Thema:

Sicherheit und Revision in SAP R/3 am Beispiel des Audit Information System (AIS)

Studienarbeit

Arbeitsgruppe Wirtschaftsinformatik

Themensteller: Prof. Dr. Claus Rautenstrauch
Betreuer: Dipl.-Wirtsch.-Inf. André Faustmann

vorgelegt von: Andrea Kreutzberg

Abgabetermin: 25. Juli 2008

Inhaltsverzeichnis

Verzeichnis der Abkürzungen und Akronyme

ABAP	Advanced Business Application Programming, Programmiersprache des Softwareherstellers SAP
Ais	Audit Information System
BDSG	Bundesdatenschutzgesetz
AIS	Audit Information System
DSB	Datenschutzbeauftragte(r)
RFC	Remote Function Call
SAP	Softwarehersteller, ursprünglich Abkürzung für „Systeme, Anwendungen und Produkte in der Datenverarbeitung“
SAP R/3	Unternehmenssoftware des Softwareherstellers SAP

Abbildungsverzeichnis

1 Motivation

Die vorliegende Studienarbeit entstand im Anschluss an ein Praktikum bei der Arbeitsgruppe Datenschutz einer Niederlassung der Deutschen Telekom AG. Dort sollte das im Einsatz befindliche SAP-System im Hinblick auf die Einhaltung der Datenschutzvorschriften gemäß Bundesdatenschutzgesetz geprüft werden.

Es ergab sich folgende Aufgabenstellung für das Praktikum:

- Sensibilisierung für das Thema Datenschutz und die Aufgaben der Datenschutzbeauftragten (DSB) in Unternehmen durch Analyse der gesetzlichen Vorgaben im Bundesdatenschutzgesetz (BDSG)
- Einarbeitung in die grundlegenden Sicherheitsmechanismen in SAP R/3 wie Benutzerauthentifizierung und das SAP R/3-Berechtigungskonzept.
- Einarbeitung in das Audit Information System (AIS), einem im SAP R/3-System zur Verfügung gestellten Hilfsmittel zur Durchführung kaufmännischer, datenschutztechnischer und systembezogener Revisionen (Audits).
- Prüfung der vorhandenen Transaktions- und Berechtigungsrollen für die DSB mit Hilfe des AIS.

Die anschließende (vollständige) Datenschutz- und Systemprüfung und eine Bewertung der Einhaltung der Datenschutzvorschriften erfolgte ausschließlich durch Mitarbeiter der Arbeitsgruppe Datenschutz und war nicht Teil des Praktikums.

In der vorliegenden Studienarbeit wird in Kapitel 2 zunächst auf die Notwendigkeit des Datenschutzes und dessen gesetzlichen Grundlagen eingegangen. Des Weiteren werden die Aufgaben des DSB erläutert. In Kapitel 3 wird das klassische SAP R/3-Berechtigungskonzept vorgestellt. Das AIS wird in Kapitel 4 eingeführt, SAP-Standardrollen, die u.a. für den DSB vorgesehen sind, werden erläutert, Schwachstellen des AIS werden aufgezeigt und es wird auf kritische Berechtigungen in den Standardrollen hingewiesen. In Kapitel 5 erfolgen abschließend eine kurze Zusammenfassung der (Praktikums)-Ergebnisse und ein Ausblick auf mögliche Anpassungen der Rollen mit kritischen Berechtigungen seitens der SAP AG.

2 Gesetzliche Grundlagen und Anforderungen an den Datenschutz

2.1 Notwendigkeit des Datenschutzes laut BDSG

Das BDSG wurde zum Schutz des Persönlichkeitsrechts des Einzelnen geschaffen, welches durch den Umgang mit seinen personenbezogenen Daten beeinträchtigt werden könnte (vgl. BDSG, § 1, Absatz 1). Dieses Gesetz ist allerdings nicht uneingeschränkt gültig, sondern muss gegen das Allgemeininteresse abgewogen werden.

