



SAP AG
Neurottstr. 16
D-69190 Walldorf

R/3-Sicherheit

R/3-Sicherheitsleitfaden: BAND III

Checklisten

Version 2.0a : Deutsch

11. Dezember 1998

Copyright

©Copyright 1998 SAP AG. Alle Rechte vorbehalten.

Weitergabe und Vervielfältigung dieser Dokumentation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch SAP AG nicht gestattet. In dieser Dokumentation enthaltene Informationen können ohne vorherige Ankündigung geändert und ergänzt werden.

Die von SAP AG oder deren Vertriebsfirmen angebotenen Software-Produkte können Software-Komponenten auch anderer Software-Häuser enthalten.

Microsoft®, WINDOWS®, EXCEL®, NT® und SQL-Server® sind eingetragene Warenzeichen von Microsoft Corporation.

IBM®, OS/2®, DB2/6000®, AIX®, OS/400® und AS/400® sind eingetragene Warenzeichen von IBM Corporation.

OSF/Motif® ist ein eingetragenes Warenzeichen von Open Software Foundation.

ORACLE® ist ein eingetragenes Warenzeichen der ORACLE Corporation, Kalifornien, USA.

INFORMIX®-OnLine *for SAP* ist ein eingetragenes Warenzeichen der Informix Software Incorporated.

UNIX® und X/Open® sind eingetragene Warenzeichen der SCO Santa Cruz Operation.

ADABAS® ist ein eingetragenes Warenzeichen der Software AG.

SECUDE® ist ein eingetragenes Warenzeichen der GMD-Forschungszentrum Informationstechnik GmbH.

SAP®, R/2®, R/3®, RIVA®, ABAP/4®, SAPaccess®, SAPoffice®, SAPmail®, SAP-EDI®, SAP Business Workflow®, SAP EarlyWatch®, SAP ArchiveLink®, R/3 Retail® sind eingetragene Warenzeichen der SAP AG.

Alle Rechte vorbehalten.

Inhaltsverzeichnis

KAPITEL 1 : EINLEITUNG.....	1-1
Kapitel 1-1 : Verwendung des R/3-Sicherheitsleitfadens.....	1-1
R/3-Sicherheitsleitfaden BAND III: Checklisten	1-2
Kapitel 1-2 : Support und Feedback	1-6
Technische Beratung.....	1-6
Feedback.....	1-6
KAPITEL 2 : CHECKLISTEN.....	2-1
Checkliste 2-1: Benutzerauthentifizierung.....	2-2
Checkliste 2-2: R/3-Berechtigungskonzept	2-7
Checkliste 2-3: Netzwerk-Infrastruktur	2-11
Checkliste 2-4: Schutz des Betriebssystems	2-14
Checkliste 2-5: Schutz der Zugriffe auf die Datenbank.....	2-20
Checkliste 2-6: Schutz des Produktivsystems (Change & Transport System).....	2-28
Checkliste 2-7 : Remote Communications (RFC & CPI-C)	2-31
Checkliste 2-8 : Secure-Store-&-Forward-Mechanismen (SSF) und digitale Signaturen	2-34
Checkliste 2-9: Protokollierung und Prüfung	2-37
Checkliste 2-10: Spezielle Themen.....	2-40

Kapitel 1 : Einleitung

Kapitel 1-1 : Verwendung des *R/3-Sicherheitsleitfadens*

Der *R/3-Sicherheitsleitfaden* besteht aus drei Bänden:

R/3-Sicherheitsleitfaden BAND I: R/3-Sicherheitsservices im Überblick

R/3-Sicherheitsleitfaden BAND II: R/3-Sicherheitsservices im Detail

R/3-Sicherheitsleitfaden BAND III: Checklisten

R/3-Sicherheitsleitfaden BAND I: R/3-Sicherheitsservices im Überblick

Der *R/3-Sicherheitsleitfaden BAND I* bietet einen allgemeinen Überblick über die in R/3 angebotenen Sicherheitsservices. In *BAND I* können Sie sich mit diesen Services vertraut machen, z. B. bevor Sie ein Sicherheitskonzept ausarbeiten oder ein R/3-System installieren.

Kapitel 1 : Einleitung

R/3-Sicherheitsleitfaden BAND II: R/3-Sicherheitsservices im Detail

Der *R/3-Sicherheitsleitfaden BAND II* behandelt die technischen Aspekte der Sicherheit im R/3-System. Er beschreibt die erforderlichen Aufgaben und enthält die Empfehlungen von SAP für die verschiedenen Komponenten des R/3-Systems. Verwenden Sie *Band II*, sobald Sie ein Sicherheitskonzept ausgearbeitet haben und dieses für Ihr R/3-System implementieren möchten.

R/3-Sicherheitsleitfaden BAND III: Checklisten

Der *R/3-Sicherheitsleitfaden BAND III* enthält die Checklisten zu den in *BAND II* behandelten Themen. Mit diesen Checklisten können Sie die ergriffenen Maßnahmen erfassen und diese überprüfen und überwachen.

Aktualisierungen

Nach Bedarf veröffentlicht SAP aktualisierte Versionen dieses Leitfadens. Sie finden diese ebenfalls regelmäßig in SAPNet.

R/3-Sicherheitsleitfaden BAND III: Checklisten

Die Voraussetzungen für die Verwendung des *R/3-Sicherheitsleitfadens BAND III* sind

- ein bestehendes Sicherheitskonzept
- ein gutes Verständnis der im *R/3-Sicherheitsleitfaden: BAND I* und *BAND II* beschriebenen Konzepte und Maßnahmen
- Zeit und Ressourcen

Sicherheit ist ein Qualitäts- und Schutzmerkmal. Eine unzureichende Sicherheit kann für Ihr Unternehmen zu Zeitverlust, Verlust von Aktiva und Geld führen. Sicherheit erfordert die Investition von Zeit und Ressourcen. SAP empfiehlt Ihnen, für die Implementierung Ihres Sicherheitskonzepts und die Pflege der gewünschten Sicherheitsstufe genügend Zeit und Ressourcen aufzuwenden.

Verwendung von BAND III

Die Checklisten in diesem Band sind eine Zusammenfassung der im *R/3-Sicherheitsleitfaden: BAND II* beschriebenen Maßnahmen. Diese Checklisten dienen als Beispiele für die verschiedenen sicherheitsrelevanten Themen, die Sie für Ihr Sicherheitskonzept berücksichtigen können.



Hinweis

Beachten Sie folgendes:

- Betrachten Sie diese Checklisten als Vorschläge und Beispiele! Diese Checklisten enthalten **keine** vollständige Sammlung von sicherheitsrelevanten Themen, die für jeden Benutzer gelten.
- Kopieren Sie diese Checklisten und passen Sie sie an Ihr individuelles Sicherheitskonzept an.
 - Definieren Sie Ihre eigenen Prioritäten.
 - Löschen Sie die Themen, die für Sie nicht relevant sind.
 - Fügen Sie nach Bedarf Themen hinzu, die nicht berücksichtigt wurden.
- Aktualisieren Sie Ihre Checklisten regelmäßig, um sie an die sich ändernden Anforderungen anzupassen.

Die **technische Beratung zum Thema Sicherheit** steht Ihnen ebenfalls bei Fragen zur Verfügung. Siehe *Kapitel 1-2 : Support und Feedback*.

Gültige Releases

Diese Version des *R/3-Sicherheitsleitfadens* gilt für die R/3-Releases 3.0, 3.1 und 4.0. Verweise auf andere Releases sind ggf. explizit angegeben.

Typografische Konventionen und Standardnotationen

Die folgenden Tabellen erklären die Bedeutung der verschiedenen Formate, Symbole und Standardnotationen in diesem Leitfaden.

Tabelle 1-1: Typografische Konventionen




Diese Darstellung	wird verwendet
Text auf Bildschirmbildern	für Texte, die vom Bildschirmbild zitiert werden, z. B. Systemmeldungen, Feldnamen, Bildschirmüberschriften, Menütitel und Menütexte
Benutzereingabe	für fest vorgegebene Benutzereingaben. Diese Begriffe oder Zeichen können Sie direkt im System eingeben.
<Variable Benutzereingabe>	für variable Benutzereingaben. Diese Begriffe und Zeichen in spitzen Klammern sind jeweils durch geeignete Eingaben zu ersetzen.
NAMEN	für Reportnamen, Programmnamen, Transaktionscodes, Tabellennamen, ABAP-Schlüsselwörter, Dateinamen und Verzeichnisse
<i>Buchtitel</i>	für Verweise auf andere Bücher oder Dokumente
Tastenschlüssel	für Tasten auf Ihrer Tastatur. Dies können Funktionstasten wie z. B. F2 oder die ENTER-Taste sein.
Namen von technischen Objekten	für Namen von technischen Objekten außerhalb des R/3-Systems (z. B. UNIX- oder Windows-NT-Dateinamen oder Umgebungsvariablen)
Dieses Piktogramm	kennzeichnet
 Beispiel	ein Beispiel. Beispiele illustrieren komplexe Sachverhalte oder die Syntax von Benutzereingaben.
 Hinweis	einen Hinweis. Hinweise enthalten wichtige Informationen wie z. B. Ausnahmen oder Sonderfälle.
 Achtung	eine Warnung. Warnungen sollen dazu beitragen, Fehler zu vermeiden, die z. B. zu einem Verlust von Daten führen können.

Tabelle 1-2: Standardnotationen

Diese Notation	wird verwendet
<sid>, <SID>	für die drei Zeichen lange System-ID; je nach Kontext Groß- oder Kleinschreibung.
<SYS>	für die R/3-Systemnummer
<sid>adm, <SID>ADM	für den R/3-Systemverwalter auf Betriebssystemebene; je nach Kontext Groß- oder Kleinschreibung. Ausnahme: Auf der AS/400 ist der Systemverwalter der Benutzer <SID>OFR.

Kapitel 1-2 : Support und Feedback

Technische Beratung

Wenn der *R/3-Sicherheitsleitfaden* nicht alle Ihre Fragen in gewünschtem Maße beantwortet, wenden Sie sich an unsere technische Beratung.

SAP bietet zur Zeit die folgenden Services:

- Support und Beratungsservices für die Ausarbeitung eines unternehmensweiten Sicherheitskonzepts
- Sicherheitsanalyse-Services
- einzelne Beratungsservices zum Thema Sicherheit in der R/3-Umgebung
- Support-Services für den Aufbau eines Windows-NT-Domänenkonzepts
- Beratungsservices für die Verwendung des Internet Transaction Servers
- Schulung CA900: Technical Revision - System Security
- Workshop für das R/3-Berechtigungskonzept

Weitere Informationen erhalten Sie bei der technischen Beratung zum Thema Sicherheit unter

Tel: **+49 6227 / 7-41537**

Fax: **+49 6227 / 7-44640**

Weitere Informationen finden Sie unter

- Fact Sheet: Technische Systemsicherheit, Materialnummer 50025796
- OSS-Hinweis 114045: Beratung: Technische Systemsicherheit

Feedback

SAP ist an Ihrer Meinung zum *R/3-Sicherheitsleitfaden* interessiert. Verwenden Sie für Kommentare zum Inhalt oder zur Qualität dieses Leitfadens den Feedbackbogen am Ende dieses Leitfadens und senden Sie ihn an folgende Adresse oder Faxnummer:

SAP AG
Abteilung CCMS & Security
Postfach 1461
D-69190 Walldorf

Fax: **+49-6227 / 7-41198**

Kapitel 2 : Checklisten

Diese Checklisten ergänzen die im *R/3-Sicherheitsleitfaden: BAND I* und *BAND II* behandelten sicherheitsrelevanten Themen. Diese Listen erheben jedoch keinen Anspruch auf Vollständigkeit und sind nicht auf Ihr individuelles Sicherheitskonzept zugeschnitten. SAP empfiehlt Ihnen, diese Checklisten an Ihr individuelles Sicherheitskonzept anzupassen. Fügen Sie nach Bedarf Themen hinzu oder löschen Sie diese, und definieren Sie Ihre eigenen Prioritäten.



