

Neue Funktionen zur Datensicherheit

in den DB2-Versionen

9.1 und 9.5

von

H.A. Pürner

DB2Sec-1

© Pürner Unternehmensberatung, Dortmund, 2008



Pürner Unternehmensberatung Ingenieurbüro für Informationstechnologie

- Gegründet 1986
- Spezialisiert auf
 - Datenbank-Technologie
 - Datenbank-Migrationen
 - Datenmodellierung
 - Tool-Beratung
 - Training
- Erreichbar:

Robert-Götz-Str. 14

44319 Dortmund

☎ 0231 5600394

✉ info@puerner.com

DB2Sec-2

© Pürner Unternehmensberatung, Dortmund, 2008



Überblick

- Anforderungen an Sicherheit und deren Überwachung
- Neue Lösungsansätze
 - Security Administrator
 - Rollen
 - Trusted Context
 - Verbesserte Audit-Funktionen
 - Label Based Access Control
 - LBAC Beispiel

DB2Sec-3

© Pürmer Unternehmensberatung, Dortmund, 2008



Globale Regelungen

- Wichtige neue Regeln zur Datensicherheit
provoziert durch Wirtschaftsskandale in den letzten Jahren
- Globalisierung zwingt Unternehmen auch Regeln anderer Staaten einzuhalten
- Folgen:
 - Deutlich erhöhte Anforderungen an Datensicherheit und ihrem Nachweis
 - Bisherige Lösungen reichen nicht mehr aus

DB2Sec-4

© Pürmer Unternehmensberatung, Dortmund, 2008



Globale Regelungen

Dank der globalen Natur des Web müssen internationale Datenschutz- und Datensicherheitsregelungen beachtet werden. Einige Beispiele solcher Regeln:

- Payment Card Industry (PCI) Data Security Standard (DSS): This regulation is owned and distributed by the PCI Security Standards Council. It is a collaborative effort between major credit card companies and is designed to protect customers' personal information.
- California Senate Bill 1386: This is an amendment that provides consumers notice of security breaches involving compromised personal information.
- Health Insurance Portability and Accountability Act of 1996 (HIPAA): This act focuses on health care and is designed to protect all forms of personal health information by defending patients rights to have their health information kept private.
- Gramm-Leach-Bliley Act of 1999 (GLBA): This act defines that the financial institutions must comply with the privacy provisions which mandate controls over customers' non political personal information (NPI) with respect to usage, protection, and distribution.
- Sarbanes-Oxley Act: This act redesigned federal regulation of public company corporate governance and reporting obligations by demanding accountability and assurance of financial reporting by executives, auditors, securities analysts and legal counsel.
- Personal Information Protection and Electronic Documents Act (PIPEDA): This act is a Canadian law that incorporates and makes mandatory provisions of the Canadian Standards Association's Model Code for the protection of personal information. PIPEDA contains various provisions to facilitate the use of electronic documents and governs how private-sector organizations collect, use, and disclose personal information in the course of commercial business.
- Data Protection Act (DPA): This is a United Kingdom Act of Parliament that defines a legal basis for the handling in the UK of information relating to living people. It is the main piece of legislation that governs protection of personal data in the UK. Compliance with the Act is overseen by an independent government authority, the Office of the Information Commissioner (OIC).

Quelle: IBM Redbook SG24-7555

DB2Sec-5

© Pürmer Unternehmensberatung, Dortmund, 2008



Globale Regelungen

Regulation	Requirement
Sarbanes-Oxley Section 302	Unauthorized changes to data
Sarbanes-Oxley Section 404	Modification to data, Unauthorized access
Sarbanes-Oxley Section 409	Denial of service, Unauthorized access
Gramm-Leach-Bliley	Unauthorized access, modification and/or disclosure
HIPAA 164.306	Unauthorized access to data
HIPAA 164.312	Unauthorized access to data
Basel II – Internal Risk Management	Unauthorized access to data
CFR Part 11	Unauthorized access to data
Japan Privacy Law	Unauthorized access to data
PCI – Requirement 7	Restrict access to cardholder data by business need-to-know
PCI – Requirement 8.5.6	Enable accounts used by vendors for remote maintenance only during the time period needed
PCI – Compensating Controls for Requirement 3.4	Provide ability to restrict access to cardholder data or databases based on the following criteria: <ul style="list-style-type: none"> • IP address/Mac address • Application/service • User accounts/groups
PCI - Requirement A.1: Hosting providers protect cardholder data environment	Ensure that each entity only has access to own cardholder data environment

Quelle: Oracle White Paper „Oracle Database Vault“, 2007

DB2Sec-6

© Pürmer Unternehmensberatung, Dortmund, 2008



Multilevel Security

- Mehrstufiges Sicherheitsverfahren
- Klassifikation von
 - Objekten (Daten)
 - Subjekten (Benutzern)
- Hierarchische Sicherheitsstufen
- Nicht-hierarchische Sicherheitskategorien
- Mandatory Access Control (MAC)
 - Security Administrator
 - Subjekte können Zugriff auf Objekte nicht kontrollieren
 - Abkehr vom Eigentümer-Prinzip

DB2Sec-7

© Pürmer Unternehmensberatung, Dortmund, 2008



Multilevel Security

Die Charakteristiken eines mehrstufigen Sicherheitssystems sind:

- Das System steuert den Zugang zu den Ressourcen.
- Das System erzwingt Zurechenbarkeit durch die Anforderung an jeden Benutzer, sich zu identifizieren, und durch Schreiben von Prüfsätzen, die sicherheitsrelevante Ereignisse den verursachenden Benutzern zuordnen.
- Das System kennzeichnet alle Ausdrücke mit Sicherheitsinformationen.
- Das System erlaubt nicht die Wiederverwendung eines Speicher-Objekts, bis es von seinen restlichen Daten gesäubert wurde.
- Das System verbirgt optional die Namen von Dateien und Verzeichnissen vor Benutzern, die für den Zugriff auf diese Datenobjekte keine Berechtigung haben.
- Das System erlaubt es Benutzern nicht, Daten herabzustufen (*write down*) (d.h. Daten auf eine niedrigere Einstufung zu schreiben als gelesen) außer mit einer expliziten Berechtigung dazu.

