Datensicherheit mit DB2 – mehr als nur Security-Settings!

Ein Vortrag für den Arbeitskreis
“IT-Revision in Kreditinstituten”

Mittwoch, 19.06.2002, Frankfurt/Main

Das Datum ist kein Kopierfehler.
Das Thema ist seit 2002 aktuell.
Präsentationslayout 2014 aktualisiert

Typische Problembereiche

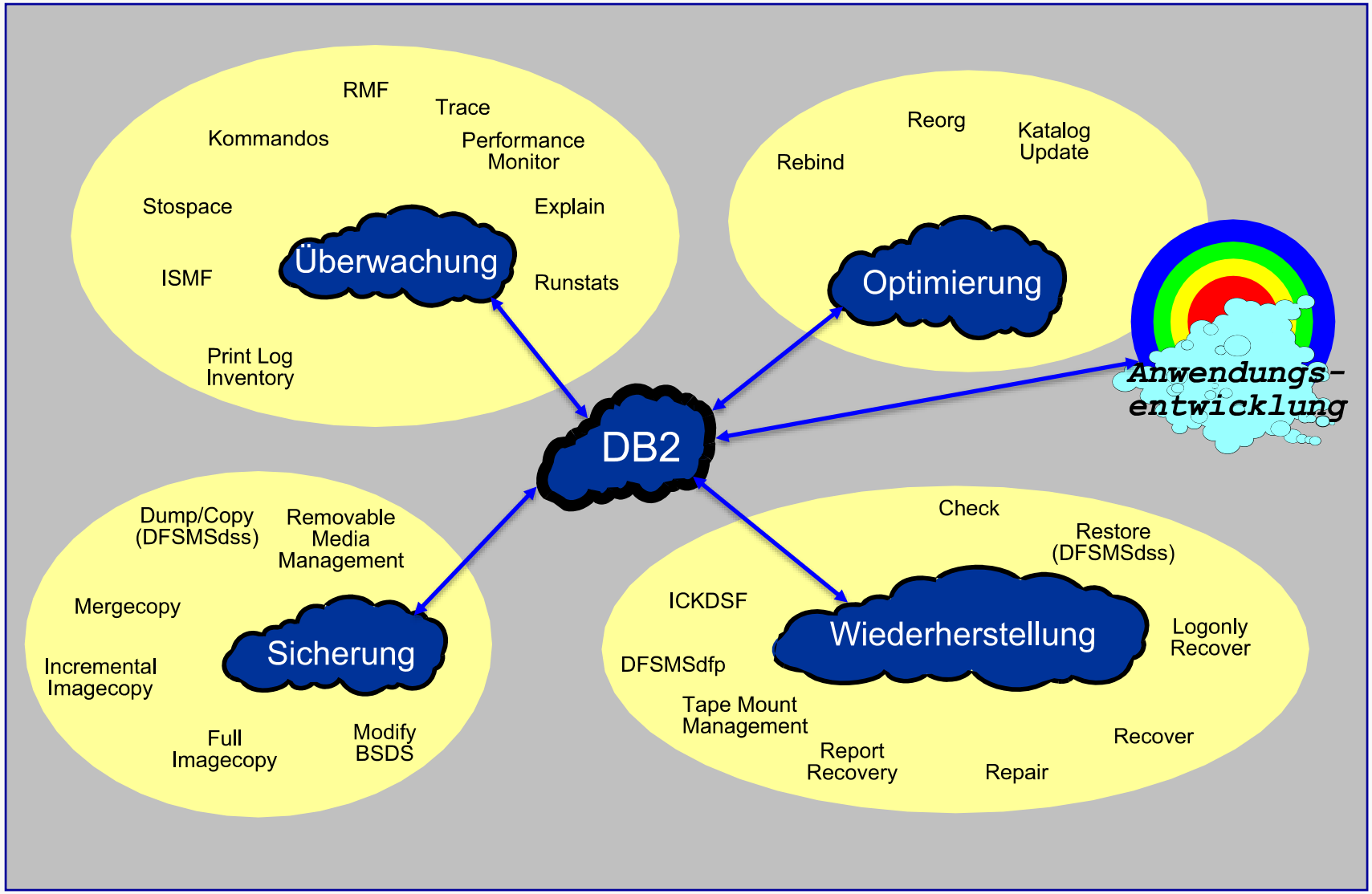
- Zugriffsschutz
  - Granularität vs. Übersichtlichkeit
  - Integration in die zentrale Security-Administration
- Sicherung und Wiederanlauf
  - Unterteilung in Online-, Offline, Off-Site
  - Nachweis der Wiederherstellbarkeit
- Beweissicherung / Nachvollziehbarkeit
  - Datenveränderungen
  - Datennutzung
  - Applikationszugriff mit Rückbezug in Trägersystem