Das Konzept der Datenvermeidung und Datensparsamkeit ist in §3a des BDSG geregelt und wird als Bestandteil des Systemdatenschutzes gesehen. Hier werden Vorgaben zur Gestaltung von Datenverarbeitungssystemen gemacht. Die verwendeten Datenverarbeitungssysteme sollten so wenig personenbezogene Daten wie möglich erheben, verarbeiten oder nutzen. Durch diese Vorgabe möchte der Gesetzgeber die Verarbeitung personenbezogener Daten bereits auf technischer Ebene beschränken, allerdings gibt es eine direkte Einschränkung im Gesetzestext, es heißt dort „soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht." (BDSG, §3a). Es handelt sich hierbei also eher um eine Zielvorgabe, die nicht in jedem Fall zwingend durchgesetzt werden kann.

2.2 Unabdingbare Rechte der Betroffenen

Die Rechte der Betroffen werden für nicht-öffentliche Stellen u. a. im §6 festgelegt. Jeder hat das Recht auf Auskunft, auf Berichtigung, auf Löschung oder Sperrung seiner Daten. Diese Rechte können nicht übertragen, abgetreten oder vererbt werden. Die Rechte von Betroffenen können des Weiteren nicht durch ein Rechtsgeschäft beschränkt werden.

2.3 Organisatorische und technische Maßnahmen zur Gewährleistung des Datenschutzes

In der Anlage zu §9 des BDSG werden die technischen und organisatorischen Maßnahmen zum Datenschutz beschrieben:

1. Zutrittskontrolle
   Nur Befugte sollen räumlichen Zugang haben; dies kann durch Sicherheitszonen und deren Kontrolle, z.B. durch Pförtner oder Chipkarten realisiert werden, bei der Arbeit

mit Personalcomputern oder mobilen Geräten ist diese Art der Kontrolle schwer durchführbar.

2. Zugangskontrolle
   Nur Befugten soll die Nutzung der Datenverarbeitungssysteme möglich sein; sie kann durch Benutzerkontrolle, z.B. mit Passwort oder Schlüssel, realisiert werden; durch die Zugangskontrolle ist die Identität des Benutzers festzustellen.

3. Zugriffskontrolle
   Nur Befugte sollen in vordefinierter Weise auf Daten zugreifen; die Befugnis kann sich auf bestimmte Bereiche der Daten und die Art des Zugriffs beschränken; mit Hilfe von Berechtigungskonzepten können Zugriffsbefugnisse differenziert vergeben werden.

4. Weitergabekontrolle
   Daten bei der Übertragung vor unberechtigtem Zugriff sichern; durch Richtlinien für den Transport, Verschlüsselung, Protokollierung und Prüfung des Empfängers kann die Weitergabe kontrolliert werden.

5. Eingabekontrolle
   Protokollierung bestimmter Systemeingaben; automatisierte Protokollierung bestimmter Vorgänge im System, um Veränderungen später nachvollziehen zu können.

6. Auftragskontrolle
   Umsetzung der Weisungen des Auftraggebers; geeignete Maßnahmen sind z.B. gezielte Auswahl des Auftragnehmers und Niederschrift von Vereinbarungen.

7. Verfügbarkeitskontrolle
   Sicherheit und Verfügbarkeit der Daten; personenbezogene Daten vor Verlust schützen, z.B. durch Virenschutz und Daten- und Programmsicherungen.

8. Gewährleistung der Zweckbindung
   Trennung der Daten nach ihrem Zweck; Daten mit unterschiedlicher Zweckbindung getrennt verarbeiten, z.B. durch unterschiedliche Verschlüsselung oder logische Trennung im Programm.

Aus den beschriebenen Anforderungen ergeben sich bestimmte Aufgaben für den Datenschutzbeauftragten (DSB), die im Abschnitt 2.4. näher erläutert werden.

2.4 Aufgaben des Datenschutzbeauftragten (DSB)

Laut BDSG §4f Absatz 1 Satz 1 müssen nicht-öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, einen Beauftragten für den Datenschutz bestellen. Ob das jeweilige Unternehmen dazu verpflichtet ist, richtet sich nach verschiedenen Kriterien wie der Verarbeitungsform der Daten und der Anzahl der Mitarbeiter. Nach §4f Absatz 3 Satz 2 ist der Beauftragte für Datenschutz weisungsfrei.

