisse wie die Vertraulichkeit bestimmter Daten, Aufgabentrennungen und die Vermeidung von Interessenkonflikten auf der

Kooperationsebene darzustellen und zu überprüfen. Dies kann die Leistungsfähigkeit der Kooperation verbessern, wenn von Kunden oder Regulierungsbehörden entsprechende Anforderungen gestellt werden.

Sicherheitsorientierte Anforderungen

Neben den synergieorientierten Anforderungen müssen auch Sicherheitsaspekte berücksichtigt werden. Dabei sollten die Anforderungen der einzelnen Partner möglichst genau abgebildet werden, um Risiken bei der Öffnung der Systeme zu minimieren. Zum einen muss aus der Sicht der Partner die individuelle Sicherheitsstrategie einbezogen werden, die die Basis für die Festlegung der relevanten Modellbereiche bildet. Zum anderen müssen organisatorische Spezifika der Partner wiedergegeben werden, weil diese die Ausgestaltung der konkreten Rollen determinieren. Da die Leistungserstellung zudem an der Schnittstelle zwischen den Unternehmen stattfindet, müssen darüber hinaus Überschneidungen von Rollen und Verantwortungsbereichen abgebildet werden.

Berücksichtigung individueller Strategien: Wenn organisatorisch eigenständige Partner zusammenarbeiten, können die individuellen Schutzziele dazu führen, dass unterschiedliche Sicherheitsstrategien zum Einsatz kommen. Die Anforderungen an die Sicherheitsstrategie können sich sogar innerhalb eines Unternehmens fallweise unterscheiden [SaCa01, S. 184]. Je nach den Sicherheitsbedürfnissen der Partner können so beispielsweise eher wenig restriktive, an eine benutzerdefinierte Zugriffskontrolle angelehnte Strategien zum Einsatz kommen. Alternativ können Partner aber auch andere Anforderungen haben, etwa systembestimmte Sicherheitsmodelle mit festen Schutzklassen oder Chinese-Wall-Konzepte, die Nutzern, abhängig von ihrem Aufgabenbereich, den Einblick in bestimmte Systembereiche verwehren [FeKu+03, S. 35]. Das in der Kooperation verwendete Sicherheitsmodell muss geeignet sein, diese Bedürfnisse wiederzugeben, um allen Partnern eine adäquate Modellierung ihrer Sicherheitsstrategie zu ermöglichen.

Berücksichtigung individueller Organisationsstrukturen: Neben unterschiedlichen Sicherheitsstrategien ist noch ein weiterer Faktor zu berücksichtigen, wenn den individuellen Schutzanforderungen der Beteiligten nachgekommen werden soll. Es ist wahrscheinlich, dass in den unterschiedlichen Unternehmen verschiedene organisatorische Strukturen vorhanden sind. So können etwa verschiedene hierarchische Strukturen und Matrixorganisationen auftreten. Diese Strukturen haben wiederum Einfluss auf die Zuordnung von Aufgaben zu Arbeitsplätzen und damit auf die zu erstellenden Rollen. Das Sicherheitsmodell muss also unterschiedliche Organisations- und damit Rollenstrukturen parallel abbilden können. Zudem kann es erforderlich sein, dass Mitarbeitern Rollen in unterschiedlichen Unternehmen zugewiesen werden, etwa wenn ein Projektmitarbeiter in der Konstruktion auf Unterlagen eines Partners zurückgreifen muss.

Mehrdimensionale Entscheidungen: Aufgrund der individuellen Schutzziele der Partner kann es erforderlich sein, bei der Rollenzuweisung mehrere Kriterien pa-

rallel zu berücksichtigen. An einem Projekt können beispielsweise interne und externe Mitarbeiter beteiligt sein. In diesem Fall sind zwar beide Projektmitglieder, aufgrund ihrer unterschiedlichen Unternehmenszugehörigkeit kann es aber notwendig sein, ihnen unterschiedliche Rechte zuzuweisen. In solchen Fällen müssen mehrdimensionale Entscheidungen dargestellt und Nutzern je nach Domäne variierende Rollen zugeordnet werden. Diese Anforderung enthält einen synergetischen Aspekt, da sie die Administration externer Nutzer vereinfacht. Sie dient aber in erster Linie individuellen Schutzzielen und erlaubt den Partnern, individuelle Entscheidungskriterien abzubilden.

