

MODUL 153

DATENMODELLE ENTWICKELN

Reto Glarner

Datenschutz und Datensicherheit



- › Sie können Schutz- und Sicherheitsbedürfnisse der Daten definieren und dokumentieren.
- › Sie kennen das Konzept der Rollen und kennen die unterschiedlichen Hierarchien der vordefinierten Rollen.
- › Sie können anhand der Kundenbedürfnisse eigene Benutzergruppen definieren.
- › Sie können Benutzer verwalten und mit korrekten Berechtigungen ausstatten.
- › Sie können die Umsetzung der Datensicherheit überprüfen.

Unterschied Datenschutz / Datensicherheit

Die Daten sind das Rückgrat jeder Unternehmung. Sie sollen ständig verfügbar sein, dürfen auf keinen Fall verloren gehen und gleichzeitig vor unbefugten Zugriffen geschützt werden. Das klingt fast ein wenig Widersprüchlich, ist aber durch eine saubere Auftrennung der Aufgaben in der Praxis durchaus realisierbar.

Folgendes sollte nicht passieren:



Artikel 1: „Schule erklärt Datenleck – und entfernt Zeugnisse“

Artikel 2: „950.000 Mailadressen von Festivalbesuchern zu verkaufen“

Artikel 3: „Daten von tausenden Studenten der Uni Magdeburg im Netz“

Wir unterscheiden Datensicherheit und Datenschutz!

Datensicherheit	
Ziele	Massnahmen
Verfügbarkeit Datenverlust verhindern	Datensicherung und Wiederherstellungstests Systemwartung und –prüfung (Ressourcen, Updates...) Redundanz (Clustering, Mirroring, ..) Schutz gegen Angriffe (Virenschutz, DOS, ..) Physischer Schutz (abgeschlossene Räume)
Integrität garantieren Schutz von Änderungen	Protokollierungen von Änderungen (Social Engineering, Hacking, ..)
Vertraulichkeit garantieren Nur Berechtigte haben Zugriff	Berechtigungssystem für den Zugang (Logins) Berechtigungssystem für die internen Strukturen (DCL Sprache) Verschlüsselung der Zugänge und Übertragung
	Für alle 3 Ziele von enormer Wichtigkeit: Schulung des Personals!

Datenschutz (=Gesetzliche Vorgaben)	
Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden¹	<p>Kernpunkte:</p> <p>Nur rechtmässige Bearbeitung Die Beschaffung muss erkennbar sein Grenzüberschreitende Nutzung Datensicherheit (s. oben) Auskunftsrecht...</p> <p>Besonders schützenswerte Daten sind Daten über:</p> <ol style="list-style-type: none"> 1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, 2. die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, 3. Massnahmen der sozialen Hilfe, 4. administrative oder strafrechtliche Verfolgungen und Sanktionen;

Der Datenschutz wird also per Gesetz definiert!

Wer macht was?

Um die rechtliche Situation müssen sich je nach Daten und Verwendungszweck die Juristen kümmern. Aus technischer Sicht ist eine Rollentrennung sinnvoll, erinnern Sie sich noch an die unterschiedlichen Aufgabenbereiche des Datenmanagement?

Datenarchitekt	Datenadministration	Datentechnik	Datennutzung
Erstellung und Pflege des Datenmodells Stützen der Anwendungsentwickler	Standardisieren von firmenweiten Datenbeständen	Installation RDBMS Pflege RDBMS Backup und Restore	Erstellen von Auswertungen unter Einhaltung des Datenschutzes

¹ Bundesgesetz über den Datenschutz <https://www.admin.ch/opc/de/classified-compilation/19920153/index.html>

Dies hilft uns nur geringfügig weiter, wir ändern die Fragestellung: *Wer kann was tun für den Datenschutz?*

Datenarchitekt	Datenadministration	Datentechnik	Datennutzung
Umsetzung eines Berechtigungssystems innerhalb der Datenbanken, Tabellen und Attribute	Review der firmenweiten Umsetzung des Datenschutzes	Physischer und logischer Schutz von Backupmedien Setzen von Richtlinien (Passwortlänge, Ablaufdatum, Komplexität) Verschlüsselung der Kommunikation Protokollierung der Zugriffe	Schnittstelle zu Juristen Kontrolle der Einhaltung (menschlicher Faktor)

Aus Sicht der Datenarchitekten können wir uns darum kümmern, dass die von uns erstellten Datenbanken mit den korrekten Berechtigungen versehen werden. Nichtsdestotrotz erweitern wir unseren Horizont bis auf Serverebene, da das Berechtigungssystem hierarchisch aufgebaut ist. Wir beginnen mit der obersten Hierarchie, den Serverrollen.