Hinweis

Für die Verwendung dieser Checklisten gelten die folgenden Richtlinien:

- Die Numerierung der Checklisten entspricht den Kapiteln im *R/3-Sicherheitsleitfaden: BAND II*.
- Spalte **Prio.**: Definieren und verwenden Sie Ihre eigenen Prioritäten.
- Die Spalte **Methode / Vorgehensweise** enthält die Transaktion, den Report oder ähnliche Anweisungen bezüglich des sicherheitsrelevanten Themas. Ein Eintrag wie NV x-x-x bezieht sich auf die entsprechende Nützliche Vorgehensweise in *BAND II*.
- Für die Spalte **Referenz** gelten die folgenden Richtlinien:
 - Die Überschrift enthält das entsprechende Kapitel im *R/3-Sicherheitsleitfaden: BAND II*. Diese Referenz gilt **immer** für die in der Checkliste enthaltenen Themen. Beachten Sie, daß jedes Kapitel in *BAND II* auch weitere Informationsquellen enthält.
 - Tabellenreferenzen beziehen sich ebenfalls auf die entsprechende Tabelle in *BAND II*.
 - Die Checkliste enthält ggf. auch Quellen, die direkt für die sicherheitsrelevanten Themen gelten (z. B. OSS-Hinweise, ein anderes Kapitel in *BAND II* oder die R/3-Onlinedokumentation).
- Die Spalte **Ergebnis / Anmerkungen** enthält ggf. Anmerkungen. Sie können diese Spalte auch für Ihre eigenen Anmerkungen verwenden.

Kapitel 2 : Checklisten

Checkliste 2-1: Benutzerauthentifizierung

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-1)	Ergebnis / Anmerkungen
Kennwörter					
		Haben Sie ein Kennwortkonzept ausgearbeitet? (Wie komplex sollten die Kennwörter sein, wie oft sollten sie geändert werden, etc.?) Haben Sie Ihre Mitarbeiter über das Konzept informiert? Können Sie das Konzept eventuell technisch umsetzen?	Firmenpolitik		
		Welche Mindestlänge haben die Kennwörter?	Setzen Sie den Profilparameter login/min_password_lng.	Tabelle 2-1-1	Vorschlagswert = 3
		Müssen die Benutzer ihre Kennwörter regelmäßig ändern?	Setzen Sie den Profilparameter login/password_expiration_time.	Tabelle 2-1-1	Vorschlagswert = 0 (Benutzer müssen ihre Kennwörter nicht ändern.)
		Verwenden die Systemverwalter und wichtige Entscheidungsträger komplexere Kennwörter?			Komplexe Kennwörter sollten die zulässige Maximallänge ausschöpfen und mindestens eine Zahl und ein Sonderzeichen enthalten.
		Verbietet Ihr Kennwortkonzept bestimmte Zeichenkombinationen (wie z. B. den Firmennamen)?	Geben Sie die Zeichenkombinationen, die Sie verbieten möchten, in Tabelle USR40 ein (NV 2-1-1).		
		Verwenden Sie ein externes Sicherheitsprodukt mit R/3 für die Authentifizierung, die außerhalb des R/3-Systems stattfindet?		Kapitel 2-3 <i>SNC-Benutzerhandbuch</i> Dokumentation des externen Sicherheitsprodukts	Durch den Einsatz eines externen Sicherheitsprodukts können Sie längere Kennwörter verwenden und verhindern, daß Kennwörter über das Netzwerk übertragen werden müssen.

Checkliste 2-1: Benutzerauthentifizierung (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-1)	Ergebnis / Anmerkungen
Schutzmaßnahmen für Standardbenutzer					
		Welche R/3-Mandanten gibt es in Ihrem R/3-System? Überwachen Sie diese regelmäßig um sicherzustellen, daß keine unbekannt Mandanten existieren?	Zeigen Sie die Tabelle T000 mit der Transaktion SM31 an, um eine Liste aller R/3-Mandanten zu erhalten.		
		Haben Sie die Standardkennwörter für die Standardbenutzer SAP*, DDIC, SAPCPIC und EARLYWATCH geändert?	NV 2-1-3		Eventuell möchten Sie SAPCPIC löschen, anstatt sein Kennwort zu ändern. Siehe unten: <i>Schutzmaßnahmen für SAPCPIC</i>
		Überwachen Sie regelmäßig den Status Ihrer Standardbenutzer?	Überprüfen Sie mit dem Report RSUSR003, ob der Benutzer SAP* in allen Mandanten angelegt wurde und ob die Kennwörter für die Standardbenutzer geändert wurden.	OSS-Hinweis 40689	
Schutzmaßnahmen für SAP*					
		Existiert SAP* in allen Mandanten?	Report RSUSR003		Löschen Sie den Benutzer SAP* nicht.
		Haben Sie SAP* in allen Mandanten deaktiviert?	NV 2-1-2	Informationen über den Profilparameter finden Sie im OSS-Hinweis 68048.	Alternative: Setzen Sie den Profilparameter login/no_automatic_user_sap* oder login/no_automatic_user_sapstar-abhängig vom Release.
		Gehört SAP* zur Gruppe SUPER?			
		Ist SAP* gesperrt?			

Kapitel 2 : Checklisten

Checkliste 2-1: Benutzerauthentifizierung (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-1)	Ergebnis / Anmerkungen
Schutzmaßnahmen für DDIC					
		In welchen Mandanten existiert DDIC?		OSS-Hinweis 11677 OSS-Hinweis 34964	DDIC wird bei der Installation in den Mandanten 000 und 001 angelegt und für Aufgaben bei der Installation, in der Softwarelogistik und für bestimmte ABAP-Dictionary-Aufgaben benötigt. DDIC ist auch in anderen Mandanten für Importe erforderlich. Löschen Sie DDIC oder dessen Profile nicht. Ändern Sie sein Standardkennwort.
Schutzmaßnahmen für SAPCPIC					
		Haben Sie das Kennwort des Benutzers SAPCPIC geändert oder den Benutzer gesperrt? Wenn Sie das Kennwort geändert haben, haben Sie die betroffenen Programme entsprechend angepaßt? Wenn Sie den Benutzer SAPCPIC gesperrt haben, sind Sie sich des Funktionsverlusts bewußt?	NV 2-1-3	OSS-Hinweis 29276 Tabelle 2-1-3	Wenn Sie SAPCPIC sperren, hängt der Funktionsverlust vom Release ab - siehe OSS-Hinweis 29276.
Schutzmaßnahmen für EARLYWATCH					
		Existiert der Benutzer EARLYWATCH nur in Mandant 066? Ist EARLYWATCH gesperrt und wird er nur bei Bedarf entsperrt?			
Schutzmaßnahmen für den Benutzer für R/3-Online-Services					
		Wenn Sie R/3-Online-Services verwenden: • Haben Sie ein Verfahren für die Aktivierung des Benutzers für R/3-Online-Services?		Kapitel 2-10 im Abschnitt <i>Schutz von R/3-Online-Services</i> OSS-Hinweis 46902	

Checkliste 2-1: Benutzerauthentifizierung (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-1)	Ergebnis / Anmerkungen
Schutzmaßnahmen gegen unberechtigte Anmeldungen					
		Überwachen Sie regelmäßig (täglich) erfolglose Anmeldeversuche?	Report RSUSR006		Report RSUSR006 zeigt alle erfolglosen Anmeldeversuche eines Benutzers und alle Benutzersperrungen an.
		Verwenden Sie das Security-Audit-Log, um Anmeldeversuche aufzuzeichnen und zu analysieren?	Transaktionen SM18, SM19 und SM20	Kapitel 2-9	Das Security-Audit-Log ist ab Release 4.0 verfügbar.
		Haben Sie den Abbruch der Sitzung nach einer bestimmten Anzahl erfolgloser Anmeldeversuche eingestellt?	Setzen Sie den Profilparameter login/fails_to_session_end	Tabelle 2-1-4	Vorschlagswert = 3
		Haben Sie die automatische Abmeldung von inaktiven Benutzern aktiviert?	Setzen Sie den Profilparameter rdisp/gui_auto_logout.	Tabelle 2-1-4	Vorschlagswert = 0 (aus)
		Werden Benutzer nach einer bestimmten Anzahl erfolgreicher Anmeldeversuche gesperrt? Ist der Vorschlagswert (12) geeignet oder haben Sie den Wert geändert?	Setzen Sie den Profilparameter login/fails_to_user_lock	Tabelle 2-1-4	Vorschlagswert = 12
		Hebt Ihr R/3-System Benutzersperrungen automatisch am selben Tag um Mitternacht auf?	Setzen Sie den Profilparameter login/failed_user_auto_unlock.	Tabelle 2-1-4	Vorschlagswert = 1 (ja)
		Überprüfen Sie das System regelmäßig auf gesperrte Benutzer?			
		Verwenden Ihre Endbenutzer Bildschirmschoner mit Kennwörtern?			
		Verwenden Sie das SAP Logon Pad anstelle des SAP Logon?			Das SAP Logon Pad verhindert Änderungen an der SAP-Anmeldekonfiguration.
		Möchten Sie weitere Anmeldeprüfungen durchführen?	Definieren Sie Ihre eigenen Anmeldeprüfungen im Customer-Exit SUSR001	OSS-Hinweis 37724	

Checkliste 2-1: Benutzerauthentifizierung (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-1)	Ergebnis / Anmerkungen
<i>Schutzmaßnahmen bei der Verwendung des Session Managers</i>					
		Verwenden Sie den Session Manager unter Windows NT oder Windows 95 mit einem der Releases 3.0E - 3.1G? Wenn ja, haben Sie die <code>slg_dll.dll</code> ausgetauscht?		OSS-Hinweis 80723	
<i>Schutzmaßnahmen für die Verwendung von SAP-Verknüpfungen</i>					
		Sind Ihre Frontends vor unberechtigten Zugriffen geschützt?	abhängig von Ihrer Infrastruktur und Ihrem Betriebssystem		

Checkliste 2-2: R/3-Berechtigungskonzept

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-2)	Ergebnis / Anmerkungen
<i>Pflege von Berechtigungen und Profilen mit dem Profilgenerator</i>					
		Haben Sie Stellenbeschreibungen in der Stellenbeschreibungsmatrix Ihres Unternehmens definiert? Haben Sie für jede Stellenbeschreibung die Menüpfade und Transaktionen angegeben, auf die die Stelleninhaber zugreifen müssen?	Firmenpolitik	<i>Authorizations Made Easy Guide, IMG oder ASAP</i>	Die technische Beratung zum Thema Sicherheit bietet einen Workshop für das R/3-Berechtigungskonzept an.
		Haben Sie Vorgehensweisen für das Anlegen und die Pflege der Aktivitätslisten, Profile und Benutzerstammsätze definiert?	Transaktion PFCG	<i>Authorizations Made Easy Guide, IMG oder ASAP</i>	
<i>Manuelle Pflege von Berechtigungen und Profilen</i>					
		Haben Sie (wie bei der Pflege mit dem Profilgenerator) Stellenbeschreibungen in der Stellenbeschreibungsmatrix Ihres Unternehmens definiert?	Firmenpolitik		
		Haben Sie die Aktivitäten festgelegt, die alle Stellenbeschreibungen durchführen dürfen, und die entsprechenden Berechtigungen definiert?	Firmenpolitik		
		Gibt es einen Standardprozeß für das Anlegen und die Zuordnung von Profilen und Berechtigungen?	Firmenpolitik		
<i>Das Infosystem Berechtigungen</i>					
		Prüfen Sie Ihren Berechtigungsplan mit dem Infosystem Berechtigungen? Prüfen Sie Ihren Berechtigungsplan regelmäßig?	Infosystem Berechtigungen (Transaktion SUIM)		

Checkliste 2-2: R/3-Berechtigungskonzept (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-2)	Ergebnis / Anmerkungen
Das Infosystem Berechtigungen (Fortsetzung)					
		Welche Berechtigungen erachten Sie als kritisch? Welche Profile enthalten diese Berechtigungen? Welche Benutzer haben diese Profile oder Berechtigungen?	Infosystem Berechtigungen (Transaktion SUIM)		<p><u>Beispiele:</u></p> <p>Um herauszufinden, welche Profile bestimmte Berechtigungen enthalten, siehe <i>Profile</i> → <i>Profile nach komplexen Selektionskriterien</i> → <i>nach enthaltenen Berechtigungen</i>.</p> <p>Um herauszufinden, welche Benutzer ein bestimmtes Profil in ihrem Benutzerstammsatz haben, siehe <i>Verwendungsnachweis</i> → <i>Verwendungsnachweise</i> → <i>für Profile</i>.</p>
		Welche anderen Informationen erachten Sie als wichtig? Welche Listen generieren Sie, um diese Informationen zu erhalten?	Transaktion SUIM		<p>Sie können z. B. die folgenden Listen generieren:</p> <ul style="list-style-type: none"> • Profilvergleiche • Transaktionen, die ein bestimmter Benutzer ausführen kann • Änderungen im Berechtigungsprofil eines Benutzers

