Rechtesystem

In diesem Abschnitt werden die Grundprinzipien des Rechtesystems erläutert.

Allgemeines

Rechte beziehen sich auf Operationen/Aktionen im System, wie etwa

- READ = lesen
- UPDATE = aktualisieren
- CREATE = anlegen

Das Recht auf eine Aktion/Operation kann dabei im System im Hinblick auf die Benutzerschnittstelle unterschiedlich implementiert sein:

- Aktion ist verfügbar, führt jedoch zu einer Fehlermeldung.
- Aktion ist nicht verfügbar (z.B. Button ausgegraut und nicht klickbar)
- Aktion ist nicht verfügbar (Button nicht sichtbar).

In der Regel versucht das System, Operationen/Aktionen überhaupt nicht anzuzeigen, wenn der betreffende Benutzer daran kein Recht hat. Unabhängig davom wird das Recht im "Backend" immer abgeprüft. Eine Manipulation des "Frontends", die etwa eine Funktion erscheinen lässt, auf die kein Recht existiert, kann trotzdem niemals dazu führen, dass die Aktion durchgeführt werden kann.

Ein Recht ist in der Regel immer erst einmal **funktionales Recht**. Das bedeutet, dass innerhalb der Programmierung beim Ausführen einer Funktion nur geprüft wird, ob das Recht im Moment zugewiesen ist oder nicht. Eine Berücksichtigung des Kontextes, in dem das Recht benötigt wird, findet nicht statt. Ein Beispiel: Das funktionale Recht "Update Benutzer" bezieht sich niemals auf einen spezifischen Datensatz, ist das Recht zugeordnet, darf jeder Benutzer geändert werden.

In weiten Bereichen der Mitgliederverwaltung reicht die Verwendung funktionaler Rechte nicht aus, da Zugriffsbeschränkungen benötigt werden, die den Zugriff auf einen **Teil der Datensätze** (in der Regel Mitglieder einer oder mehrere Gruppierung/en) reduzieren. Das bedeutet, dass der Kontext, in dem das Recht geprüft wird, berücksichtigt werden muss. Diese Rechte werden in der Dokumentation als **inhaltsbasierte Rechte** (auch datensatzbeschränkte Rechte, Filterrechte, Gruppierungsfilterrechte) bezeichnet, falls sich die Art des Rechtes nicht aus dem Zusammenhang ergibt.

Rechte in der Systemadministration: Funktionale Rechte

Funktionale Rechte (alle) werden im Rahmen der Benutzerverwaltung über Rechte-Gruppen den Benutzern zugeordnet (siehe Benutzer). Sie gelten ohne Beschränkung auf bestimmte Datensätze in der kompletten Systemadministration. Funktionale Rechte finden keine Anwendung in der Mitgliederverwaltung (s.u.).

> Tatsächlich umfassen die funktionalen Rechte auch die "datensatzbeschränkten" Rechte der Mitgliederverwaltung (s.u.), letztere sind einfach eine Teilmenge der kompletten funktionalen Rechte. Die Rechteverwaltung ist jedoch so aufgebaut, dass die funktionalen und datensatzbasierten Rechte und Rechtegruppen getrennt verwaltet werden können.

Rechte in der Mitgliederverwaltung/Gruppierungsverwaltung: Datensatzbasierte Rechte

Datensatzbeschränkte Rechte (manchmal ist auch von "Gruppierungsfilter-Rechten" die Rede, weil die Datensatzbeschränkung sich immer auf Gruppierungen bezieht) kommen überall innerhalb der Mitgliederverwaltung zum Einsatz, dort gibt es keine reinen funktionalen Rechte. In der Regel werden diese Rechte - im Gegensatz zu rein funktionalen Rechten - nicht in der Benutzerverwaltung zugewiesen, sondern im Rahmen der Tätigkeitszuordnung (siehe Zugeordnete Tätigkeiten (Tätigkeitszuordnungen)).