DB2Sec-8

© Pürmer Unternehmensberatung, Dortmund, 2008



Klassische Sicherheitslösungen

DB2

- Statisches SQL: Benutzer dürfen Programme ausführen (EXECUTE PACKAGE), haben aber keine Rechte an anderen DB2-Objekten (Tabellen, Views)
- Dynamisches SQL: Vereinfacht gesagt müssen Benutzer die entsprechenden Rechte an den bearbeiteten Objekten besitzen

Klassische Anwendungen

- Berechtigungsprüfungen finden in den Anwendungsprogrammen statt, nicht in der Datenbank
- EXECUTE PACKAGE häufig an PUBLIC vergeben

Anwendungen mit Application Server

- Berechtigungsprüfungen finden in den Anwendungsprogrammen statt. Der Datenbankzugriff erfolgt mit der User-ID des Application Server.
- AS-User verfügt über weitreichende Objekt-Rechte

DB2Sec-9

© Pürmer Unternehmensberatung, Dortmund, 2008



DB2 Berechtigungen

Ältere Konzepte

- Administrative Berechtigungsprofile
 - wie SYSADM, DBADM...
- Objektbezogene Rechte
 - wie Lesen, Ändern oder Einfügen von Zeilen einer Tabelle oder Sicht
 - Eigentümer-Orientierung

Neue Konzepte

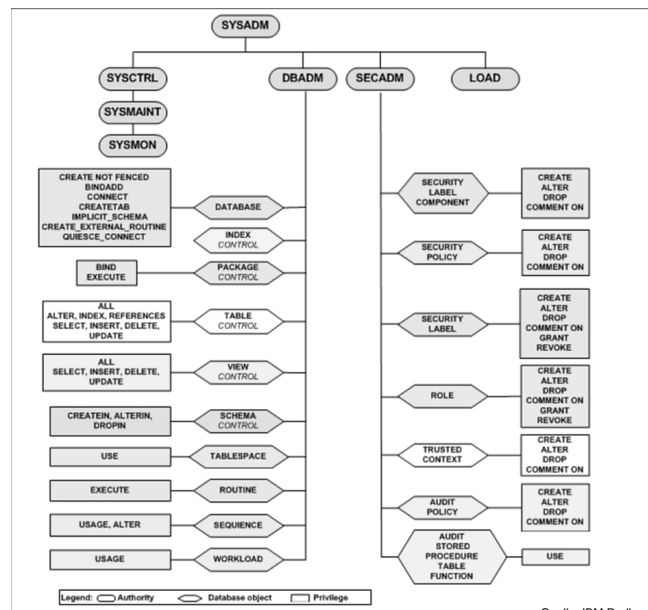
- Administratives Berechtigungsprofil SECADM
- Rollen
 - DB2-verwaltete Gruppenprofile
- Label Based Access Control (LBAC)
 - für Tabellenspalten und -zeilen
- Trusted Context
 - Berechtigungen nur mit definierten Verbindungen

DB2Sec-10

© Pürmer Unternehmensberatung, Dortmund, 2008



DB2 V9.5 Berechtigungsstruktur



Quelle: IBM Redbook.SG24-7555

DB2Sec-11

© Pürmer Unternehmensberatung, Dortmund, 2008



Security Administrator SECADM

- Vergabe durch SYSADM
- Nur Benutzer, keine Gruppen
- Datenbankbezogen
- Keine Berechtigung zum Datenzugriff
- GRANT SECADM ON DATABASE TO USER *db2sec*

DB2Sec-12

© Pürmer Unternehmensberatung, Dortmund, 2008



Security Administrator SECADM

CREATE, ALTER, COMMENT ON, DROP

- Audit policies, security label components, security policies, trusted contexts

CREATE, COMMENT ON, DROP :

- Roles, security labels

GRANT, REVOKE

- Roles, exemptions, security labels, SET SESSIONUSER privileges

Nutzung von AUDIT Stored Procedures und Table Functions:

- SYSPROC.AUDIT_ARCHIVE, SYSPROC.AUDIT_LIST_LOGS, SYSPROC.AUDIT_DELM_EXTRACT

Nutzung des AUDIT-Befehls zur Verknüpfung einer Audit Policy mit einer Datenbank oder einem Datenbank-Objekt

Transfer der Eigentums an einem fremden Objekt mit dem Befehl
TRANSFER OWNERSHIP

DB2Sec-13

© Pürmer Unternehmensberatung, Dortmund, 2008



Rollen

- DB2-Objekt mit einer oder mehreren Berechtigungen
- Entsprechen Gruppen ohne Bezug zu externen Sicherheitsmechanismen (OS, LDAP, KERBEROS)
- Vergabe nur durch SECADM
- Vereinfachte Rechte-Vergabe an Nutzer
- Nutzung in Trusted Context
- Aufbau von Rechte-Hierarchien (GRANT ROLE ... TO ROLE ..)
-> *mit Gruppen nicht so möglich*
- Rollen im Gegensatz zu Gruppenberechtigungen werden berücksichtigt beim CREATE von
 - PACKAGEs mit statischem SQL
 - TRIGGERS
 - VIEWS
 - MQTs
 - SQL Routinen