Checkliste 2-2: R/3-Berechtigungskonzept (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-2)	Ergebnis / Anmerkungen
Organisation von Verwaltungsaufgaben					
		Haben Sie die Benutzerverwaltungsaufgaben auf mehrere Gruppen aufgeteilt, so daß die Aufgaben von verschiedenen Verwaltern durchgeführt und geprüft werden? (Vier-Augen-Prinzip)			Wenn Sie in einer zentralen Umgebung arbeiten, ist es eventuell angebracht, daß ein einziger Super-User alle Aufgaben der Benutzer- und Berechtigungspflege durchführt. In einer dezentralen Umgebung empfiehlt SAP Ihnen die Aufteilung der Aufgaben auf mehrere Verwalter.
		Gehören Ihre Verwalter zur Gruppe SUPER?			Nur ein Verwalter mit dem Profil S_A.SYSTEM kann Benutzer ändern, die zur Gruppe SUPER gehören.
		Welche Aufgaben dürfen die Verwalter durchführen und welche nicht? Welche Berechtigungen oder Profile haben die Verwalter bzw. zu welcher Aktivitätsgruppe gehören sie?		Tabellen 2-2-1 und 2-2-2	
Berechtigungsprüfungen					
		Integrieren Sie Berechtigungsprüfungen in Ihre eigenen Entwicklungen?	Transaktion SE93 AUTHORITY-CHECK auf Programmebene	OSS-Hinweis 67766 (für Informationen zu S_TCODE)	Beim Transaktionsstart über das Menü oder die Befehlszeile wird in R/3 automatisch eine Berechtigungsprüfung zu dem Objekt S_TCODE durchgeführt (ab Release 3.0E).
		Weisen Sie Reports Reportklassen zu?	Report RSCSAUTH	OSS-Hinweis 7642 Report-dokumentation zu RSCSAUTH	

Checkliste 2-2: R/3-Berechtigungskonzept (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-2)	Ergebnis / Anmerkungen
Berechtigungsprüfungen (Fortsetzung)					
		Weisen Sie Berechtigungsgruppen Tabellen zu?	Weisen Sie eine Berechtigungsgruppe Tabellen in der Tabelle TDDAT zu.		SAP liefert eine Anzahl Tabellen mit vordefinierten Berechtigungsgruppen aus.
Verringerung des Umfangs der Berechtigungsprüfungen in R/3					
		Ist es notwendig, den Umfang der Berechtigungsprüfungen zu reduzieren? Haben Sie die damit verbundenen Sicherheitsaspekte berücksichtigt?	Firmenpolitik		SAP empfiehlt Ihnen, diese Option genau zu durchdenken, bevor Sie Berechtigungsprüfungen unterdrücken.
		Wie ist der Profilparameter <code>auth/no_check_in_some_cases</code> gesetzt? Ist der Parameter auf den gewünschten Wert gesetzt? Überprüfen Sie den Wert regelmäßig um sicherzustellen, daß der Wert in der Zwischenzeit nicht geändert wurde?			
		Reduzieren Sie den Umfang der Berechtigungsprüfungen? Haben Sie ermittelt, welche Prüfungen Sie deaktivieren möchten, bevor Sie diese deaktivieren?	So reduzieren Sie den Umfang der Berechtigungsprüfungen: 1. Setzen Sie den Profilparameter <code>auth/no_check_in_some_cases</code> auf den Wert <code>Y</code> . 2. Kopieren Sie die SAP-Vorschlagswerte mit der Transaktion SU25. 3. Ändern Sie die einzelnen Werte mit der Transaktion SU24.		Verwenden Sie diese Option nur für einzelne Transaktionen. Verwenden Sie sie nicht für Massenänderungen.
		Wenn Sie den Umfang der Berechtigungsprüfungen reduzieren, überprüfen Sie regelmäßig die deaktivierten Berechtigungsprüfungen, um sicherzustellen, daß diese nicht geändert wurden?	Transaktion SU24		

Checkliste 2-3: Netzwerk-Infrastruktur

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-3)	Ergebnis / Anmerkungen
Netzwerktopologie					
		Haben Sie beim Aufbau Ihrer Netzwerktopologie Sicherheitsrisiken berücksichtigt?	Firmenpolitik		
		Wie ist Ihre Netzwerktopologie aufgebaut? Welche Subnetze und LANs haben Sie? Welche Server befinden sich in einem Subnetz oder LAN? Sind Ihre Frontend-LANs und Ihre Server-LANs getrennt? Welche Sicherheitsanforderungen stellen Sie an Ihre Subnetze oder LANs?	Firmenpolitik		Die Definition Ihrer Netzwerktopologie ist ein sehr individueller Prozeß. Wenden Sie sich an die technische Beratung zum Thema Sicherheit.
Netzwerkdienste					
Allgemeine Netzwerkdienste					
		Die folgenden Fragen beziehen sich auf allgemeine Netzwerkdienste für Windows NT und UNIX (z. B. sendmail und NFS): <ul style="list-style-type: none"> • Welche Ports sind auf Ihren Servern offen? Welche Dienste sind an diesen Ports zugelassen? • Haben Sie die Netzwerkdienste deaktiviert, die Sie nicht benötigen? 	Zeigen Sie eine Liste der 'offenen' Ports mit dem Befehl <code>netstat -a</code> an. Deaktivieren Sie in der Datei <code>services</code> nicht erforderliche Dienste.	Kapitel 2-4	Die Dienste werden auf Ports in der Datei <code>services</code> abgebildet, die unter folgenden Pfaden abgelegt sind: <ul style="list-style-type: none"> • UNIX: <code>/etc/services</code> • Windows NT: <code>/winnt/system32/drivers/etc/services</code>
		Verwenden Sie statische Kennwortdateien?			

Checkliste 2-3: Netzwerk-Infrastruktur (Fortsetzung)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-3)	Result / Comments
Netzwerkdienste (Fortsetzung)					
SAP-Netzwerkdienste					
		<p>Die folgenden Fragen beziehen sich auf SAP-spezifische Netzwerkdienste:</p> <ul style="list-style-type: none"> • Welche Ports verwenden Sie für die verschiedenen SAP-Netzwerkdienste (z. B. SAPgui, Message-Server, externe RFC-Programme und SAPIpd)? • Verwenden Sie den SAProuter? • Verwenden Sie Secure Network Communications (SNC)? • Ist die Datei <code>services</code> für Ihre SAP-spezifischen Dienste korrekt konfiguriert? 		Tabelle 2-3-1	
Router und Paketfilter					
		Verwenden Sie Router und Paketfilter? Wie sind sie konfiguriert?			
Firewall und SAProuter					
		Ist Ihr Server-LAN durch eine Firewall und einen SAProuter geschützt?			Ein SAProuter allein schützt Ihr R/3-Netzwerk nicht.
		<p>Wenn Sie den SAProuter verwenden:</p> <ul style="list-style-type: none"> • Wie ist Ihre Konfigurationsdatei (<code>saproustab</code>) konfiguriert? Erfüllt die Konfiguration Ihre Sicherheitsanforderungen? • Protokollieren Sie die Aktivitäten? Verwenden Sie Kennwörter? 		OSS-Hinweis 30289 R/3-Online-dokumentation: <i>BC - SAProuter</i>	<p>Sie können SAProuter-Aktivitäten wie z. B. den Aufbau und Beendigung einer Verbindung protokollieren.</p> <p>Sie können Ihren SAProuter auch mit einem Kennwort schützen.</p>

Checkliste 2-3: Netzwerk-Infrastruktur (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-3)	Ergebnis / Anmerkungen
Secure Network Communications (SNC)					
		Verwenden Sie ein externes Sicherheitsprodukt und SNC, um die Verbindungen zwischen Komponenten zu schützen? Wenn ja: <ul style="list-style-type: none"> • Welche Kommunikationsverbindungen sichern Sie mit SNC? • Welche Schutzstufe ist für die verschiedenen Kommunikationsverbindungen erforderlich? • Ist Ihr System entsprechend konfiguriert, daß es diese Schutzstufen bietet? 		<i>SNC-Benutzerhandbuch</i> Dokumentation des externen Sicherheitsprodukts OSS-Hinweis 66687	

Checkliste 2-4: Schutz des Betriebssystems

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-4)	Ergebnis / Anmerkungen
R/3-Sicherheit unter UNIX					
Schutz bestimmter UNIX-Eigenschaften, -Dateien und -Services					
		Sind Ihre SUID/SGID-Programme (z. B. <code>sendmail</code>) auf dem neusten Stand? Verwenden Sie Versionen, bei denen bekannte Fehler korrigiert sind?			
		Verwenden Sie eine Schattenkennwortdatei? Hat nur der Benutzer <code>root</code> auf diese Datei Zugriff?			
		Verwenden Sie den Yellow-Pages-Service (NIS-Service)? Haben Sie Alternativen in Erwägung gezogen?			Bevor Sie NIS einsetzen, sollten Sie die Notwendigkeit dieses Services überdenken. Es gibt normalerweise Alternativen, und aus Sicherheitsgründen rät SAP Ihnen, diesen Service möglichst nicht zu verwenden.
		Verwenden Sie den Network-File-System-Service (NFS-Service)? Wenn ja: <ul style="list-style-type: none"> Haben Sie Alternativen in Erwägung gezogen? Wird NFS nur verwendet, wo dies erforderlich ist? Sind Sie sehr vorsichtig bei der Zuweisung von Schreibberechtigungen oder der Verteilung der HOME-Verzeichnisse? Zu welchen Clients lassen Sie Exporte zu? Exportieren Sie nur an eine begrenzte Anzahl "vertrauenswürdiger" Clients? 			In Bereichen, in denen NFS häufig verwendet wird (z. B. zur Einrichtung eines globalen Verzeichnisses für Anwendungsserver oder im Transport Management System), gibt es oft alternative Lösungen. SAP empfiehlt Ihnen, andere Alternativen zu erwägen, bevor Sie sich für die Verwendung dieses Services entscheiden.
		Wenn Sie diese Services verwenden, geschieht dies nur in einem sicheren LAN?			

Checkliste 2-4: Schutz des Betriebssystems (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-4)	Ergebnis / Anmerkungen
R/3-Sicherheit unter UNIX (Fortsetzung)					
Schutz bestimmter UNIX-Eigenschaften, -Dateien und -Services (Fortsetzung)					
		Haben Sie die Benutzer <code>root</code> , <code><sid>adm</code> und <code><db><sid></code> geschützt? Ist <code><db><sid></code> auf Ihren Anwendungsservern gesperrt?			Diese Benutzer sollten die einzigen Benutzer auf Ihren Anwendungsservern und Ihrer Hauptinstanz sein.
		Haben Sie die <code>.rhosts</code> -Dateien für diese und alle anderen Benutzer, die Sie als kritisch erachten, geschützt?	Leeren Sie für kritische Benutzer die <code>.rhosts</code> -Dateien und weisen Sie als Zugriffsrechte <code>000</code> zu.		
		Haben Sie die Datei <code>/etc/hosts.equiv</code> gelöscht oder ist diese leer?			
		Haben Sie Ihr System mit Patches zur Sicherheit von Ihrem Lieferanten auf dem neusten Stand gehalten?			
Einstellung von Zugriffsrechten für R/3-Verzeichnisse unter UNIX					
		Wie sind die Zugriffsrechte für R/3-Verzeichnisse und -Dateien eingestellt? Entsprechen sie Ihren Sicherheitsanforderungen?		Tabelle 2-4-1	
		Wie ist Ihr <code>UMASK</code> definiert? Entspricht es Ihren Sicherheitsanforderungen?			

Checkliste 2-4: Schutz des Betriebssystems (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-4)	Ergebnis / Anmerkungen
R/3-Sicherheit unter Windows NT					
Windows-NT-Benutzer und -Gruppen in einer R/3-Umgebung					
		Wie sind Ihre lokalen und globalen Gruppen definiert? Zu welchen Gruppen gehören Ihre Benutzer und Gruppen?		Tabelle 2-4-2	R/3-Verwalter sind z. B. im allgemeinen Mitglieder der globalen Gruppe SAP_<SID>_GlobalAdmin und der lokalen Gruppe SAP_<SID>_LocalAdmin.
		Verwenden Sie einen Domänencontroller?			SAP empfiehlt die Installation von R/3 auf einem Domänencontroller nicht!
		Haben Sie den NT-Standardbenutzer Administrator deaktiviert? Haben Sie weitere Benutzer für Verwaltungsaufgaben angelegt?			
		Haben Sie die Mitgliedschaft von SID<ADM> in den Gruppen Administrators oder Domain Administrators storniert? Ändern Sie regelmäßig sein Kennwort? Sind seine Zugriffsrechte auf R/3-instanzenspezifische Ressourcen beschränkt?			
		Haben Sie das Benutzerrecht Log on locally von SAPService<SID> storniert? Sind seine Zugriffsrechte auf R/3-instanzenspezifische Ressourcen beschränkt? Haben Sie seine Berechtigungen so eingeschränkt, daß er sich nicht interaktiv am System anmelden kann? Haben Sie die Einstellung change passwd at logon deaktiviert?			

