

## Aspekte des Datenschutzes bei SAP

[Einführung](#)

[Konzeptionelle Probleme bei SAP R/3](#)

[Einzelprobleme bei SAP R/3](#)

[Häufig zu beobachtende Praxisprobleme](#)

[Anforderungen an eine ordnungsgemäße R/3-Installation](#)

[Weitere Hinweise und Links](#)

---

### Einführung

Die datenschutzrechtliche Diskussion um SAP bezog sich früher fast ausschließlich auf den Bereich des Arbeitnehmer-Datenschutzes. Von Personal- und Betriebsräten wurde vor allem problematisiert, inwieweit die im Rahmen der Personalplanung erfassten Arbeitnehmer-Daten zu Leistungs- und Verhaltenskontrollen zweckentfremdet genutzt werden können. Dabei galt es vor allem zu verhindern, dass Betriebsdaten, die beispielsweise in der Fertigung oder im Lager erhoben werden, aufgrund der hohen Integrationsdichte des Systems unbemerkt an anderer Stelle wieder auftauchen und mit Hilfe der SAP-Abfragesprache ABAP/4 beliebig ausgewertet werden. Durch den Einzug von SAP in Bereiche, in denen über betriebliche Daten hinaus auch sensible Kunden- oder Patientendaten verwaltet werden, erhält die Auseinandersetzung um den Datenschutz eine neue Dimension.

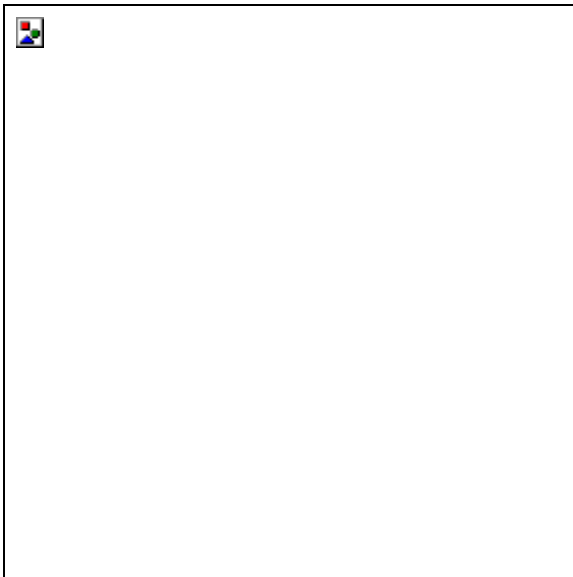
Die Diskussion ist mittlerweile zunehmend geprägt durch die Komplexität von SAP-Systemen, insbesondere des SAP-Berechtigungskonzepts, in dem festgelegt wird, welche Funktionen ein Anwender ausführen darf und auf welche Daten er zugreifen kann. Es besteht aus folgenden Komponenten:

- Ein **Berechtigungsobjekt** kann aus bis zu zehn **Berechtigungsfeldern** bestehen. Berechtigungsobjekte werden in **Objektklassen** unterteilt, die einen bestimmten Bereich betreffen wie etwa den Vertrieb oder die Materialwirtschaft.
- **Berechtigungsfelder** definieren beispielsweise zu schützende SAP-Elemente (Buchungskreise, Werke etc.) und zu schützende Aktivitäten (Ändern, Hinzufügen, Löschen etc.).
- **Berechtigungen** beziehen sich auf ein Berechtigungsobjekt und stellen die Ausprägung von Werten zu den Feldern eines Berechtigungsobjekts dar. Dabei ist sowohl die Vergabe von Einzelwerten als auch von Wertebereichen möglich. Zu einem Berechtigungsobjekt können diverse Ausprägungen (Berechtigungen) erstellt werden. Die Prüfung der Berechtigung erfolgt gegenüber den Feldinhalten, wobei die Berechtigungsfelder in UND-Verknüpfung geprüft werden.
- Ein **Profil** ist eine Zusammenfassung von Berechtigungen. Ein Profil kann sich z.B. auf eine Funktion, einen Arbeitsplatz oder einen Anwendungsbereich beziehen. Mehrere Profile können in einem **Sammelprofil** zusammen gefasst werden.
- **Benutzerstammsätze** beinhalten schließlich die für einen Benutzer zugelassenen Profile bzw. Sammelprofile. Änderungen, die sich innerhalb eines Profils oder Sammelprofils vollziehen, wirken sich auf alle Benutzer aus, die das Profil bzw. Sammelprofil besitzen.