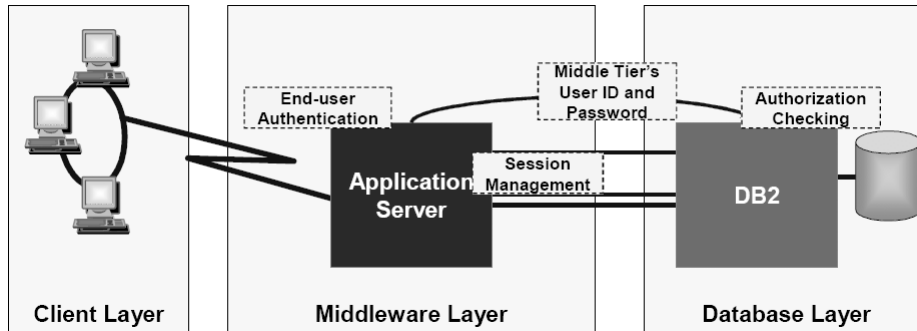
DB2Sec-14

© Pürmer Unternehmensberatung, Dortmund, 2008



Trusted Context

Server-Verbindung ohne Trusted Context



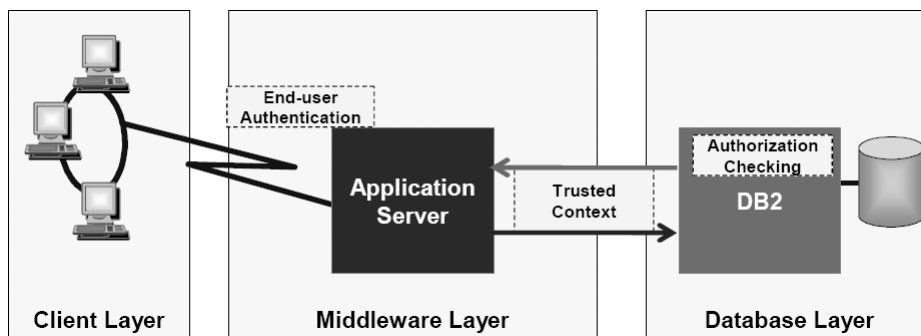
Quelle: IBM Redbook SG24-7555

DB2Sec-15

© Pürmer Unternehmensberatung, Dortmund, 2008



Trusted Context



Quelle: IBM Redbook SG24-7555

DB2Sec-16

© Pürmer Unternehmensberatung, Dortmund, 2008



Trusted Context

Konzept einer als gesichert angesehenen Verbindung zwischen DB2 und einem externen Objekt

- Kontext-abhängige Berechtigungen
- Nur 1 Trusted Context je User
- Mehrere User je Trusted Context
- Katalog:
 - SYSCAT.CONTEXTS
 - SYSCAT.CONTEXTATTRIBUTES
 - SYSCAT.SURROGATEAUTHIDS

DB2Sec-17

© Pürmer Unternehmensberatung, Dortmund, 2008



Trusted Context Syntax

```
CREATE TRUSTED CONTEXT appServer  
  BASED UPON CONNECTION USING SYSTEM AUTHID  
    appServerID  
  ATTRIBUTES (ADDRESS 'host-1.dept.organization.com',  
              ADDRESS 'host-2.dept.organization.com'  
              ENCRYPTION 'HIGH')  
  DEFAULT ROLE appServerRole  
  WITH USE FOR PUBLIC WITHOUT AUTHENTICATION,  
  UserA WITH AUTHENTICATION ROLE mgrRole  
  ENABLE
```

DB2Sec-18

© Pürmer Unternehmensberatung, Dortmund, 2008



Trusted Context

- Nur explizit aufgebaute Trusted Contexts erlauben Umschalten der User-ID
- Implizit aufgebauter Trusted Context => nur Rollenzuordnung
- Expliziter Trusted Context nur über CLI und JDBC => Auswirkung auf Programmcode
- Umschalten der User-ID
 - Nur auf Transaktionsgrenze erlaubt
sonst ROLLBACK und Terminierung der Verbindung
 - Alter Benutzer verliert seine Umgebung (z.B. HOLD Cursor, Temp Tables)

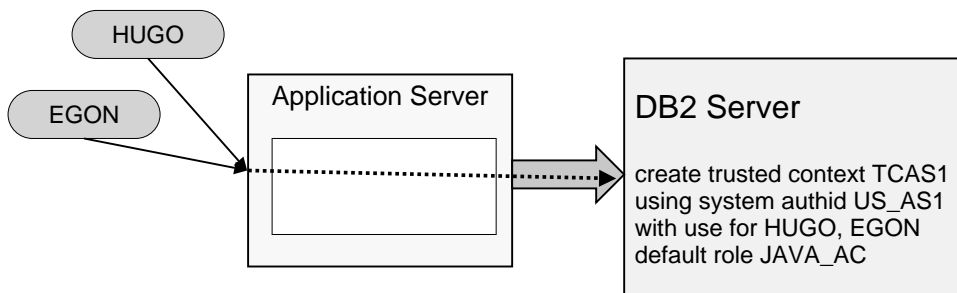
DB2Sec-19

© Pürmer Unternehmensberatung, Dortmund, 2008



Trusted Context Beispiel mit Dynamic SQL

- Objekt-Rechte für dynamische SQL werden an Rolle JAVA_AC vergeben
- Rolle wird Benutzern nur bei Nutzung der Verbindung TCAS1 zugeordnet
- Benutzer-IDs im DB2-Server bekannt
- Audit-Möglichkeit über End-Benutzer
- Vereinfachte Rechte-Verwaltung