Checkliste 2-4: Schutz des Betriebssystems (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-4)	Ergebnis / Anmerkungen
R/3-Sicherheit unter Windows NT (Fortsetzung)					
R/3 im Windows-NT-Domänenkonzept					
		Wie ist Ihr Domänenkonzept aufgebaut? Sind Ihre R/3-Ressourcen in einer anderen Domäne als Ihre Windows-NT-Ressourcen (z. B. Domäne <i>MASTER</i> für Windows-NT- und <i>SAP</i> für R/3-Ressourcen)?		<i>R/3-Installationsleitfaden für Windows NT</i>	
		Verwenden Sie das Vertraute Domänenmodell? Wenn ja: <ul style="list-style-type: none"> Haben Sie Alternativen in Erwägung gezogen? Ist die Vertrauensstellung nur in eine Richtung definiert? Vertraut nur die R/3-Domäne (<i>SAP</i>) der Windows-NT-Domäne (<i>MASTER</i>) und nicht umgekehrt? 			
Schutz von R/3-Ressourcen					
		Befinden sich alle Ihre R/3-Server in derselben Domäne?			
		Haben Sie die Mitgliedschaft von <SID>ADM in der Gruppe Administrator storniert?			
		Wie sind die Zugangskontrolllisten für R/3-Ressourcen definiert (\usr\sap\<sid>\...)?			
		Wie sind Ihre R/3-Benutzer definiert (z. B. als Domänenbenutzer und nicht als lokale Benutzer)? Wie sind Ihre globalen und lokalen Benutzergruppen definiert? Wie sind deren Zugriffsrechte definiert? Sind diese Definitionen für Ihr Sicherheitskonzept geeignet?			

Checkliste 2-4: Schutz des Betriebssystems (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-4)	Ergebnis / Anmerkungen
R/3-Sicherheit unter Windows NT (Fortsetzung)					
Schutz der R/3-Ressourcen (Fortsetzung)					
		Wer sind Ihre Systemverwalter?			Die Standardsystemverwalter sind <SID>ADM und SAPService<SID>.
		Welche Zugriffsrechte bestehen für die Datei sapntstartb.exe?			Nur Benutzer, die Mitglieder der lokalen Gruppe SAP_<SID>_LocalAdmin sind, sollten die Anwendung sservmgr.exe verwenden können, um das R/3-System zu starten und zu stoppen. Diese Berechtigung hängt von den Zugriffsrechten für die Datei sapntstartb.exe ab.
		Kann nur der Benutzer, der das R/3-System startet, auch interne Werkzeuge wie z. B. dpmon.exe oder gwmon.exe starten?			
		Arbeiten Sie mit einer Installation mit mehreren R/3-Systemen? Wenn ja: <ul style="list-style-type: none"> • Wer sind Ihre Verwalter? • Verwalten Sie die Systeme separat? • Befinden sich die Systeme auf einem Server? • Wenn ja: <ul style="list-style-type: none"> - Sind die Zugriffsrechte für den gemeinsamen Speicher korrekt eingestellt? 			SAP empfiehlt Ihnen, den lokalen Gruppen SAP_<SID>_LocalAdmin die Zugriffsrechte <i>Full Control</i> für die Datei saposcol.exe (gemeinsamer Speicher) zu geben, wenn Sie mehrere R/3-Systeme auf einem Server betreiben: Starten Sie saposcol.exe, bevor Sie R/3 starten.

Checkliste 2-4: Schutz des Betriebssystems (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-4)	Ergebnis / Anmerkungen
Logische Betriebssystemkommandos in R/3					
		Welche Betriebssystemkommandos haben Sie in R/3 definiert? Wer hat die Pflegeberechtigung für diese Kommandos?	Transaktion SM69 Berechtigungsobjekt: S_RZL_ADM mit dem Wert 01 im Feld <i>Aktivität</i> .	R/3-Online-dokumentation: <i>BC - Computing Center Management System → Externe Betriebssystemkommandos</i>	
		Wer hat die Berechtigung für die Ausführung dieser Kommandos?	Transaktion SM49 Berechtigungsobjekt: S_LOG_COM, wobei die Felder <i>Command</i> , <i>Opsystem</i> und <i>Host</i> definiert sein müssen		

Checkliste 2-5: Schutz der Zugriffe auf die Datenbank

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-5)	Ergebnis / Anmerkungen
Allgemeine Empfehlungen					
		Haben Sie das Standardkennwort für SAPR3 (<SID>OFR auf AS/400) geändert?			
		Sind die USR*-Tabellen vor Zugriffen geschützt?			
		Ist die Tabelle T000 vor Schreibzugriffen geschützt?			
		Welche sonstigen Tabellen erachten Sie als kritisch? Sind diese entsprechend geschützt? (z. B. SAPUSER, RFCDES, PA*, HCL*)			
Zugriff mit Datenbank-Werkzeugen					
		Greifen Sie nur mit R/3-Werkzeugen auf die Datenbank zu? Wenn Sie andere Werkzeuge für den Zugriff auf die Datenbank verwenden (z. B. SQL-Schnittstelle oder Open Database Connectivity): <ul style="list-style-type: none"> • Haben Sie hierfür spezifische Benutzer angelegt? • Sind deren Berechtigungen auf die erforderlichen Tabellen beschränkt? • Sind deren Berechtigungen auf die Leseberechtigung beschränkt? 			Im Hinblick auf die Sicherheit empfiehlt SAP Ihnen, nicht mit anderen Werkzeugen als R/3-Werkzeugen auf die Datenbank zuzugreifen. Wenn Sie für den Zugriff auf die Datenbank andere Werkzeuge verwenden, ist die Datenkonsistenz oder der Berechtigungsschutz nicht gewährleistet.

Checkliste 2-5: Schutz der Zugriffe auf die Datenbank (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-5)	Ergebnis / Anmerkungen
ORACLE unter UNIX					
Änderung der Kennwörter der Datenbank-Standardbenutzer (ORACLE / UNIX)					
		Haben Sie die Kennwörter der Datenbank-Standardbenutzer geändert?	UNIX-Befehl <code>passwd</code> (NV 2-5-1) <code>svrmgrl</code> oder <code>sqldba</code> <code>chdbpass</code> (NV 2-5-2) OPSS-Mechanismus	Tabelle 2-5-1	
		Ändern Sie das Kennwort des Benutzers <code><sid>adm</code> regelmäßig?			
		Ist die Datei <code>chdbpass</code> vor unberechtigten Zugriffen geschützt?			
Schutz der SAPDBA-Operationen (ORACLE / UNIX)					
		Möchten Sie für SAPDBA-Operationen den Expertenmodus verwenden? Wenn ja: <ul style="list-style-type: none"> Ist die Kennwortdatei <code>passwd.dba</code> vor unberechtigten Zugriffen geschützt? 			
Vergabe von Berechtigungen für datenbankbezogene Dateien und Verzeichnisse (ORACLE / UNIX)					
		Wie sind die Berechtigungen für ORACLE-Verzeichnisse und -Dateien eingestellt? Entsprechen sie Ihren Sicherheitsanforderungen?	UNIX-Befehl <code>chmod</code> (NV 2-5-3)	Tabelle 2-5-2	

Checkliste 2-5: Schutz der Zugriffe auf die Datenbank (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-5)	Ergebnis / Anmerkungen
ORACLE unter UNIX (Fortsetzung)					
Vergabe von Berechtigungen für SAPDBA-Werkzeuge (ORACLE / UNIX)					
		Für ORACLE-Versionen < 7.3: <ul style="list-style-type: none"> • Gehört <sid>adm zur UNIX-Gruppe dba? Für ORACLE-Versionen >= 7.3: <ul style="list-style-type: none"> • Gehört <sid>adm zur UNIX-Gruppe oper? 			
ORACLE unter Windows NT					
Änderung der Kennwörter der Datenbank-Standardbenutzer (ORACLE / Windows NT)					
		Haben Sie die Kennwörter der Datenbank-Standardbenutzer geändert?	SVRMGR30, SVRMGR23, SQLDBA72 OPSS-Mechanismus (NV 2-5-7)	Tabelle 2-5-3	
		Für welche Benutzer haben Sie OPSS-Benutzer zugeordnet? Ist deren Anzahl begrenzt?	NV 2-5-4, NV 2-5-5 und NV 2-5-6	OSS-Hinweis 50088 OSS-Hinweis 48736	
Vergabe von Berechtigungen für datenbankbezogene Dateien und Verzeichnisse (ORACLE / Windows NT)					
		Wer hat Zugriff auf die ORACLE-Dateien und Verzeichnisse?		Tabelle 2-5-4	SAP empfiehlt Ihnen, nur den Gruppen SAP_<SID>_LocalAdmin und SYSTEM die Berechtigung <i>Full Control</i> zu geben.

Checkliste 2-5: Schutz der Zugriffe auf die Datenbank (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-5)	Ergebnis / Anmerkungen
ORACLE unter Windows NT (Fortsetzung)					
Vergabe von Berechtigungen für SAPDBA-Werkzeuge (ORACLE / Windows NT)					
		Für ORACLE-Versionen < 7.3: <ul style="list-style-type: none"> Gehört <SID>ADM zu der lokalen Gruppe ORA_<SID>_DBA? Für ORACLE-Versionen >= 7.3: <ul style="list-style-type: none"> Gehört <SID>ADM zur lokalen Gruppe ORA_<SID>_OPER? 			
INFORMIX unter UNIX					
Änderung der Kennwörter der Datenbank-Standardbenutzer (INFORMIX / UNIX)					
		Haben Sie die Kennwörter der Datenbank-Standardbenutzer geändert?	UNIX-Befehl <code>passwd</code> (NV 2-5-8)	Tabelle 2-5-5	
		Haben Sie einen Upgrade von einem älteren Release als 2.1J/2.2D durchgeführt? Wenn ja: <ul style="list-style-type: none"> Haben Sie die Umgebungsvariable <code>INFORMIX_DB_PASSWD</code> und alle Verweise auf diese aus den Konfigurationsdateien der Benutzer <code><sid>adm</code> und <code>informix</code> gelöscht? 			
Vergabe von Berechtigungen für datenbankbezogene Dateien und Verzeichnisse (INFORMIX / UNIX)					
		Wie sind die Berechtigungen für INFORMIX-Verzeichnisse und -Dateien eingestellt? Entsprechen sie Ihren Sicherheitsanforderungen?	UNIX-Befehl <code>chmod</code> (NV 2-5-9)	Tabelle 2-5-6	

Checkliste 2-5: Schutz der Zugriffe auf die Datenbank (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-5)	Ergebnis / Anmerkungen
ADABAS					
Änderung der Kennwörter der Datenbank-Standardbenutzer (ADABAS / UNIX und NT)					
		Haben Sie die Kennwörter der Datenbank-Standardbenutzer geändert? Haben Sie die Tabelle <code>SAPUSER</code> aktualisiert?	CONTROL, XSQL oder XQUERY (NV 2-5-10 - NV 2-5-14)	Tabelle 2-5-7	
Schutz der CONTROL-Operationen (ADABAS / UNIX und NT)					
		Wer sind die CONTROL-Benutzer und wer die OPERATOR-Benutzer? Welche Aufgaben führen sie durch?			
Spezifische Maßnahmen für ADABAS unter UNIX (ADABAS / UNIX)					
		Haben Sie die Kennwörter der Betriebssystembenutzer geändert?	UNIX-Befehl <code>passwd</code> (NV 2-5-15)	Tabelle 2-5-8	
		Wie sind die Berechtigungen für ADABAS-Verzeichnisse und -Dateien eingestellt? Entsprechen sie Ihren Sicherheitsanforderungen?	UNIX-Befehl <code>chmod</code> (NV 2-5-16)	Tabelle 2-5-9	
Spezifische Maßnahmen für ADABAS unter Windows NT (ADABAS / Windows NT)					
		Haben Sie das Kennwort des Benutzers <code><SID>ADM</code> geändert?			
		Wie sind die Berechtigungen für das Verzeichnis <code>%DBROOT%\config</code> eingestellt?			SAP empfiehlt Ihnen, nur der Gruppe Administrators die Berechtigung <i>Full Control</i> zu geben. Andere Gruppen sollten keine Berechtigung haben.
		Möchten Sie den Zugriff auf die Datenbank mit anderen Datenbank-Werkzeugen ausschließen? Wenn ja, sind die Berechtigungen für das Verzeichnis <code>%DBROOT%</code> richtig eingestellt?			SAP empfiehlt Ihnen, nur der Gruppe Administrators die Berechtigung <i>Full Control</i> zu geben. Andere Gruppen sollten keine Berechtigung haben.