§4g des BDSG regelt die Aufgaben des DSB:

„(1) Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. […] Er hat insbesondere

1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; […]

(2) Dem Beauftragten für den Datenschutz ist von der verantwortlichen Stelle eine Übersicht über die in § 4e Satz 1 genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen.“ (BDSG, §4g).

§ 4g kann ist als Grundlage für die spätere, genaue Definition der Aufgaben des DSB zu sehen. Er ist jedoch noch keine vollständige Antwort bezüglich des genauen Inhalts dieser Aufgaben. Hierfür sind jeweils die Verarbeitungsziele und die Bedingungen des konkreten Falls ausschlaggebend (vgl. Otto (2008), S. 13).

Aus den oben erwähnten §§ 4, 6 und 9 sowie den hier nicht näher erläuterten §§ 28, 31,33 und 34 ergeben sich folgende Aufgaben für den DSB:

- Kontrolle der Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung (§§4,28, BDSG) in Zusammenhang mit der besonderen Zweckbindung (§31) und der Übermittlung von personenbezogenen Daten (§§4b,28)

- Vorabkontrolle (§4d Absatz 5 und 6) als Ergänzung zur Zulässigkeitsprüfung bei der Verarbeitung besonders sensitiver Daten

- Überwachung der ordnungsgemäßen Progammanwendung (§4g Absatz 1 Nr.1)

- Maßnahmen zur Datensicherheit (§9 und Anlage zu §9), insbesondere
  - Überprüfung des Berechtigungskonzeptes (Zugriffskontrolle)
  - Auswertung der Protokollierung (z.B. Eingabekontrolle,§31)

- Führen von Übersichten gemäß §§ 4e,4g

- Sicherstellung der Rechte der Betroffenen

Der DSB muss zur Erfüllung seiner Aufgaben Kontrollen durchführen, diese können angemeldet und stichprobenartig erfolgen. Auf Angaben, die der DSB in Form von Übersichten zur Verfügung gestellt bekommt, sollte er sich nicht ohne weiteres verlassen. Die Angaben sollten mit Hilfe der entsprechenden Kontrollrechte überprüft werden.

3 Das SAP R/3-Berechtigungskonzept

3.1 Allgemeine Informationen zum SAP R/3-Berechtigungskonzept

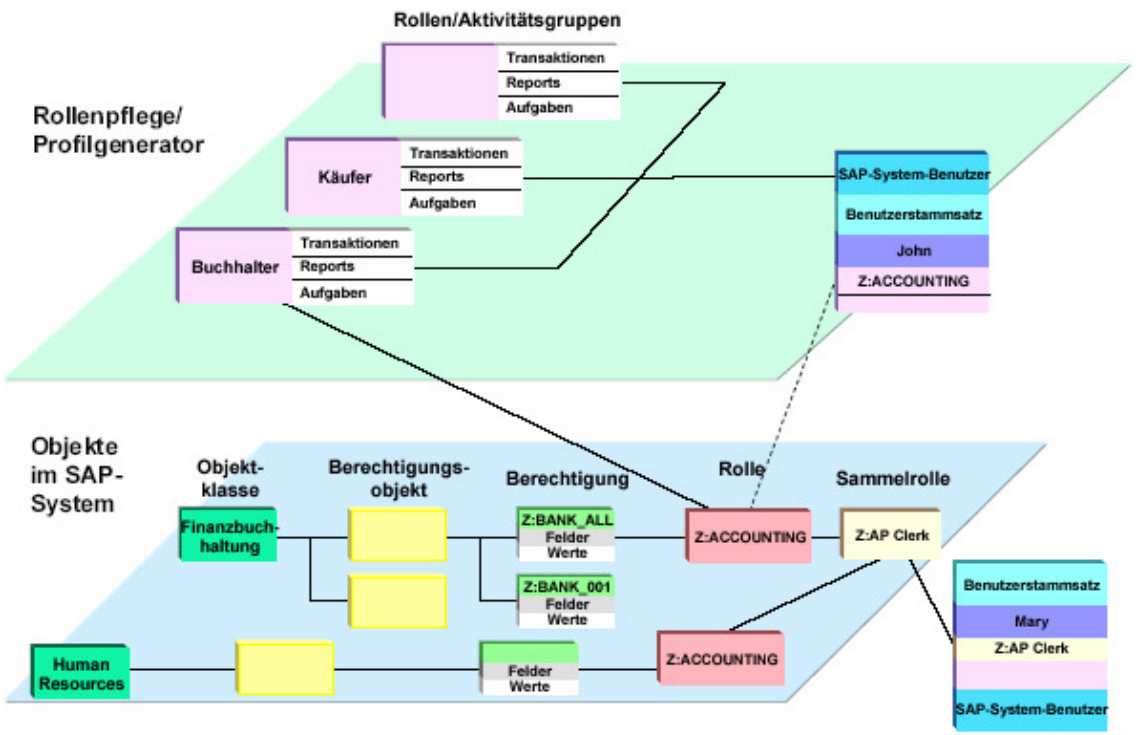
Das SAP R/3-Berechtigungskonzept dient zum Schutz der Transaktionen und Programme im R/3-System vor unberechtigter Nutzung. Benutzer dürfen eine Transaktion nur dann ausführen, wenn sie über die notwendigen Berechtigungen verfügen. Um dies zu gewährleisten, enthalten die SAP R/3-Programme und Transaktionen so genannte Berechtigungsprüfungen (vgl. SAP AG (2001), S. 6).