Tabelle 1 enthält eine Zusammenfassung der Anforderungen.

Ziele	Anforderung	Wesentliche Aspekte
synergiebezogen	Partnerübergreifende Nutzeridentitäten	• Übergreifende Identifikation von Nutzern • Austauschbare Authentifikationsinformationen
	Konsistente Gesamtsicht	• Zentrale Administration aller Rechte • Prüfung kooperationsweiter Rechtekombinationen
sicherheitsbezogen	Individuelle Organisationsstrukturen	• Parallele Abbildung unterschiedlicher Strukturen • Partnerspezifische Zuordnung von Rollen zu Mitarbeitern
	Individuelle Zugriffsstrategien	• Berücksichtigung individueller Sicherheitsanforderungen • Abbildung unterschiedlicher Strategien in verschiedenen Teilbereichen des Systems
	Mehrdimensionale Entscheidungen	• Variable Kriterien für Zuordnung von Mitarbeitern zu Rollen

Tabelle 1: Anforderungen an Rollenmodelle in Kooperationen

4 Beurteilung von Sicherheitsmodellen in Kooperationen

Im Rahmen von polyzentrischen Kooperationen existieren verschiedene Varianten zur Ausgestaltung von Sicherheitsmodellen. Diese können hinsichtlich der Verteilung der Modellbestandteile in zentrale und dezentrale Konzepte unterteilt werden. Dabei lassen sich zwei Extrempositionen identifizieren: zum einen kann das gesamte Modell (Subjekte, Rollen, Berechtigungen) zentral angelegt werden. Als

Alternative ist es möglich, als kleinstes gemeinsames Bindeglied ein Modell der Subjekte zu entwerfen und Rollen sowie Berechtigungen dezentral zu verwalten. Dazwischen sind weitere Differenzierungen denkbar. Zum besseren Verständnis werden im Folgenden die beiden Extrempositionen dargestellt, bewertet und verglichen.

Die Bewertung wird anhand der oben ermittelten kooperationsspezifischen Anforderungen vorgenommen. Auf die in 3.1 dargestellten allgemeinen Anforderungen an Sicherheitsmodelle wird im Folgenden nicht explizit eingegangen, da sie von gängigen RBAC-basierten Sicherheitsmodellen erfüllt werden [Ecke03, S. 198]. Lediglich Abweichungen werden dargestellt.

4.1 Zentrale Rollenmodelle

Soll ein Zugriffsschutzsystem für kooperativ genutzte Anwendungen eingerichtet werden, ist es zunächst notwendig, ein Sicherheitsmodell zu erstellen, das die gewünschten Sicherheitsstrategien abbildet. Zu diesem Zweck kann, dem Trend zum Einsatz von RBAC und verwandten Ansätzen folgend, ein gemeinsames rollenbasiertes Sicherheitsmodell erstellt werden. In diesem Fall werden partnerübergreifend für die relevanten Systeme alle Nutzer, Rollen und Berechtigungen an zentraler Stelle modelliert (vgl. Abb. 2).

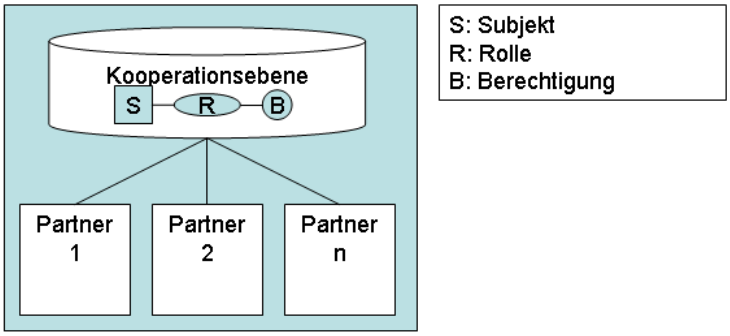

Abbildung 2: Zentrales Rollenmodell für kooperativ genutzte Anwendungen

Dabei ist zu untersuchen, ob dieser Ansatz die in Kap. 3.1 spezifizierten Anforderungen erfüllen kann.

