SAP®-Systeme und Unternehmensdaten –

wie sicher sind sie wirklich?

Thomas Tiede
IBS Schreiber GmbH
Geschäftsführer

Agenda

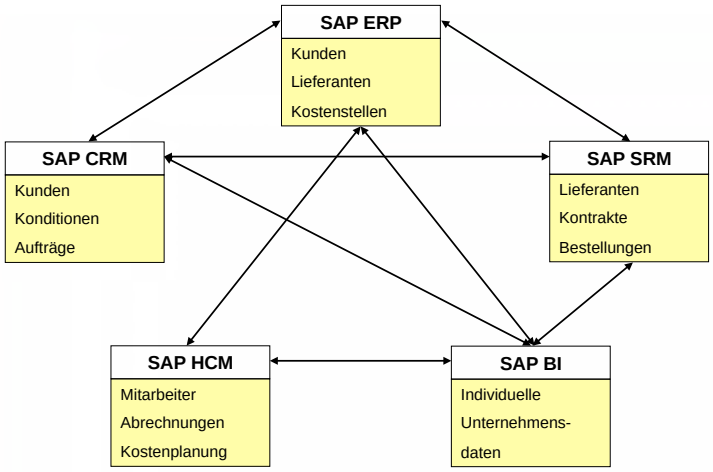
1 Sensible Unternehmensdaten – Wo und wie werden sie gespeichert?

2 Unterschätzte Gefahren: Reporting, Funktionsbausteine, RFC

3 Live Demo: Effektive Methoden zum Hacken eines Systems und Verschleiern der eigenen Spuren

4 Möglichkeiten zur Absicherung

1 Sensible Unternehmensdaten – Wo und wie werden sie gespeichert?
1.1 SAP Systeme und ihre Daten



3

1 Sensible Unternehmensdaten – Wo und wie werden sie gespeichert?
1.2 Speicherung der Daten

Daten werden in Tabellen in der Datenbank gespeichert.
Stammdaten werden „transparent“ (=in DB lesbar) gespeichert.
Zugriff ist möglich über DB und SAP.

Beispiele für Tabellen mit sensiblen Daten:

KN*	Kundendaten
LF*	Lieferantendaten
BUT*	Business Partner (BP)
ADR*	Adressdaten
DPAY*	Zahlungsprogramm - Daten automatischer Zahlungen
PA*	Mitarbeiterdaten

4

1 Sensible Unternehmensdaten – Wo und wie werden sie gespeichert?
1.3 Zugriffsmöglichkeiten auf Daten (1)

Über Standardfunktionalitäten (Transaktionen)

Über die SAP Tabellenanzeige

Über das SAP Reporting

Über Fernzugriffe auf das SAP-System (RFC)

- Von anderen SAP-Systemen
- Von anderen DV-Systemen
- Von Standardprogrammen wie MS Excel, MS Access etc.
- Von allen gängigen Programmiersprachen aus

5

1 Sensible Unternehmensdaten – Wo und wie werden sie gespeichert?
1.3 Zugriffsmöglichkeiten auf Daten (2)

Transaktionen zur Tabellenanzeige (Auszug)

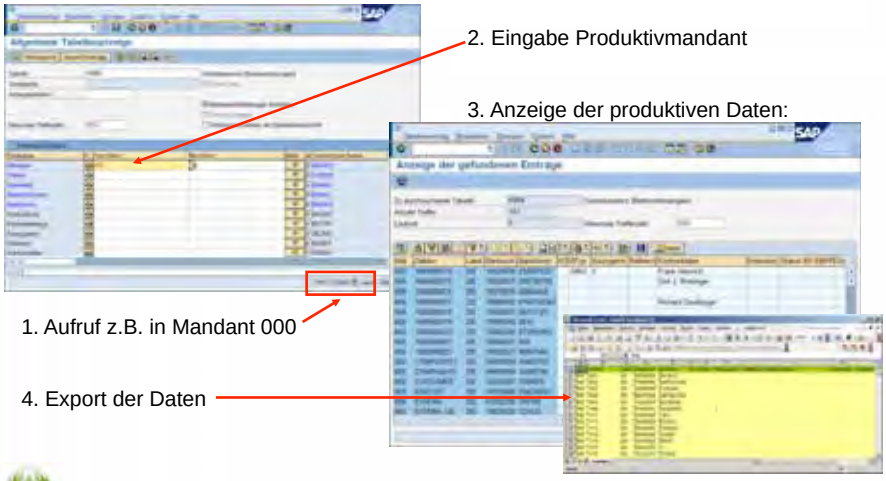
SE16	Data Browser
SE16N	Allgemeine Tabellenanzeige
N	Schnellstart SE16N
UASE16N	Tabellenanzeige
SE17	Allgemeine Tabellenanzeige
SM30	Aufruf View-Pflege
SM31	Aufruf Viewpflege analog SM30
CACS_DET_ACCAS_30	Aufruf generierte Tabellen/Views
CX0A7	Merkmalswerte pflegen
CX0A8	Merkmalswerte anzeigen
KCS5	Merkmalsausprägungen Pflegen (View)
KEP6	Pflegen Merkmale
PRP_UNIT	PP: Zulässige Dimensionen