Hinweis: Nachfolgend werden teilweise Themen aus der Datentechnik behandelt. Dies sind jedoch nur Fragmente, welche zum Verständnis des Berechtigungskonzept für Datenarchitekten notwendig sind. Das Ziel ist nicht die beiden Aufgabenbereiche zu mischen oder gar gleichzustellen.



Vertiefung «Protokollierung der Zugriffe»

4_SQL Server effizient absichern mit C2-Überwachung, DLL-Trigger und Server Audit.pdf

Rollen

Rollen sind eigentlich Benutzergruppen, denen ein oder mehrere Benutzer zugeordnet werden können. Der SQL Server bietet für Berechtigungen drei grundlegende Hierarchien an Rollen:

1. Serverrollen (gelten für das ganze RDBMS bzw. Instanz)
2. Datenbankrollen (gelten für die jeweiligen Datenbanken)
3. Benutzerdefinierte Rollen (Gelten für Datenbanken, Tabellen, Attribute)

Zurück zum Fallbeispiel von Tante Emma:

Der Datenbankserver wird nicht nur intern vom Personal von Tante Emma benutzt, sondern auch von der Marketingfirma, welche die Flyer versendet. Für die maximale Sicherheit wird auf dem SQL Server *ausschliesslich* die Windows-Authentifizierung eingesetzt. Es werden vier Kategorien von Benutzerinnen und Benutzern unterschieden:

- › Kategorie **DB-Administration**: 2 Mitarbeiter der IT Firma (Datentechniker, DB-Architekt)
 - › alle Administrationstätigkeiten über den ganzen SQL Server.
- › Kategorie **Datenerfassung und -bereinigung**: 4 Mitarbeiter von Tante Emma (Datennutzer)
 - › Daten laufend pflegen und Neuerfassung von Kunden, Lieferanten und Interessenten sowie Produkten
 - › Neue Tabellen und Views anlegen zum Zweck des Imports und Bereitstellung für externe Benutzer
- › Kategorie **Datenauswertung**: 1 Mitarbeiter von Tante Emma (Datennutzer)
 - › Datenbankabfragen in Form von SQL-Skripts für Produkt- und Verkaufsstatistiken
- › Kategorie **externe Datennutzer**: 1 Mitarbeiter der Marketingfirma (Datennutzer ausserhalb der Domäne, externer Zugriff übers Internet)
 - › Datenbankabfragen in Form von VIEWS, kein direkter Zugriff auf die originalen Tabellen!

Auftrag 1



Anhang A – Sicherheit und Zugriffsberechtigungen

Ordnen Sie den Benutzern der vier Zugriffskategorien die nötigen Server- und/oder Datenbankrollen zu!

Kategorie	Serverrolle	Datenbankrolle
DB-Administration		
Datenerfassung		
Datenauswertung		
Externe Datennutzer		

Auftrag 2

Exemplarisch für den Laden von Tante Emma benötigen wir für die Abbildung der drei Zugriffskategorien folgende drei Benutzer:

Kategorie	Windowsbenutzername	Anmeldebenutzername	Datenbankbenutzername
DB-Administration	<i>dbAdmin</i>	<i>dbAdmin</i>	<i>dbAdmin</i>
Datenerfassung	<i>dbModifier</i>	<i>dbModifier</i>	<i>dbModifier</i>
Datenauswertung	<i>dbReporter</i>	<i>dbReporter</i>	<i>dbReporter</i>

- Erstellen Sie die drei Benutzer *dbAdmin*, *dbModifier*, *dbReporter* in der Windowsbenutzerverwaltung als normale Benutzer ohne Sonderrechte. Als Kennwort, welches nie abläuft, vergeben Sie *sml12345*.
- Im Management Studio des SQL Servers erstellen Sie als nächstes die Anmeldungen.

Sie können eine neue Serveranmeldung (Anmeldung) hinzufügen, indem Sie im Management Studio im Objekt-Explorer den Ordner *Sicherheit* öffnen. Darunter finden Sie den Ordner *Anmeldungen* vor. Über das Kontextmenü wählen Sie den Befehl *Neue Anmeldung...* aus. Um ein Windows-Benutzerkonto für den Zugriff auf den Datenbankserver freizugeben, tragen Sie den Benutzernamen in der Syntax *Domäne\Benutzer* ein oder suchen den Namen über den von Betriebssystemaufgaben bekannten Suchdialog.

- Weisen Sie der neuen Anmeldung bei der Erstellung ihre Serverrollen gemäss Auftrag 1 zu.

Dazu wechseln Sie auf die Seite *Serverrollen*. Dort klicken Sie die Kontrollkästchen neben jenen Rollen an, die sie zuordnen möchten.