Partnerübergreifende Nutzeridentitäten lassen sich mit einem zentralen rollenbasierten Modell problemlos darstellen. Die Nutzer werden im RBAC-Modell als globale, systemübergreifende Konstrukte betrachtet, die auf ebenso globale Rollen abgebildet werden. Erst die Berechtigungen, die den Rollen zugewiesen werden, sind dann einzelnen Systemen oder Anwendungsfunktionen zugeordnet [FeKu$^+$03, S. 61]. Die Nutzeridentitäten werden im Modell also übergreifend dargestellt.

Wird ein physischer Anwender als Nutzer in einem RBAC-System authentifiziert, ist diese Zuordnung für alle Teile des Modells gültig. Diese Anforderung kann demnach im vorliegenden Szenario unterstützt werden.

Die Etablierung einer **konsistenten Gesamtsicht** ist problemlos möglich. Da alle relevanten Informationen im zentralen Modell vorhanden sind, können Änderungen und Überprüfungen problemlos vorgenommen werden.

Grundsätzlich können **individuelle Zugriffsstrategien** in RBAC-Modellen ebenfalls abgebildet werden. Das Modell kann auf unterschiedliche Weise konfiguriert werden, um sowohl benutzerbestimmte als auch systembestimmte Kontrollstrategien festzulegen [OsSa^{+}00]. Sollen die einzelnen Benutzer weitgehende Kontrolle über die ihnen unterstehenden Systemelemente haben, ist allerdings ein komplexes System administrativer Rollen anzulegen, in denen festgeschrieben wird, welcher Nutzer für welche Rechtevergabe zuständig ist. Durch die Möglichkeit, den Nutzern verschiedene Rollen zuzuordnen, können sich Strategien in Teilbereichen des Systems durchaus unterscheiden. So ist es möglich, die Berechtigungen im Verantwortungsbereich eines Partners durch Nutzer vergeben zu lassen, während andere Systembereiche einer strikteren Kontrolle unterworfen sind. Weiterhin können mit Hilfe eines zentralen rollenbasierten Modells systemweite Beschränkungen angelegt werden, so dass etwa kooperationsweit nachgewiesen werden kann, dass bestimmte Nutzer vom Zugriff auf bestimmte Funktionen ausgeschlossen sind.

Die Abbildung **individueller Organisationsstrukturen** ist in einem gemeinsamen Modell jedoch problematisch. Grundsätzlich impliziert das Konzept von RBAC, dass sich die Partner auf ein übergreifend gültiges Rollenmodell einigen. In diesem Modell sind dann aufgabenspezifische Berechtigungen für Systeme verschiedener Partner enthalten. Wenn sich die Partner nicht auf eine gemeinsam akzeptierte Rollenstruktur einigen können, muss eine Vielzahl von einzelnen Rollen angelegt werden, die jeweils Aufgaben aus der Sicht einzelner Partner darstellen. Nutzern, die unternehmensübergreifende Tätigkeiten ausüben, müssen dann ggf. mehrere Rollen zugewiesen werden, die Teilbereiche ihrer Aufgaben enthalten. Darunter kann die Übersichtlichkeit des Modells erheblich leiden und der Administrationsaufwand steigt.

Die Abbildung **mehrdimensionaler Zugriffsentscheidungen**, bei denen Kombinationen verschiedener Kriterien für die Gewährung von Berechtigungen ausschlaggebend sind, ist mittels RBAC nicht möglich. Im Modell werden Zugriffsentscheidungen ausschließlich auf der Basis von Rollenzugehörigkeiten gefällt. Um eine bestimmte Berechtigung zu erhalten, muss ein Nutzer einer Rolle zugeordnet sein, die dieses Recht enthält. Diese Zuordnung muss ex-ante durch einen Administrator erfolgen, ebenso muss die entsprechende Rolle angelegt sein. Sind nun mehrere Kriterien für die Entscheidung relevant, ob ein Nutzer bestimmte Zugriffsrechte erhält, müssen diese bei der Rollenzuordnung berücksichtigt werden. Ggf. müssen mehrere Rollen für unterschiedliche Kombinationen von Merk-

