

Mario Linkies, Frank Off

Sicherheit und Berechtigungen in SAP -Systemen

Galileo Press

Inhalt

	Vorwort von Prof. Wolfgang Lassmann	15
	Vorwort von Dr. Sachar Paulus	17
1	Einleitung	21
1.1	Motivation.....	21
1.2	Inhalt.....	23
1.3	Lesart.....	24
1.4	Danksagung.....	24
 Teil 1 Grundlagen des Risikomanagements und der IT-Sicherheit		
2	Risiko- und Kontrollmanagement	27
2.1	Sicherheitsziele.....	27
2.2	Unternehmenswerte.....	30
2.2.1	Typen von Unternehmenswerten.....	31
2.2.2	Klassifizierung von Unternehmenswerten.....	32
2.3	Risiken.....	33
2.3.1	Risikotypen.....	34
2.3.2	Klassifizierung von Risiken.....	37
2.4	Kontrollen.....	38
2.4.1	Kontrolltypen.....	38
2.4.2	Klassifizierung von Kontrollen.....	39
3	Sicherheitsstrategie	43
3.1	Status quo.....	43
3.2	Komponenten.....	45
3.2.1	Rahmenbedingungen.....	46
3.2.2	Strategie.....	47

3.2.3	Methoden.....	48
3.2.4	Best Practices.....	48
3.2.5	Dokumentation.....	49
3.3	Best Practices einer SAP-Sicherheitsstrategie.....	49
3.3.1	Vorgehensweise.....	50
3.3.2	Prinzip der Informationsverantwortung.....	59
3.3.3	Identity Management.....	63
4	Anforderungen	71
4.1	Legale Anforderungen.....	71
4.1.1	Sarbanes-Oxley Act.....	72
4.1.2	Basel II.....	81
4.1.3	CoBS.....	84
4.2	Innerbetriebliche Anforderungen.....	86
4.3	Zusammenfassung.....	88
5	Sicherheitsstandards	89
5.1	Internationale Sicherheitsstandards.....	89
5.1.1	Internationaler Sicherheitsstandard ISO 17799.....	90
5.1.2	Internationaler Sicherheitsstandard CoBIT.....	94
5.1.3	COSO - Integriertes Rahmenwerk für das Unternehmensrisikomanagement.....	97
5.2	Länderspezifische Sicherheitsstandards.....	101
5.2.1	Amerikanischer Standard NIST Special Publications 800-12.....	101
5.2.2	Deutscher Sicherheitsstandard IT-Grundschutz des BSI.....	105
6	Grundlagen der technischen Sicherheit	111
6.1	Kryptografie.....	111
6.1.1	Symmetrisches Verschlüsselungsverfahren.....	112
6.1.2	Asymmetrisches Verschlüsselungsverfahren.....	113
6.1.3	Hybrides Verschlüsselungsverfahren.....	114
6.1.4	Hash-Verfahren.....	116
6.1.5	Digitale Signatur.....	117
6.2	Public-Key-Infrastruktur.....	119
6.3	Authentisierungsverfahren.....	121
6.3.1	Benutzername und Passwort.....	121
6.3.2	Challenge Response.....	122
6.3.3	Kerberos.....	122
6.3.4	Secure Token.....	123
6.3.5	Digitales Zertifikat.....	124
6.3.6	Biometrie.....	124

6.4	Netzwerkgrundlagen.....	124
6.4.1	OSI-Schichtenmodell.....	125
6.4.2	Wichtige Netzwerkprotokolle.....	128
6.4.3	Firewall-Technologien im Überblick.....	129
6.4.4	Secure-Socket-Layer-Verschlüsselung.....	131

Teil 2 Sicherheit in SAP NetWeaver und Anwendungssicherheit

7 SAP-Anwendungen und Technologie 135

7.1	Global Security Positioning System.....	135
7.2	SAP-Applikationen.....	135
7.3	SAP NetWeaver.....	137
7.4	Sicherheitstechnologien.....	139
7.4.1	Berechtigungen, Risiko- und Änderungsmanagement und Revision.....	140
7.4.2	Identity Management.....	141
7.4.3	Gesicherte Authentisierung und Single Sign-On (SSO).....	143
7.4.4	Technische Sicherheit.....	143
7.4.5	Einflussfaktoren.....	145

