LU06a Berechtigungskonzepte

Lernziele

- Die drei Varianten von Berechtigungskonzepten nennen und erläutern können.
- Zu jeder der drei Varianten mindestens ein konkretes Produkt/Anwendung nennen können.
- Die Datengrundlage (Datenbankmodell) für jedes Konzept aufzeichnen und erläutern können.

Grundlagen

Ein Berechtigungskonzept beschreibt ein System, in dem die Nutzung von Ressourcen nicht uneingeschränkt möglich ist, sondern eine genaue Definition der Nutzung je Benutzer und Ressource erfolgt. Obwohl ursprünglich aus dem organisatorischen Umfeld kommend haben Berechtigungskonzepte, vor allem im Zusammenhang mit Systemen zur Informationstechnik, eine wichtige Bedeutung. Ressourcen sind hier beispielsweise Daten und Informationen, aber auch die technische Infrastruktur wie Systemzugänge, Speicherplatz, Rechnerleistung, Computerprogramme usw.

Schützenswerte Ressourcen können beispielsweise Hardware sein:

- Computer
- Rechenzeit
- Prozess-Priorisierung
- Drucker

Aber auch Software oder Daten müssen oft geschützt werden:

- Scripte und Applikationen
- Datenbankobjekte (Tabellen, Views, Stored-Procedures, Instanzen)

Schutz bedeutet also die Ressourcen vor Veränderung oder Zerstörung (z. B. Datensicherheit) zu schützen. Es bedeutet aber auch zu ihren unrechtmässigen Gebrauch (z. B. Datenschutz) zu verhndern.

Merke: Ein Berechtigungskonzept dient dem Schutz eine Ressource vor Veränderung oder Zerstörung, verhindert aber auch ihren unrechtmäßigen Gebrauch.

3 Varianten der Zugriffs-Steuerung

Es gibt verschiedene Ansätze dieses Thema zu vermitteln. Nachfolgend wollen wir uns auf die nachfolgenden drei Aspekte fokussieren.

- Benutzer-Ebene
- Gruppen-Ebene
- Rollen-Ebene

3.1 Benutzerbezogene Zugriffs-Steuerung

Rein Benutzerbezogene Konzepte neigen zur Unübersichtlichkeit und sind deshalb oft nur rudimentär ausgeprägt. Die Berechtigungen hängen direkt am User. Anpassungen müssen deshalb dann auch auf User-Ebene durchgeführt werden, was einen linearen Aufwand mit sich bringt. Sprich bei vielen Usern hat die Systemadministration sehr viel Arbeit.

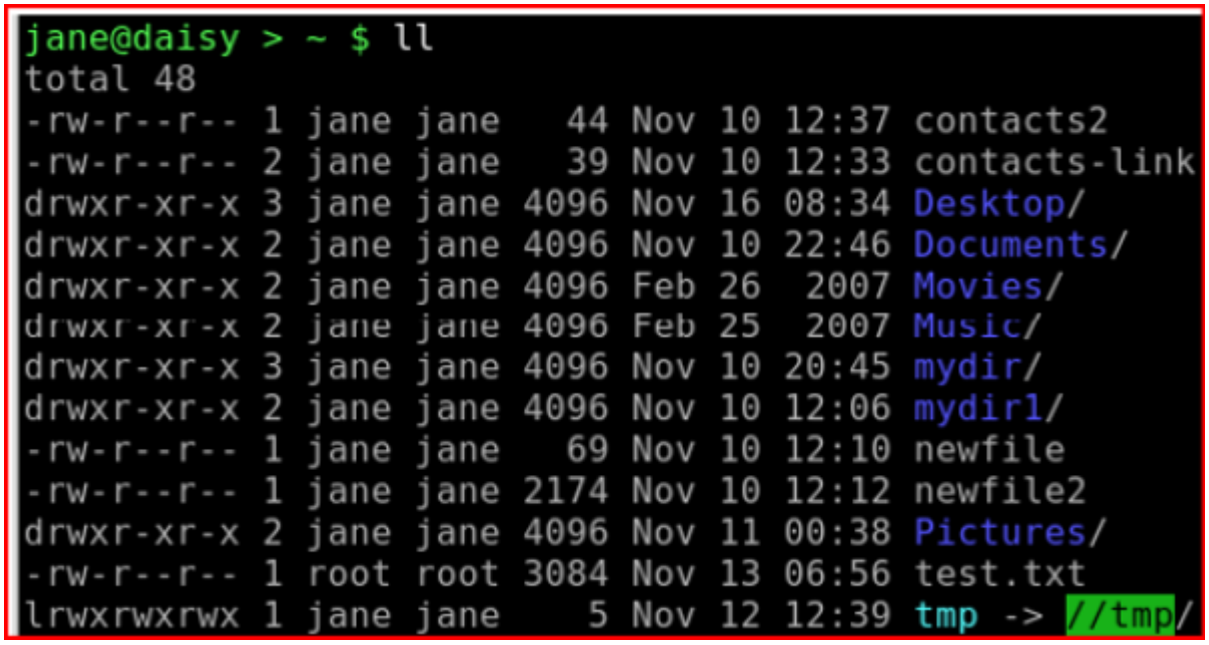
Das nachfolgende Entity Relationship Modell einer Benutzersteuerung auf Datenbankebene zeigt eine mögliche Umsetzung auf reiner Benutzerebene:

3.2 Gruppenbezogen Zugriffs-Steuerung

Besser ist ein Konzept über Benutzergruppen, da mittels dieser sich Berechtigungen zusammenfassen lassen. Das ist beispielsweise der Fall wenn die Berechtigungen aller Mitarbeitenden der Personalbuchhaltung angepasst werden müssen. Dies kann an einer Stelle durchgeführt werden und muss nicht einzeln beim Mitarbeitenden geschehen.

Das Betriebssystem UNIX ist ein Beispiel eine Benutzerverwaltung über Gruppen. Für jedes Objekt (Prozess, Datei, Verzeichnis, etc.) werden im Kern drei Gruppen zugelassen. Diese lassen sich beispielweise durch den Befehl *ls –lrt* ermitteln:

- Eigentümer (user)
- Gruppe (group)
- Die restliche Welt/Sonstige (others)



Jedem der eben genannten Objekte können via dem Befehl *chmod* drei Arten von Berechtigungen gegeben werden:

- Lesen (r=read)
- Schreiben (w=write)
- Ausführen (x=execute)

Neben der symbolischen Darstellung (z.B. rwxrwxr-x) gibt es auch noch eine oktale Darstellung. Die Grundrechte (Lesen, Schreiben, Ausführen) und Kombinationen daraus werden hierbei durch eine einzelne Ziffer repräsentiert und dem Eigentümer, der Gruppe und allen anderen zugeordnet. Je nach Anwendung wird dabei von unterschiedlichen Grundwerten ausgegangen und entweder Rechte gegeben oder entzogen.