Dieses Konzept ist im Alltag einfach zu handhaben (bei der Tätigkeitszuordnung stehen bei korrekter Konfiguration in der Regel nur sehr wenige Rechtegruppen zur Auswahl) und ist zugleich enorm flexibel, weil die Rechteverteilung auf Basis von Tätigkeiten stattfindet, welche ein Mitglied nicht nur in seiner Stammgruppierung ausübt (= der Gruppierung, in der er geführt wird), sondern auch in anderen Gruppierungen. Damit kann jemand z.B. auf Ortsgruppenebene ein einfaches Mitglied ohne weitere Rechte sein, aber über seine Tätigkeit als Funktionär z.B. in einer Diözese weitreichende Rechte haben. Über das nachfolgend beschriebene Konzept der Ebenen- und Baumrechte ist es gleichzeitig auch noch möglich, Rechte in die Hierarchie zu bekommen, ohne dass diese gesondert auf jeder Ebene neu zugewiesen werden müssten.

Ebenenrechte

Ebenenrechte können bei der Zuordnung einer Tätigkeit zu einem Mitglied vergeben werden - es ist jedoch nicht zwingend, eine Tätigkeitszuordnung auch mit Rechten zu versehen. Rechte werden hier nicht durch Einzelrechte definiert, sondern durch die Auswahl einer Rechtegruppe (siehe Gruppen (MV)), die für diese Tätigkeit zulässig ist (siehe Gruppen (MV) pro Tätigkeit). Da die Rechte nur auf der Ebene genau **einer** Gruppierung vergeben wurden, erhält das Mitglied mit Vergabe der Tätigkeit keine Rechte in anderen Gruppierungen

Baumrechte

Die Vergabe der Baumrechte erfolgt analog der Vergabe der Ebenenrechte bei der Anlange einer Tätigkeit für ein Mitglied. Die Baumrechte führen allerdings nicht dazu, dass ein Mitglied in der Gruppierung, in welcher die Tätigkeit zugeordnet wurde, zusätzliche Rechte bekommt, sondern ausschliesslich auf allen Organisationsstrukturen (Gruppierungen), die sich unterhalb dieser Gruppierung befinden.

Das führt zu dem Problem, das Benutzer auf der obersten Ebene (Root/Wurzel-Ebene) keine Baumrechte zugewiesen bekommen können, da es oberhalb der Wurzel keine Tätigkeitszuordnungen (und damit verbundene Rechtezuweisungen) gibt. Das Problem wird dadurch gelöst, dass über einen Systemadministrator **ausgewählten Benutzern** Baumrechte über die Benutzer-Administration vergeben werden. Das erfolgt im Admin-Bereich über Personen -> Benutzer, "Root Rechtegruppe-Baum".

Achtung: Generell sollte dieses Recht nur temporär oder nur ausgesuchten Benutzer vergeben, da mit dieser Zuweisung das Rechtemanagement über Tätigkeitszuordnungen ausgehebelt wird.

Resultierende Rechte

Die resultierenden oder effektiven Rechte sind die Rechte, die ein Mitglied tatsächlich in einer Gruppierung hat, und zwar als Ebenenrechte und als Baumrechte (s.o.). So ist es denkbar, dass ein Benutzer Mitglied in einer Gruppierung G1 ist und dort über keinerlei Rechte verfügt, da er aber eine Tätigkeit in der übergeordneten Gruppierung G2 ausübt, die auch mit Baumrechten verbunden ist, erhält er nun auch Rechte in G1. Es ist sogar denkbar, dass gemeinsam benötigte Rechte (Beispiel: um schreiben zu können, muss auch das Leserecht vorhanden sein) aus unterschiedlichen Ebenen kommen.

Rechteprüfung in der Mitgliederverwaltung

Jeder Operation ist ein eigenständiges, (datensatzbasiertes) Recht (s.o.) zugeordnet. Bei der Überprüfung, ob der angemeldete Benutzer über das benötigte Recht verfügt, wird in der Mitgliederverwaltung nicht einfach nur die Zuordnung des Benutzers zu den Rechtegruppen überprüft. Es erfolgt vielmehr eine auf den kontextbezogene Prüfung:

- Der Kontext bezieht sich dabei immer auf die **Gruppierung**, in der die Operation ablaufen soll. In der Regel ergibt sich der Kontext aus der in der Baumansicht gewählten Gruppierung (nachfolgend im Beispiel mit G1 bezeichnet).
- Die Rechteverwaltung innerhalb der Mitgliederverwaltung basiert auf der Rechtezuordnung, die bei der Anlage von Tätigkeiten zu Mitgliedern explizit ausgewählt wird (Zugeordnete Tätigkeiten (Tätigkeitszuordnungen)). Aus diesem Grund kann die Mitgliederverwaltung auch nur von Benutzern verwendet werden, denen ein Mitglied zugeordnet ist.
- In der Baumansicht (Gruppierungsbaum) sind nur Gruppierungen sichtbar, die sich auf dem Pfad zu der/den Gruppierung/en befinden, auf welche der Benutzer Rechte hat.
- Für die Anzeige der möglichen Funktionen auf den Mitgliedern einer Gruppierung (anzeigen, bearbeiten, ...) muss dem aktuell angemeldeten Benutzer ein Mitglied zugeordnet sein.

Technischer Hintergrund

MenuItem (caea_menuitem)

Ein Recht ist das Bindeglied zwischen der Programmierung innerhalb des Systems und der zugehörigen Administration, die definiert, wer tatsächlich welche Rechte erhält. Rechte, die innerhalb der Programmierung nicht berücksichtigt wurden, können auch nicht administriert werden. Umgekehrt kann jedes Recht, das programmtechnisch berücksichtigt wurde, dynamisch administriert werden. *MenuItem* ist der technische Begriff für einen Eintrag im Rechtesystem (umgangsprachlich würde man schlicht "Recht" sagen, s.o.). Für jedes Recht, dass programmtechnisch berücksichtigt wurde, wird ein Platzhalter in der zugehörigen Datenbanktabelle erzeugt. Die Anlage von neuen MenuItems macht in der Regel keinen Sinn, da eine Verbindung zu Programmcode nicht existiert und damit keine funktionalen Auswirkungen verbunden sind.

In der Regel sind mehrere Rechte für die Abbildung eines abgeschlossenen Arbeitsablaufes notwendig (etwa Administration Benutzer: anlegen, sehen, editieren, löschen). Innerhalb der Abbildung der *MenuItems* wird dies durch die Zuordnung eines *MenuItems* zu einem *Menu* (Feld *menu_number*) erreicht. Das heißt, dass mehrere Rechte (*MenuItems*) die gleiche *menu_number* haben können, jedoch unterschiedliche *menuitem_order*. Nur die Kombination aus *menu_number* und *menuitem_order* ist eineindeutig und damit der Platzhalter für das programmtechnisch umgesetzte Recht. Die Felder "*name*", "*entity_name*" und "*securityoperation*" dienen nur Erläuterung, wozu der *MenuItem* programmtechnisch zugeordnet ist und sind eine Hilfe für den Administrator, zu verstehen, wo und wie das Recht in der Programmierung verwendet wurde.

Gruppen (caea_group)

Eine Gruppe hält eine Menge von Rechten (*MenuItems*) zusammen. Ein *MenuItem* kann dabei beliebigen unterschieldichen Gruppen zugeordnet sein. Die Gruppierung von *MenuItems* (über die *menu_number*) spielt keine Rolle.

Benutzer (caea_user)

Innerhalb der Mitgliederverwaltung sind fast alle Funktionen über das Rechtesystem zugriffsbeschränkt (Ausnahmen: Login-Seite, Passwort vergessen). Der Zugang zum System ist nur für "Benutzer" aus der Tabelle *caea_user* möglich. Bei der Anmeldung werden der Benutzername und das zugeordnete Passwort geprüft. Nach erfolgreicher Anmeldung wird eine Session erzeugt. Diese (bzw. ein Platzhalter für diese) wird über einen Session-Context im Web-Layer mittels Cookie an den Benutzer übertragen.

> ⚠ Es müssen Cookies erlaubt sein, um das System zu benutzen.

Die funktionalen Rechte des Benutzers ergeben sich aus der Zuordnung des Benutzers zu Gruppen (s.o.). Ein Benutzer kann dabei mehreren Gruppen zugeordnet sein. Die resultierenden (funktionalen) Rechte des Benutzer ergeben sich aus der Vereinigungsmenge der *MenuItems* aller Gruppen, denen der Benutzer zugeordnet ist. Die Überprüfung der Rechte erfolgt "on the fly". Das heißt, dass in der Regel eine Änderung der Rechte auch innerhalb einer laufenden Session berücksichtigt wird.