

Herbert Stauffer

Security für Data-Warehouse- und Business-Intelligence- Systeme

Konzepte, Vorgehen und Praxis

Edition TDWI



Inhaltsverzeichnis

1	Einleitung	1
1.1	Aufbau des Buches	2
1.2	Grundkonzept	3
1.3	Ganzheitliche Betrachtung von Security	4
1.3.1	Ordnungsmäßigkeit des Betriebs	5
1.3.2	Schutz vor kriminellen Aktivitäten	5
1.3.3	Angemessene Verfügbarkeit der Services	5
1.3.4	Standards, Methoden und Zertifikate	6
1.4	Klassen von potenziellen Schäden	6
1.5	Unterschiede zu transaktionalen Systemen	8
2	Anforderungen an die Schutzwürdigkeit von Systemen	13
2.1	Rechtliche Anforderungen an Daten	13
2.2	Branchenspezifische regulatorische Anforderungen	25
2.3	Betriebliche Anforderungen	26
Teil I	Behandlung von externen Bedrohungen	27
3	Vorgehensmodell zur Behandlung und Eliminierung von Bedrohungen	29
3.1	Anstoß	30
3.2	Sicherheitsprozess	30
3.3	Hilfsmittel	31

4	Schutzobjekte einer BI-Architektur und Aspekte der Bedrohungsmodellierung	35
4.1	Perspektiven der Bedrohungsmodellierung	35
4.2	Strukturorientierte Bedrohungsmodellierung	35
4.3	Angriferorientierte Bedrohungsmodellierung	37
4.4	Wertorientierte Bedrohungsmodellierung	40
4.5	Vorgehensweise	40
5	Risikobeurteilung (Gewichtung)	43
5.1	Wahrscheinlichkeit des Eintretens	44
5.1.1	Bedrohungsfaktoren	44
5.1.2	Verwundbarkeiten/Schwächen	46
5.2	Auswirkung	47
5.2.1	Technische Auswirkungen	48
5.2.2	Betriebswirtschaftliche Auswirkungen	50
6	Risikobehandlung	53
6.1	Verschiedene Arten der Risikobehandlung	53
6.2	Langfristige Sicherstellung und Weiterentwicklung der Maßnahmen	56
Teil II	Berechtigungsstrukturen, Prozesse und Systeme	59
7	Unterschiedliche Berechtigungen in einer BI-Architektur	61
7.1	Unterschiedliche Zugriffsregelung je Data Warehouse Layer	63
7.2	Funktionale Berechtigungen (Toolrechte)	65
7.3	Fachliche Berechtigungen (Datenrechte)	65
7.4	Besondere Berechtigungsobjekte	67
7.4.1	Reports, Cockpits und Dashboards	67
7.4.2	Semantischer Layer	68
7.4.3	Mobile Endgeräte	68
7.4.4	Data Dictionaries	68

8	Applikatorische Berechtigungen in BI-Systemen	71
8.1	Skill- und Rollenmodelle	71
8.2	Einordnung der Rollen	75
8.3	Implementierungsarten für applikatorische Berechtigungen	76
8.3.1	Matrixmodell	77
8.3.2	Einzelrechtemodell	78
8.3.3	Vergleich Einzelrechte- zu Matrixmodell	79
8.3.4	Möglichkeiten zum späteren Wechsel des Modells	80
8.4	Datenzugriff mit technischen oder persönlichen Usern	80
8.5	Herausforderung 1: multiple Rollen	82
8.5.1	Additive Rechtevergabe am Beispiel eines Datenwürfels ...	83
8.5.2	Restriktive Rechtevergabe am Beispiel eines Datenwürfels .	84
8.5.3	Multiple technische Rollen bei funktionalen Rechten	85
8.6	Herausforderung 2: unterschiedliche Rechte in hierarchischen Daten	86
8.7	Alternatives Konzept: Überwachen statt Verhindern	89
9	Autorisierung und Authentifizierung	93
9.1	Zuständigkeit für Freigabe von Berechtigungsanträgen	93
9.2	Weitere Rollen	95
9.3	Drei Komponenten bei der Berechtigungsvergabe	96
9.4	Autorisierungsprozesse	97
9.4.1	Rechte und Rollen	97
9.4.2	Rollen und Anwender	99
9.5	Einsatz von Autorisierungstools	100
9.6	Arten der Authentifizierung (Login)	101
9.7	Segregation of Duties (SoD)	107
9.8	Systemübergreifende Rechteverwaltung	108
9.8.1	Rollenimport aus operativen Systemen in ein Data Warehouse	109
9.8.2	Vergabe von Rollen für mehrere Systeme	109
9.8.3	Beibehalten oder Wechsel der Data Ownership im Data Warehouse	110
9.9	Protokollierung von Datenzugriff und -verwendung	111