Mit Einführung des Profilgenerators stellt SAP ein Werkzeug zur Verfügung, mit dem sich Rollen erstellen lassen, aus denen Profile generiert werden können.

- Für eine **Einzelrolle** können zunächst die benötigten Transaktionen in einem Menü zusammengestellt werden. Auf Grundlage der ausgewählten Transaktionen werden Vorschläge für Berechtigungen generiert, die in einer hierarchischen Struktur dargestellt werden und teilweise mit Werten vorbelegt sind. Die Vorschlagswerte stammen aus SAP-Tabellen und sollten geprüft bzw. müssen ergänzt werden. Anschließend werden aus diesen Werten Profile mit entsprechenden Berechtigungen generiert.
- Einzelrollen können zu einer **Sammelrolle** zusammengefasst werden. So wäre es beispielsweise möglich, bestimmte Funktionen in einer Einzelrolle zu definieren, während ein gesamter Arbeitsplatz durch die Zusammenstellung der Einzelrollen zu einer Sammelrolle dargestellt wird.
- Einzelrollen bzw. Sammelrollen werden **Benutzerstammsätzen** zugewiesen.

Auswertungsmöglichkeiten z.B. über Benutzer, Profile, Berechtigungen, Berechtigungsobjekte, Rollen und Änderungsbelege bietet das Informationssystem Berechtigungen.



---

### Konzeptionelle Probleme bei SAP R/3

1. Zugriffsrechte für die Benutzer der R/3-Anwendung werden nicht auf Betriebssystem- oder Datenbankebene, sondern auf Anwendungsebene vergeben. Aus Sicht des Datenbank- und Betriebssystems ist das komplette R/3-System mit all seinen Anwendern nur ein einziger Benutzer. SAP hinterlegt die Daten unverschlüsselt auf der Datenbank. Daher müssen entsprechende Maßnahmen getroffen werden, damit keinem Anwender ein direkter Datenbankzugriff möglich ist. Neben der Entwicklung eines kundenspezifischen Berechtigungskonzepts ist somit ein umfassendes Sicherheitskonzept notwendig, das weitere Ebenen wie z.B. die Kommunikation (Netzwerk, Firewall, SAP-Router etc.),

die Datenbank und die zugrunde liegenden Betriebssysteme einbezieht.

2. Zugriffsrechte werden nicht pro Datenbank-Objekt vergeben, sondern in Form von Berechtigungen auf Anwendungsebene. Die Prüfung der Berechtigungen findet durch Authority Checks in den ABAP/4-Programmen und Transaktionen statt.  
Um auszuschließen, dass ein SAP-Benutzer Zugriff auf ein bestimmtes Datum hat, ist es daher notwendig, sämtliche Programme daraufhin zu überprüfen, ob der Authority Check dem Benutzer den Zugriff ermöglicht oder nicht. Um zu verhindern, dass Authority Checks in den Programmen verändert werden, ist eine Trennung von Test und Produktion umso wichtiger.

3. Komplexes Berechtigungskonzept :

Die Überprüfung, ob ein Benutzer ein bestimmtes Programm aufrufen darf, stellt sich als ein baumartiges Geflecht von

- Berechtigungen,
- Profilen, Sammelprofilen
- und ggf. Rollen und Sammelrollen

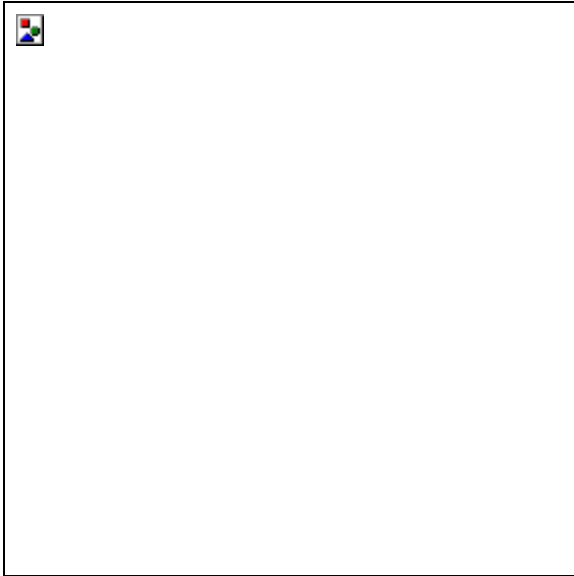
dar und ist sehr komplex.