8 SAP Web Application Server 149

8.1	Einführung und Funktionalität.....	149
8.1.1	Übersicht.....	149
8.1.2	Technische Architektur.....	150
8.2	Risiken und Kontrollen.....	151
8.3	Anwendungssicherheit.....	159
8.3.1	Technisches Berechtigungskonzept für Administratoren.....	159
8.3.2	Berechtigungskonzept für Java-Anwendungen.....	166
8.3.3	Einschränkung der Berechtigungen bei RFC-Aufrufen.....	172
8.4	Technische Sicherheit.....	176
8.4.1	Einführung eines Single-Sign-On-Authentisierungsmechanismus ..	176
8.4.2	Anbindung des SAP Web AS an ein zentrales LDAP-Verzeichnis ..	178
8.4.3	Änderung der Standardpasswörter für Standardbenutzer.....	180
8.4.4	Sicherheitskonfiguration des SAP Gateway.....	180
8.4.5	Einschränkung des Betriebssystemzugriffs.....	182
8.4.6	Wichtige sicherheitsrelevante Systemparameter konfigurieren ..	183
8.4.7	Konfiguration von verschlüsselten Kommunikationsverbindungen (SSL und SNC).....	185
8.4.8	Überflüssige Internet-Dienste einschränken.....	190
8.4.9	Sichere Netzwerkarchitektur für den Einsatz des SAP Web AS für das Internet.....	192

8.4.10	Einführung eines Application Level Gateways zur Absicherung von Internet-Anwendungen.....	192
8.4.11	Einführung von Härungsmaßnahmen auf Betriebssystemebene	192
8.4.12	Einführung eines Qualitätssicherungsprozesses für die Softwareentwicklung.....	193

9 SAP ERP Central Component 197

9.1	Einführung und Funktionalität.....	197
9.2	Risiken und Kontrollen.....	197
9.3	Anwendungssicherheit.....	204
9.3.1	Authentisierung.....	204
9.3.2	Berechtigungen.....	205
9.3.3	Weitere Berechtigungskonzepte.....	219
9.3.4	Best-Practice-Lösungen.....	229
9.4	Technische Sicherheit.....	238

10 mySAP ERP Human Capital Management 239

10.1	Einführung und Funktionalität.....	239
10.2	Risiken und Kontrollen.....	239
10.3	Anwendungssicherheit.....	246
10.3.1	HCM-Stammdatenberechtigungen.....	248
10.3.2	HCM-Bewerberberechtigungen.....	249
10.3.3	HCM-Personalplanungsberechtigungen.....	249
10.3.4	HCM-Reporting-Berechtigungen.....	250
10.3.5	Strukturelle Berechtigungen.....	250
10.3.6	Berechtigungen für die Personalentwicklung.....	251
10.3.7	Tolerierte Berechtigungen.....	251
10.3.8	Berechtigungen für Prüfverfahren.....	251
10.3.9	Kundeneigene Berechtigungsprüfungen.....	251
10.3.10	Indirekte Rollenzuordnung über die Organisationsstruktur.....	252
10.3.11	Zusätzliche Transaktionen mit Relevanz für interne Kontrollen ..	252
10.4	Technische Sicherheit.....	253

11 SAP Industry Solutions 255

11.1	Einführung und Funktionalität.....	255
11.2	Risiken und Kontrollen.....	256
11.3	Anwendungssicherheit.....	258
11.3.1	SAPMaxSecure.....	258
11.3.2	SAP-Rollenmanager.....	260
11.4	Technische Sicherheit.....	263

12 SAP NetWeaver Business Intelligence 265

12.1	Einführung und Funktionalität.....	265
12.2	Risiken und Kontrollen.....	267
12.3	Anwendungssicherheit.....	269
12.3.1	Berechtigungen.....	269
12.3.2	Weitere Konzepte.....	274
12.4	Technische Sicherheit.....	279

13 SAP NetWeaver Master Data Management 281

13.1	Einführung und Funktionalität.....	281
13.2	Risiken und Kontrollen.....	282
13.3	Anwendungssicherheit.....	287
13.3.1	Identity Management und Berechtigungen.....	287
13.3.2	Revisionssicherheit.....	293
13.4	Technische Sicherheit.....	293
13.4.1	Kommunikationssicherheit.....	293
13.4.2	Weitere wichtige GSPS-Komponenten.....	294

14 mySAP Customer Relationship Management 295

14.1	Einführung und Funktionalität.....	295
14.2	Risiken und Kontrollen.....	295
14.3	Anwendungssicherheit.....	297
14.4	Technische Sicherheit.....	304
14.4.1	Technische Absicherung der mobilen Anwendung.....	305
14.4.2	Weitere wichtige GSPS-Komponenten.....	305

15 mySAP Supplier Relationship Management 307

15.1	Einführung und Funktionalität.....	307
15.2	Risiken und Kontrollen.....	308
15.3	Anwendungssicherheit.....	309
15.3.1	Wichtige Berechtigungen.....	310
15.3.2	Regelbasierte Sicherheitsüberprüfungen anhand von Geschäftspartnerattributen.....	318
15.3.3	Benutzermanagement.....	321
15.4	Technische Sicherheit.....	322