Unternehmen, die SAP R/3 einsetzen, sollten über einen sorgfältig erarbeiteten *Berechtigungsplan* verfügen, der den jeweils aktuellen Gegebenheiten des Unternehmens regelmäßig angepasst wird. Der Berechtigungsplan sollte gut dokumentiert sein, damit ein Nachvollzug z. B. durch externe Prüfer möglich ist.

Die Zuweisung von Berechtigungen in SAP R/3 basiert auf der Zuordnung der Benutzer zu so genannten *Rollen* oder *Aktivitätsgruppen* (die beiden Begriffe können synonym verwendet werden, in früheren Versionen vor SAP R/3 Release 4.6C wurden Rollen als Aktivitätsgruppen bezeichnet). Die Definition der Rollen orientiert sich an den verschiedenen Aufgaben der Mitarbeiter im Unternehmen. Die Zuordnung jedes Benutzers zu den entsprechenden Rollen stellt sicher, dass er über alle für seine Stellenbeschreibung notwendigen Berechtigungen verfügt, jedoch keine Berechtigungen hat, die er nicht benötigt.

3.2 Rollenpflege und Profilgenerator

Die Rollenpflege und der Profilgenerator sind Hilfsmittel zur Administration der Rollen, Berechtigungen und Profile. Die Rollen stellen eine Abstraktion der eigentlichen Berechtigungen und Profile dar, die im SAP R/3-System als Objekte realisiert sind. In **Abb. 3.1** wird der Zusammenhang zwischen der Ebene der Rollenpflege/ des Profilgenerators und der Objektebene verdeutlicht.



Quelle: SAP AG (2001), S. 10

Abb. 3.1: Berechtigungs- und Rollenpflege im SAP-System

Über die Rollenpflege und den Profilgenerator werden Rollen für die verschiedenen Stellenbeschreibungen mit den zulässigen Aktivitäten der Mitarbeiter definiert. Daraus ermittelt der Profilgenerator die Berechtigungen für Benutzer, die einer bestimmten Rolle angehören.

3.3 Aufteilung administrativer Aufgaben

Administratoren ermöglicht die Rollenpflege bzw. der Profilgenerator folgende Aufgaben:

- Zuweisung von Stellenbeschreibungen zu Transaktionen.
- Pflege von Rollen.
- Generierung und Pflege von Berechtigungsprofilen.
- Zuweisung von Benutzern.
- Aktualisierung von Benutzerstammsätzen.

Aufgrund dieser umfassenden Rechte empfiehlt sich die Aufteilung dieser Aufgaben auf mehrere Administratoren, z. B. einen *Berechtigungsadministrator*, einen *Berechtigungsprofiladministrator* und einen *Benutzeradministrator* (vgl. SAP AG (2001), S. 12).

