Erweitertes rollenbasiertes Zugriffskontrollmodell - eRBAC

Das eRBAC ist ein auf dem RBAC basierendes erweitertes Zugriffskontrollmodell.

<insert Einleitungsbla>

Objekttypen

Neben den Entitäten Objekt, Operator und Zugriffsrecht wird die zusätzliche Entität Objekttyp eingeführt. Durch eine Typisierung von Objekten, wird im eRBAC zwischen dem Öffnen einer Anwendungssoftware und dem Aufruf von Objekten innerhalb einer Anwendungssoftware Unterschieden. Es werden als Objekttypen:

- Anwendung für Objekte, die den Einstiegspunkt in eine Anwendungssoftware darstellen und
- Klasse für Objekte, die Klassen innerhalb einer Anwenungssoftware repräsentieren

Jeder Rolle sind mindestens ein Objekt des Typs Anwendung und beliebig viele Objekte des Typs Klasse zugeordnet. Durch diese Einteilung zwischen Anwendung und Klasse kann eine Aufrufstruktur durch eine, eine automatische Weiterleitung zwischen Authentifizierung und Zugriffskontrolle, implementiert werden. Dazu besitzt ein Objekt des Typs Anwendung noch zusätzlich die Attribute Aufrufadresse, welche die Adresse der aufzurufenden Anwendung speichert und Aufrufbezeichnung welche den Namen der Anwendung zur Darstellung in bspw. Menüs behinhaltet.

Objekte und Operatoren können in eRBAC unabhängig voneinander definiert werden. Durch expliziete Zuordnung von Operatoren zu Objekten werden die Zugriffsrechte festgelegt. So können aus Gründen der Informationssicherheit unerwünschte Kombinationen vermieden werden.

Rollentypen und Rollen in eRBAC

In eRBAC werden Rollen in Rollentypen mit getrennten Sicherheitsrichtlinine eingeteilt. Die folgenden Rollentypen sind in eRBAC definiert:

- Anwendungsrollen
- Virtuelle Rollen
- Administrationsrollen
- Delegationsrollen

Anwendungsrollen bündeln die Zugriffsrechte vom öffnen der Anwendung bis hin zur Überprüfung jedes einzelnen Zugriffs auf von außen zugreifbare Funktionen eines Anwendungssystems. Sie können sowohl einem Subjekt direkt zugeordnet als auch in einer Rollenhierachie eingebunden werden.

Virtuelle Rollen sind Anwendungsrollen zum kapseln von Zugriffsrechten welche von mehreren Rollen benötigt werden. Dieser Rollentyp wird keinem Subjekt zugeordnet, sondern wird nur in der Rollenhierachie verwendet

Delegationsrollen werden benutzt um einen vorher durch die Administration als delegierbar gekennzeichnetee Teilmenge der Zugriffsrechte einer Anwendungsrolle zu delegieren. Delegationsrollen sind disjunkt zu Administrationst-/ und Anwendungsrollen. Delegation ist ein Mittel,

Zugriffsrechte über Rollen auf Zeit an ein anderes Subjekt zu übertragen. Folgene Konzepte gelten für die Delegation:

- Dauer: Die Subjektzuordnung kann mit einer Zeitangabe versehen werden, falls die Delegation nur zeitlich beschränkt werden soll.
- Monotonie: Es wird das Konzept der monotonen Delegation umgesetzt. Der Delegierende behält seine Zugriffsrechte.
- Gesamtheit: Es müssen die Zugriffsrechte der zu delegierenden Rolle nicht in ihrer Gesamtheit delegiert werden.
- Administration: Die Delegation wird vom Besitzer der Rolle vorgenommen.
- Delegationsstufen: Es wird eine einstufige Delegation unterstützt.
- Mehrfache Delegation: Es kann eine Rolle vom Delegierenden an mehr als ein Subjekt delegiert werden oder ein Subjekt kann für mehr als einen Delegierenden Delegierter sein.
- Vereinbarung: Der Delegierende entscheidet alleine über die Delegation.

Administrationsrollen bündel die Zugriffsrechte, die für die Rechteverwaltung notwendig sind. Die Administratorrolle ist aber disjunkt von den Rollen der anderen Rollentypen. Die Basiskomponenten dieser Rolle Vorbedingung und Rollenbereiche orientieren sich nicht an der bestehenden Subjekt- bzw. Zugriffsrechtszuordnung, sondern an davon separat definierten Subjekt- bzw. Zugriffsrechtepools, die sich am Aufbau der Organisation orientieren. den Administrationsrollen zugeordneten Subjekte können folgende Aufgaben wahrnehmen:

- Grundlagen: Objekte, Operatoren und Zugriffsrechte neu anlegen.
- Rollenverwaltung: Rollen anlegen, Zugriffsrechte zuordnen, Aufgabentrennung festlegen und Rollen in eine Rollenhierarchie einordnen.
- Subjektverwaltung: Subjekte mit ihren Zugangsdaten anlegen und die Subjektzuordnung vornehmen.
- Delegationsverwaltung: Festlegen, welche Zugriffsrechte und Rollen delegierbar sind.
- Domänenverwaltung: Zuordnen von Schlüsselwerten aus dem Anwendungssystem zur Festlegung der Attribute für die Personalisierung und die Domänenbeschränkung.

In eRBAC wird nur eine einstufige Delegations unterstützt. Es ist aber eine Mehrfachdelegation erlaubt. Ein Rücknahme der Delegation ist durch den Delegierenden und der Adminsitration möglich.

Personalisierung von Rollen

Durch eine Single-Sign-On-Authentifizierung wird zwar die Identität eines Subjektes unternehmensweit festgelegt, es kann aber notwendig sein, weitere Attribute des Subjektes bekannt zu machen. Die Daten zur personalisierung müssen im Zugriffskontrollsystem hinterlegt werden um an das Anwendungssystem übergeben zu werden. Dabei wird bei der Rolle hinterlegt, welche Datenobjekte aus dem Zielanwendungssystem für die Personalisierung eines Subjektes herangezogen werden. Für jedes Subjekt werden die Prmärschlüssel des entsprechenden Datenobjektes hinterlegt.

In FlexNow werden anhand der Organisationseinheit die zu bearbeitenden Lehrveranstaltungen und Prüfungen eines Prüfenden festgelegt. Es reicht in FN2RBAC der Schlüssel der Organisationseinheit aus, um diesen an das Anwendungssystem FlexNow zu übergeben und damit die entsprechenden Daten filtern und anzeigen zu können. Die anzuzeigenden Daten werden von der Geschäftslogik ermittelt. Ein mögliches Nutzungsszenario an Hochschulen ist, dass Mitarbeiter für mehrere Lehrstühle arbeiten. Durch dieses Konzept kann ein Mitarbeiter für verschiedene Lehrstühle Notenlisten bearbeiten, ohne dafür unterschiedliche Zugangsdaten zu benötigen.

Domänenbeschränkung durch parametrisierte Rollen

Alle Subjekte einer zugeordneten Tolle besitzend dieSelben Zugriddsrechte, aber jedes Subjekt dard nur die für Ihn erlaubten Daten sehen. Um nicht für jedes Subjekt eine persönliche Rolle anlegen zu müssen, wird die Domäne der Ergebnismenge über Parameter beschränkt. Dazu werdenn die Rollen parametrisiert. Zur Parametrieseirung werden in eRBAC Parameter hinterlegt und den Rollen zugeordnet, die je nach Zielanwendungssystem unterschiedlich sind. Nach der Subjektzuordnung werden jedem Subjekt die erlaubten Attributwerte für die Domänenbeschränkung eingetragen.