Teil III Sicherstellen des operativen Betriebs **113**

10	Operativer Betrieb (Verfügbarkeit)	115
10.1	Ermitteln der Businesskritikalität	115
10.1.1	Anforderungen an IT-Services	116
10.1.2	Strukturierung eines IT-Serviceportfolios	116
10.1.3	Herleiten von Business-Intelligence-Services	118
10.1.4	Wert eines Business-Intelligence-Service	119
10.1.5	Bestimmen des Service Level	121
10.2	Backup und Restore	125
10.3	Disaster Recovery und Notfallkonzepte	131
10.3.1	Prävention	133
10.3.2	Inhalt und Struktur von Notfallplänen	135
10.3.3	Disaster Recovery einüben	136
10.4	Spezifische Technologien	139
10.4.1	Mobile Plattformen	139
10.4.2	Cloud-Anwendungen und Rechenzentrum-Outsourcing	141
10.4.3	Hadoop-Plattformen und Data Lakes	142
10.4.4	Sandboxes	143
10.4.5	Data Science Labs	143
10.4.6	NoSQL-Datenbanken	144
10.5	Räumliche Sicherheit	146

Teil IV Standards, Methoden und Normen **151**

11	Normen, Standards und Organisationen	153
11.1	ISO 15408 – Common Criteria for IT Security Evaluation	154
11.2	ISO 27000 ff.	156
11.2.1	Struktur von ISO 27000 ff.	156
11.2.2	Beurteilung	160
11.3	Bundesamt für Sicherheit in der Informationstechnik (BSI)	161
11.3.1	BSI-Standards	161
11.3.2	IT-Grundschutz-Kataloge	163
11.3.3	Weitere Hilfsmittel	165
11.3.4	Kritikpunkte am BSI-Framework	166
11.4	ISIS12	166
11.4.1	Das ISIS12-Vorgehensmodell	167
11.4.2	Tools und Hilfsmittel	169
11.4.3	Zertifizierung	170
11.4.4	Schwächen von ISIS12	170

11.5 OWASP 172

11.5.1 Hilfsmittel 173

11.5.2 Beurteilung 174

11.6 ITIL 2011 174

11.6.1 Security-Aspekte in den ITIL-Phasen 175

11.6.2 Beurteilung 179

11.7 STRIDE 179

11.8 OSSTMM 3 184

11.9 MELANI 184

11.10 Data Center Tier Standard 185

Teil V Hilfsmittel und Checklisten 187

12 Checklisten und Handlungsfelder 189

12.1 Rollenbezeichnungen in einem zentralen Autorisierungssystem ... 189

12.2 Berücksichtigung von Sicherheitsaspekten beim Aufbau
eines neuen Systems 192

12.2.1 Datenschutz-Checkliste zu VDSG Art. 9 192

12.2.2 Initiale Prüfungen 195

12.2.3 Datenbearbeitung 199

12.2.4 Aufbewahrung und Löschung 200

12.3 Security-Prüfungen für Data Warehousing und
Business Intelligence 200

12.3.1 Sourcing (ETL-/ELT-Prozesse) 201

12.3.2 Persistente Datenspeicherung und -abfragen 202

12.3.3 Frontend und User-Zugriff (Autorisierung) 203

12.3.4 Repository und Administration 205

12.3.5 Generelle Infrastruktur und Komponenten sowie
Organisation 206

12.3.6 Mobile Geräte und Plattformen 207

12.3.7 Mobile Datenträger 208

12.3.8 Elektronische Datenübertragung 209

12.4 Interne Risiken/Bedrohungen und Schutzmöglichkeiten 211

12.4.1 Interne Risiken/Bedrohungen 211

12.4.2 Behandlung von internen Risiken/Bedrohungen 214

12.5 Umgang mit IT- und Admin-Usern 217

13	Security Penetration Testing	221
13.1	Fünf Schritte des Penetration Testing	222
13.1.1	Schritt 1: Klärung der Ziele und des Rahmens	222
13.1.2	Schritt 2: Vorbereitung	224
13.1.3	Schritt 3: Erste Phase des Angriffs (Auffinden von Sicherheitslücken)	226
13.1.4	Schritt 4: Zweite Phase des Angriffs (Eindringen in das System)	226
13.1.5	Schritt 5: Auswertung und Maßnahmenplan	226
13.2	Grenzen von Penetrationstests	227
13.3	Personenbezogener Angriff	228
13.3.1	Social Engineering	228
13.3.2	IGEL-Prinzip	233
13.4	Technischer Angriff	234
13.5	Physischer Angriff	236
14	Ausblick und Trends	239
 Anhang		 243
A	Security-Tools	245
A.1	Tools für Sicherheitskonzepte	246
A.2	Security-Penetration-Test-Suiten	246
A.3	User Activity Tracking	247
A.4	Spezifische Tools für einzelne Aufgaben in Penetrationstests	249
A.4.1	Portscanner	249
A.4.2	Vulnerability-Scanner	249
A.4.3	Sniffer	250
A.4.4	Paketgeneratoren	251
A.4.5	Passwortcracker	253
A.5	Passwortmanager	254
A.6	Passwortgeneratoren	256
A.7	Verzeichnisdienste	257
B	Privacy versus Security	259
C	Lizenzmanagement	261
D	Glossar	263
E	Quellenverzeichnis	275
E.1	Literatur	275
E.2	Weblinks	280
	Index	283