DB2Sec-20

© Pürmer Unternehmensberatung, Dortmund, 2008



AUDIT-Funktionen

- DB2-Kommando db2audit -> SYSADM
- Archivierung von Audit Logs
- Audit Policy (mit CREATE) -> SECADM
 - Kleinere Audit trails
 - Weniger Overhead
 - In 9.5 neue Kategorie: EXECUTE
- AUDIT SQL-Befehl auf den Ebenen Database, Table, Trusted Context, User/Groups/Roles, Authorities (SYSADM,DBADM,SECADM)
zum Beispiel:

```
AUDIT DATABASE USING POLICY auditdb
```

DB2Sec-21

© Pürmer Unternehmensberatung, Dortmund, 2008



AUDIT Policy Kategorien

AUDIT

- Überwachung der Audit-Definitionen oder des Zugriffs auf das Audit-Log

CHECKING

- Aufzeichnung von Zugriffs- oder Manipulationsversuchen bei der Autorisierungsprüfung von Datenbank-Objekten oder -Funktionen

CONTEXT

- Aufzeichnung des Kontexts von Datenbank-Operationen

OBJMAINT

- Überwachung des Anlegens und Löschens von Daten-Objekten

SECMAINT

- Aufzeichnung des Gewährens und Widerrufens von Objekt- oder Datenbankrechten oder DBADM-Berechtigung, sowie von Änderungen der Konfigurationsparameter SYSADM_GROUP, SYSCTRL_GROUP oder SYSMaint_GROUP

SYSADMIN

- Aufzeichnung von Operationen, für die SYSADM-, SYSMaint- oder SYSCTRL-Berechtigung erforderlich sind

DB2Sec-22

© Pürmer Unternehmensberatung, Dortmund, 2008



AUDIT Policy

Kategorien

VALIDATE

- Aufzeichnung der Authentifizierung von Benutzern oder der Suche von zugehörigen Sicherheitsinformationen

EXECUTE

- Überwachung der Ausführung von SQL-Befehlen sowie optional Aufzeichnung der Eingabedaten zu den ausgeführten Befehlen
- neue Kategorie auf Datenbank-Ebene, ersetzt CONTEXT für SQL-Befehle
- Ausreichende Informationen zur Wiederholung von Befehlen, um ihre Auswirkung zu verstehen
- liefert:
 - Befehlstext
 - Datentyp, Länge, Wert von Eingabevariablen und Parametermarkern (außer LOBS, LONG, XML und strukturierte Typen)
 - Kompilierungsumgebung
 - Zähler für gelesene, zurückgegebene und geänderte Zeilen

DB2Sec-23

© Pürmer Unternehmensberatung, Dortmund, 2008



DB2 Label Based Access Control

- DB2 Label Based Access Control (LBAC) ist eine flexible Implementierung der Mandatory Access Control (MAC) auf der Ebene von Spalten **und** Zeilen.
- Zeilen- und spaltenbezogener Schutz kann zusammen oder getrennt genutzt werden.
- LBAC ergänzt die bestehende Discretionary Access Control (DAC) in DB2.
- Beim Zugriff auf eine Tabelle erzwingt DB2 nun zwei Ebenen der Kontrolle:
 - DAC auf Tabellenebene stellt sicher, daß die Autorisierungs-ID die erforderlichen Rechte besitzt, um die gewünschte Operation auf der Tabelle ausführen zu dürfen.
 - LBAC sichert dies auf Zeilen- und/oder Spaltenebene.

DB2Sec-24

© Pürmer Unternehmensberatung, Dortmund, 2008



Label Based Access Control in DB2

- Security Administrator SECADM
- Eine Policy definiert Label-Komponenten und Zugriffsregeln
- Labels für Zeilen, Spalten und Benutzer
- Eine zusätzliche Spalte für Zeilen-Labels je geschützter Tabelle, unabhängig von der Anzahl der Label-Komponenten
- Drei Arten von Label-Komponenten: Set, Array oder Tree
 - Set: Aufzählung ohne Strukturierung, z.B. Verkaufsregionen Nord, Süd, West, Ost
 - Array: geordnete Aufzählung mit einfacher Hierarchie, z.B. Geheimhaltung vertraulich, geheim, streng geheim
 - Tree: Baumstruktur, z.B. zur Abbildung einer Firmenhierarchie Mitarbeiter, Abteilungsleiter, Bereichsleiter, Vorstand
- Maximal 16 Komponenten

DB2Sec-25

© Pürmer Unternehmensberatung, Dortmund, 2008



Label Based Access Control in DB2

LBAC – Label Component ARRAY

- **Array** – ordered set that can be used to represent a simple hierarchy

▶ ['Top Secret', 'Secret', 'Confidential', 'Unclassified']

▶ User has label { 'Unclassified' }

▶ User has label { 'Secret' }

Label	Value
'Secret'	1
'Confidential'	2
'Unclassified'	3
'Top Secret'	4
'Secret'	5

Label	Value
'Secret'	1
'Confidential'	2
'Unclassified'	3
'Top Secret'	4
'Secret'	5

Label	Value
'Secret'	1
'Confidential'	2
'Unclassified'	3
'Top Secret'	4
'Secret'	5