Aus der Aufgabenverteilung ergibt sich dann folgende Vorgehensweise bei der Nutzung des Profilgenerators:

- Der *Berechtigungsdatenadministrator* kann ein Rolle anlegen, Transaktionen auswählen und Berechtigungsdaten pflegen. Er kann ein Profil nicht generieren, lediglich sichern.
- Der *Berechtigungsprofiladministrator* kann die Daten genehmigen und das Berechtigungsprofil bzw. die Profile generieren.
- Der Benutzeradministrator weist den Benutzern nun die Rolle und den Benutzerstammsätzen die Berechtigungsprofile zu (vgl. SAP AG (2001), S. 12).

3.4 Manuelle Pflege von Berechtigungen und Profilen

Berechtigungen und Profile können auch ohne Verwendung des Profilgenerators manuell gepflegt werden. Auch hier müssen jedoch zuerst alle Stellenbeschreibungen festgelegt werden. Erst dann können die erforderlichen Berechtigungen für jede Stellenbeschreibung definiert werden. In einem Profil können mehrere Berechtigungen zusammengefasst werden. Danach werden jedem Benutzer die Profile zugewiesen, die er für seine Aufgaben im Unternehmen benötigt (vgl. SAP AG (2001), S. 14).

3.5 Sicherheitsrisiken bei manueller Pflege

Die Probleme einer manuellen Pflege sind umfassend. Es kommt häufig zu vielen Redundanzen in den Berechtigungen durch die Zuweisung diverser Profile, denen teilweise sehr ähnliche Stellenbeschreibungen zugrunde liegen. Bei Unternehmen mit sehr vielen SAP R/3-Benutzern ist der Administrationsaufwand bei manueller Pflege daher kaum noch zu bewältigen. Die vergebenen Profile und Berechtigungen werden zunehmend untransparent. Der Profilgenerator sollte deshalb unbedingt eingesetzt werden.

4 Das AIS

4.1 Ziel des AIS

Das AIS wurde konzipiert, um verschiedenen Anwendergruppen (intern und extern) als Hilfsmittel für die Revision zu dienen. SAP selbst beschreibt das AIS als „Werkzeugkasten des Revisors“. Es soll der „Verbesserung des Prüfungsablaufes und der Prüfqualität“ dienen (SAP AG (2001)).

Das AIS bietet Funktionen für das kaufmännische Audit und das System Audit sowie Hilfestellungen für den betrieblichen Datenschutzbeauftragten. Er kann mit Hilfe des AIS Datenschutzprüfungen durchführen, Informationen zu Auskunftsersuchen (gemäß §6 BDSG) erstellen und ihm zur Verfügung gestellte Übersichten kontrollieren. (vgl. Otto (2008), S. 35).

4.2 AIS-Standardrollen

Das AIS wird im Standardumfang des SAP R/3 ausgeliefert und enthält Sammlungen, Strukturierungen und Voreinstellungen von Standardprogrammen. Seit Release 4.6c wird das AIS als rollenbasierte Pflegeumgebung angeboten im Gegensatz zur vorher gehenden Menütechnik.

Jeder Nutzer benötigt für die Arbeit im AIS verschiedene Einzelrollen, die auf seine jeweiligen Aufgabestellungen zutreffen. Die Rollen werden im Benutzerstamm hinterlegt und bilden damit das Benutzermenü. Mit einem SAP R/3 System 71 Standardrollen für das AIS ausgeliefert. Diese Standardrollen können über die Auswahl SAP*AUDITOR* angezeigt werden.

Die Standardrollen sind in 2 Kategorien aufgeteilt, die Transaktionsrollen und die Berechtigungsrollen. Die Transaktionsrollen definieren nur das Benutzermenü und die Berechtigungsrollen nur die Berechtigungen. Ohne die Trennung dieser Rollen müssten die Berechtigungen erheblich modifiziert werden, um sie an die Anforderungen des jeweiligen Audits anzupassen. Werden die Berechtigungen aus dem Benutzermenu generiert, so ergeben sich daraus auch Änderungsberechtigungen. Auditoren sollten aber nur mit Anzeigeberechtigungen ausgestattet sein. Aufgrund der Trennung der Bereiche lassen sich spätere Korrekturen und Ergänzungen einfacher umsetzen.