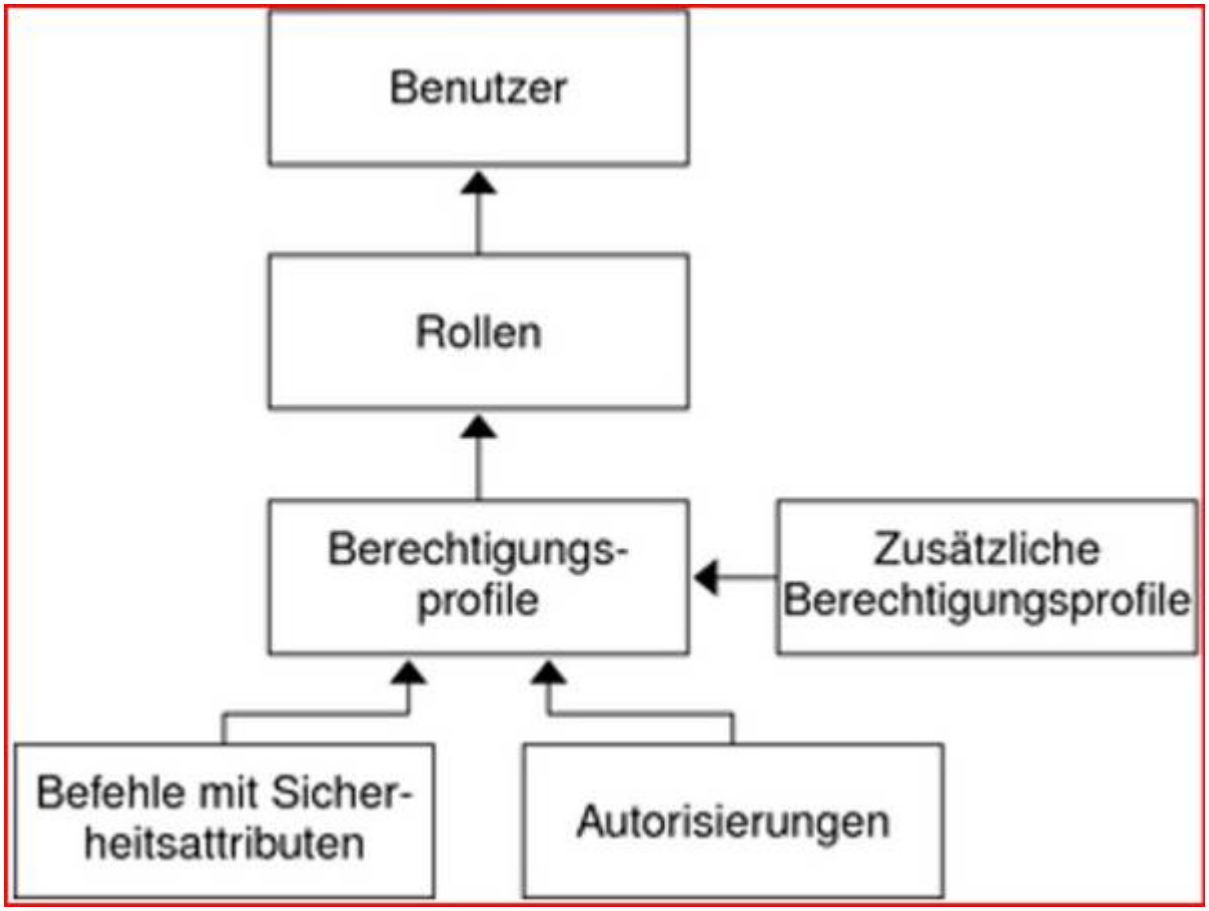
Bei *chmod* wird beispielsweise von der Grundeinstellung *keine Rechte* (000) ausgegangen und Rechte gegeben, wohingegen bei *umask* von *alle Rechte vorhanden* (777) ausgegangen und Rechte entzogen werden. Entsprechend sind die Werte je nach Anwendung anders.

Die nachfolgende Tabelle zeigt verschiedene Darstellungen dieser Unix-Gruppenrechte

Mögliche Werte für:				
	chmod (octal)	**umask (octal)**	**Symbolisch**	**Binäre Entsprechung**
Lesen, schreiben und ausführen	7	0	rwx	111
Lesen und Schreiben	6	1	rw-	110
Lesen und Ausführen	5	2	r-x	101
Nur lesen	4	3	r--	100
Schreiben und Ausführen	3	4	-wx	011
Nur Schreiben	2	5	-w-	010
Nur Ausführen	1	6	--x	001
Keine Rechte	0	7	---	000

3.3 Rollenbezogene Zugriffskontrolle

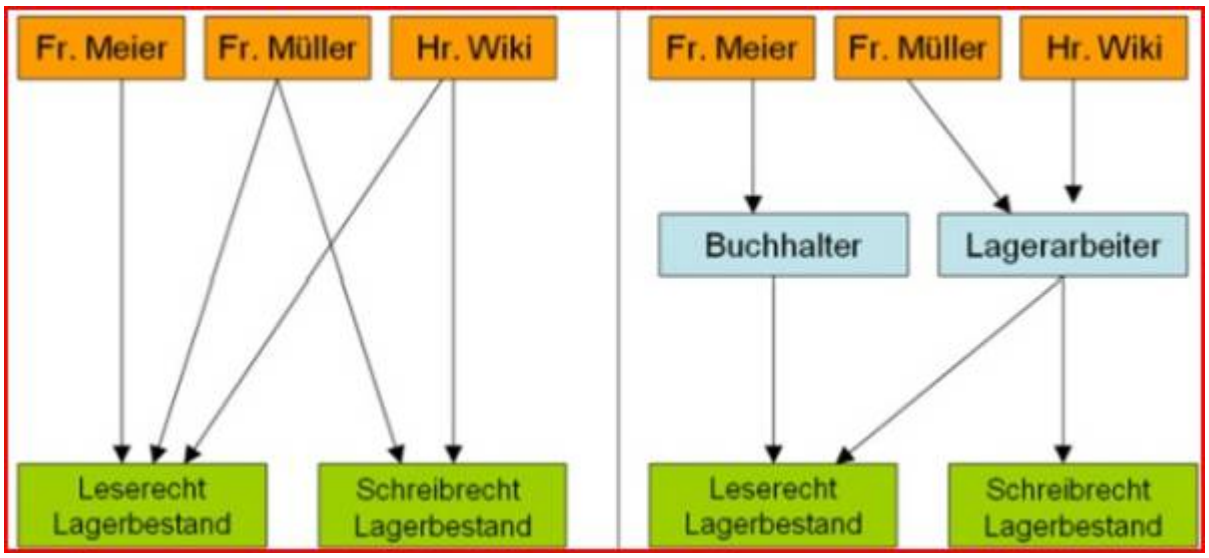
Das Verwalten der Benutzerrechte via Rollen erweitert die Gruppenverwaltung. Jedem Mitarbeiter, der nun konkret in der Personalbuchhaltung arbeitet, wird diese Rolle zugeordnet. Ein Mitarbeiter kann aber durchaus mehrere Rollen haben, wenn er mehrere Funktionen bekleidet. Auf diese Weise wird erreicht, dass sowohl Veränderungen in den Zuständigkeiten der einzelnen Mitarbeiter als auch Veränderungen im Geschäftsprozess, nur an jeweils einer Stelle im Berechtigungskonzept nachvollzogen werden müssen, und dieses konsistent und überschaubar bleibt.