Wer im Rahmen einer Prüfung oder Systemrevision die Zugriffsrechte einzelner Benutzer überprüfen möchte, kann deshalb nur schrittweise versuchen, dieses Geflecht zu entwirren. Zunächst muss überprüft werden, welche Rollen und Profile mit welchen Berechtigungen die einzelnen Benutzer besitzen. Einem Benutzer können auch Sammelrollen bzw. Sammelprofile zugeordnet werden. Anschließend wird festgestellt, in welchen Programmen und Transaktionen die den Berechtigungen entsprechenden Berechtigungsobjekte genutzt werden und auf welche Daten die jeweiligen Programme und Transaktionen zugreifen.

Die Komplexität wird zusätzlich noch dadurch erhöht, dass es möglich ist, den Zugriff auf Programme und Transaktionen von dem Besitz mehrerer Berechtigungen abhängig zu machen. Es ist daher äußerst mühsam, den Kreis der Zutrittsberechtigten abschließend zu bestimmen.

Folglich kann auch in umgekehrter Reihenfolge nur sehr umständlich geprüft werden, welche Benutzer auf ausgesuchte Datenfelder zugreifen können.

Die Komplexität eines R/3-Systems wird bereits am Umfang der Berechtigungsobjekte deutlich. Das R/3-Release 3.1i umfasste schon 543 Berechtigungsobjekte, während das Release 4.0B 710 Berechtigungsobjekte enthält. Unter 4.6C spricht man bereits von ca. 900 Berechtigungsobjekten.

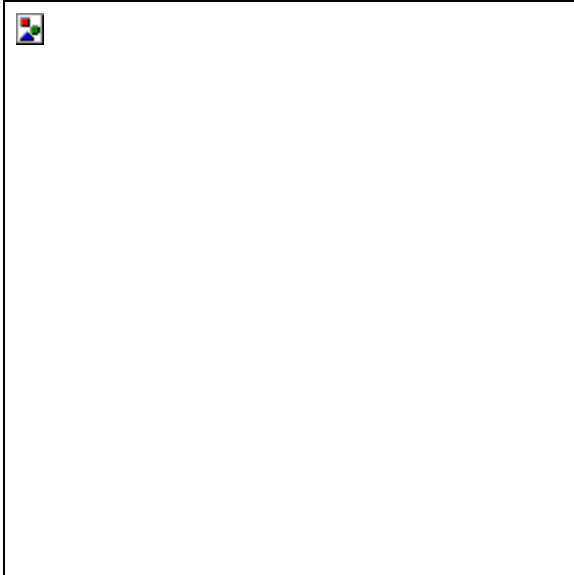


---

### Einzelprobleme bei SAP R/3

1. Die zwischen Client und Server transportierten Daten, insbesondere die aus dem Passwort gebildeten Hashwerte, werden lediglich komprimiert, jedoch nicht verschlüsselt übertragen. Eine verschlüsselte Datenübertragung ist nur möglich, wenn Zusatzsoftware eingesetzt wird.
2. Die von SAP ausgelieferten Standard-Profile sind oftmals so gestaltet, dass die Berechtigungen über das erforderliche Maß hinausgehen. Aufgrund der Komplexität des Berechtigungskonzepts werden die Standard-Profile jedoch in vielen Fällen ungeprüft zur Nutzung übernommen. Sowohl Standard-Profile als auch die ausgelieferten Vorlagen für Rollen sollten beispielhaft zur Erstellung selbst definierter Berechtigungen dienen und nicht ungeprüft übernommen werden.
3. Um Benutzern nach einem Releasewechsel auch weiterhin einen reibungslosen Systemzugriff zu garantieren, wird ihnen in der Regel das Standard-Profil SAP\_NEW zugeordnet, das den Zugriff für sämtliche hinzugekommenen Berechtigungsobjekte ermöglicht. Dadurch erhalten die Anwender jedoch auch Zugriffsrechte für Objekte, die sie normalerweise nicht benötigen. Um zu verhindern, dass den Benutzern mittels SAP\_NEW zusätzliche Zugriffsrechte eingeräumt werden, sollten die im Profil SAP\_NEW enthaltenen und für den jeweiligen Releasewechsel benötigten zusätzlichen Berechtigungen in die jeweiligen Profile eingearbeitet werden.
4. Im Kernel des R/3-Systems ist der Pseudob Benutzer SAP\* implementiert, der nicht gelöscht werden kann und uneingeschränkte Rechte auf das System hat. Eine Sicherung gegen eine unbefugte Nutzung dieser Kennung ist nur möglich, wenn in jedem Mandanten zu der Kennung SAP\* ein Benutzerstammsatz angelegt wird, das Initialkennwort verändert und der SAP\*-Kennung keinerlei Rechte zugewiesen werden. Allerdings besteht weiterhin das Risiko, dass der Benutzerstammdatensatz vom Datenbank-Administrator gelöscht und neu generiert wird.