Die Berechtigungsrollen sind in ihrer Bezeichnung nahezu identisch mit den dazugehörigen Trankaktionsrollen. Die Berechtigungsrollen sind lediglich an der Erweiterung „_A“ zu erkennen. Das „_A“ steht hierbei für die englische Bezeichnung

für Berechtigung: Authority. Die Transaktionsrolle für den Datenschutzbeauftragten heißt beispielsweise SAP_AUDITOR_DS und die dazugehörige Berechtigungsrolle SAP_AUDITOR_DS_A. Alle Einzelrollen für das AIS sind übrigens in der Sammelrolle SAP_AUDITOR (AIS – Audit Information System) zusammengefasst.

4.3 Funktionen des AIS

Das AIS enthält 2 Hauptbereiche, das kaufmännische Audit und das System Audit. Das kaufmännische Audit ist nicht Gegenstand dieser Studienarbeit und wird daher auch nicht näher betrachtet. Das System Audit des AIS gliedert sich in 3 Hauptbereiche: die allgemeine Systemprüfungen, Analyse der Nutzer und Berechtigungen sowie die Prüfung des Repository und der Tabellen. Daraus resultieren umfangreiche Funktionen zur Analyse des Systemzustandes, wie Benutzerverwaltung, Systemprotokollierung und Transportwesen.

Über das Infosystem „Benutzer und Berechtigungen“ kann das SAP-Berechtigungskonzept analysiert werden, es können z.B. verschiedene Auswertungen über Benutzer, Rollen oder Änderungsbelege (Protokollierung der Benutzer-/Rollenverwaltung) generiert werden. Zusätzlich gewährt das System Audit Zugriff auf verschiedene Systemprotokolle und Statusanzeigen (workload anlysis) für Benutzer, Transaktionen, Programme sowie Server.

Neben den 2 Hauptbereichen enthält das AIS auch spezielle Funktionalitäten zum Datenschutzaudit, diese beschränken sich aber bisher nur auf das Dateiregister[1]. Die folgenden Transaktionen für die Dateiregister zu personenbezogenen Daten sind im AIS verfügbar:

- Verwendungsnachweis von Domänen zu nicht-leeren DB-Tabellen
- Dateiregister für Mitarbeiterdaten
- Dateiregister für Bewerberdaten
- Dateiregister für Lieferantendaten
- Dateiregister für Kundendaten
- Dateiregister für Partnerdaten

[1] Im BDSG wurde der Begriff Dateiregister im Jahr 2003 durch den Begriff Übersichten ersetzt. In SAP R/3 ist bis dato keine Anpassung des Begriffs erfolgt.

- Dateiregister für Sachbearbeiterdaten
- Dateiregister für Verkäufergruppendaten
- Dateiregister für Patientendaten
- Dateiregister für R/3-Nutzer
- Ausgabe Felddokumentation mit erlaubten Daten

Weitere für den DSB relevante Funktionalitäten finden sich u.a. im bereits erwähnten System Audit, weshalb dem DSB in der Praxis oft zusätzlich die Berechtigungen zum System Audit erteilt werden. Diese Vorgehensweise ist aufgrund kritischer Berechtigungen im System Audit jedoch zu überdenken (s.Abschnitt 4.5). Eine bessere Lösung wäre die Erweiterung der Standardrolle SAP_AUDIT_DS um die relevanten Transaktionen und die korrespondierenden Berechtigungen.

4.4 Schwachstellen des AIS aus Datenschutzsicht

Eines der grundlegenden Probleme des AIS besteht darin, dass einige SAP-Funktionalitäten nicht auf Anzeigeberechtigungen beschränkt werden können. In der Praxis ergibt sich dadurch für die zuständigen Administratoren für die Vergabe von Berechtigungen folgendes Dilemma: entweder wird dem Auditor der Zugriff auf die entsprechenden Funktionen gänzlich verweigert oder er erhält mit den erhaltenen Berechtigungen auch unerwünschte Änderungsrechte, die teilweise auch kritische Funktionen betreffen. Eine ausführliche Beschreibung dieser kritischen Funktionen erfolgt in Abschnitt 4.5.