© IBM, 2005

DB2Sec-26

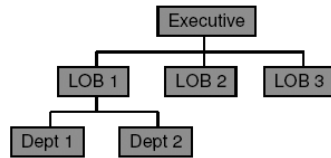
© Pürmer Unternehmensberatung, Dortmund, 2008



Label Based Access Control in DB2

LBAC – Label Component TREE

- Tree – represents a more complex hierarchy that can have multiple nodes and branches



Label	Value
'Dept 1'	1
'Dept 2'	2
'Lob 1'	3
'Executive'	4
'Lob 2'	5

- ▶ User has label { 'Lob 1' }
- ▶ User has label { 'Dept 2' }

Label	Value
'Dept 1'	1
'Dept 2'	2
'Lob 1'	3
'Executive'	4
'Lob 2'	5

Label	Value
'Dept 1'	1
'Dept 2'	2
'Lob 1'	3
'Executive'	4
'Lob 2'	5

© IBM, 2005

DB2Sec-27

© Pürmer Unternehmensberatung, Dortmund, 2008



Schrittweises Vorgehen

Die Konzeptionsphase umfaßt:

- Erhebung der Sicherheitsanforderungen durch
 - Analyse der Anwendungen
 - Analyse der verarbeiteten Informationen
 - Analyse der Benutzeranforderungen
- Erstellung eines Sicherheitskonzepts mit
 - Klassifikation der Daten entsprechend ihrer Sensitivität
 - Zugriffskriterien der Benutzer
 - Festlegung der Benutzer-Freigaben

Die technische Implementierung erfolgt in den Schritten:

1. Definition von Policy und deren Komponenten
2. Definition der Daten-Labels
3. Definition der Benutzer-Labels
4. Anwenden der Policy auf die Objekte (Tabellen)
5. Erzeugen der konkreten Label-Werte in den Objekten

DB2Sec-28

© Pürmer Unternehmensberatung, Dortmund, 2008



Das Fall-Beispiel

- Die kleine Republik von Costa Banana hat die Zeichen der Zeit erkannt:
- Zentrale Datei zur Terroristenbekämpfung
- für Polizei und Geheimdienst
- mit registrierten Terrorverdächtigen mit persönlichen Stammdaten, Bewegungsdaten, Verweisen auf Kriminal- und Geheimdienst-Dateien und sonstigen Kennzeichen
- Datei steht Polizei und Geheimdienst zur Verfügung.
- Da die Datenfelder von unterschiedlicher Sensitivität sind, stehen sie auch nicht allen Polizisten zur Verfügung.
- Costa Banana ist in 4 autonome Provinzen (Nord, Süd, West, Ost) aufgeteilt:
- Polizisten dürfen nur die Daten der Verdächtigen sehen, für die Dienststellen ihrer Provinz zuständig sind.
- Der zentrale Geheimdienst hat Zugriff auf alle Daten.
- Verantwortlich für die Pflege der von der Polizei eingebrachten Daten sind die Sonderkommissionen "Anti-Terror" in den vier Provinzen.

DB2Sec-29

© Pürmer Unternehmensberatung, Dortmund, 2008



Das Fall-Beispiel

- Weitere Zugriffsbeschränkungen:
- normale Polizisten nur auf als terrorverdächtig eingestufte (TV)
- Kriminaldirektoren auf die als aktiv eingestuften (AT)
- Die Sonderkommissionen auch auf die Anführer (Top Terroristen - TT).
- Die Polizei darf die Datenfelder IDGEHDienst (ID DB Geheimdienst) und VMANNKZ (V-Mann-Kennzeichen) nicht sehen.
- Aus Sicherheitsgründen ist VMANNKZ auch im Geheimdienst nur ausgewählten Beamten zugänglich.
- Innerhalb der Polizei sind die Felder GEFEINSTUFUNG (Gefährdungseinstufung), IDKRIMREG (ID im Kriminal-Register), IDTERRORNETZ und BEZTERRORNETZ (ID und Bezeichnung in der Datei "Terrornetzwerke") nur den Sonderkommissionen zugänglich.

DB2Sec-30

© Pürmer Unternehmensberatung, Dortmund, 2008



Benutzer

In Vertretung der möglichen Benutzer betrachten wir die folgenden:

- "Harry" - ein einfacher Polizist der Nordprovinz
- "Derrick" - ein Kriminaldirektor der Ostprovinz
- "Soko" - ein Mitglied der Sonderkommission der Westprovinz
- "Schlphut" - ein anonymer Angehöriger des Geheimdiensts
- "Bond" - ein Special Agent des Geheimdiensts mit V-Mann-Berechtigung

DB2Sec-31

© Pürmer Unternehmensberatung, Dortmund, 2008



Anti-Terror-Datei

PNR	- Eindeutige Identifikation
NAME	- Name
VORNAME	- Vorname
NAMENSZUSATZ	- Namenszusatz, Geburtsname oder Deckname
HERKUNFTSLAND	- Staat, in der die Person geboren wurde
GESCHLECHT	- Kennzeichen für Geschlecht (M, F)
GEDDAT	- Geburtsdatum
ERSTEINDAT	- Datum der ersten Einreise
LETZTEINDAT	- Datum der letzten Einreise
LETZTAUSDAT	- Datum der letzten Ausreise
STAATSANGEH	- aktuelle Staatsangehörigkeit
ZUST_DIENSTS_ST	- zuständige Polizei-Dienststelle
PROVINZ	- Provinz der zuständige Polizei-Dienststelle
GEFEINSTUFUNG	- Einstufung der von der Person ausgehenden Gefährdung
	TV - Terrorverdächtig
	AT - Aktiver Terrorist
	TT - Rädelsführer, Top Terrorist
VMANNKZ	- Kennzeichen, ob als V-Mann tätig
IDKRIMREG	- Identifikation im Kriminalregister
IDTERRORNETZ	- Identifikation des Terroristen-Netzwerks, dem die Person angehört
BEZTERRORNETZ	- Kurzbezeichnung des Terroristen-Netzwerks
IDGEHDienst	- Identifikation in der Datenbank des Geheimdiensts

