Zusammenfassung

Gegenstand dieser Arbeit ist die rollenbasierte Zugriffskontrolle und deren Administrierung, bei denen ein dezentraler Ansatz zu Grunde gelegt wird. Dies wird durch die Einführung so genannter Autorisierungssphären erreicht, die es ermöglichen, hybride Zugriffsstrategien für bestimmte Teile einer Organisation dezentral zu spezifizieren und dabei die lokalen Erfordernisse zu berücksichtigen. Dabei besteht auch die Möglichkeit, die Aspekte einer verteilten Umgebung bei der Modellierung der Zugriffsprivilegien miteinzubeziehen.
Im Gegensatz zu anderen rollenbasierten Zugriffssystemen wird eine Trennung zwischen der eigentlichen Rollenhierarchie und dem Aufbau einer Organisation in Bereiche, Abteilungen und Arbeitsgruppen vorgenommen. Diese werden als Organisationseinheiten modelliert und gemäß den Gegebenheiten der Organisation hierarchisch strukturiert. Dies ermöglicht eine Vereinfachung der Rollenhierarchie, da in dieser Arbeit die Zugriffsprivilegien an Rollen in einer Organisationseinheit vergeben werden.

Eine völlig autonome Spezifizierung von Zugriffsprivilegien ist aus organisatorischer Sicht nicht sinnvoll. Daher sind die Autorisierungssphären gemäß den Gegebenheiten der Organisation hierarisch geordnet. Hierdurch ist es möglich, ein Vererbungsprinzip einzuführen, dem gemäß in einer übergeordneten Autorisierungssphäre festgelegt werden kann, welche der eigenen Zugriffsstrategien auch in bestimmten untergeordneten Autorisierungssphären gelten sollen. Sofern die Organisationsstruktur kein reines Einliniensystem ist, kann es aufgrund der hybriden Zugriffsprivilegien in Autorisierungssphären, die zwei direkte Vorgänger haben, zu Vererbungskonflikten kommen. Diese zeigen sich dadurch, dass zwei gegensätzliche Zugriffsprivilegien an diese Autorisierungssphäre vererbt werden. Sobald diese Vererbungskonflikte erkannt werden, können sie mittels verschiedener vorgestellter Lösungsstrategien aufgehoben werden.

In modernen Organisationen ist ein Zugriff auf Daten einer anderen Abteilung unerlässlich. Dabei müssen sowohl die Zugriffsstrategien beachtet werden, die den Arbeitsablauf für die Rolle festlegen, als auch die Zugriffsstrategien, die zur Sicherung der Daten spezifiziert werden. Im vorliegenden dezentralen Ansatz bedeutet dies, dass zwei Autorisierungssphären bei einer entsprechenden Zugriffsanfrage involviert sind. Wenn diese nicht zum selben Ergebnis kommen, liegt ein Koordinierungskonflikt vor. Dieser muss von einer übergeordneten koordinierenden Autorisierungssphäre durch entsprechende Regeln aufgelöst werden.

Zusätzlich zur Spezifizierung der Zugriffsstrategien sowie deren Vererbung und Koordinierung wird auch die eigentliche Umsetzung des Vererbungsprinzips und der Koordinierung von Zugriffen mittels fest vorgegebener Regeln in einer Datalog–Sprache modelliert. Durch die durchgehende Verwendung einer Datalog–Sprache bei der Auswertung einer Zugriffsanfrage kann nachgewiesen werden, dass die in dieser Arbeit fest vorgegebenen Regeln, das Vererbungsprinzip und die Koordinierung der Zugriffsanfragen korrekt umsetzen.

Neben den Zugriffsregeln müssen auch Rollen, Organisationseinheiten, Autorisierungssphären etc. und die entsprechenden Hierarchien dezentral administriert werden. Dabei ist nicht ein einzelner Administrator zuständig, sondern die Mitglieder eines Autorisierungsteams sind gemeinschaftlich verantwortlich.Diese werden hierzu in einen administrativen Prozess eingebunden, der in zwei Schritte unterteilt ist. Zunächst wird von einem einzelnen Benutzer ein Administrierungsvorschlag initiiert, der dann auf unterschiedliche Weise vom Autorisierungsteam bestätigt werden muss. Durch zusätzliche Administrierungsregeln können die Rechte zur Initiierung und auch die Beteiligung an der Bestätigung modelliert werden.

Die eigentlichen Abläufe bei der Bestätigung lassen sich formal nicht mittels Datalog spezifizieren. Daher wird eine neue Klasse von Petri–Netzen, sogenannte Administrationsnetze (Admin-Netze), eingeführt. Diese Administrationsnetze erlauben eine detaillierte Spezifizierung der Prozesse, wobei sowohl die beteiligten Administratoren als auch die Vorschläge, inklusive verschiedener Versionen und Teilvorschläge, erfasst werden. Die Interaktion mit den Administratoren wird durch spezielle Transitionen modelliert. Komplexere Abläufe lassen sich mittels Subnetze strukturieren. Hierdurch wird auch die formale Analyse der Administrationsnetze erleichtert.