Im AIS ist es derzeit nicht möglich, Prüfungen oder Auswertungen auf einen Mandanten zu beschränken.

Durch die Umstellung des AIS von der Menütechnik auf eine rollenbasierte Pflegeumgebung ergibt sich ein unstrukturiertes Benutzermenü, in dem keine logischen Einheiten zu erkennen sind. Eine sinnvolle Strukturierung kann bisher nur manuell durch den Benutzer vorgenommen werden.

Die SAP-Standardrolle für den DSB gewährleistet Zugriff auf die „Dateiregister“ zu personenbezogenen Daten. Im BDSG wurde der Begriff Dateiregister bereits 2003 durch die Bezeichnung „Übersichten“ ersetzt. Hier sollte eine Begriffsanpassung in SAP R/3 erfolgen.

4.5 Beispiele für kritische Berechtigungen in den SAP-Standardrollen

Kritische Berechtigungen sind Berechtigungen, die es ermöglichen, Aktivitäten im SAP-System auszuführen, die ein Sicherheitsrisiko darstellen. Dies kann die Möglichkeit beinhalten, die Veränderbarkeit im System zu setzen (einschließlich des Produktivsystems), Transporte durchzuführen oder Benutzerberechtigungen zu vergeben. Grundsätzlich sind solche kritischen Berechtigungen für den Betrieb des Systems zwar notwendig, jedoch sollten sie nur speziellen Nutzern vorbehalten sein (z.B. Notfallbenutzern), um das Risiko, das diese Berechtigungen beinhalten, möglichst gering zu halten.

Die Standardrolle SAP_AUDITOR_DS_A hat laut SAP-Beschreibung keinen reinen Lesezugang. Der DSB sollte aber, seinen Aufgaben entsprechend, nur diesen Lesezugang haben. Durch die Berechtigungen dieser Standardrolle sind Transaktionscodes ausführbar, die elementare und hochgradig sicherheitskritische Einstellungsmöglichkeiten erlauben. Es ist u. a. die Transaktion „SU26“ (Ausschalten von Berechtigungsprüfungen) enthalten. Diese Transaktion sollte nur restriktiv oder in Ausnahmesituationen im Produktivsystem verwendet werden (vgl. Otto (2008), S. 50).

Die Standardrolle SAP_CA_AUDITOR_SYSTEM_DISPLAY, die laut Beschreibung reinen Lesezugriff erlauben soll, sind kritische Berechtigungen und Transaktionen enthalten. Dies ist besonders problematisch, weil sich die Unternehmen z.B. aus Zeitgründen ggf. auf die Definitionen von SAP verlassen und diese nicht selbst überprüfen. Die Rolle enthält z.B. das Berechtigungsobjekt „S_PROGRAM“, das festlegt, welche ABAP-Programme ausgeführt werden dürfen. Darin kann auch die Berechtigung zur Variantenpflege der Programme vergeben werden („VARIANT“). Diese Berechtigung ist auch ist auch für die Standardrolle SAP_CA_AUDITOR_SYSTEM_DISPLAY vergeben. SAP selbst weist in der Dokumentation zur AIS-Benutzerverwaltung darauf hin, dass im Produktivsystem niemals Änderungsberechtigungen für das Objekt „S_PROGRAM“ vergeben werden dürfen. Die Berechtigung ist also als kritisch einzustufen. (vgl. Otto (2008), S.51)

Auch einige Transaktionen, die in der obigen Rolle enthalten sind, sind kritisch. Die Transaktion „SCC3“, die Protokolle zu Mandantenkopien anzeigt, erlaubt zur Laufzeit auch das Löschen dieser Systemprotokolle. Somit ist diese Transaktion nicht nur unter Datenschutzgesichtspunkten kritisch, sondern auch in Bezug auf die rechtlichen Vorgaben zur Nachvollziehbarkeit und zum Risikomanagement (vgl. Otto (2008), S.51). Die Rolle enthält mindestens 3 weitere kritische Transaktionen. So ermöglicht „RSRFCCHK“ (Remote Function Call mit Anmeldedaten), die Änderung der Einstellungen für RFC Destinationen. „RSABAUTH“ (Reportberichtsgruppen

aktualisieren) ermöglicht die Definition von Berechtigungsgruppen. „SU05“ (Verwaltung der Internet Benutzer) ermöglicht die Pflege der Internet Benutzer. (vgl. Otto (2008), S.51).