DB2Sec-32

© Pürmer Unternehmensberatung, Dortmund, 2008



Fall-Bespiel DB2

Zum Schutz der Zeilen gegen unberechtigten Zugriff werden 2 Komponenten benötigt. Mit der ersten werden die Gefährdungseinstufungen hierarchisch abgebildet:

```
CREATE SECURITY LABEL COMPONENT SLC_GKZ
ARRAY ['TT', 'AT', 'TV'];
```

Mit der zweiten wird die staatliche Struktur von Costa Banana (Zentralstaat mit 4 Provinzen) modelliert:

```
CREATE SECURITY LABEL COMPONENT SLC_STAAT
TREE ('Zentralstaat' ROOT,
'Nordprovinz' UNDER 'Zentralstaat',
'Ostprovinz' UNDER 'Zentralstaat',
'Suedprovinz' UNDER 'Zentralstaat',
'Westprovinz' UNDER 'Zentralstaat'
);
```

DB2Sec-33

© Pürmer Unternehmensberatung, Dortmund, 2008



DB2 LBAC-Komponenten

Für den Schutz der Tabellenspalten wird eine dritte Komponente mit hierarchischer Struktur benötigt:

```
CREATE SECURITY LABEL COMPONENT SLC_LVL
ARRAY ['streng-geheim', 'geheim', 'vs', 'frei'];
```

Die Sicherheitsrichtlinie umfasst diese drei Komponenten:

```
CREATE SECURITY POLICY ANTI_TERROR_POLICY
COMPONENTS SLC_LVL, SLC_STAAT, SLC_GKZ
WITH DB2LBACRULES
RESTRICT NOT AUTHORIZED WRITE SECURITY LABEL;
```

DB2Sec-34

© Pürmer Unternehmensberatung, Dortmund, 2008



DB2 Spalten-Labels

Dann sind die Kesssätze (Labels) mit den Werten zu definieren, die in der weiteren Verarbeitung benötigt werden. Für die zu schützenden Spalten werden folgende Labels angelegt:

```
CREATE SECURITY LABEL ANTI_TERROR_POLICY.VS
COMPONENT SLC_LVL 'vs';

CREATE SECURITY LABEL ANTI_TERROR_POLICY.GH
COMPONENT SLC_LVL 'geheim';

CREATE SECURITY LABEL ANTI_TERROR_POLICY.SGH
COMPONENT SLC_LVL 'streng-geheim';
```

DB2Sec-35

© Pürmer Unternehmensberatung, Dortmund, 2008



DB2 Zeilen-Labels

Für die zu schützenden Zeilen werden Labels mit den Kombinationen aus SLC_STAAT und SLC_GKZ gebildet.

```
CREATE SECURITY LABEL ANTI_TERROR_POLICY.NPROV_POL
COMPONENT SLC_STAAT 'Nordprovinz', COMPONENT SLC_GKZ 'TV';

CREATE SECURITY LABEL ANTI_TERROR_POLICY.OPROV_POL
COMPONENT SLC_STAAT 'Ostprovinz', COMPONENT SLC_GKZ 'TV';

CREATE SECURITY LABEL ANTI_TERROR_POLICY.SPROV_POL
COMPONENT SLC_STAAT 'Suedprovinz', COMPONENT SLC_GKZ 'TV';

CREATE SECURITY LABEL ANTI_TERROR_POLICY.WPROV_POL
COMPONENT SLC_STAAT 'Westprovinz', COMPONENT SLC_GKZ 'TV';
```

DB2Sec-36

© Pürmer Unternehmensberatung, Dortmund, 2008



DB2 Zeilen-Labels

Analog sind die Labels für aktive Terroristen (AT) und Top-Terroristen zu vergeben, zum Beispiel:

```
CREATE SECURITY LABEL ANTI_TERROR_POLICY.NPROV_KD
COMPONENT SLC_STAAT 'Nordprovinz', COMPONENT SLC_GKZ 'AT';
...

CREATE SECURITY LABEL ANTI_TERROR_POLICY.NPROV_SK
COMPONENT SLC_STAAT 'Nordprovinz', COMPONENT SLC_GKZ 'TT';
...
```

DB2Sec-37

© Pürmer Unternehmensberatung, Dortmund, 2008



DB2 User-Labels

Der höchste Kennsatz für einen Benutzer ist:

```
CREATE SECURITY LABEL ANTI_TERROR_POLICY.GHD
COMPONENT SLC_STAAT 'Zentralstaat', COMPONENT SLC_GKZ 'TT',
COMPONENT SLC_LVL 'streng-geheim';
```

Dieser wird dem Datenbank-Administrator vorübergehend zugeordnet, um die notwendigen Änderungen an Tabelle und Daten durchführen zu können. Außerdem wird er außerhalb der Regeln für die Policy gestellt:

```
GRANT SECURITY LABEL ANTI_TERROR_POLICY.GHD
TO USER db2inst9 FOR ALL ACCESS;
GRANT EXEMPTION ON RULE ALL
FOR ANTI_TERROR_POLICY TO USER db2inst9;
```