4 Vergleich

4.1 Benutzter VS Gruppe/Rolle

Das nebenstehende Schaubild vergleicht die zwei Konzepte: Verwaltung auf reiner Benutzerebene mit der Verwaltung durch Rollen. Die Definition von Benutzerrollen gehört zum Aufgabenfeld der Berechtigungsadministration, die Zuordnung von Rollen an Benutzer dagegen als Teil der Benutzeradministration.



4.2 Rollen vs. Gruppe TBD

4. Vergleich der drei Arten

Aspekt	Benutzerbezogen	Gruppenbezogen	
Zuweisung	Rechte werden direkt einzelnen Benutzern zugewiesen	Benutzer werden Gruppen zugeordnet, Gruppen haben Rechte	Benutzer werden Rollen zugeordnet, Rollen haben Rechte
Fokus	Individuell, feingranular	Organisatorisch (Abteilung, Team)	Funktional (Aufgabe, Verantwortung)
Beispiel	Max darf Ordner X lesen	Max ist in Gruppe Marketing ⇒ Zugriff auf Marketing-Ordner	Max hat Rolle Rechnungsprüfer ⇒ darf Rechnungen freigeben
Verwaltung	Hoher Verwaltungsaufwand bei vielen Benutzern	Weniger Aufwand, da Rechte pro Gruppe verwaltet werden	Sehr übersichtlich, besonders bei vielen Aufgaben oder Wechseln
Flexibilität	Sehr flexibel, jeder Benutzer individuell einstellbar	Weniger flexibel bei Spezialfällen (Benutzer gehört oft mehreren Gruppen)	Flexibel bei Aufgabenwechsel, Rechte folgen der Rolle
Eignung	Kleine Systeme oder Sonderfälle	Organisationseinheiten mit gemeinsamen Aufgaben	Unternehmensweit, funktionale Prozesse
Admin-Aufwand	Sehr hoch – jeder Benutzer muss individuell verwaltet werden	Mittel – Gruppenrechte zentral, nur Mitgliedschaften ändern	Niedrig bis mittel – Rechte zentral pro Rolle, einfache Zuweisung bei Benutzerwechsel

Quellennachweis

- http://de.wikipedia.org/wiki/Berechtigungskonzept
- http://de.wikipedia.org/wiki/Role_Based_Access_Control
- http://de.wikipedia.org/wiki/Zugriffsrecht
- http://technet.microsoft.com/de-de/library/cc721640%28v=office.15%29.aspx

- http://de.wikipedia.org/wiki/Unix-Dateirechte
- http://de.wikipedia.org/wiki/Chmod
- http://wiki.ubuntuusers.de/Rechte
- http://de.wikipedia.org/wiki/Darwin_%28Betriebssystem%29
- http://wiki.ubuntuusers.de/MySQL_Workbench
- http://de.wikibooks.org/wiki/Oracle:_Benutzerverwaltung
- http://help.sap.com/printdocu/core/print46c/de/data/pdf/BCCCMUSR/BCCCMUSR.pdf
- http://www.linupedia.org/opensuse/Zugriffsrechte