Checkliste 2-5: Schutz der Zugriffe auf die Datenbank (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-5)	Ergebnis / Anmerkungen
DB2 common server unter UNIX (ab Release 4.0B)					
Änderung der Kennwörter der Datenbank-Standardbenutzer (DB2/CS / UNIX)					
		Haben Sie die Kennwörter der Datenbank-Standardbenutzer geändert?	UNIX-Befehl <code>passwd</code> (NV 2-5-17) DB2 Control Center	Tabelle 2-5-10 R/3-Online- dokumentation: <i>BC SAP Database Administration: DB2 common server</i>	
		Ändern Sie gelegentlich den Wert der Umgebungsvariablen <code>DB2DB6EKEY</code> (oder je nach Release <code>DB6EKEY</code>)?			Wenn Sie den Wert von <code>DB2DB6EKEY</code> ändern, müssen Sie ihn in allen <code>.dbenv_<Hostname>.csh</code> - und <code>.dbenv_<Hostname>.sh</code> -Profilen auf allen Hosts ändern. Nachdem Sie den Wert geändert haben, müssen Sie auch die Kennwörter von <code><sid>adm</code> und <code>sapr3</code> ändern.
Vergabe von Berechtigungen für datenbankbezogene Dateien und Verzeichnisse (DB2/CS / UNIX)					
		Wie sind die Berechtigungen für DB2/CS-Verzeichnisse und -Dateien eingestellt? Entsprechen sie Ihren Sicherheitsanforderungen?	UNIX-Befehl <code>chmod</code> (NV 2-5-18)	Tabelle 2-5-11	

Checkliste 2-5: Schutz der Zugriffe auf die Datenbank (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-5)	Ergebnis / Anmerkungen
DB2 common server unter Windows NT					
Vergabe von Benutzern und Gruppen (DB2/CS / Windows NT)					
		Entspricht die Vergabe von Benutzern und Gruppen SAPs Standardvorschlägen? Entspricht sie Ihren Sicherheitsanforderungen? Arbeiten Sie mit einem Domänencontroller? Stimmt Ihre Vergabe von Benutzern und Gruppen entsprechend überein?		Tabelle 2-5-12 Tabelle 2-5-13	
Verwaltung der Kennwörter der Datenbank-Standardbenutzer (DB2/CS / Windows NT)					
		Ändern Sie regelmäßig die Kennwörter der Benutzer <sid>adm und sapsr3? Verwenden Sie hierfür das DB2 Control Center?	DB2 Control Center	R/3-Online-dokumentation: <i>BC SAP Database Administration: DB2 common server</i>	Nur durch die Verwendung des DB2 Control Center wird die Konsistenz gewährleistet. SAP empfiehlt Ihnen, die Kennwörter nicht auf Betriebssystemebene zu ändern.
Zuordnung von Umgebungsvariablen (DB2/CS / Windows NT)					
		Ändern Sie den Wert der Umgebungsvariablen DB2DB6EKEY? Wer darf den Wert dieser Variablen ändern?	NV 2-5-20	Tabelle 2-5-15	
Vergabe von Berechtigungen für datenbankbezogene Dateien und Verzeichnisse (DB2/CS / Windows NT)					
		Wer hat Zugriff auf die DB2/CS-Dateien und -Verzeichnisse?		Tabelle 2-5-16	

Checkliste 2-5: Schutz der Zugriffe auf die Datenbank (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-5)	Ergebnis / Anmerkungen
DB2/400					
Allgemeine Beschreibung des DB2/400-Sicherheitskonzepts (DB2/400)					
		Sind Sie mit dem DB2/400-Sicherheitskonzept vertraut?			
		Auf welcher Sicherheitsstufe arbeiten Sie?	Ändern Sie die Sicherheitsstufe mit dem Befehl <code>WRKSYSVAL</code> .		SAP empfiehlt Ihnen, für den Betrieb von R/3 die Sicherheitsstufe 40 zu verwenden. Vorschlagswert = 40 ab V4R2; für ältere Releases war der Vorschlagswert 30.
Änderung der Kennwörter der Datenbank-Standardbenutzer (DB2/400)					
		Haben Sie die Kennwörter der Datenbank-Standardbenutzer geändert?	CHGPWD, CHGUSRPRF (NV 2-5-21)	Tabelle 2-5-17	Wenn Sie verteilte Verzeichnisse auf mehreren AS/400-Systemen über <code>/QFileSvr.400</code> verwenden, müssen Sie auf allen AS/400-Systemen für alle Benutzer (<code><SID>OPR</code> , <code><SID>OFR</code> und <code>SAP<nn></code>) dieselben Kennwörter verwenden.

Checkliste 2-6: Schutz des Produktivsystems (Change & Transport System)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-6)	Ergebnis / Anmerkungen
Die R/3-Systemlandschaft					
		Haben Sie Ihre Entwicklungs-, Qualitätssicherungs- und Produktivsysteme voneinander getrennt?			
		Führen Sie Ihre Änderungen (einschließlich Customizing) nur im Entwicklungssystem durch?			
		Haben Sie Abläufe für Änderungen und deren Transport in das Produktivsystem definiert?			
		Verwenden Sie für den Transport von Änderungen ein gemeinsames Transportverzeichnis? Wenn ja: <ul style="list-style-type: none"> Befinden sich alle Systeme, die das gemeinsame Transportverzeichnis verwenden, in einem sicheren LAN? 		Kapitel 2-3	
		Haben Sie mehrere R/3-Systeme? Wenn ja: <ul style="list-style-type: none"> Sind sie in logisch differenzierte Systemlandschaften getrennt? 			Durch die Trennung der verschiedenen R/3-Systeme in logisch differenzierte Systemlandschaften, jede mit ihrem eigenen gemeinsamen Transportverzeichnis, können Sie verhindern, daß sich Änderungen in einem System auf ein anderes System (zufällig oder absichtlich) auswirken. Wie Sie festlegen, welche Systeme zu welchen Landschaften gehören, hängt jedoch von Ihren eigenen Prioritäten und Ihrer Infrastruktur ab.
		Wer darf Imports in die verschiedenen Systeme durchführen?			

Checkliste 2-6: Schutz des Produktivsystems (Change & Transport System)

Checkliste 2-6: Schutz des Produktivsystems (Change & Transport System) (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-6)	Ergebnis / Anmerkungen
Die R/3-Systemlandschaft (Fortsetzung)					
		Archivieren Sie die Transportinformationen?		OSS-Hinweis 41731 oder 41732	
		Verwenden Sie das Transport Management System (TMS)? Wenn ja: <ul style="list-style-type: none"> • Wer darf Importe starten? Sind die Berechtigungen korrekt zugeordnet? (Systemverwaltungsberechtigungen) • Verwenden Sie für das Produktivsystem ein separates Verzeichnis? Wenn ja, transportieren Sie Hot Packages in beide Verzeichnisse? 	Transaktion STMS	R/3-Online- dokumentation: <i>BC - Transport Management System</i>	TMS ist ab Release 3.1H verfügbar.
Einstellen der Systemänderbarkeit					
		In welchen Systemen sind Änderungen erforderlich? Für welche Objekte? Sind Ihre Systeme für Änderungen korrekt konfiguriert?	Transaktionen SE03 und SE06		
Definition des Transportprozesses					
		Wie ist Ihr Transportweg definiert? Wie ist Ihr Transportprozeß definiert?	Verwenden Sie die Transaktion SE06 oder TMS (ab 3.1H). Sie müssen den Transportweg auch auf Betriebssystemebene in die Datei TPPARAM eingeben.		

Checkliste 2-6: Schutz des Produktivsystems (Change & Transport System) (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-6)	Ergebnis / Anmerkungen
Zuständigkeiten und die entsprechenden Berechtigungen in R/3					
		Welche Zuständigkeiten haben Sie für den Änderungs- und Transportprozeß definiert? Wer kann welche Aufgaben durchführen? Sind die entsprechenden Berechtigungen vergeben?		Tabelle 2-6-1	
Notänderungen im Produktivsystem					
		Vermeiden Sie Änderungen in Ihrem Produktivsystem?			
		Haben Sie sichergestellt, daß Benutzer im Produktivsystem keine Transportberechtigungen, Programmierberechtigungen oder Debugging-Berechtigung mit Ersetzen haben?		Tabelle 2-6-2 OSS-Hinweis 52937 OSS-Hinweis 65968	
		Haben Sie eine Vorgehensweise für Notänderungen in Ihrem Produktivsystem definiert? Gewährleistet diese Vorgehensweise, daß alle Änderungen überwacht und von einer anderen Person überprüft werden? (Vier-Augen-Prinzip)			

Checkliste 2-7 : Remote Communications (RFC & CPI-C)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-7)	Ergebnis / Anmerkungen
Allgemeine Sicherheitsmaßnahmen					
		Für welche Systeme lassen Sie RFC-Verbindungen zu? Sind diese Systeme durch entsprechende Netzwerkmaßnahmen (SAProuter und Paketfilter) gesichert?		Kapitel 2-3	
		Sehen Sie in Ihren Funktionsbausteinen, die über RFC aufgerufen werden können, Berechtigungsprüfungen vor?			
		Wer ist für die Pflege von RFC-Destinationen berechtigt (Transaktion SM59)? Haben Sie diese Berechtigungen an so wenige Benutzer wie möglich vergeben?	Die erforderlichen Berechtigungsobjekte sind <ul style="list-style-type: none"> • S_ADMI_FCD mit dem Wert NADM • S_TCODE mit dem Wert SM59 		
		Verwenden Sie RFC-Destinationen mit vollständigen Anmeldeinformationen? Wenn ja: <ul style="list-style-type: none"> • Speichern Sie nur Anmeldeinformationen für Nicht-Dialogbenutzer? • Sind deren Berechtigungen in den Zielsystemen eingeschränkt? 	Überprüfen Sie RFC-Destinationen mit dem Programm RSRFCCHK.		In dieser Tabelle sollten Sie nur Daten von Nicht-Dialogbenutzern speichern. R/3 erfragt beim Aufbau der Verbindung die Anmeldeinformationen von Dialogbenutzern.
		Nur für die Releases 3.0C/D: <ul style="list-style-type: none"> • Haben Sie den OSS-Hinweis 43417 gelesen und die erforderlichen Maßnahmen ergriffen? 		OSS-Hinweis 43417	

Checkliste 2-7 : Remote Communications (RFC & CPI-C) (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-7)	Ergebnis / Anmerkungen
Allgemeine Sicherheitsmaßnahmen (Fortsetzung)					
		Verwenden Sie das RFC Software Development Kit? Sind Sie sicher, daß es nicht in Ihrem Produktivsystem installiert ist?			
		Sind externe Serverprogramme in der Datei <code>secinfo</code> definiert?	Überprüfen Sie Ihre Gateways mit dem Programm RSGWLST.		
		Haben Sie die entfernte Überwachung Ihres SAP-Gateways deaktiviert?	Setzen Sie den Profilparameter <code>gw/monitor to 1</code> .	OSS-Hinweis 64016	
RFC-Berechtigungen					
		Gehen Sie bei der Vergabe von RFC-Berechtigungen vorsichtig vor? Führen Sie bei der Vergabe von RFC-Berechtigungen einen Trace durch, um herauszufinden, welche Funktionsgruppen für die Durchführung einer Aktion erforderlich sind? Vergeben Sie nur die Funktionsgruppen, die in der Berechtigung des Benutzers erforderlich sind?	Das für die Verwendung von RFC erforderliche Berechtigungsobjekt ist <code>S_RFC</code> . NV 2-10-1 beschreibt, wie Sie den Trace durchführen.		NV 2-10-1 in <i>BAND II</i> beschreibt, wie Sie einen Trace für ALE-Anwendungen durchführen. Sie können diese Vorgehensweise auch für andere RFC-Anwendungen verwenden.
Vertrauensbeziehungen zwischen R/3-Systemen (RFC)					
		Verwenden Sie ein Szenario aus sich vertrauenden Systemen? Wenn ja: <ul style="list-style-type: none"> Haben die Systeme in dem Szenario dieselben Anforderungen bezüglich der Sicherheitsstufe? Sind die Benutzerverwaltung und das Berechtigungskonzept für alle Systeme in dem Szenario aus sich vertrauenden Systemen identisch? 			Ein Szenario aus sich vertrauenden Systemen bildet ein 'virtuelles' R/3-System. Deswegen sollten alle Sicherheitsanforderungen, die Benutzerverwaltung und das Berechtigungskonzept für alle Systeme in dem Szenario aus sich vertrauenden Systemen identisch sein.