malen modelliert werden. Dies kann beispielsweise der Fall sein, wenn einzelne Partner den Zugriff auf Projektdaten nicht nur danach differenzieren wollen, ob ein Nutzer Projektmitglied ist, sondern auch nach seiner Unternehmenszugehörigkeit. In diesem Fall wären bei *m* Projekten und *n* Partnerunternehmen *m*n* separate Rollen mit entsprechenden Berechtigungen anzulegen. Die Abbildung von Zugriffsentscheidungen, die nicht nur aufgrund eines Aufgabenprofils getroffen werden, ist in RBAC-Modellen also sehr schwer umzusetzen. Hier kann jedoch ein Vertrauensverhältnis zwischen den Partnern eine exzessive Detaillierung des Modells überflüssig werden lassen.

Tabelle 2 fasst die Charakteristika der Lösung mit einem zentralen Modell zusammen (+ = möglich, O = eingeschränkt, - = problematisch).

Anforderung	Erfüllbarkeit	
Partnerübergreifende Nutzeridentitäten	• Möglich, Nutzer als globale Konstrukte modelliert • Ermöglicht zentrale Authentifizierung und Rollenzuweisung	+
Konsistente Gesamtsicht	• Möglich, zentrales Modell impliziert Verfügbarkeit aller benötigten Informationen	+
Individuelle Zugriffsstrategien	• Möglich, Abbildung verschiedener Strategien durch unterschiedliche Konfiguration von Teilbereichen des Modells	+
Individuelle Organisationsstrukturen	• Problematisch, denn Modell impliziert gemeinsame Rollendefinitionen • Sehr feine Granularität erfordert Vielzahl von Rollen und damit hohen Aufwand	-
Mehrdimensionale Entscheidungen	• Eingeschränkt, über zusätzliche Rollen abbildbar • Vertrauen kann ggf. Modellierung ersetzen	O

Tabelle 2: Erfüllung der Anforderungen bei zentralem Rollenmodell

4.2 Dezentrale Rollenmodelle

Als Alternative zu einem gemeinsamen, kooperationsübergreifenden Sicherheitsmodell kann die Rechtezuordnung auch stärker dezentralisiert werden.

Eine Authentifizierung der Nutzer durch die jeweiligen Arbeitgeber kann hier als ausreichend angesehen werden, denn zwischen den Partnern besteht aufgrund ihrer Kooperationsbeziehungen ein Vertrauensverhältnis. Es ist daher möglich, ein gemeinsames Modell der existierenden Nutzer zu erstellen und Nutzeridentitäten partnerübergreifend zu akzeptieren.

Die Zuordnung von Rollen zu Nutzern kann nicht nur in einem gemeinsamen Modell, sondern auch dezentral bei den einzelnen Partnern erfolgen. Dies ist z. B. dann sinnvoll, wenn ein gemeinsames Rollenmodell aufgrund stark divergierender Vorstellungen der Partner nicht erstellt werden kann bzw. zu komplex wird. Die einzelnen Partner können dann als Alternative lokale Rollenmodelle pflegen oder Berechtigungen innerhalb ihrer Systeme direkt an Subjekte vergeben (wobei im Folgenden vom Vorhandensein lokaler Rollenmodelle ausgegangen wird). Dann muss jedoch ein Vorgehen gefunden werden, anhand dessen diese Zuweisungen erfolgen. Die Zuordnung kann manuell vorgenommen werden, indem die Rollenzuweisungen der Nutzer jeweils dezentral angelegt werden. Diese Variante steigert den Administrationsaufwand für die gesamte Kooperation deutlich, da die Zuordnungen der Nutzer bei jedem relevanten Partner einzeln verwaltet werden müssen. Sie birgt zudem die Gefahr unvollständiger Berechtigungen und begünstigt das Entstehen von „übrig gebliebenen" Rechten, wenn sich die Aufgabenbereiche von Nutzern ändern. Sinnvoller ist ein System, das die Zuordnung automatisiert. Hierfür müssen Kriterien festgelegt werden, die für die Zuordnungsentscheidung relevant sind. Es ist also ein von allen Teilnehmern akzeptiertes Beschreibungssystem nötig, anhand dessen die Nutzer charakterisiert werden. Diese festgelegten, zugriffsrelevanten Eigenschaften werden als Credentials bezeichnet [Bisk02].