Transaktionen für das Reporting (Auszug)

EWFM	Offene Mahnläufe suchen
EWFZ	Offene Zahlungsläufe suchen
OODR	Reportvariante für Zeitauswertung
SA38	ABAP/4 Reporting
SA38PARAMETER	Einplanung PFCG_TIME_DEPENDENCY
SC38	Starten Report Remote
SE15	Dictionary-Infosystem
SE38	ABAP Editor
SE80	Object Navigator
SE84	Repository-Infosystem
SE90	Prozeßmodell-Infosystem
SEU_INT	Object Browser
START_REPORT	Starten eines Reports
SUB%	Interner Aufruf: Submit über OK-Code

6

1 Sensible Unternehmensdaten – Wo und wie werden sie gespeichert?
1.4 Beispiel: Zugriff auf Kundenbankverbindungen mit UASE16N



7

2 Unterschätzte Gefahren: Reporting, Funktionsbausteine, RFC
2.1 Reporting (1)

Reports = ausführbare ABAP-Programme
ca. 60.000 Reports in NetWeaver 7.0 / ERP2005
ca. 20 Transaktionen zum Ausführen von Reports
Besondere Problematik: Reports ohne Berechtigungsprüfungen

Beispiele für kritische Reports:

RK_SE16N	Aufruf Oberfläche SE16N
UA_SE16N_START	Aufruf Oberfläche UASE16N
RSTBPDEL	Tabellenänderungsprotokolle löschen
RSCDOK99	Änderungsbelege löschen
RSVCAD03	Versionen löschen (keine Berechtigungsprüfung!)

8

2 Unterschätzte Gefahren: Reporting, Funktionsbausteine, RFC
2.1 Reporting (2)

Für wen sind Berechtigungen zum Reporting zulässig?

Administratoren
KeyUser
Prüfer

Und die „normalen“ Anwender?

Anwender benötigen keine Reporting-Berechtigung (z.B. SA38)!
Benötigte Reports sind über Transaktionen in Rollen zu berechtigen.
Reports können in eigenen Infosystemen zusammengefasst werden.

9

2 Unterschätzte Gefahren: Reporting, Funktionsbausteine, RFC
2.2 Funktionsbausteine (1)

- Funktionsbausteine sind ABAP-Programme und können wie Reports ausgeführt werden
- Es existieren ca. 380.000 Funktionsbausteine in einem SAP NetWeaver / ERP2005 (Auflistung aller Funktionsbausteine in Tabelle TFDIR)
- Funktionsbausteine können aufgerufen werden mit den Transaktionen SE15, SE37, SE80, SE84, SE85, SE90, SEU_INT
- Remotefähige Funktionsbausteine können systemübergreifend ausgeführt werden

10

2 Unterschätzte Gefahren: Reporting, Funktionsbausteine, RFC
2.2 Funktionsbausteine (2)

Beispiele für kritische Funktionsbausteine

EBA_ABAP_EXECUTE	Ausführen von beliebigen ABAP-Quelltexten
EBA_TABLE_UPDATE	Ändern beliebiger Tabellen
RFC_ABAP_INSTALL_AND_RUN	Ausführen von beliebigen ABAP-Quelltexten
SUPRN_INS_OR_DEL_PROFILE	Zuordnen von Profilen zu Benutzern ohne Berechtigungsprüfungen

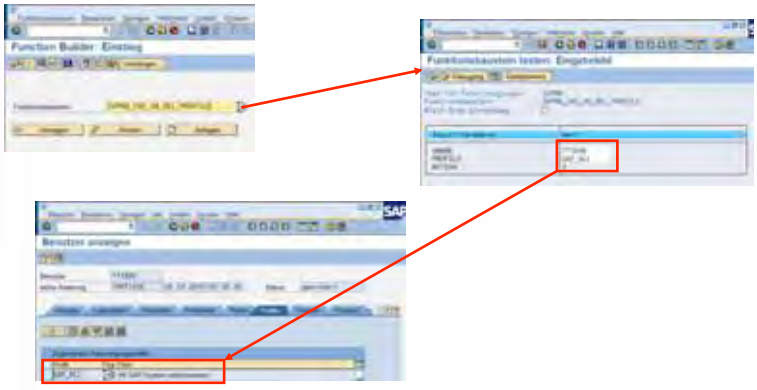
Beispiele für Funktionsbausteine zum Auslesen von Tabelleninhalten