IBM Universal Database bzw. DB2

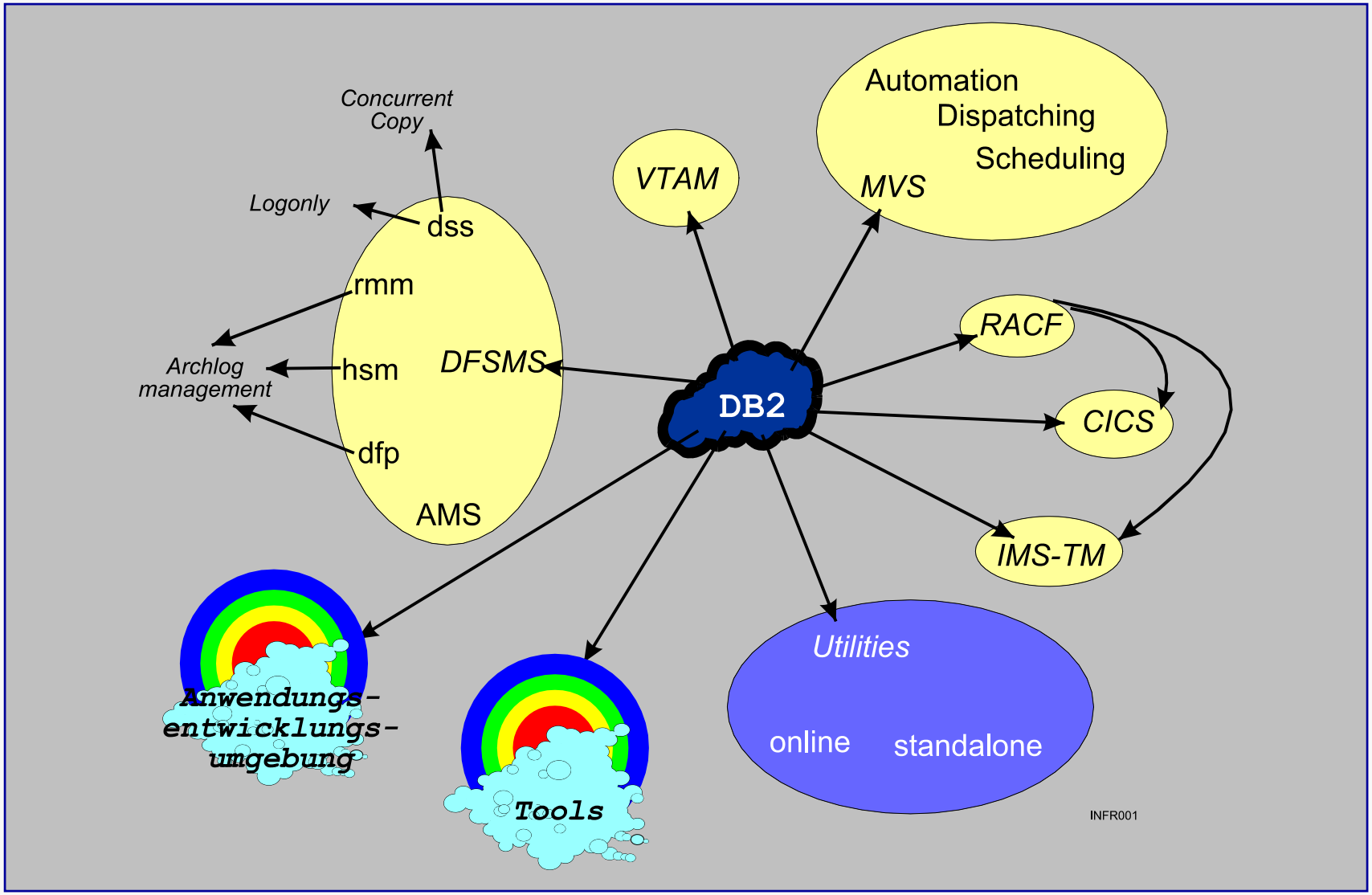
- Plattformen
  - z/OS
  - AS/400
  - Windows NT bzw. Windows 2000
  - LINUX
  - Diverse UNIX-Distributionen
- Distributionen
  - Von Einzelplatz bis Cluster (außer bei z/OS)

- Einige Fakten
  - SQL92
  - Robuste Betriebsablaufsicherung
  - Benötigt generell viele Systemressourcen
  - DRDA-fähig (AR und AS) via SNA und TCP/IP
  - Standard-Installation (z/OS mit SMP/E)
  - Hochverfügbarkeits-konfiguration möglich

