Inhalt

Einleitung 17

1 Risiko- und Bedrohungsanalyse für SAP-Systeme 25

1.1 SAP-Systeme und die Cyber-Bedrohung 29
1.2 Vorgehen zum Erstellen einer Risikomatrix 31
1.2.1 Risikoinformationen kritisch bewerten 31
1.2.2 Risikoanalyse auf Basis internationaler Normen 33
1.2.3 Ein Risiko identifizieren 34
1.2.4 Grafische Darstellung des Risikos 38
1.2.5 Bestimmung des Angriffsvektors und der Verletzbarkeit 39
1.2.6 Bestimmung des Angreifers und der Verletzbarkeit 40
1.2.7 Bestimmung der technischen Auswirkungen eines Angriffs 41
1.2.8 Formalisierter Risikofaktor aus dem Modell 43
1.3 Internationale Standardmethoden für eine Risikoanalyse 44
1.3.1 Open Web Application Security Project 44
1.3.2 NIST Risk Assessment 46
1.3.3 Bundesamt für Sicherheit in der Informationstechnik 48

2 Eine Sicherheitsstrategie entwickeln 53

2.1 Ziele einer Sicherheitsstrategie 57
2.1.1 Interne und externe Aufgaben 58
2.1.2 Status quo feststellen 60
2.1.3 Penetrationstest zur Überprüfung des Status quo 61
2.2 Kosten und Nutzen abwägen 65
2.3 Unternehmensbeispiele für Sicherheitsstrategien 67
2.3.1 Übungszentrum Netzverteidigung 68
2.3.2 Cyber Control Center der Telekom 73

Bibliografische Informationen
http://d-nb.info/1074838580

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

2.4 Abschließende Überlegungen zur Sicherheitsstrategie 77

3 SAP-Sicherheit – Standards und aktuelle SAP-Werkzeuge 79

3.1 SAP-Sicherheit in der klassischen Sicht 79
3.1.1 Ebene 1: Rich Client bzw. SAP GUI 80
3.1.2 Ebene 2: Anwendungsserver und Message Server 81
3.1.3 Ebene 3: Datenbankserver 81
3.1.4 Die klassische Drei-Ebenen-Architektur 82
3.1.5 Verletzbarkeit der historischen SAP-Architektur 82
3.1.6 SAP-Sicherheitshinweise 83
3.2 SAP NetWeaver: Sicherheit mit neuer Softwaregeneration 84
3.3 SAP Enterprise Threat Detection 86
3.3.1 Einsatz in der SAP-internen IT 86
3.3.2 Architektur der Komponenten 87
3.3.3 Archive 88
3.3.4 Anonymisierung personenbezogener Daten 88
3.3.5 Muster in Log-Dateien erkennen lernen 90
3.4 SAP Code Vulnerability Analysis 91
3.5 SAP Solution Manager als Steuerungsinstrument 97
3.5.1 SAP EarlyWatch 97
3.5.2 Security Self-Service über den SAP Solution Manager 98
3.5.3 Custom Code Lifecycle Management 98
3.6 Ausblick 99

4 Netzwerksicherheit herstellen 101

4.1 Netzwerk, Switches, Router und Firewalls 101
4.1.1 Das ISO/OSI-Referenzmodell 101
4.1.2 Verschlüsselung der Netzwerkverbindungen mit SNC 106
4.1.3 Firewall in der SAP-Umgebung (ISO/OSI) 107

4.2 SAP-Landschaft analysieren 109
4.2.1 Tier 1: SAP-GUI-Client 110
4.2.2 Tier 1: Zugang aus dem Internet und Übergang ins Intranet 111
4.2.3 Tier 2: Übergang von Intranet zur SAP-Tier 115
4.2.4 Tier 3: Die SAP-Systeme 117
4.3 Virtuelle Netzwerke und Software-Defined Networks 117
4.3.1 Die Idee einer neuen offenen Netzwerkarchitektur 121
4.3.2 Sicherheit im Software-Defined Network ... 122

5 Werkzeugkasten des SAP-Sicherheitsexperten 123

5.1 Kali-Linux-Distribution 123
5.1.1 Die Geschichte der Kali-Distribution 124
5.1.2 Download und Installation 124
5.1.3 Kali Linux und SAP 125
5.2 Rot gegen Blau: Werkzeuge für Angriff und Verteidigung 126
5.2.1 Vor dem Angriff: Die Zielanalyse 126
5.2.2 Angriff: Netzwerkerkennung und -analyse mit Nmap 129
5.2.3 Angriff: Server-Erkennung und -analyse mit Metasploit 133
5.3 Kommerzielle Produkte für Penetrationstests im Bereich SAP 136
5.3.1 Onapsis X1 und Onapsis OSP 136
5.3.2 ERPScan 137
5.3.3 Virtual Forge 137
5.3.4 ESNC: Enterprise Security and Compliance 137
5.3.5 Werth IT Auditor 137
5.4 Gegenmaßnahmen zum Schutz des Netzwerks 138
5.5 Patch-Management mit dem SAP Solution Manager 139
5.6 Klassische Angriffsvektoren für Hacker und Penetrationstester 141
5.6.1 Oracle-Hack 142