Credential-basierte Sicherheitsmechanismen sind insbesondere im Kontext von verteilten Systemen mit unbekannten Nutzern und unsicheren Übertragungskanälen entwickelt worden, in denen keine zentralen Zugriffsschutzmodelle erstellt werden können. Dabei werden die Beschreibungen in der Regel in digital signierten Zertifikaten abgelegt [SaCa+01] [Bisk02]. Im hier behandelten Kontext kann allerdings auf den Einsatz von Zertifikaten verzichtet werden, da das System geschlossen ist. Die Nutzer sind bekannt und das Vorhandensein sicherer Übertragungskanäle zwischen den Systemen kann sichergestellt werden. Die Speicherung der Credentials kann in Datenbanken oder Verzeichnisdiensten erfolgen.

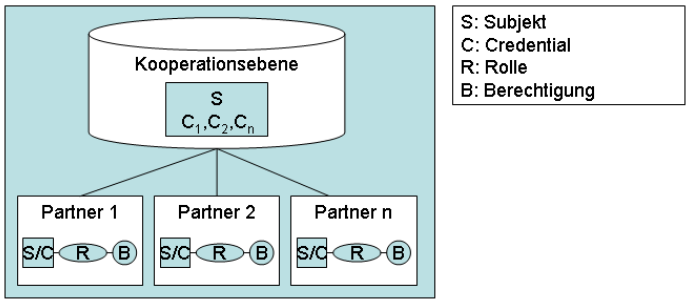

Abbildung 3: Credentialbasierter Ansatz mit dezentraler Rechtevergabe

Beispiele für relevante Credentials können Unternehmenszugehörigkeit, Projektmitarbeit, aber auch zwischen den Partnern abgeschlossene Vertraulichkeitsvereinbarungen sein. Damit kann etwa externen Nutzern, die an einem Projekt beteiligt sind, automatisch ein weitergehender Zugriff gewährt werden als nicht Beteiligten.

Das zentrale Rollenmodell wird hier also durch ein Nutzermodell ersetzt. Dieses wird dann auf der Ebene der Partner mit den lokalen Sicherheitsmodellen verknüpft. Abbildung 3 verdeutlicht das dezentrale System.

Dieses System zeigt hinsichtlich der Anforderungen teilweise andere Eigenschaften als das zentrale Modell (vgl. Tab. 3).

Eine **partnerübergreifende Nutzeridentifikation** ist auch bei dezentraler Rollenzuweisung möglich, da systemglobale Nutzeridentifikationen vorgesehen sind. Die Nutzeridentifikationen sind, ebenso wie die Credentials, für alle beteiligten Systeme gültig. Zudem wird vorausgesetzt, dass Authentifizierungen an Partnersystemen gültig sind. Dadurch kann auf eine Public-Key-Infrastruktur verzichtet werden, die in offenen credentialbasierten Systemen zur Feststellung der Gültigkeit von Credentials erforderlich ist.

Eine **konsistente Gesamtsicht** kann im dezentralen Modell nur schwer hergestellt werden. Wenn die Informationen über Berechtigungen dezentral verwaltet werden, müssen sie erst aufwändig aggregiert werden, um eine Übersicht bzw. eine übergreifende Verwaltung zu ermöglichen.

Die Berücksichtigung **individueller Zugriffsstrategien** ist in diesem Ansatz problemlos möglich. Da den Partnern nur Nutzerinformationen übermittelt werden, haben sie vollständige Kontrolle über die Ausgestaltung der Rechte(-vergabe) in ihren Systemen. Damit können individuelle Rollenkonzepte umgesetzt werden. Alternativ können aber auch gänzlich andere Kontrollsysteme etabliert werden, etwa herkömmliche Discretionary Access Control oder regelbasierte Varianten. Zudem können Ansätze genutzt werden, die das etablierte RBAC-Modell erweitern und Autorisierungsmechnismen umsetzen, die über den Fokus des Modells

hinausgehen [AoMi04]. Dann ist es allerdings unter Umständen nicht mehr möglich, die Vergabe von Zugriffsrechten über die Systemgrenzen hinweg zu aggregieren und zu überwachen. Sicherheitsmodelle können also nicht mehr systemweit geprüft werden und eine Übersicht über die gesamten Rechte bestimmter Nutzer geht verloren. Diese Abweichungen sind deshalb nur in Einzelfällen sinnvoll.