Administrationsbereiche



RZ-Infrastruktur für DB2



Verantwortlichkeiten (große Installation)

- Verantwortungsposition
  - Systemtechnik
  - Daten-Administration
  - Datenbank-Administration
  - Analyse
  - Programmierung
  - Operating
  - Speicherverwaltung
  - Security-Management
  - Endbenutzer
- Aufgaben
  - Hardware und Software Planung
  - Kapazitätsplanung
  - Tool-Auswahl
  - Installation
  - System-Unterstützung
  - System-Sicherheit
  - Anwendungs-Sicherheit
  - Systemsicherung- und Wiederherstellung
  - Anwendungs-Datensicherung und -wiederherstellung
  - Performance-Überwachung und –Tuning
    - systemweit
    - Database
    - Anwendung
  - Produktionsübernahmen
  - Entwicklung von Hilfsroutinen
  - Job Scheduling
  - Daten-Analyse
  - Anwendungsdesign
  - Design Reviews
  - Anlegen von Objekten
  - Programmierung und Test

Analyseansatzpunkte

- Systemparametrisierung
- Einbettung ins Betriebssystem
- Zugangspfade zum DBMS
- Authentisierung
- Autorisierungszuweisung
- Betriebliche Absicherung
- Maßnahmen zur Beweissicherung
- Konfigurations- und Changemanagement

Systemparametrisierung

- Zentrales Parametermakro DSNZPARM
  - Assembler-Quellmodul
  - APF-autorisiertes Lademodul
  - Aufgliederung in diverse Bereiche
  - Zuweisung betrieblich und sicherheitstechnisch kritischer Parameter
    - Install SYSADM-Kennung
    - Interne oder externe Security
    - Checkpointing für Recoverylog
    - SQL-Optimierungsverhalten
  - Übersteuerung zur Laufzeit möglich

Einbettung ins Betriebssystem

- Basisschutz muss gegeben sein
  - APF-Bibliotheken
  - PROCLIB-Bibliotheken
  - Started Task-Management
- Ressourcenschutz
  - Dateien (Primär- und Sekundärbestände)
  - Zugriff auf die DBMS
- Berücksichtigung bei Business-Contingency-Planning

Zugangspfade zum DBMS

- Trägersysteme
  - CICS TS
  - IMS
  - TSO (interaktiv oder Batch)
  - Batch via. CAF
  - RRSF
- Remote-Zugänge
  - SNA
  - TCP/IP
- Programmiertechniken
  - Static SQL
  - Dynamic SQL
  - Call-Level-Interface
  - Application-Server

Authentisierung

- RACF-Anbindung
  - Connect
  - Identify
  - Signon
- Probleme
  - „already verified“
  - Nutzung übersetzter SQLIDs
  - Modifikationen in den User-Exits

Autorisierungszuweisung

- Administrative Berechtigungen
  - SYSADM vs. SYSCTRL
  - SYSOPR
  - DBADM vs. DBCTRL
- Endbenutzerberechtigungen
  - Daten
  - Applikationen
- Applikationsinfrastruktur
  - Static SQL
  - Dynamic SQL
  - Stored Procedures

Betriebliche Absicherung

- Transaktionssicherung
- Datenbankgestützte referenzielle Integrität
- Logging und Recovery
- Sicherungskopien
- Fortgeschrittene Wiederherstellungsverfahren
- Parallel Sysplex, Data Sharing und Plattenspiegelung

- Applikatorische Integritätssicherung

Maßnahmen zur Beweissicherung

- (Audit-)Trace
- Log-Daten
- Applikatorische Verfahren

Changemanagement

- Einsatz neuer
  - Systemsoftware
  - Anwendungssoftware
  - Datenbankstrukturen

Untersuchungsideen

- Kernuntersuchungen
  - Systeminstallation und Parametrisierung
  - Sicherung und Wiederherstellung
  - Autorisierungsprüfungen
  - Interfaces für „Incoming-Requests“
- Organisatorische Prüfungen
  - An- und Abmeldung von Datenbankstrukturen
  - Administrationsverfahren
  - Berechtigungsvergabe (mglw. im Rahmen RACF)
  - Datenschutzaspekte
- Randprüfung
  - DB2-Connections im CICS
  - SQL-Programmierstandard
  - Datenzugang von den Trägersystemen
  - Testsysteme

Kontakt

F-IT Security and Audit
Christoph Franke

Leinemühle 6
06343 Mansfeld

Fon: +49 7533 91927-0
Fax: +49 7533 91927-19
Kontakt@F-IT.biz

Ihr Ansprechpartner:
Dipl.-Inform. Christoph Franke, CISA
christoph.franke@F-IT.biz