5. Zugriffsrechte können nicht terminalbezogen für einzelne Arbeitsplatzrechner vergeben werden, sondern sind netzweit aufrufbar.



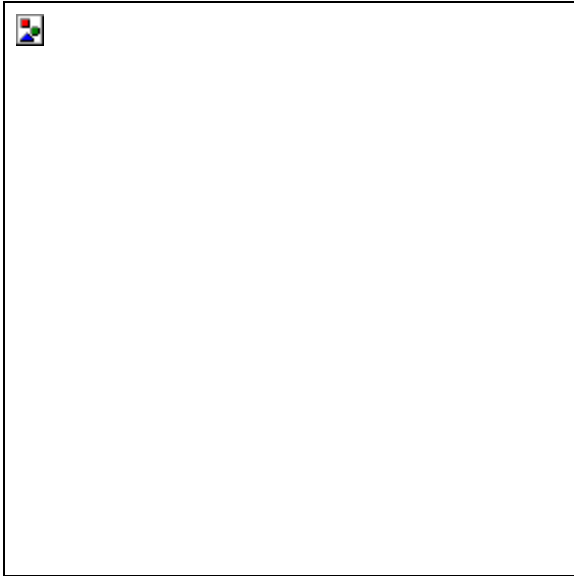
---

### Häufig zu beobachtende Praxisprobleme

1. Die gebotene Trennung von Test und Produktion wird oftmals nicht durchgehalten.
2. Die von SAP angebotenen Rollenvorlagen und Profile zur Funktionstrennung der Benutzer- und Berechtigungsadministration (Benutzeradministrator, Berechtigungsadministrator und Aktivierungsadministrator bei Nutzung von Profilen/ Benutzeradministrator, Berechtigungsdatenadministrator und Berechtigungsprofiladministrator bei Nutzung von Rollen) werden oftmals nicht genutzt.
3. Zahlreiche Benutzer haben die Berechtigung SAP\_ALL.
4. Komplexität führt zu Intransparenz:

Als Folge der Intransparenz werden von den zuständigen Systemverwaltern zunächst die zur Verfügung gestellten Standardprofile dahingehend geprüft, ob sie direkt oder in leicht modifizierter Form für einzelne Benutzer übernommen werden können. Wenn die Standardrechte nicht ausreichen, werden die Berechtigungen solange erweitert, bis der Zugriff auf die gewünschten Systemressourcen gewährt wird. Leider wird bei dieser Art der Berechtigungsvergabe nicht geprüft, ob durch die zusätzlich vergebenen Berechtigungen vielleicht auch der Zugriff auf andere Programme oder Transaktionen freigegeben wird.

5. Die Intransparenz wird durch kurzfristige und schlecht dokumentierte Änderungen zusätzlich erhöht. Das SAP-Berechtigungskonzept ist vollständig kaum prüfbar.



---

### **Anforderungen an eine ordnungsgemäße SAP R/3-Installation**

1. Es sollte ein geeignetes Berechtigungs-, Administrations- und Freigabekonzept vorliegen.
2. Es sollten getrennte Test- und Produktionsumgebungen eingerichtet sein. Der Transport von der Test- in die Produktivumgebung sollte durch entsprechende Transportaufträge erfolgen.
3. Benutzerstammdatensätze sollten durch einen Benutzeradministrator, Profile und Berechtigungen durch einen Berechtigungsadministrator und einen Aktivierungsadministrator verwaltet werden. Bei Verwendung von Rollen kann zwischen einem Benutzeradministrator, einem Berechtigungsdatenadministrator und Berechtigungsprofiladministrator unterschieden werden.
4. Zur Erhöhung der Transparenz und Erleichterung der Administration sollten im Berechtigungskonzept geeignete Namenskonventionen für Benutzer sowie Rollen bzw. Profile und Berechtigungen festgelegt werden.
5. Es sollte eine angemessene und zeitnahe Dokumentation der entwickelten Berechtigungen und seiner Änderungen erfolgen.
6. Die Fachmodule sollten von Moduladministratoren betreut werden.
7. Die Freigabe von ABAP/4-Programmen sowie Änderungen an Berechtigungen erfordern einen entsprechenden schriftlichen Antrag der jeweiligen Fachverantwortlichen.
8. Eigene Entwicklungen sollten in das Berechtigungskonzept eingebunden werden.
9. Es sollten möglichst keine redundanten Berechtigungen vergeben werden, d.h. Berechtigungen sollten sich nur auf ein Profil beziehen und nicht auf mehrere Profile. Die Vergabe nicht-redundanter Berechtigungen verbessert die Transparenz des

Berechtigungskonzepts, da von einer Berechtigungsänderung nicht mehrere Profile zugleich betroffen sind.