Checkliste 2-7 : Remote Communications (RFC & CPI-C) (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-7)	Ergebnis / Anmerkungen
Berechtigungen für externe Serverprogramme (RFC & CPI-C)					
		Welche externen Serverprogramme dürfen über das Gateway gestartet werden? Welche dürfen sich am Gateway registrieren? Haben Sie sie in die Datei <code>secinfo</code> eingetragen? Pflegen Sie diese Datei regelmäßig?	Überprüfen Sie Ihre Gateways mit dem Programm <code>RSGWLST</code> .	R/3-Online-dokumentation: <i>BC - SAP-Kommunikation: Konfiguration</i> → <i>SAP-Gateway</i>	Der Pfad und der Dateiname dieser Datei ist im Profilparameter <code>gw/sec_info</code> definiert. Der Standardpfad und -dateiname in diesem Parameter ist <code>/usr/sap/<SID>/<Instanz>/data/secinfo.</code>
		Lassen Sie die Ausführung externer Betriebssystemkommandos oder externer Programme in der Hintergrundverarbeitung über das Gateway zu?	Tragen Sie das Programm <code>sapxpg</code> in der Datei <code>secinfo</code> ein.		
Secure Network Communications für Remote Communications (RFC & CPI-C)					
		Verwenden Sie Secure Network Communications (SNC) und ein externes Sicherheitsprodukt? Wenn ja: <ul style="list-style-type: none">Sichern Sie auch RFC und CPI-C-Verbindungen mit SNC? Ist Ihr System korrekt konfiguriert?		Kapitel 2-3 <i>SNC-Benutzerhandbuch</i>	Verfügbar für RFC und CPI-C ab Release 4.0

Checkliste 2-8 : Secure-Store-&-Forward-Mechanismen (SSF) und digitale Signaturen

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-8)	Ergebnis / Anmerkungen
		Gibt es Gesetze oder Bestimmungen für den Anwendungsbereich, für den Sie digitale Signaturen verwenden möchten? Wenn ja, welche? Halten Sie sich an diese?			
		Verwenden Sie ein externes Sicherheitsprodukt für Secure-Store-&-Forward-Mechanismen (SSF) in R/3?		OSS-Hinweis 86927 OSS-Hinweis 66687	SSF ist ab Release 4.0 verfügbar. Wenn Sie die SSF-Mechanismen verwenden, gelten für Sie die folgenden Abschnitte <i>Schutz von privaten Schlüsseln</i> und <i>Schutz von öffentlichen Schlüsseln</i> .
Schutz von privaten Schlüsseln					
Hardwarelösungen					
		Verwenden Sie für die Authentifizierung Smartcards? Hat jeder Benutzer seine eigene Smartcard?			Benutzer sollten keine gemeinsamen Smartcards benutzen.
Softwarelösungen					
		Verwenden Sie eine Softwarelösung? Ist die Datei oder das Verzeichnis, in dem die Benutzer- und Schlüsselinformationen abgelegt sind, vor unberechtigten Zugriffen geschützt?			
Schutz von öffentlichen Schlüsseln					
		Verwenden Sie (oder das Sicherheitsprodukt) für die Speicherung von öffentlichen Schlüsseln ein Adreßbuch? Wenn ja: <ul style="list-style-type: none"> Ist das Adreßbuch vor unberechtigten Zugriffen geschützt? 			

Checkliste 2-8 : Secure-Store-&-Forward-Mechanismen (SSF) und digitale Signaturen

Checkliste 2-8 : Secure-Store-&-Forward-Mechanismen (SSF) und digitale Signature (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-8)	Ergebnis / Anmerkungen
SAP Security Library (SAPSECULIB)					
Schutz der privaten Schlüssel der R/3-Anwendungsserver					
		Ist die Datei <code>SAPSECU.pse</code> vor unberechtigten Zugriffen geschützt?		OSS-Hinweis 110600	Die Datei <code>SAPSECU.pse</code> ist im Unterverzeichnis <code>sec</code> des im Profilparameter <code>DIR_INSTANCE</code> angegebenen Verzeichnisses abgelegt. Normalerweise darf nur der Benutzer <code><sid>adm</code> auf diese Datei zugreifen.
		Haben Sie den Verdacht, daß diese Datei mißbraucht wurde?	Generieren Sie das Schlüsselpaar des Anwendungsservers wie folgt neu: 1. Löschen Sie die Dateien im Verzeichnis <code>sec</code> . 2. Starten Sie den Anwendungsserver erneut.		
		Mußten Sie den öffentlichen Schlüssel des R/3-Anwendungsserver mit der obigen Vorgehensweise ersetzen? Gibt es Anwendungen, die für die Authentifizierung den alten Schlüssel verwenden?	Machen Sie den Schlüssel den Anwendungen, die ihn benötigen, bekannt.		
		Verwenden Sie in R/3 keine digitalen Signaturen? Möchten Sie <code>SEPSECULIB</code> deaktivieren?	Ersetzen Sie die Datei <code>SAPSECU.pse</code> durch eine beliebige Datei und starten Sie den Anwendungsserver erneut.		Dies ist nur möglich, wenn Sie keine Anwendungen verwenden, die den öffentlichen Schlüsseln des Anwendungsservers benötigen.

Checkliste 2-8 : Secure-Store-&-Forward-Mechanismen (SSF) und digitale Signature (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-8)	Ergebnis / Anmerkungen
SAP Security Library (SAPSECULIB) (Fortsetzung)					
Schutz der öffentlichen Schlüssel der R/3-Anwendungsserver					
		Verwenden Sie selbst signierte oder von der CA signierte Zertifikate?			Wenn Sie kein externes Sicherheitsprodukt verwenden, signiert der R/3-Anwendungsserver sein eigenes Zertifikat.

Checkliste 2-9: Protokollierung und Prüfung

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-9)	Ergebnis / Anmerkungen
Audit-Informationssystem (AIS)					
		Überprüfen und überwachen Sie die Sicherheit Ihres R/3-Systems regelmäßig mit dem Audit-Informationssystem (AIS)?	Transaktion SECR	OSS-Hinweis77503 OSS-Hinweis 100609	Informationen zur Verfügbarkeit des AIS finden Sie in diesen OSS-Hinweisen.
Security-Audit-Log					
		Überwachen Sie sicherheitsrelevante Ereignisse in Ihrem R/3-System mit dem Security-Audit-Log? Wenn ja: <ul style="list-style-type: none"> Überwachen Sie diese regelmäßig? 	Aktivieren Sie das Security-Audit-Log mit der Transaktion SM19 und definieren Sie Selektionskriterien. Analysieren Sie den Inhalt des Security-Audit-Logs mit der Transaktion SM20. Löschen Sie alte Protokolle mit der Transaktion SM18.	R/3-Online-dokumentation: BC - Systemdienste → Security-Audit-Log	Das Security-Audit-Log ist ab Release 4.0B verfügbar.
Systemprotokolle					
		Überprüfen Sie das Systemprotokoll regelmäßig auf fehlgeschlagene Anmeldeversuche und Benutzersperren?	Transaktion SM21	R/3-Online-dokumentation: BC - Systemdienste → Systemprotokolle	
Tagesstatistik im CCMS					
		Zeichnen Sie eine Tagesstatistik der Benutzeraktivitäten auf?	Setzen Sie den Profilparameter stat/level.		
		Überprüfen Sie nach Bedarf die Tagesstatistik?	Transaktion STAT		

Checkliste 2-9: Protokollierung und Prüfung (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-9)	Ergebnis / Anmerkungen
Protokollierung von spezifischen Aktivitäten					
Anwendungsprotokollierung					
		Aktivieren Sie die Anwendungsprotokollierung für Ihre Eigenentwicklungen?	Transaktion SGL0		
		Überprüfen Sie nach Bedarf die Anwendungsprotokolle?	Transaktion SGL1		
Protokollierung beim Ausführen des Workflow					
		Überwachen Sie Workflow-Aktivitäten mit den Analysefunktionen des SAP Business Workflow?	Transaktionen SWI2, SWI5, etc.		
Protokollierung über Änderungsbelege (Änderungen an betriebswirtschaftlichen Objekten)					
		Welche Objekte erachten Sie als kritisch oder unterliegen Revisionen? Haben Sie für diese Objekte Änderungsbelege aktiviert?	Gehen Sie wie folgt vor: <ol style="list-style-type: none"> 1. Legen Sie ein Änderungsbelegobjekt an (Transaktion SCD0). 2. Markieren Sie <i>Änderungsbeleg</i> bei den Datenelementen aller Felder, für die Sie Änderungsbelege erstellen möchten (Transaktion SE11). 3. Generieren Sie einen Verbucher für das Objekt (Transaktion SCD0). 4. Fügen Sie die entsprechenden Aufrufe des in Schritt 3 generierten Funktionsbausteins in die entsprechenden Programme ein. 		

Checkliste 2-9: Protokollierung und Prüfung (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-9)	Ergebnis / Anmerkungen
Protokollierung von spezifischen Aktivitäten (Fortsetzung)					
Protokollierung von Datenänderungen in Tabellen					
		Welche Tabellen erachten Sie als kritisch oder unterliegen Revisionen? Haben Sie die Tabellenaufzeichnung generell aktiviert? Haben Sie die Tabellenaufzeichnung für die Tabellen aktiviert, die Sie protokollieren möchten?	Gehen Sie wie folgt vor: 1. Setzen Sie den Profilparameter <i>rec/client</i> . 2. Setzen Sie das Kennzeichen <i>Datenänderungen protokollieren</i> für die Tabellen, die Sie protokollieren möchten.	OSS-Hinweis 1916 OSS-Hinweis 112388	
Protokollierung von Änderungen an Benutzerstammsätzen, Profilen und Berechtigungen					
		Überprüfen Sie regelmäßig Änderungen an Benutzerstammsätzen, Profilen und Berechtigungen?	Infosystem Berechtigungen oder Transaktion SU01		

Checkliste 2-10: Spezielle Themen

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-10)	Ergebnis / Anmerkungen
Schutz von R/3-Internet-Anwendungskomponenten (IACs)					
Architektur des ITS					
		Verwenden Sie Internet-Anwendungskomponenten?			
		Befinden sich AGate und WGate auf separaten Rechnern?			
Sichere Netzwerk-Infrastruktur für den ITS					
		Wie ist Ihre Netzwerk-Infrastruktur aufgebaut? Wo befinden sich in Ihrer Infrastruktur Paketfilter und Router?		Kapitel 2-3	
		Verwenden Sie für Ihr Internet-System ein (mit ALE repliziertes) separates System anstelle Ihres Produktivsystems?			
Konfiguration der Server- und Netzwerkkomponenten					
Schutz des Web-Servers					
		Welche Kommunikationsprotokolle benötigen Sie (z. B. HTTP, HTTPS)? Wie ist Ihr Web-Server konfiguriert? Haben Sie ihn so konfiguriert, daß nur die Kommunikationsprotokolle zugelassen sind, die Sie benötigen?		Kapitel 2-3 Kapitel 2-4	
		Ist Ihr Web-Server, auf dem sich das WGate befindet, von Ihrem firmeninternen Netzwerk abgeschottet?			

Checkliste 2-10: Spezielle Themen (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-10)	Ergebnis / Anmerkungen
Schutz von R/3-Internet-Anwendungskomponenten (IACs) (Fortsetzung)					
Konfiguration der Server- und Netzwerkkomponenten (Fortsetzung)					
Schutz des AGate-Servers					
		Wo befindet sich Ihr AGate? Ist es vor dem externen Netzwerk mit einer Firewall und einem SAProuter geschützt?		Kapitel 2-3	SAP empfiehlt Ihnen, das AGate in Ihrem firmeninternen Netzwerk zu platzieren.
		Wie sind die TCP-Ports für den ITS (<code>sapavx<xx>_<INST></code>) in der Datei <code>/etc/services</code> definiert?			
		Sind die Portzuordnungen für den WGate- und den AGate-Host identisch?			
		Steuern Sie die Verbindung zwischen dem WGate und dem AGate über den SAProuter? Wie ist Ihr SAProuter für WGate↔AGate-Verbindungen konfiguriert? Stimmen die Einträge im Windows-NT-Registry?			
		Verwenden Sie weitere Firewall-Produkte, um die TCP-Verbindung vom WGate zum AGate zuzulassen? Stimmen die Einträge im Windows-NT-Registry?			