5.6.2 Gegenmaßnahmen zum Schutz der Datenbank ... 143
5.6.3 Gegenmaßnahmen zum Schutz der Netzwerke ... 143

6 Schutz von SAProuter und SAP Web Dispatcher ... 145

6.1 Der SAProuter im SAP-Netzwerk ... 145
6.1.1 Wann wird der SAProuter eingesetzt? ... 146
6.1.2 Wann wird der SAProuter nicht eingesetzt? ... 147
6.1.3 SAProuter installieren ... 148
6.1.4 Kontrolle und Protokollierung von Verbindungen zu SAP-Systemen ... 149
6.1.5 SAProuter und Secure Network Communications SNC ... 150
6.1.6 SAProuter-String-Information ... 151
6.2 Angriff auf den SAProuter ... 152
6.3 Gegenmaßnahme: Härten des SAProuters ... 153
6.4 Der SAP Web Dispatcher im SAP-Netzwerk ... 154
6.5 Angriff auf den SAP Web Dispatcher ... 157
6.6 Gegenmaßnahme: Härten des SAP Web Dispatchers ... 160

7 Schutz des SAP NetWeaver AS ABAP ... 163

7.1 Die ABAP-Laufzeitumgebung ... 163
7.2 Der SAP NetWeaver AS ABAP als Angriffsziel ... 164
7.3 Berechtigungen nach dem Need-to-know-Prinzip ... 168
7.3.1 Need-to-know-Prinzip umsetzen ... 168
7.3.2 Benötigte Anwendungen und Programme ermitteln ... 170
7.4 Schutz des SAP NetWeaver AS ABAP gegen Angriffe ... 179
7.4.1 Angriffsfläche verringern ... 179
7.4.2 Sicherheitslücken aufspüren ... 182
7.4.3 Kritische Rechte kontrollieren ... 184
7.5 Dokumentation der Absicherungsmaßnahmen ... 187
7.5.1 Generelle Anforderungen ... 188
7.5.2 Das Sicherheitskonzept ... 189
7.5.3 Das Berechtigungskonzept ... 189

8 Schutz des SAP NetWeaver AS Java 191

8.1 Härten des SAP NetWeaver AS Java 192
8.1.1 Zugriffe einschränken 192
8.1.2 Nicht benötigte Dienste deaktivieren 195
8.1.3 Kommunikationssicherheit herstellen 197
8.1.4 Passwort-Regeln festlegen 202
8.1.5 Java-Berechtigungen verstehen 205
8.2 Angriffe auf den AS Java und Gegenmaßnahmen 206

9 Schutz von Remote Function Calls 209

9.1 Technische Komponenten der RFC-Verbindungen 210
9.2 RFC-Berechtigungen verstehen und einsetzen 214
9.3 Unified Connectivity: eine weitere Schutzebene 223
9.4 RFC-Sicherheit auf Client-Seite herstellen 224
9.5 RFC-Callback-Sicherheit aktivieren 226
9.6 Den RFC-Gateway absichern 228
9.7 Verschlüsselung aktivieren 230

10 Passwortschutz 233

10.1 Technologie und Logik von Hash-Prüfungen 233
10.2 Technische Implementierung der Passwörter im SAP-System 236
10.3 Werkzeuge: John the Ripper und HashCat 242
10.4 Wörterbücher beim Angriff 244
10.5 Angriff auf die Passwörter (Hashes) 244
10.6 Gegenmaßnahmen: harte Passwörter, SSO und Hashes löschen 245
10.6.1 Schutz gegen Hash-Diebstahl 245
10.6.2 Nutzung eines sicheren Hash-Algorithmus 251
10.6.3 Bereinigung alter Hash-Werte 256
10.6.4 Passwort-Policy einführen 257
10.6.5 Single Sign-on statt lokale Passwörter nutzen 261

11 Schutz des Transportsystems 263

11.1 Transport Management System 263
11.2 Angriffe auf das Transportsystem 265
11.2.1 Schutz vor Angriffen über das Dateisystem 265
11.2.2 Schutz vor Angriffen mit speziellen Transportobjekten 269
11.2.3 Schutz vor Angriffen über die Systembenutzer des TMS 271
11.2.4 Transport von Schad-Code und Sicherheitslücken 273
11.3 Gegenmaßnahme: Härtung des CTS mithilfe des SAP Solution Managers 278

12 Schutz der Datenbank 281

12.1 Die Rolle der Datenbank in SAP-Systemen 281
12.2 Generelle Risiken und Absicherungsmaßnahmen 283
12.2.1 Zugriff und Zugang 283
12.2.2 Daten und Inhalte 288
12.3 Funktionstrennung in einer Oracle-Datenbank 290
12.4 Angriffe auf SAP-Datenbanken 293
12.4.1 SAP-Datenbankschnittstelle 293
12.4.2 Datenbankangriffe aus SAP-Anwendungen 295
12.4.3 Gegenmaßnahmen zum Schutz vor ABAP-basierten Angriffen 297
12.4.4 Ausspähen des SAP-Datenbankservers 298
12.4.5 Direkte Angriffe auf Betriebssystemebene 301
12.4.6 Gegenmaßnahmen zum Schutz vor Angriffen auf Betriebssystemebene 303
12.4.7 Beispiel: Datenbanksicherheit mit IBM Guardium 304