10. In der Produktionsumgebung sollten keine Standard-Profile bzw. Standard-Rollen zum Einsatz kommen.
11. In der Produktionsumgebung sollte das Standard-Profil SAP\_NEW nicht zum Einsatz kommen. Die im Standard-Profil SAP\_NEW enthaltenen Berechtigungen sollten in die bestehenden Profile integriert werden.
12. Der Zugriff auf Berechtigungsobjekte, die keiner Zugriffsbeschränkung unterliegen, sollte über ein zentrales Profil erfolgen, das allen Benutzern zugeordnet wird.
13. Reports sollten in der Regel nicht mit Hilfe der Transaktion sa38 ausgeführt werden, sondern durch Aufruf eines Transaktionscodes.
14. Berechtigungen und Profile sollten über Rollen mit Hilfe des Profilgenerators erstellt werden.
15. Sofern Windows NT als Server-Betriebssystem benutzt wird, sollte SAP als eigene Domäne definiert werden.
16. Zur Erhöhung der Sicherheit bei der Anbindung von SAP-Clients an SAP-Server sollte ein sogenannter SAP-Router eingesetzt werden. Durch entsprechende Einträge in den Zugriffstabellen kann beispielweise festgelegt werden, welche Maschinen oder Benutzer mit dem SAP-Server kommunizieren dürfen. Der Verbindungsaufbau kann zusätzlich noch durch Passwörter geschützt werden.
17. Sofern die Daten zwischen Client und Server über unsichere Netze transportiert werden, sollten die Daten verschlüsselt übertragen werden - dies gilt auch für die Authentisierungsinformationen. Mit SNC (Secure Network Communications) steht eine Softwareschicht zur Verfügung, über die R/3 mit externen Sicherheitsprodukten zusammenarbeiten kann.
18. R/3-Anwendungen können SSF (Secure Store & Forward) verwenden und damit Daten in ein sicheres Format bringen, damit sie beispielsweise geschützt sind, wenn sie transportiert oder extern auf Datenträgern abgelegt werden sollen. Die Verschlüsselung erfolgt auf der Basis von X.509. Für SNC (vgl. Ziff. 17) und SSF stehen externe Sicherheitsprodukte zur Verfügung.

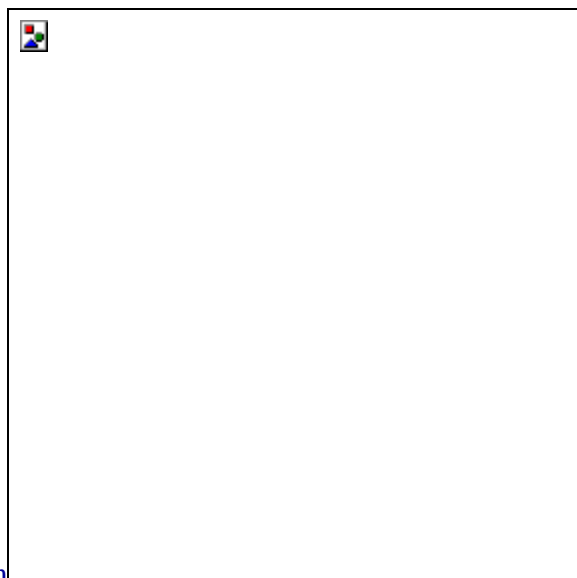


---

### Weitere Hinweise und Links

[http://www.datenschutz-bremen.de/technik/datenschutz\\_sap.htm](http://www.datenschutz-bremen.de/technik/datenschutz_sap.htm) -  
[top](#) **Jahresberichte von Datenschutzbeauftragten**

- Jahresbericht des Berliner Datenschutzbeauftragten für das Jahr 1998  
[Technische und organisatorische Datenschutzfragen bei Standardsoftware-Produkt SAP R/3](#)
- 28. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten 1999  
[SAP R/3](#)



<http://www.hessen.de/sdsb/tb28/k10p4.htm>