Checkliste 2-10: Spezielle Themen (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-10)	Ergebnis / Anmerkungen
Schutz von R/3-Internet-Anwendungskomponenten (IACs) (Fortsetzung)					
Konfiguration der Server- und Netzwerkkomponenten (Fortsetzung)					
Schutz der R/3-Server					
		Bieten Sie zusätzlichen Schutz zwischen dem AGate und dem R/3-Anwendungsserver? (Befindet sich eine Firewall zwischen dem AGate und dem Anwendungsserver?)		OSS-Hinweis 104576	
Verwendung von Sicherheitsservices / Vertraulichkeit					
Zwischen dem Web-Browser und dem Web-Server					
		Bieten Sie Ihre Services externen Benutzern oder nur internen Benutzern an?			
		Verwenden Sie für die Kommunikation zwischen dem Web-Browser und dem Web-Server HTTPS und X.509-Zertifikate? Haben Sie eine Firmen-CA (Certificate Authority) eingerichtet oder verwenden Sie eine externe CA?			
		Wie ist Ihr Web-Server konfiguriert? Ist er so konfiguriert, daß er nur Verbindungsanfragen akzeptiert, die gültige Browser-Zertifikate vorlegen? Welche Browser-Zertifikate akzeptieren Sie?			
Zwischen dem WGate und dem AGate					
		Ab ITS 2.0: <ul style="list-style-type: none"> • Verwenden Sie Secure Network Communications (SNC), um die über die Verbindung zwischen dem WGate und dem AGate übertragenen Daten zu verschlüsseln? 		Kapitel 2-3	

Checkliste 2-10: Spezielle Themen (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-10)	Ergebnis / Anmerkungen
Schutz von R/3-Internet-Anwendungskomponenten (IACs) (Fortsetzung)					
Verwendung von Sicherheitsservices / Vertraulichkeit (Fortsetzung)					
Zwischen AGate und R/3					
		Ab ITS 2.2: <ul style="list-style-type: none"> • Verwenden Sie Secure Network Communications (SNC) , um die über die Verbindung zwischen dem AGate und R/3 übertragenen Daten zu verschlüsseln? 			
Authentifizierung von Benutzern					
		Haben Sie Servicebenutzer, die geschützt werden sollten? Wenn ja: <ul style="list-style-type: none"> • Ist das AGate vor unberechtigten Zugriffen geschützt? 			
Schutz der Integrität der Verbindung					
		Haben Sie eine Internet- oder Intranet-Infrastruktur? Verwenden Sie Proxies und Lastverteilung? Bis zu welchem Grad müssen Sie IP-Adressen vergleichen und verifizieren? Wie ist der folgende Registry-Schlüssel definiert? <ul style="list-style-type: none"> • HKEY_LOCAL_MACHINE\SOFTWARE\SAP\ITS\2.0\ <INST>\Connects\IPChecking 			Der Vorschlagswert ist 255.255.255.255. Er gibt an, daß die ganze IP-Adresse verglichen werden sollte. Der Wert 255.255.0.0 gibt z. B. an, daß nur die führenden Zahlen der Adresse verglichen werden sollten.
Einstellung von Sicherheitsstufen					
		Mit welcher Sicherheitsstufe betreiben Sie Ihren ITS (1,2 oder 3)?	Sie können die Sicherheitsstufe mit dem Befehlszeilenprogramm <code>itsvprotect</code> ändern.		

Checkliste 2-10: Spezielle Themen (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-10)	Ergebnis / Anmerkungen
Schutz von R/3-Internet-Anwendungskomponenten (IACs) (Fortsetzung)					
Angabe zulässiger R/3-Internetanwendungen					
		Verwenden Sie transaktionale IACs?	Definieren Sie eine Servicedatei für die Transaktion.		Sie können nur Transaktionen aufrufen, für die eine entsprechende Servicedatei existiert. Die Definition einer Servicedatei ist Teil des Prozesses der Erstellung der Transaktion.
		Wenn Sie WebRFC oder WebReporting verwenden und ein Release höher als 4.5 haben: <ul style="list-style-type: none"> Haben Sie die Reports, Berichtsbäume und Funktionsbausteine, die über das Internet aufgerufen werden können, explizit freigegeben? 	Transaktion SMW0		
		Wenn Sie WebRFC oder WebReporting verwenden und Release 3.1H haben: <ul style="list-style-type: none"> Haben Sie den verfügbaren Patch ausgeführt, mit dem Sie die Ausführung von Reports, die eine leere Berechtigungsgruppe enthalten, verhindern können? 		OSS-Hinweis 92725	
		Wenn Sie WebRFC oder WebReporting nicht verwenden: Möchten Sie die Verwendung von WebRFC deaktivieren?	Löschen Sie die Datei SAPXGWFC.d11.		
Schutz von ALE-Anwendungen					
		Verwenden Sie ALE-Anwendungen?			
		Wie sind Ihre ALE-Benutzer eingerichtet? Welche Zuständigkeiten gibt es und wer hat welche Berechtigungen?	Transaktion SALE		
		Wo sind Ihre Benutzer und Kennwörter abgelegt? Sind diese Informationen vor unberechtigten Zugriffen geschützt?	systemabhängig		ALE-Benutzer und Kennwörter sind i. a. außerhalb des R/3-Systems abgelegt.

Checkliste 2-10: Spezielle Themen (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-10)	Ergebnis / Anmerkungen
Schutz von ALE-Anwendungen (Fortsetzung)					
		Ist Ihr Verteilungsmodell vor unberechtigten Zugriffen geschützt?	Das für die Pflege des Verteilungsmodells erforderliche Berechtigungsobjekt ist B_ALE_MODL.		
		Sind die Berechtigungen im Zielsystem für ALE-Benutzer auf einem Minimum gehalten?			
		Richten Sie spezielle Benutzer für ALE ein? Haben diese nur ALE-Berechtigungen?			
		Vermeiden Sie es, anderen Benutzern ALE-Berechtigungen zu geben?			
		Sind Ihre ALE-Benutzer im Zielsystem CPIC-Benutzer?			
		Verwenden Sie die Hintergrundverarbeitung oder die Direktverarbeitung?			
		Hintergrundverarbeitung: <ul style="list-style-type: none"> • Welche Berechtigungen haben Ihre ALE-Benutzer? Vermeiden Sie es, ihnen Berechtigungen für die empfangende Anwendung zu geben? 			
		Direktverarbeitung: <ul style="list-style-type: none"> • Welche Berechtigungen haben Ihre ALE-Benutzer? Sind sie auf die erforderlichen Anwendungsberechtigungen beschränkt? 	Berechtigungstrace (NV 2-10-1)		

Checkliste 2-10: Spezielle Themen (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-10)	Ergebnis / Anmerkungen
Schutz von R/3-Online-Services					
		Kennen Sie die von SAP getroffenen Schutzmaßnahmen? Ergreifen Sie die von SAP empfohlenen Maßnahmen?		OSS-Hinweis 35010 OSS-Hinweis 46902 OSS-Hinweis 35493	
		Verwenden Sie für die Verbindung einen Hardware-Router? Beschränken Sie die Berechtigungen für den Router?			
		Verwenden Sie das Programm SAProuter? Verwenden und überprüfen Sie die SAProuter-Protokolle? Verwenden Sie Kennwörter bei der Verbindungsherstellung?			
		Verwenden Sie separate Benutzer für Online-Services? Sind sie an die Art des erforderlichen Services angepaßt? Sind sie in Testmandanten eingerichtet?			
		Überwachen Sie die erfolgten Aktivitäten und analysieren Sie diese nach einer Sitzung?	Transaktion STAT		
		Schützen Sie die Benutzerkennwörter?	Geben Sie Kennwörter auf separatem Weg (Telefon oder separate Dokumente) bekannt.		Geben Sie keine Benutzerkennwörter über die Remote-Verbindung bekannt.
		Ändern Sie das Kennwort des Benutzers <sid>adm sofort, wenn Sie einen Zugriff mit diesem Benutzer erlauben müssen?			
		Deaktivieren Sie Benutzer und Kennwörter nach Beendigung einer Sitzung?			
		Deaktivieren Sie die Remote-Verbindung und schließen Sie die OSS-Verbindungen nach Beendigung der Tätigkeit?			

Checkliste 2-10: Spezielle Themen (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-10)	Ergebnis / Anmerkungen
Schutz von R/3-Online-Services (Fortsetzung)					
		Legen Sie zeitliche Begrenzungen für OSS-Verbindungen fest?			
Virenschutz und Integritätsprüfungen					
		Verwenden Sie Virenprüfprogramme? Aktualisieren Sie diese regelmäßig? Sind Ihre Benutzer über die Gefahren durch Viren informiert? Verwenden sie ungeprüfte Software?			
Schutz spezifischer Tabellen, Berechtigungsobjekte usw.					
Berechtigung SAP_ALL					
		Haben Sie die in SAP_ALL enthaltenen Berechtigungen auf mehrere Benutzer aufgeteilt? Hat nur ein Benutzer die Berechtigung SAP_ALL? Wird das Kennwort dieses Benutzers geheimgehalten und an einem sicheren Ort aufbewahrt? Verwenden Sie diesen Benutzer nur in Notfällen?			

Checkliste 2-10: Spezielle Themen (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-10)	Ergebnis / Anmerkungen
Schutz spezifischer Tabellen, Berechtigungsobjekte usw. (Fortsetzung)					
Berechtigung SAP_NEW					
		Haben Sie eine lange Liste von SAP_NEW-Profilen?	Überdenken Sie Ihr Berechtigungskonzept und setzen Sie dieses neu fest.		
		Löschen Sie nach dem Upgrade Ihre SAP_NEW_*-Profile? Haben Sie die in den SAP_NEW_*-Profilen enthaltenen Profile verteilt? Haben Sie deren Werte gepflegt? Haben Sie die SAP_NEW_*-Profile nach der Verteilung und der Pflege gelöscht?	Gehen Sie wie folgt vor: 1. Löschen Sie die SAP_NEW_*-Profile, die Sie nicht verteilen müssen. (Die Profile sind bereits verteilt.) 2. Verteilen Sie den Rest der SAP_NEW_*-Profile und pflegen Sie deren Werte. 3. Löschen Sie das Profil SAP_NEW.		

Checkliste 2-10: Spezielle Themen (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-10)	Ergebnis / Anmerkungen
Schutz spezifischer Tabellen, Berechtigungsobjekte usw. (Fortsetzung)					
Tabelle T000					
		Haben nur Systemverwalter Pflegeberechtigungen für die Tabelle T000?	Das erforderliche Berechtigungsobjekt ist S_ADMI_FCD.		
		Haben Sie einen Prozeß für das Anlegen und Pflegen von Mandanten definiert?			
		Enthält das Berechtigungsobjekt S_TCODE die Tabellen- und Mandantenpflege transaktionen SCC4, SM30 und SM31?			
		Sind die Felder im Berechtigungsobjekt S_TABU_DIS auf die folgenden Werte gesetzt? <ul style="list-style-type: none"> • Feld: Aktivität; Werte: 02, 03 • Feld: Berechtigungsgruppe; Wert: SS 			
		Ist für das Berechtigungsobjekt S_TABU_CLI das Feld <i>Kennzeichen für mandantenunabhängige Pflege</i> auf den Wert x gesetzt?			
HR-Tabellen					
		Für die Releases 3.0A-C: <ul style="list-style-type: none"> • Haben Sie die HR-Tabellen explizit der Berechtigungsgruppe PA zugewiesen? • Haben Sie die Gruppe PA aus dem Berechtigungsobjekt S_TABU_DIS ausgeschlossen? 			

Checkliste 2-10: Spezielle Themen (Fortsetzung)

Nr.	Prio.	Sicherheitsrelevantes Thema	Methode / Vorgehensweise	Referenz (BAND II, K. 2-10)	Ergebnis / Anmerkungen
Schutz spezifischer Tabellen, Berechtigungsobjekte usw. (Fortsetzung)					
HR-Berechtigungsprofil P_BAS_ALL					
		Haben Sie allen HR-Tabellen die Klasse PC oder PS zugewiesen? Haben Sie das Feld <i>Berechtigungsgruppe</i> in P_BAS_ALL auf PC und PS beschränkt?		OSS-Hinweis 11796	
Systemprofil-Parameterdateien					
		Sind die Systemprofil-Parameterdateien <SID>_<Instanz>, START_<Instanz> und DEFAULT.PFL vor unberechtigten Zugriffen geschützt? Überprüfen Sie regelmäßig, daß die Dateien authentisch sind?			