Die Abbildung **individueller Organisationsstrukturen** wird durch die dezentrale Rollenzuordnung ebenfalls vereinfacht. Da die einzelnen Sichtweisen der Partner nicht mehr in einem gemeinsamen Modell zusammengefasst werden müssen, können die lokalen Modelle problemlos an die Gegebenheiten einzelner Partner angepasst werden. Da die Notwendigkeit entfällt, verschiedene Strukturen in einem Modell abzubilden, erhöht sich zudem die Übersichtlichkeit der einzelnen Modelle.

Die Möglichkeiten, **mehrdimensionale Zugriffsentscheidungen** darzustellen, sind allerdings nach wie vor begrenzt. Wenn bei den Partnern rollenbasierte Systeme eingesetzt werden, ist auch hier die explizite Modellierung aller gewünschten Rollenvarianten möglich. Allerdings verringert sich die Anzahl der erforderlichen Varianten im Vergleich zum oben genannten Beispiel. Wenn wieder die Projektmitgliedschaft und die Unternehmenszugehörigkeit relevante Kriterien sind, müssen nur noch Rollen für interne und externe Mitglieder der jeweiligen Projekte angelegt werden. In bestimmten Fällen, etwa wenn eine größere Zahl von Kriterien in die Entscheidung einfließen soll oder wenn sich die Kriterien und ihre Kombinationen häufig ändern, können Zugriffssteuerungen sinnvoller sein, die Rechte auf der Basis logischer Regeln dynamisch zur Laufzeit vergeben [SaCa+01]. Diese können auch Mechanismen zur Auflösung von Konflikten zwischen Regeln enthalten.

Eine Zusammenfassung der Bewertung findet sich in Tab. 3 (+ = möglich, O = eingeschränkt, - = problematisch).

Anforderung	Erfüllbarkeit	
Partnerübergreifende Nutzeridentitäten	• Möglich, Nutzer und Beschreibungselemente als globale Konstrukte • Ermöglicht ebenfalls zentrale Authentifizierung, aber nur Beschreibung	+/O
Konsistente Gesamtsicht	• Problematisch, erfordert Aggregation der Berechtigungen auf zentraler Ebene	-
Individuelle Zugriffsstrategien	• Möglich: Abbildung verschiedener Strategien in lokalen Modellen, keine Konsensfindung erforderlich • In Einzelfällen Integration nicht rollenbasierter Modelle möglich	+
Individuelle Organisationsstrukturen	• Möglich: Dezentrale Modelle werden von Partnern eigenständig entwickelt • Erhöhte Übersichtlichkeit der Einzelmodelle	+
Mehrdimensionale Entscheidungen	• Möglich, weniger zusätzliche Rollen als bei zentralem Modell erforderlich • Ggf. Einsatz von regelbasierten Systemen für komplexere Entscheidungen	+/O

Tabelle 3: Erfüllung der Anforderungen bei dezentralen Rollenmodellen

4.3 Vergleich der Ansätze

Für die Erstellung von Sicherheitsmodellen für kooperativ genutzte IT-Systeme kommen grundsätzlich ein zentraler und ein dezentraler Ansatz in Frage. In Bezug auf die zu erfüllenden Anforderungen weisen die beiden Modelle folgende Gemeinsamkeiten und Unterschiede auf:

Beide Modelle ermöglichen übergreifende Nutzeridentitäten, die zwischen den beteiligten Systemen übertragen werden können. Da im dezentralen Modell allerdings keine gemeinsamen Rollen definiert werden, müssen Nutzer anhand von Beschreibungselementen charakterisiert werden. In beiden Fällen können somit Synergien bezüglich Administration und Zugriffsgewährung realisiert werden.