TABLE_ENTRIES_GET_VIA_RFC
EBA_TABLE_SELECT
RFC_GET_TABLE_ENTRIES
RFC_READ_TABLE
SRTT_TABLE_DISPLAY

11

2 Unterschätzte Gefahren: Reporting, Funktionsbausteine, RFC
2.2 Funktionsbausteine (3)

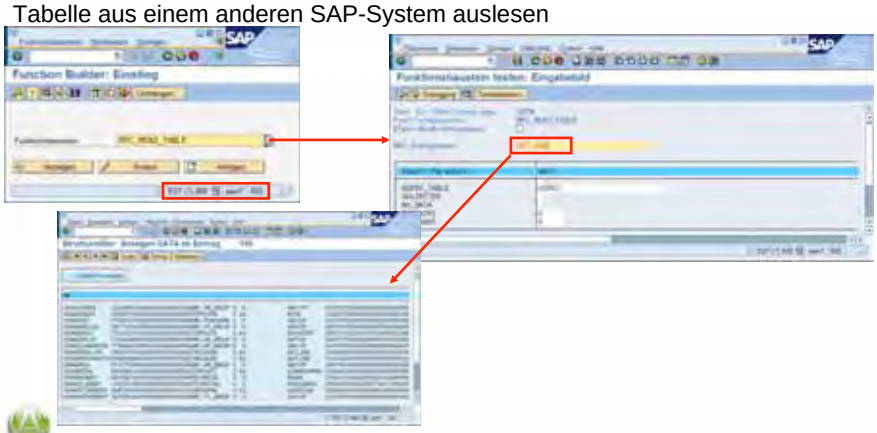
Beispiel Ausführen von Funktionsbausteinen: SAP_ALL zuordnen



12

2 Unterschätzte Gefahren: Reporting, Funktionsbausteine, RFC
2.2 Funktionsbausteine (4)

Beispiel Ausführen von Funktionsbausteinen:
Tabelle aus einem anderen SAP-System auslesen



13

2 Unterschätzte Gefahren: Reporting, Funktionsbausteine, RFC
2.2 Funktionsbausteine (5)

Berechtigungen auf Funktionsbausteinen im Produktivsystem

Zulässige Berechtigung: *Anzeigen von Funktionsbausteinen*
- Berechtigungsobjekt S_DEVELOP
  - Aktivität: 03 (Anzeigen)
  - Objekttyp: FUGR
  - …

Unzulässige Berechtigung: *Ausführen von Funktionsbausteinen*
- Berechtigungsobjekt S_DEVELOP
  - Aktivität: 16 (Ausführen)
  - Objekttyp: FUGR
  - …

14

2 Unterschätzte Gefahren: Reporting, Funktionsbausteine, RFC
2.3 RFC (Remote Function Call) (1)

- Per RFC können Funktionsbausteine von externen Programmen aus ausgeführt werden
- Es existieren ca. 30.000 remote-fähige Funktionsbausteine
- Eine Ausführungsberechtigung für S_DEVELOP (Aktivität 16) ist zum remote Ausführen der Funktionsbausteine nicht notwendig
- Es ist eine Berechtigung auf dem Berechtigungsobjekt S_RFC erforderlich
- S_RFC-Berechtigungen sind sehr häufig zu umfangreich vergeben