Die obige Auflistung der kritischen Berechtigungen und Transaktionen erhebt keinen Anspruch auf Vollständigkeit. Es sind weit mehr solcher Transaktionen und Berechtigungen bekannt. Da im SAP-System ca. 50.000 Transaktionen definiert sind, ist es für den Anwender nahezu unmöglich, den Überblick zu behalten. Die kritischen Berechtigungen sind besonders schwerwiegend, wenn sie in den Rollen von Anwendern enthalten sind, die möglicherweise über nicht genügend Detailkenntnisse im System verfügen, da sie es nicht regelmäßig nutzen. Dies kann z.B. auf den DSB zutreffen, der aufgrund seiner zahlreichen Aufgaben und auf Gründen des Zeitmangels vielleicht nicht immer die Möglichkeit hat, sich vor einer Datenschutzprüfung hinreichend in die Feinheiten des Systems einzuarbeiten. Die vorhandenen Sicherheitsmängel könnten dazu führen, dass, wenn auch unabsichtet, kritische Transaktionen ausgeführt werden, die schwerwiegende Folgen haben können. Daher ist dringender Handlungsbedarf zur Unterbindung dieser kritischen Berechtigungen in den Standardrollen erforderlich.

5 Zusammenfassung und Ausblick

In der vorliegenden Studienarbeit wurden die gesetzlichen Vorgaben zum Datenschutz in Unternehmen anhand des BDSG aufgezeigt und die Aufgaben des DSB definiert. Das in SAP R/3 zur Verfügung gestellte AIS wurde hinsichtlich der Verwendbarkeit für Datenschutzprüfungen durch den DSB analysiert und Schwachstellen wurden hervorgehoben. Des Weiteren wurden Standardrollen im AIS vorgestellt und einige darin enthaltene kritische Berechtigungen und Transaktionen erläutert.

Es gibt verschiedene Autoren, die Vorschläge zur Abänderung der Standardrollen gemacht haben, um kritische Berechtigungen und Transaktionen zu vermeiden. Hier sei z.B. auf Anna Otto verwiesen, die im Rahmen ihrer Diplomarbeit neue Datenschutzrollen für das AIS entwickelt hat. Aufgrund der Vielzahl der neuen Rollen musste auf eine Analyse in dieser Studienarbeit verzichtet werden.

Die Vorschläge werden von der SAP AG durchaus wohlwollend zur Kenntnis genommen und werden in Zukunft sicher in das System integriert werden. Die SAP AG hat im Juni 2008 außerdem einen neuen Datenschutzleitfaden veröffentlicht, der im Rahmen dieser Studienarbeit aber nicht mehr berücksichtigt werden konnte.

Literaturverzeichnis

Bundesdatenschutzgesetz (BDSG 1990) vom 22.08.2006, BGBl I
http://www.bundesrecht.juris.de/bdsg_1990/__1.html. 24.Juli 2008

Otto, A. (2008): Entwicklung von Datenschutzrollen für das AIS im SAP ERP. Saarbrücken

SAP AG (Hrsg.) (1998): R/3 Sicherheitsleitfaden Band II – R/3 Sicherheitsservices im Detail. Version 2.0a. Walldorf.

SAP AG (Hrsg.) (2001): R/3 Sicherheitsleitfaden Band II – R/3 Berechtigungskonzept. Version 3.0. Walldorf.

SAP AG (Hrsg.) (2001) Leitfaden Datenschutz für SAP R/3 Release 4.6
http://www.sap.com/germany/revis/infomaterial/index.epx. 24.Juli 2008

Abschließende Erklärung

Ich versichere hiermit, dass ich die vorliegende Studienarbeit selbständig, ohne unzulässige Hilfe Dritter und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Magdeburg, den 25. Juli 2008