DB2Sec-38

© Pürmer Unternehmensberatung, Dortmund, 2008



DB2 Implementierung

Nun kann der DBA die nötigen Änderungen durchführen. Der Zeilenschutz wird aktiviert durch:

```
ALTER TABLE "DB2INST9"."ATDATEICB"  
  ADD COLUMN POL_TAG DB2SECURITYLABEL  
  ADD SECURITY POLICY ANTI_TERROR_POLICY;
```

Der Schutz der Spalten wird aktiviert durch:

```
ALTER TABLE "DB2INST9"."ATDATEICB"  
  ALTER COLUMN GEFEINSTUFUNG SECURED WITH VS  
  ALTER COLUMN IDKRIMREG SECURED WITH VS  
  ALTER COLUMN IDTERRORNETZ SECURED WITH VS  
  ALTER COLUMN BEZTERRORNETZ SECURED WITH VS  
  ALTER COLUMN IDGEHDienst SECURED WITH GH  
  ALTER COLUMN VMANNKZ SECURED WITH SGH;
```

DB2Sec-39

© Pümer Unternehmensberatung, Dortmund, 2008



DB2 Implementierung

Die neue Label-Spalte muss noch mit den gewünschten Werten versorgt werden, zum Beispiel:

```
UPDATE ATDATEICB  
  set POL_TAG= SECLABEL_BY_NAME ('ANTI_TERROR_POLICY', 'NPROV_POL')  
  where PROVINZ='Nord' and GEFEINSTUFUNG = 'TV';  
...  
  set POL_TAG= SECLABEL_BY_NAME ('ANTI_TERROR_POLICY', 'SPROV_POL')  
  where PROVINZ='Sued' and GEFEINSTUFUNG = 'TV';  
...  
UPDATE ATDATEICB  
  set POL_TAG= SECLABEL_BY_NAME ('ANTI_TERROR_POLICY', 'WPROV_SK')  
  where PROVINZ='West' and GEFEINSTUFUNG = 'TT';  
...
```

Ob die Kennsätze richtig gesetzt wurden, kann überprüft werden mit:

```
select name, provinz, gefeinstufung,  
       seclabel_to_char('ANTI_TERROR_POLICY', POL_TAG)  
  from atdateicb;
```

DB2Sec-40

© Pümer Unternehmensberatung, Dortmund, 2008



DB2 Benutzer-Berechtigungen

```
CREATE SECURITY LABEL ANTI_TERROR_POLICY.NPOL
  COMPONENT SLC_STAAT 'Nordprovinz', COMPONENT SLC_GKZ 'TV',
  COMPONENT SLC_LVL 'frei';
CREATE SECURITY LABEL ANTI_TERROR_POLICY.OKD
  COMPONENT SLC_STAAT 'Ostprovinz', COMPONENT SLC_GKZ 'AT',
  COMPONENT SLC_LVL 'frei';
CREATE SECURITY LABEL ANTI_TERROR_POLICY.WSK
  COMPONENT SLC_STAAT 'Westprovinz', COMPONENT SLC_GKZ 'TT',
  COMPONENT SLC_LVL 'vs';
CREATE SECURITY LABEL ANTI_TERROR_POLICY.GHM
  COMPONENT SLC_STAAT 'Zentralstaat', COMPONENT SLC_GKZ 'TT',
  COMPONENT SLC_LVL 'geheim';
GRANT SECURITY LABEL ANTI_TERROR_POLICY.NPOL
  TO USER harry FOR READ ACCESS;
GRANT SECURITY LABEL ANTI_TERROR_POLICY.OKD
  TO USER derrick FOR READ ACCESS;
GRANT SECURITY LABEL ANTI_TERROR_POLICY.WSK
  TO USER soko FOR ALL ACCESS;
GRANT SECURITY LABEL ANTI_TERROR_POLICY.GHM
  TO USER schlphut FOR ALL ACCESS;
GRANT SECURITY LABEL ANTI_TERROR_POLICY.GHD
  TO USER bond FOR ALL ACCESS;
```

DB2Sec-41

© Pürmer Unternehmensberatung, Dortmund, 2008



DB2

Abfrage Harry,
Polizist Nordprovinz:

The screenshot shows the DB2 Command Editor interface. The command window contains the following SQL query:

```
select NAME,NAHENSZUSATZ,GESCHLECHT,GEBDAT, Provinz, ZUST_DIENSTS_ST
from DB2INST9.atdate1cib;
```

The result set displays 32 records. The record for Harry is highlighted in blue. The columns are NAME, NAHENSZUSATZ, GESCHLECHT, GEBDAT, Provinz, and ZUST_DIENSTS_ST.