Eine konsistente Gesamtsicht ist hingegen nur im zentralen Modell problemlos möglich. Im dezentralen Modell wird sie erschwert und bei Integration alternativer Zugriffsmodelle kann sie gänzlich unmöglich werden. Damit können übergreifende Modelleigenschaften nur in der zentralen Variante nachgewiesen werden.

Die individuelle Zugriffssteuerung ist ebenfalls in beiden Modellvarianten möglich. Im zentralen Modell muss die dezentrale Verantwortung wenn nötig über administrative Rollen abgebildet werden. Die dezentrale Lösung hat den Vorteil, dass die einzelnen Partner volle Kontrolle über ihre Modelle haben. Zudem können bei einem Credential-Ansatz alternative Zugriffssteuerungen eingebunden werden, was in Sonderfällen von Interesse sein kann.

Die Berücksichtigung individueller Organisationsstrukturen ist im zentralen Modell schwierig, da hierfür eine Vielzahl einzelner Rollen erforderlich ist. Kann kein Konsens bezüglich der Rollengestaltung erzielt werden, sind dezentrale Modelle sinnvoller. Diese werden von den Partnern entwickelt und nicht in ein gemeinsames Modell überführt. Daher sind sie für die lokalen Administratoren übersichtlicher und einfacher zu verwalten.

Mehrdimensionale Entscheidungen können schließlich systembedingt in beiden Varianten nur eingeschränkt berücksichtigt werden, da sie stets zahlreiche Rollen erfordern. Im zentralen Modell ist die detaillierte Modellierung ggf. nicht möglich und muss durch Vertrauen ersetzt werden, während der Administrationsaufwand im dezentralen Modell durch die geringere Rollenzahl tendenziell geringer ist.

Grundsätzlich ist ein zentrales Sicherheitsmodell immer dann sinnvoll, wenn die synergieorientierten Anforderungen betont werden sollen. Eine konsistente Gesamtsicht und die partnerübergreifende Verwaltung von Nutzeridentitäten und -berechtigungen können hier besser realisiert werden. Die auf individuellen Schutz abzielenden Anforderungen können hingegen besser in dezentralen Modellen umgesetzt werden, da diese eine partnerspezifischere Modellierung individueller Strategien und Organisationsstrukturen erlauben.

5 Fazit

In kleinen Kooperationen, in denen sich die Anforderungen der Partner nur wenig unterscheiden, ist ein zentrales Sicherheitsmodell vergleichsweise einfach umzusetzen. Je größer die Anzahl der Partner jedoch wird, je stärker die geforderten Sicherheitsstrategien divergieren und je komplizierter eine Einigung auf Rollen und notwendige Berechtigungen wird, desto sinnvoller erweist sich der Einsatz eines dezentralen Modells. In diesen Fällen muss man sich auf den Austausch von Nutzeridentitäten und Credentials beschränken.

Wenn das gemeinsam erarbeitete Sicherheitsmodell in konkrete Softwareprodukte umgesetzt werden soll, zeigen sich allerdings noch erhebliche Defizite. Die etablierten Zugriffskontrollmechanismen stammen weitgehend aus dem Bereich der Großrechner und berücksichtigen die Anforderungen von verteilten Systemen, die aus einer Vielzahl einzelner Anwendungen bestehen, nur unvollständig. Derzeit verfügen viele betrieblich genutzte Anwendungen über proprietäre Sicherheitsme-

chanismen ohne Schnittstellen nach außen. Eine partnerübergreifende Sicherheitslösung muss in vielen Fällen erst implementiert bzw. beim Entwurf neuer Anwendungen berücksichtigt werden.

Erste Ansätze in diesem Bereich sind etwa die Entwicklung von SAML und XACML [LoPr+03], die als Austauschstandards für Authentifizierungs- und Autorisierungsinformationen dienen. Wenn solche Standards und Mechanismen in Softwareprodukte integriert werden, wird eine anwendungs- und unternehmensübergreifende Zugriffskontrolle möglich und kooperationsweite Sicherheitsmodelle können umgesetzt werden. Dies eröffnet neue Perspektiven für eine zwischenbetriebliche IT-Integration, die die Ausschöpfung von Synergiepotenzialen verbessert ohne individuelle Sicherheitserfordernisse zu vernachlässigen.