16 mySAP Supply Chain Management 325

16.1	Einführung und Funktionalität.....	325
16.2	Risiken und Kontrollen.....	325
16.3	Anwendungssicherheit.....	326
16.3.1	Berechtigungen für iPPE Workbench.....	326
16.3.2	Berechtigungen für Supply Chain Planning.....	327
16.3.3	Berechtigungen für Event Management.....	327
16.4	Technische Sicherheit.....	328

17 SAP Strategie Enterprise Management 331

17.1	Einführung und Funktionalität.....	331
17.2	Risiken und Kontrollen.....	332
17.3	Anwendungssicherheit.....	333
17.4	Technische Sicherheit.....	333

18 SAP Solution Manager 335

18.1	Einführung und Funktionalität.....	335
18.2	Risiken und Kontrollen.....	338
18.3	Anwendungssicherheit.....	340
18.4	Technische Sicherheit.....	343
18.4.1	Systemüberwachungsfunktion.....	343
18.4.2	RFC-Kommunikationssicherheit.....	343
18.4.3	Wichtige weitere GSPS-Komponenten.....	344

19 SAP Enterprise Portal 345

19.1	Einführung und Funktionalität.....	345
19.1.1	Technische Architektur.....	346
19.1.2	Bedeutung der User Management Engine.....	348
19.2	Risiken und Kontrollen.....	352
19.3	Anwendungssicherheit.....	360
19.3.1	Aufbau und Design von Portalrollen.....	360
19.3.2	Delegierte Benutzeradministration für Portalrollen unter Einbeziehung der Informationseigner.....	367
19.3.3	Abgleich der Portalrollen mit den ABAP-Rollen derSAP- Backend-Anwendungen.....	370
19.3.4	Änderungsmanagement-Prozess für neue Portalinhalte.....	376
19.4	Technische Sicherheit.....	378

19.4.1	Anschluss des SAP EP an ein zentrales LDAP-Verzeichnis oder SAP-System.....	378
19.4.2	Einführung eines Single-Sign-On-Mechanismus auf Basis einer Ein-Faktor-Authentisierung.....	380
19.4.3	Einführung eines Single-Sign-On-Mechanismus auf Basis einer integrierten Authentisierung.....	384
19.4.4	Einführung eines Single-Sign-On-Mechanismus auf Basis von personenbezogenen Zertifikaten.....	386
19.4.5	Konfiguration für anonymen Zugriff.....	388
19.4.6	Sichere Erstkonfiguration.....	389
19.4.7	Definition und Implementierung von Sicherheitszonen.....	390
19.4.8	Sichere Netzwerkarchitektur.....	393
19.4.9	Einführung eines Application Level Gateways zur Absicherung von Portalanwendungen.....	396
19.4.10	Konfiguration von verschlüsselten Kommunikationsverbindungen.....	400
19.4.11	Einsatz eines Viren-Scanners zur Vermeidung einer Vireninfection.....	402

20 SAP Exchange Infrastructure 405

20.1	Einführung und Funktionalität.....	405
20.2	Risiken und Kontrollen.....	409
20.3	Anwendungssicherheit.....	414
20.3.1	Berechtigungen für den Integration Builder.....	414
20.3.2	Passwörter und Berechtigungen für technische Service-Benutzer.....	416
20.4	Technische Sicherheit.....	417
20.4.1	Definition von technischen Service-Benutzern für Kommunikationsverbindungen während der Laufzeit.....	417
20.4.2	Einrichtung der Verschlüsselung für Kommunikationsverbindungen.....	419
20.4.3	Digitale Signatur für XML-basierte Nachrichten.....	425
20.4.4	Verschlüsselung von XML-basierten Nachrichten.....	430
20.4.5	Netzwerkseitige Absicherung von Integrationsszenarien.....	430
20.4.6	Audit des Integration Builders und der SAP XI-Kommunikation	432
20.4.7	Absichern des File-Adapters auf Betriebssystemebene.....	435

21 SAP Partner Connectivity Kit 437

21.1	Einführung und Funktionalität.....	437
21.2	Risiken und Kontrollen.....	438
21.3	Anwendungssicherheit.....	441
21.4	Technische Sicherheit.....	442
21.4.1	Eigener technischer Service-Benutzer für jedes angeschlossene Partnersystem.....	442

21.4.2	Einrichtung der Verschlüsselung für Kommunikationsverbindungen.....	442
21.4.3	Digitale Signatur für XML-basierte Nachrichten.....	442
21.4.4	Netzwerkseitige Absicherung von Integrationsszenarien.....	443
21.4.5	Audit des Nachrichtenaustausches.....	443
21.4.6	Absichern des File-Adapters auf Betriebssystemebene.....	443