13 SAP HANA und die Sicherheit der In-Memory-Datenbanken 309

13.1 Sicherheit in SAP HANA 310
13.2 Architektur von SAP HANA 312

13.2.1 Die Datenbankwelt aus der Sicht des Hauptspeichers 312
13.2.2 In-Memory Column Stores 313
13.3 Grundlagen der Sicherheitskonzepte für HANA 315
13.3.1 Speicherorientierte Datenbank: Die SAP HANA XS Engine 316
13.3.2 Benutzer- und Rollenmanagement 316
13.3.3 Authentifizierung und Single Sign-on 317
13.4 Absicherung der Webanwendungen 318
13.4.1 Angriffsvektoren auf die neuen Werkzeuge 320
13.4.2 Serverseitiges JavaScript 320
13.4.3 Maßnahmen zur Härtung von Webanwendungen 322
13.5 Penetrationstest auf SAP-HANA-Applikationen ausführen 323
13.6 Angriffe auf den Hauptspeicher 324
13.6.1 Risikoabschätzung zum Angriffsvektor Hauptspeicher 325
13.6.2 Verschlüsselung bei SAP HANA 326
13.6.3 Cloud und Verschlüsselung 327

14 Erkennung von Angriffsmustern und Forensik 329

14.1 Die Quelle der Muster: die wichtigsten Log-Dateien 330
14.1.1 Vorbemerkung zur forensischen Analyse 331
14.1.2 Security Audit Log 332
14.1.3 Systemlog 334
14.1.4 Gateway-Logging 335
14.1.5 Logging von Internet Communication Manager und SAP Web Dispatcher 336
14.1.6 Logging des SAP NetWeaver Application Server Java 338
14.1.7 Logging des Message Servers 339
14.1.8 Logging von Datenänderungen in Tabellen 339
14.1.9 Logging von Änderungen an Benutzern und Berechtigungen 341
14.1.10 Logging von Änderungsbelegen 341
14.1.11 Systemtrace 342

14.1.12 Entwickler-Trace 343
14.1.13 Logging des SAProuter 345
14.1.14 Logging von Datenbankzugriffen (SQL Audit) 346
14.2 Auswertung mit Transaktion ST03 346
14.3 Auswertung mit Funktionsbausteinen 347
14.4 Usage and Procedure Logging 349
14.5 Netzwerkinformationen, Terminals und SAP-Benutzer-Sessions 351
14.5.1 Snort 351
14.5.2 Onapsis Detection and Response 353
14.5.3 IBM Guardium 354
14.6 Werkzeuge zur Auswertung der Muster: Security Information and Event Management 354
14.6.1 IBM Security QRadar SIEM und HP ArcSight 355
14.6.2 SAP Enterprise Threat Detection 355
14.6.3 Splunk 356
14.7 Sicherheitsmuster 357
14.8 Grundlegende Sicherheitsaktivitäten 358

15 Mobile Anwendungen sichern 361

15.1 Netzwerkarchitektur für den mobilen Zugriff auf SAP-Systeme 362
15.2 Komponenten der Sicherheitsstrategie für die SAP-Mobile-Infrastruktur 366
15.2.1 Sicherheit für mobile Geräte 367
15.2.2 Sicherheit für mobile Anwendungen 367
15.2.3 Sicherheit für mobile Dokumente 370
15.2.4 Enterprise Integration 370
15.3 Angriffe auf die mobile Landschaft 378
15.3.1 Wireless Access Point 378
15.3.2 Single Sign-on und Identity Access Management 380
15.3.3 Gestohlene Cookies 381
15.3.4 SAP Web Dispatcher 381
15.3.5 SAP Gateway und SAP-Backend 381

16 Sicherheit im Internet der Dinge 383

16.1 Sicherheitsebenen des Internets der Dinge 385
16.1.1 Hardware- und Softwareebene des Internets der Dinge 385
16.1.2 Ebene der Daten – Big Data 389
16.1.3 Ebene der Anwendungs- und Produktentwicklung 390
16.1.4 Ebene der Fertigung 392
16.1.5 Ebene des technischen Betriebs 393
16.1.6 Ebene des Marketings für das Internet der Dinge 395
16.2 SAP-Architektur für das Internet der Dinge 396
16.3 Kryptografie im Internet der Dinge 400
16.3.1 Verschlüsselung auf ASIC und FPGA 402
16.3.2 Das Spiel mit dem Zufall 404
16.4 Gefährdungspotenzial für das Internet der Dinge im SAP-Bereich 406
16.5 Angriffswerkzeuge für Hardware-Hacks 407
16.6 Anatomie eines Hardware-Hacks 410
16.7 Anatomie eines Industrieanlagen-Hacks 413

Die Autoren 417

Index 419