Literatur

[AoMi04] Ao, X.; Minsky, N. H.: On the role of roles: from role-based to role-sensitive access control, Proceedings of the ninth ACM symposium on Access control models and technologies, Yorktown Heights, New York, USA 2004, S. 51-60.

[Bisk02] Biskup, J.: Credential-basierte Zugriffskontrolle: Wurzeln und ein Ausblick, Bonn 2002.

[Coas37] Coase, R. H.: The nature of the firm. In: Economica 4 (1937) S. 386-405.

[DrMu+04] Dridi, F.; Muschall, B.; Pernul, G.: Administration of an RBAC System, Big Island, Hawaii 2004.

[Ecke03] : Eckert, C.: IT-Sicherheit: Konzept - Verfahren - Protokolle, 2, München 2003.

[FeKu+03] Ferraiolo, D. F.; Kuhn, D. R.; Chandramouli, R.: Role-based access control, Boston, Mass. 2003.

[FeSa+01] Ferraiolo, D. F.; Sandhu, R.; Gavrila, S.; Kuhn, D. R.; Chandramouli, R.: Proposed NIST standard for role-based access control. In: ACM Trans. Inf. Syst. Secur. 4 (2001) 3, S. 224-274.

[LoPr+03] Lorch, M.; Proctor, S.; Lepro, R.; Kafura, D.; Shah, S.: First experiences using XACML for access control in distributed systems, Proceedings of the 2003 ACM workshop on XML security, Fairfax, Virginia 2003, S. 25-37.

[OeHa03] Oelsnitz, D. v. d.; Hahmann, M.: Wissensmanagement: Strategie und Lernen in wissensbasierten Unternehmen, Stuttgart 2003.

[OsSa+00] Osborn, S.; Sandhu, R.; Munawer, Q.: Configuring role-based access control to enforce mandatory and discretionary access control policies. In: ACM Trans. Inf. Syst. Secur. 3 (2000) 2, S. 85-106.

[Rote90] Rotering, C.: Forschungs- und Entwicklungskooperationen zwischen Unternehmen: eine empirische Analyse, Stuttgart 1990.

[SaCa01] Samarati, P.; Capitani di Vimercati, S.: Access Control: Policies, Models, and Mechanisms, In: Focardi, R.; Gorrieri, R.: Foundations of Security Analysis and Design: Tutorial Lectures, Berlin 2001, S. 137-196.

[SaCo+96] Sandhu, R. S.; Coyne, E. J.; Feinstein, H. L.; Youman, C. E.: Role-Based Access Control Models. In: Computer 29 (1996) 2, S. 38-48.

[Sand01] Sandhu, R.: Future Directions in Role-Based Access Control Models. In: Lecture notes in computer science 2052 (2001) S. 22-26.

[Sand98] Sandhu, R.: Role-based Access Control. In: Advances in computers 46 (1998) S. 238-287.

[Schi99] Schier, K.: Vertrauenswürdige Kommunikation im elektronischen Zahlungsverkehr: ein formales Rollen- und Aufgabenbasiertes Sicherheitsmodell für Anwendungen mit multifunktionalen Chipkarten, Hamburg 1999.

[Seuf02] Seufert, S. E.: Der Entwurf strukturierter rollenbasierter Zugriffskontrollmodelle. In: Informatik Forschung und Entwicklung, Bd. 17 (2002) 1, S. 1-11.

[StWu01] Stevens, G.; Wulf, V.: Elektronische Archive in virtuellen Organisationen. In: Informatik-Spektrum 24 (2001) 6, S. 369-377.

[Stru99] Struthoff, R.: Führung und Organisation von Unternehmensnetzwerken: ein Konzeptentwurf am Beispiel intraorganisatorischer Netzwerke in der Automobilzulieferindustrie, Göttingen 1999.

[TaSt02] Tanenbaum, A. S.; Steen, M. v.: Distributed systems: principles and paradigms, Upper Saddle River, N.J 2002.

[Wohl02] Wohlgemuth, O.: Management netzwerkartiger Kooperationen: Instrumente für die unternehmensübergreifende Steuerung, Wiesbaden 2002.