NAME	NAHENSZUSATZ	GESCHLECHT	GEBDAT	Provinz	ZUST_DIENSTS_ST
HAAS	-	F	1963-08-24	Nord	1. Kommi'ssariat
THOMPSON	-	M	1978-02-02	Nord	1. Kommi'ssariat
RYAN	-	F	1971-05-11	Nord	1. Kommi'ssariat
STERN	-	M	1975-07-07	Nord	1. Kommi'ssariat
PULASKI	-	F	2003-05-26	Nord	1. Kommi'ssariat
HENDERSON	-	F	1971-05-15	Nord	1. Kommi'ssariat
SPENSER	-	M	1980-12-18	Nord	1. Kommi'ssariat
CONNELL	-	M	1972-10-18	Nord	1. Kommi'ssariat
NICHOLLS	-	F	1976-01-19	Nord	1. Kommi'ssariat
ADAMSON	-	M	1977-05-17	Nord	1. Kommi'ssariat
PIANKA	-	F	1980-04-12	Nord	1. Kommi'ssariat
SCOTTEN	-	F	1979-02-21	Nord	1. Kommi'ssariat
BROWN	-	M	1971-05-29	Nord	1. Kommi'ssariat
LUTZ	-	F	1978-03-19	Nord	1. Kommi'ssariat
JEFFERSON	-	M	1980-05-30	Nord	1. Kommi'ssariat
MARINO	-	M	2002-03-31	Nord	1. Kommi'ssariat
JOHNSON	-	F	1976-10-05	Nord	1. Kommi'ssariat
PEREZ	-	F	2003-05-26	Nord	1. Kommi'ssariat
PARKER	-	M	1965-07-09	Nord	1. Kommi'ssariat
SMITH	-	M	1976-10-27	Nord	1. Kommi'ssariat
SETRIGHT	-	F	1961-04-21	Nord	1. Kommi'ssariat
LEE	-	M	1971-07-18	Nord	1. Kommi'ssariat
GOONOT	-	M	1956-05-17	Nord	1. Kommi'ssariat
HEMINGER	-	F	1973-08-14	Nord	1. Kommi'ssariat
ORLANDO	-	M	1972-10-18	Nord	1. Kommi'ssariat
WATZ	-	F	1976-01-19	Nord	1. Kommi'ssariat
YAMAMOTO	Kanikaze	M	1981-01-05	Nord	1. Kommi'ssariat
JOHN	-	F	1978-03-19	Nord	1. Kommi'ssariat
MONTEVERDE	-	M	1984-03-31	Nord	1. Kommi'ssariat
SCHWARTZ	-	F	1966-03-28	Nord	1. Kommi'ssariat
SPRINGER	-	F	1961-04-21	Nord	1. Kommi'ssariat
WONG	-	F	1971-07-18	Nord	1. Kommi'ssariat

32 record(s) selected.

Statement termination character: ;

DB2Sec-42

© Pürmer Unternehmensberatung, Dortmund, 2008



DB2 Implementierung

Abfrage Derrick - Kriminaldirektor Ost:

```
select NAME,NAMENSZUSATZ,GESCHLECHT,GEBDAT, Provinz, ZUST_DIENSTS_ST
from DB2INST9.atdateich;
```

NAME	NAMENSZUSATZ	GESCHLECHT	GEBDAT	PROVINZ	ZUST_DIENSTS_ST
MEHTA	-	M	1962-08-11	Ost	1.Kommissariat
ALONZO	-	M	1956-05-17	Ost	1.Kommissariat

2 record(s) selected

DB2Sec-43

© Pürmer Unternehmensberatung, Dortmund, 2008



DB2 Implementierung

Soko - Sonderkommission Anti-Terror Westprovinz:

```
select NAME,NAMENSZUSATZ,GESCHLECHT,GEBDAT, Provinz, ZUST_DIENSTS_ST, GEFEINSTUFUNG
from DB2INST9.atdateich;
```

NAME	NAMENSZUSATZ	GESCHLECHT	GEBDAT	PROVINZ	ZUST_DIENSTS_ST	GEFEINSTUFUNG
GEYER		M	1955-09-15	West	1.Kommissariat	TV
WALKER	Die Flasche	M	1982-06-25	West	1.Kommissariat	TV
SMITH		M	1969-11-12	West	1.Kommissariat	TV
Bush	The Warrior	M	1944-02-29	West	3.SK Kölsch	TT
Ente	Duck	M	1872-01-01	West	WaschPo	AT

5 record(s) selected.

DB2Sec-44

© Pürmer Unternehmensberatung, Dortmund, 2008



DB2 Implementierung

Schlphut - Special Agent Schlapphut vom Geheimdienst:

```
select NAME,NAMENSZUSATZ,GESCHLECHT, Provinz, ZUST_DIENSTS_ST, IDGEHDIENTST
from DB2INST9.atdateicb where IDGEHDIENTST is not null;
```

NAME	NAMENSZUSATZ	GESCHLECHT	PROVINZ	ZUST_DIENSTS_ST	IDGEHDIENTST
PEREZ	-	F	Nord	1.Kommissariat	45628
BinImLaden	Der Araber	M	Sued	2.Kommissariat	4712
Bush	The Warrior	M	West	3.SK Kölsch	876554
Fisher	Molotow-Cocktail	M	Ost	AutobahnPolizei	87621

4 record(s) selected.

DB2Sec-45

© Pürmer Unternehmensberatung, Dortmund, 2008



Fazit

- ☞ Das Beispiel zeigt, wie mit den kennsatz-gesteuerten Sicherheitsrichtlinien fein abgestimmte, von den Datenwerten abhängige Zugriffsrechte definiert werden können. Der Vorteil dieser Implementierungen ist, dass sie nicht umgangen werden können.
- ☺ DB2 verfügt mit maximal 16 Komponenten einer Policy und dem Schutz von Zeilen und Spalten standardmäßig über deutlich mehr Möglichkeiten als mancher Wettbewerber.
- ☺ Der Schutz von Spalten ist in DB2-LBAC integriert und kann somit sehr einfach realisiert werden.
- ☺ Zur Implementierung benötigt ein DB2-Sicherheitsadministrator Grundkenntnisse in SQL.

DB2Sec-46

© Pürmer Unternehmensberatung, Dortmund, 2008