- Legen Sie fest, in welcher Datenbank zugleich ein Benutzer mit den entsprechenden Datenbankrollen für die neue Anmeldung erstellt werden soll. In unserem Fall betrifft dies die Datenbank **Laden**. (Falls Sie diese nicht mehr haben, erstellen Sie diese mit dem Script aus AB02)

Den Benutzer für können Sie auf der Seite Benutzerzuordnung festlegen. Als Benutzername wird standardmässig der Anmeldename vorgeschlagen. Um diesen Namen zu editieren, klicken Sie einfach in die Spalte Benutzer.

Für eine ausgewählte Datenbank können Sie im unteren Bereich des Dialogs die Datenbankrollen auswählen, die dem neuen Benutzer zugewiesen werden sollen.

Der Datenbankzugriff für eine Anmeldung kann auch später über die jeweilige Datenbank erteilt werden.

- Überprüfen die Einstellungen auf der Datenbank *Laden* der Benutzer *dbModifier* und *dbReporter*. Rechtsklick auf Datenbank *Laden* – *Eigenschaften* – *Berechtigungen* – *dbModifier* bzw. *dbReporter* auswählen – *effektive Berechtigung*.

dbModifier

Permission	Permission	Permission	Permission
ALTER ANY ASSEMBLY	ALTER ANY ROUTE	CREATE CONTRACT	CREATE RULE
ALTER ANY ASYMMETRIC KEY	ALTER ANY SCHEMA	CREATE DATABASE DDL EVENT NOTIFICATION	CREATE SCHEMA
ALTER ANY CERTIFICATE	ALTER ANY SERVICE	CREATE DEFAULT	CREATE SERVICE
ALTER ANY CONTRACT	ALTER ANY SYMMETRIC KEY	CREATE FULLTEXT CATALOG	CREATE SYMMETRIC KEY
ALTER ANY DATABASE DDL TRIGGER	CHECKPOINT	CREATE FUNCTION	CREATE SYNONYM
ALTER ANY DATABASE EVENT NOTIFICATION	CONNECT	CREATE MESSAGE TYPE	CREATE TABLE
ALTER ANY DATASPACE	CREATE AGGREGATE	CREATE PROCEDURE	CREATE TYPE
ALTER ANY FULLTEXT CATALOG	CREATE ASSEMBLY	CREATE QUEUE	INSERT REFERENCES
ALTER ANY MESSAGE TYPE	CREATE ASYMMETRIC KEY	CREATE REMOTE SERVICE BINDING	SELECT
ALTER ANY REMOTE SERVICE BINDING	CREATE CERTIFICATE	CREATE ROUTE	DELETE UPDATE

dbReporter

Permission
CONNECT
SELECT

- Testen Sie nun die Berechtigungen indem Sie sich nacheinander mit den verschiedenen Benutzern anmelden² und folgendes Testszenario durchspielen. Die Tests sind jeweils im Management Studio in einem Abfragefenster durchzuführen: (die Abfragen finden Sie als Datei vorbereitet)

Anmeldung	Test	erwartetes Resultat	effektives Resultat
dbAdmin	CREATE DATABASE Test;	DB erstellt	
	DROP DATABASE Test;	DB gelöscht	
	CREATE LOGIN test WITH PASSWORD= 'test';	User erstellt	
	DROP LOGIN test;	User gelöscht	
	USE Laden; GRANT SELECT ON KUNDE TO guest;	Berechtigung erteilt	
	REVOKE SELECT ON KUNDE TO guest;	Berechtigung entzogen	
	CREATE VIEW test AS	View erstellt	

² alle Programme schliessen und von Windows abmelden und mit dem gewünschten Benutzer neu anmelden.

	SELECT Vorname + ' ' + Name AS Kundenname, Preis AS Lieferkosten FROM KUNDE INNER JOIN LIEFERKOSTEN ON KUNDE.LieferkostenID = LIEFERKOSTEN.LieferkostenID		
	DROP VIEW test;	View gelöscht	
dbModifier	CREATE DATABASE Test;	Verweigert	
	CREATE LOGIN test WITH PASSWORD= 'test';	Nicht berechtigt	
	USE Laden; GRANT SELECT ON KUNDE TO guest;	Nicht berechtigt	
	CREATE VIEW test AS SELECT Vorname + ' ' + Name AS Kundenname, Preis AS Lieferkosten FROM KUNDE INNER JOIN LIEFERKOSTEN ON KUNDE.LieferkostenID = LIEFERKOSTEN.LieferkostenID	View erstellt	
	DROP VIEW test;	View gelöscht	
	SELECT * FROM EINHEIT;	Wird angezeigt	
	INSERT INTO EINHEIT(Name) VALUES('TEST');	Satz eingefügt	
	DELETE FROM EINHEIT WHERE Name = 'TEST';	Satz gelöscht	
dbReporter	CREATE DATABASE Test;	Verweigert	
	CREATE LOGIN test WITH PASSWORD= 'test';	Nicht berechtigt	
	USE Laden; GRANT SELECT ON KUNDE TO guest;	Nicht berechtigt	
	CREATE VIEW test AS SELECT Vorname + ' ' + Name AS Kundenname, Preis AS Lieferkosten FROM KUNDE INNER JOIN LIEFERKOSTEN ON KUNDE.LieferkostenID = LIEFERKOSTEN.LieferkostenID	Nicht berechtigt	
	SELECT * FROM EINHEIT;	Wird angezeigt	
	INSERT INTO EINHEIT(Name) VALUES('TEST');	Nicht berechtigt	
	DELETE FROM EINHEIT WHERE Name = 'TEST';	Nicht berechtigt	