Index

<		Windows-NT-Verwalter	2-16	Berechtigungsprüfungen	2-9
<SID>_<Instanz>	2-50	Benutzerauthentifizierung	2-2	Umfang reduzieren	2-10
A		ITS	2-43	Berechtigungstrace	2-45
ADABAS	2-24	Benutzersperren	2-5, 2-37	Betriebssystemkommandos	2-19
Adreßbuch	2-34	Benutzerstammsätze	2-7	Bildschirmschoner	2-5
AGate	2-40, 2-41, 2-42, 2-43	Beratung zum Thema Sicherheit	1-3, 1-6, 2-7	C	
AIS		Berechtigungen	2-7, 2-8	CA	
siehe	Audit-Informationssystem	ADABAS unter UNIX	2-24	siehe	Certificate Authority
Aktivitätslisten	2-7	ADABAS unter Windows NT	2-24	Certificate Authority	2-36, 2-42
ALE		ALE-Benutzer	2-45	Change and Transport System	2-28
siehe	Application Link Enabling	DB2/CS unter UNIX	2-25	chdbpass	2-21
Änderungsbelege	2-38	DB2/CS unter Windows NT	2-26	CPI-C	2-31, 2-32, 2-33
Änderungsoptionen	2-29	INFORMIX unter UNIX	2-23	Berechtigungen	2-33
Anmeldeversuch	2-37	ORACLE unter UNIX	2-21	D	
Anmeldung	2-5	ORACLE unter Windows NT	2-22	DB2 Control Center	2-25, 2-26
Anwendungsprotokollierung	2-38	R/3 unter UNIX	2-15	DB2/400	2-27
Application Link Enabling	2-44, 2-45	R/3 unter Windows NT	2-18	DB2/CS unter UNIX	2-25
Audit-Informationssystem	2-37	S_TCODE	2-31	DB2/CS unter Windows NT	2-26
auth/no_check_in_some_cases	2-10	SAP_ALL	2-47	DB2DB6EKEY	2-25, 2-26
Authentifizierung	2-2	Windows NT	2-16	DDIC	2-4
ITS	2-43	Berechtigungskonzept	2-7	DEFAULT.PFL	2-50
Automatische Abmeldung	2-5	Berechtigungsobjekte		Digitale Signatur	2-34, 2-35, 2-36
B		B_ALE_MODL	2-45	DIR_INSTANCE	2-35
Benutzer		RZL_ADM	2-19	Domänencontroller	2-16
DDIC	2-4	S_ADMI_FCD	2-31, 2-49	Domänenkonzept	2-17
EARLYWATCH	2-4	S_LOG_COM	2-19	E	
R/3-Online-Services	2-4	S_RFC	2-32	EARLYWATCH	2-4
SAP*	2-3	S_TABU_CLI	2-49	Entwicklungssystem	2-28
SAPCPIC	2-4	S_TABU_DIS	2-10, 2-49	etc/services	2-11, 2-41
		S_TCODE	2-49		
		Berechtigungsprofile			
		P_BAS_ALL	2-50		

Index

Externe Serverprogramme	2-32	ALE-Benutzer	2-44	Ö	
F		DB2/400	2-27	Öffentlicher Schlüssel	2-34, 2-36
Feedback	1-6	DB2/CS unter UNIX	2-25	OPSS-Mechanismus	
Firewall	2-12, 2-41	DB2/CS unter Windows NT	2-26	UNIX	2-21
G		INFORMIX unter UNIX	2-23	Windows NT	2-22
Gateway	2-32, 2-33	ORACLE unter UNIX	2-21	ORACLE	
Gemeinsames Transportverzeichnis	2-28	ORACLE unter Windows NT	2-22	UNIX	2-21, 2-22
gw/monitor	2-32	OSS-Service-Benutzer	2-46	Windows NT	2-22
gw/sec_info	2-33	SAPR3	2-20	P	
H		UNIX	2-14	P_BAS_ALL	2-50
HR-Tabellen	2-49	Windows NT	2-16	Paketfilter	2-12, 2-31, 2-40
HTTP/HTTPS	2-40, 2-42	Kennwortkonzept	2-2	passwd.db	2-21
I		L		Prioritäten	2-1
IAC		login/failed_user_auto_unlock	2-5	Privater Schlüssel	2-34, 2-35
siehe Internet-Anwendungskomponenten		login/fails_to_session_end	2-5	Produktivsystem	2-28
INFORMIX		login/fails_to_user_lock	2-5	Notänderungen	2-30
UNIX	2-23	login/min_password_lng	2-2	Profile	2-7
INFORMIX_DB_PASSWD	2-23	login/no_automatic_user_sap*	2-3	Profilgenerator	2-7
Infosystem	2-7, 2-8	login/no_automatic_user_sapstar	2-3	Profilparameter	
Infosystem Berechtigungen	2-7, 2-8, 2-39	login/password_expiration_time	2-2	auth/no_check_in_some_cases	2-10
Internet	2-40	N		DIR_INSTANCE	2-35
Internet Transaction Server	2-40	Network File System (NFS)	2-14	gw/monitor	2-32
Sicherheitsstufen	2-43	Netzwerk		gw/sec_info	2-33
Internet-Anwendungskomponenten	2-40, 2-41, 2-42, 2-43, 2-44	Firewall	2-12, 2-41	login/failed_user_auto_unlock	2-5
ITS		Internet	2-40	login/fails_to_session_end	2-5
siehe Internet Transaction Server		ITS	2-41	login/fails_to_user_lock	2-5
itsvprotect	2-43	Paketfilter	2-12, 2-31, 2-40	login/min_password_lng	2-2
K		Router	2-12, 2-40	login/no_automatic_user_sap*	2-3
Kennwörter	2-2, 2-12	SAProuter	2-12, 2-31, 2-41	login/no_automatic_user_sapstar	2-3
ADABAS	2-24	Netzwerkdienste	2-11, 2-12	login/password_expiration_time	2-2
		Netzwerk-Infrastruktur	2-11, 2-12, 2-13	login/password_expiration_time	2-2
		Netzwerksicherheit	2-11, 2-12, 2-13	rdisp/gui_auto_logout	2-5
		Notationen	1-4	rec/client	2-39
				stat/level	2-37
				Protokollierung	2-37, 2-38, 2-39
				Protokollierung beim Ausführen des Workflow	2-38

Protokollierung über Änderungsbelege	2-38	S		DB2/CS unter Windows NT	2-26
Protokollierung von Änderungen an Benutzerstammsätzen	2-39	SAP Business Workflow	2-38	INFORMIX unter UNIX	2-23
Protokollierung von Änderungen an Profilen und Berechtigungen	2-39	SAP Logon Pad	2-5	ORACLE unter UNIX	2-21, 2-22
Protokollierung von Datenänderungen in Tabellen	2-39	SAP Security Library	2-35, 2-36	ORACLE unter Windows NT	2-22, 2-23
Prüfung	2-37, 2-38, 2-39	SAP*	2-3	Sicherheit des Betriebssystems	
Q		SAP_ALL	2-47	Logische Betriebssystemkommandos in R/3	2-19
Qualitätssicherungssystem	2-28	sapavx<xx>_<INST>	2-41	UNIX	2-14, 2-15
R		SAPCPIC	2-4	Windows NT	2-16, 2-17, 2-18
R/3-Online-Services	2-4, 2-46	SAPDBA	2-22	Sicherheitskonzept	1-1
R/3-Ressourcen		ORACLE unter UNIX	2-21	Sicherheitsprodukt	2-2, 2-13, 2-33, 2-34, 2-36
Windows NT	2-17, 2-18	ORACLE unter Windows NT	2-23	Sitzungsabbruch	2-5
rec/client	2-39	SAP-Gateway	2-32	slg_dll.dll	2-6
Referenzen	2-1	sapntstartb.exe	2-18	Smartcard	2-34
Releases		saposcol.exe	2-18	SNC	
gültige	1-3	SAProuter	2-12, 2-31, 2-41, 2-46	siehe	Secure Network Communications
Remote Communications	2-31, 2-32, 2-33	Kennwörter	2-12	Sperren	2-5, 2-37
Reportklassen	2-9	Protokollierung	2-12	SSF	
Reports		saprouttab	2-12	siehe	Secure Store & Forward
RSCSAUTH	2-9	SAPSECU.pse	2-35	Standardbenutzer	2-3
RSUSR003	2-3	SAPSECULIB		DDIC	2-4
RSUSR006	2-5	siehe SAP Security Library. SAP Security Library		EARLYWATCH	2-4
RFC	2-31, 2-32, 2-33	SAP-Verknüpfungen	2-6	Kennwörter	2-3
Berechtigungen	2-32	SAPXGWFC.dll	2-44	SAP*	2-3
Secure Network Communications	2-33	sapxpg	2-33	SAPCPIC	2-3, 2-4
Vertrauensbeziehungen zwischen R/3-Systemen	2-32	secinfo	2-32, 2-33	START_<Instanz>	2-50
RFC Software Development Kit	2-32	Secure Network Communications	2-2, 2-12, 2-13, 2-33, 2-42, 2-43	stat/level	2-37
Router	2-12, 2-40	Secure Store & Forward	2-34, 2-35, 2-36	Stellenbeschreibungen	2-7
RSGWLST	2-32, 2-33	Security-Audit-Log	2-5, 2-37	SUID/SGID-Programme	2-14
RSRFCCHK	2-31	Session Manager	2-6	Support	1-6
		Sicherheit der Datenbank	2-20	SUSR0001	2-5
		ADABAS	2-24	Systemlandschaft	2-28, 2-29
		allgemein	2-20	Systemprofilparameter	2-50
		Datenbank-Werkzeuge	2-20	Systemprotokolle	2-5, 2-37
		DB2/400	2-27	T	
		DB2/CS unter UNIX	2-25	Tabelle T000	2-49
				Tabellen	

Index

HCL*	2-20	SM19	2-5, 2-37	ITS	2-42
PA*	2-20	SM20	2-5, 2-37	Verteilungsmodell	2-45
RFCDES	2-20	SM21	2-37	Vertrauensbeziehungen zwischen R/3-Systemen - RFC	2-32
SAPUSER	2-20	SM30	2-49	Vertrautes Domänenmodell	2-17
T000	2-3, 2-20, 2-49	SM31	2-3, 2-49	Virenschutz	2-47
TDDAT	2-10	SM49	2-19	W	
USR*	2-20	SM59	2-31	Web-Browser	2-42
USR40	2-2	SM69	2-19	WebReporting	2-44
Tabellenaufzeichnung	2-39	SMW0	2-44	WebRFC	2-44
Tabellenklassen	2-10	STAT	2-37, 2-46	Web-Server	2-40, 2-42
Tagesstatistik	2-37	STMS	2-29	WGate	2-40, 2-41, 2-42
TCP-Port	2-41	SU01	2-39	Windows NT	2-16, 2-17, 2-18
Technische Beratung	1-3, 1-6	SU24	2-10	Berechtigungen	2-16
siehe auch	Beratung zum Thema Sicherheit	SU25	2-10	Domänencontroller	2-16
TPPARAM	2-29	SUIM	2-7	Domänenkonzept	2-17
Transaktionen		SWI2	2-38	R/3-Benutzer und -Gruppen	2-16
PFCG	2-7	SWI5	2-38	R/3-Ressourcen	2-17, 2-18
SALE	2-44	Transport Management System	2-29	Vertrautes Domänenmodell	2-17
SCC4	2-49	Transporte	2-29	WRKSYSVAL	2-27
SCD0	2-38	U		Y	
SE03	2-29	UMASK	2-15	Yellow Pages (NIS)	2-14
SE06	2-29	UNIX	2-14, 2-15	Z	
SE11	2-38	Network File System (NFS)	2-14	Zertifikat	2-36, 2-42
SE93	2-9	Yellow Pages (NIS)	2-14		
SECR	2-37	V			
SGL0	2-38	Verschlüsselung			
SGL1	2-38				
SM18	2-5, 2-37				

R/3-Sicherheitsleitfaden / Feedbackbogen

An:

SAP AG
 Abteilung CCMS & Security
 Postfach 1461
 D-69190 Walldorf

Fax: **+49-6227 / 7-41198**

Absender:

Name:
 Position:
 Abtlg.:
 Firma:
 Adresse:

 Telefon: Fax:
 E-Mail:

Thema: Feedback zum R/3-Sicherheitsleitfaden

Feedback zum R/3-Sicherheitsleitfaden, Band Version Kapitel
 R/3-Release Datenbank Betriebssystem

Haben Sie die gewünschten Informationen in diesem Leitfaden gefunden?

- ja
- nein

Inwieweit wird der R/3-Sicherheitsleitfaden Ihren Anforderungen gerecht?

- sehr gut
- gut
- ausreichend
- gar nicht

Warum oder warum nicht?
 (Verwenden Sie den Platz unten.)

Möchten Sie

- weitere Informationen erhalten?
- weitere Informationen hinzufügen?
- auf fehlende Informationen hinweisen?
- einen Fehler melden?
- sonstiges:

Feedback (verwenden Sie ggf. zusätzliche Blätter):

.....

Danke für Ihre Mithilfe.