15

2 Unterschätzte Gefahren: Reporting, Funktionsbausteine, RFC
2.3 RFC (Remote Function Call) (2)

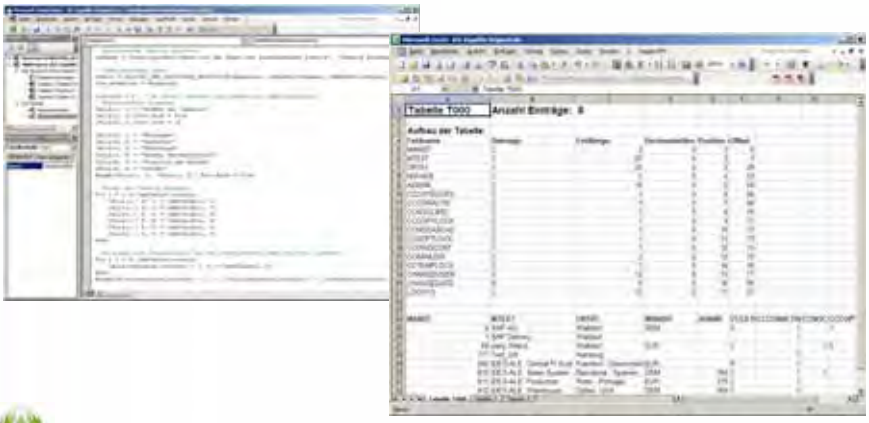
Beispiel: Aufruf Funktionsbaustein zum Tabellen auslesen aus MS Excel

```
' Objekt erstellen und Verbindung herstellen
Dim fns As Object
Set fns = CreateObject("SAP.Functions")

' Verbindungsobjekt erstellen
Dim conn As Object
Set conn = fns.Connection
…
' Auszulesende Tabelle ermitteln
tabname = UCase(InputBox("Geben Sie den Namen der auszulesenden Tabelle", "Tabelle
auswählen", "T000"))

' Tabelleninhalt auslesen: Funktionsbaustein RFC_GET_TABLE_ENTRIES
result = fns.RFC_GET_TABLE_ENTRIES(Exception, BYPASS_BUFFER:=" ", FROM_KEY:=" ",
GEN_KEY:=" ", MAX_ENTRIES:=0, TABLE_NAME:=tabname, TO_KEY:=" ",
NUMBER_OF_ENTRIES:=num_entries, entries:=entries)
the_exception = Exception
…
```

16

2 Unterschätzte Gefahren: Reporting, Funktionsbausteine, RFC
2.3 RFC (Remote Function Call) (3)

Beispiel: Aufruf Funktionsbaustein zum Tabellen auslesen aus MS Excel



17

3 Live Demo: Effektive Methoden zum Hacken eines Systems und Verschleiern der eigenen Spuren

…

18

4 Möglichkeiten zur Absicherung
4.1 Zugriff auf Tabellen

Transaktionen zur Tabellenanzeige

- Transaktionen zur Tabellenpflege / -anzeige (z.B. SE16, SE16N) sind an die Anwender nicht zu vergeben.
- Zu pflegende Tabellen sind über Parametertransaktionen den Anwendern zuzuordnen.

Berechtigungsobjekt S_TABU_DIS

- Auch die Aktivität 03 (Anzeigen) ist kritisch!
- Es sind nur die Berechtigungsgruppen zu berechtigen, auf die der Anwender zugreifen darf!
- Eine Berechtigung für alle Tabellen ist grundsätzlich nicht zu vergeben!

19

4 Möglichkeiten zur Absicherung
4.2 Ausführen von Reports

Transaktionen für das Reporting

- Transaktionen für das Reporting (z.B. SA38) sind an die Anwender nicht zu vergeben.
- Die Reports sind den Anwendern über einzelne Transaktionen oder über Bereichsmenüs zuzuordnen.

Berechtigungsobjekt S_PROGRAM

- Werden Reporting-Transaktionen zugeordnet, so können Reports über das Objekt S_PROGRAM geschützt werden.
- Hierfür muss ein eigenes Konzept erstellt werden. Die fortlaufende Pflege dieser Berechtigung ist aufwändig.

20

4 Möglichkeiten zur Absicherung
4.3 Funktionsbausteine

- Das Ausführen von Funktionsbausteinen ist im Produktivsystem zu unterbinden.
- Folgende Berechtigung ist nicht zu vergeben:
  Berechtigungsobjekt S_DEVELOP
  Aktivität: 16 (Ausführen)
  Objekttyp: FUGR
- Im Entwicklungs- und Konsolidierungssystem dürfen keine RFC-Verbindungen ins Produktivsystem existieren, in denen Benutzer und Kennwort hinterlegt sind.

4 Möglichkeiten zur Absicherung
4.4 RFC (Remote Function Call)

- Das Berechtigungsobjekt S_RFC ist nur an Anwender zu vergeben, die es für eine externe Kommunikation benötigen.
- Das Berechtigungsobjekt S_RFC ist nicht mit einem Stern für das Feld „Funktionsgruppen“ auszuprägen. Den Anwendern sind nur die Funktionsgruppen zuzuordnen, die sie benötigen.

Fragen?

23

Vielen Dank

Thomas Tiede
IBS Schreiber GmbH
International Business Services
for auditing and consulting

Zirkusweg 1
D-20359 Hamburg

Tel.: +49 40 6969 8515
Mail: Thomas.Tiede@IBS-Hamburg.com
www.ibs-hamburg.com
www.checkaud.de

24