22 SAP Mobile Infrastructure 445

22.1	Einführung und Funktionalität.....	445
22.2	Risiken und Kontrollen.....	447
22.3	Anwendungssicherheit.....	451
22.3.1	Berechtigungskonzept für SAP MI-Anwendungen.....	451
22.3.2	Berechtigungskonzept für die Administration.....	455
22.3.3	Einschränkung der Berechtigungen des RFC-Benutzers auf Backend-Anwendungen.....	456
22.4	Technische Sicherheit.....	457
22.4.1	Einrichtung von verschlüsselten Kommunikationsverbindungen	457
22.4.2	Synchronisationskommunikation absichern.....	458
22.4.3	Überflüssige Dienste auf dem SAP MI-Server deaktivieren.....	460
22.4.4	Sichere Netzwerkarchitektur.....	461
22.4.5	Monitoring.....	462

23 Datenbankserver 463

23.1	Einführung und Funktionalität.....	463
23.2	Risiken und Kontrollen.....	464
23.3	Anwendungssicherheit.....	466
23.4	Technische Sicherheit.....	468
23.4.1	Ändern von Standardpasswörtern.....	468
23.4.2	Entfernen von nicht benötigten Datenbankbenutzern.....	470
23.4.3	Einschränkung des Datenbankzugriffs.....	471
23.4.4	Konzeption und Implementierung eines Datenbanksicherungskonzeptes.....	471
23.4.5	Konzeption und Implementierung eines Upgrade-Konzeptes. . .	472

24 SAP Web Dispatcher 473

24.1	Einführung und Funktionalität.....	473
24.2	Risiken und Kontrollen.....	473
24.3	Anwendungssicherheit.....	475
24.4	Technische Sicherheit.....	475
24.4.1	Einsatz des SAP Web Dispatcher als Reverse Proxy.....	475
24.4.2	Konfiguration des SAP Web Dispatcher als URL-Filter.....	477

24.4.3	SSL-Konfiguration.....	479
24.4.4	Monitoring.....	481

25 SAProuter 483

25.1	Einführung und Funktionalität.....	483
25.2	Risiken und Kontrollen.....	483
25.3	Anwendungssicherheit.....	484
25.4	Technische Sicherheit.....	484

26 SAP Internet Transaction Server 487

26.1	Einführung und Funktionalität.....	487
26.2	Risiken und Kontrollen.....	489
26.3	Anwendungssicherheit.....	492
26.3.1	Zugriffsrechte auf die Service-Dateien setzen.....	492
26.3.2	Administrationskonzept.....	494
26.4	Technische Sicherheit.....	495
26.4.1	DMZ-Netzwerksegmentierung einrichten.....	495
26.4.2	Verschlüsselung der Kommunikationsverbindungen einrichten ...	496
26.4.3	Zertifikatsbasiertes Authentisierungsverfahren einrichten.....	498
26.4.4	Pluggable Authentication Service einrichten.....	499

27 SAP GUI 503

27.1	Einführung und Funktionalität.....	503
27.2	Risiken und Kontrollen.....	504
27.3	Anwendungssicherheit.....	506
27.3.1	Signaturarten.....	506
27.3.2	Unterstützte elektronische Dokumentenformate.....	508
27.3.3	Technische Umsetzung der SSF-Funktionen.....	508
27.3.4	Speicherung der digital signierten Dokumente.....	511
27.3.5	Installation der SSF-Funktionen.....	513
27.4	Technische Sicherheit.....	513
27.4.1	SSO für das WebGUI durch Integration in die Betriebssystemauthentisierung.....	513
27.4.2	SSO für das WebGUI durch Verwendung von digitalen Zertifikaten.....	514
27.4.3	Restriktion des Zugangs auf einen SAP Web AS mithilfe des SAProuter.....	516

28 Webbrowser 517

28.1	Einführung und Funktionalität.....	517
28.2	Risiken und Kontrollen.....	518
28.3	Anwendungssicherheit.....	519
28.4	Technische Sicherheit.....	519
28.4.1	Anti-Viren-Software und deren Aktualisierung für den Desktop.....	519
28.4.2	Einsatz einer Personal Firewall für den Desktop.....	520
28.4.3	Sicherheitseinstellungen für den Webbrowser.....	520

29 Mobile Endgeräte 523

29.1	Einführung und Funktionalität.....	523
29.2	Risiken und Kontrollen.....	523
29.3	Anwendungssicherheit.....	526
29.4	Technische Sicherheit.....	527
29.4.1	Verwendung von mobilen Endgeräten mit Authentisierungsmechanismus.....	527
29.4.2	Einrichtung einer Verschlüsselungsmethodik für Speichermedien.....	528
29.4.3	Verwendung eines Virenschutzes.....	528
29.4.4	Einrichtung einer Personal Firewall.....	528
29.4.5	Etablierung eines Backup-Konzeptes.....	529
29.4.6	Aufsetzen von Zugriffsrechten auf wichtige Systemdateien.....	529
29.4.7	Etablierung eines Sicherheitsbewusstseins beim Benutzer.....	530

A Die Autoren 531

Index 533