Auftrag 3

Die Benutzer der Kategorie „Datenauswertung“ sollen nicht auf die ganze Datenbank zugreifen können. Um die Berechtigungen innerhalb einer Datenbank abzugrenzen reichen die eingebauten Datenbankrollen nicht aus. (db_datareader kann **alle** Daten innerhalb einer Datenbank auslesen)

Zudem soll die Abfrage für die externen Benutzer möglichst einfach gestaltet werden, es soll eine einzige Tabelle zur Verfügung stehen, welche alle relevanten Daten anzeigt.

Glücklicherweise stellt der SQL Server für diese Anforderungen die richtigen Werkzeuge zur Verfügung:

Anforderung: Umformung der Daten für die einfachere Abfrage → Einsatz von Views

Die Anweisung unten wurde so erstellt, dass die externe Marketingfirma alle relevanten Daten auslesen kann, auf die Artikel und Rechnungen aber keinen Zugriff erhält:

```
USE Laden
GO
CREATE VIEW NURKUNDENNAME AS
SELECT Name, Vorname FROM KUNDE
GO
```

Anforderung: Benutzer sollen nur gewisse Daten auslesen dürfen → Benutzerdefinierte Rollen

Erstellen Sie per Skript einen neues SQL-Login „dbExternalUser“ (Passwort sml12345)

```
CREATE LOGIN
```

Erstellen Sie einen neuen Benutzer „dbExternalUser“ für dieses Login

```
CREATE USER
```

Erstellen Sie eine neue benutzerdefinierte Rolle „rlExternalUser“

```
CREATE ROLE
```

Geben Sie der neuen Rolle Leseberechtigung auf der oben erstellten VIEW

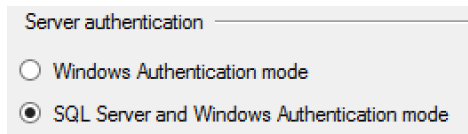
```
GRANT SELECT ON
```

Wenden Sie die neue Rolle „rlExternalUser“ für den Benutzer „dbExternalUser“ an.

```
exec sp_addrolemember 'rlExternalUser','dbExternalUser'
```

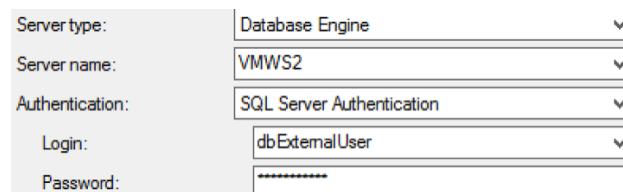
Testen des Logins:

Bevor das SQL Benutzer Login funktioniert, muss der SQL Server in den „gemischten Modus“ gebracht werden. BMW1 -> Eigenschaften -> Sicherheit -> SQL Server und Windows Authentifizierungsmodus



(Neustart des SQL Servers notwendig)

Melden Sie sich am SQL Server mit dem neuen Benutzer „dbExternalUser“ an und testen Sie, ob die Berechtigungen funktionieren!



Nun sollten keine Tabellen mehr angezeigt werden. Lediglich die VIEW „NURKUNDENNAME“ kann ausgeführt werden.

Mit benutzerdefinierten Rollen kann eine höhere Granularität erzeugt werden als mit den eingebauten Server- und Datenbankrollen. Mittels DCL (GRANT, REVOKE) können Berechtigungen auf Tabellen- und sogar Attributebene erteilt bzw. entzogen werden.

Zur Repetition hier nochmals die komplette Syntax:

```
GRANT privilege_name  
ON object_name  
TO {user_name | PUBLIC | role_name}  
[WITH GRANT OPTION];
```

```
REVOKE privilege_name  
ON object_name  
FROM {user_name | PUBLIC | role_name}
```