

Hacking von SAP®-Systemen

Angriffe verstehen und abwehren

DAS INHALTS- VERZEICHNIS

» Hier geht's
direkt
zum Buch

Inhalt

Einleitung	19
------------------	----

1 Aktuelle Angriffsvektoren und Sicherheitsstrategien für SAP-Landschaften 27

1.1 Der Aufstieg der Cybersicherheitsindustrie	28
1.2 Die Konsequenzen für die technische Sicherheit von IT-Systemen	30
1.3 Resilienz gegen externe und interne Bedrohungen	33
1.4 Strategie für eine resiliente SAP-Sicherheitsorganisation	36
1.4.1 Dokumentation der eigenen Systeme	36
1.4.2 Festlegung der Verantwortlichkeiten innerhalb der IT-Organisation	38
1.4.3 Security Monitoring und Event Handling (SIEM)	40
1.5 Typische Angriffsvektoren für SAP-Systeme	40
1.5.1 Netzwerkangriffe mit dem Ziel der Serververschlüsselung	41
1.5.2 Interne Angriffe durch Mitarbeiter und Passwortdiebstahl	47
1.5.3 Gezielte externe Angriffe	49

2 SAP-Sicherheit per Default: Standards und aktuelle SAP-Sicherheitswerkzeuge 53

2.1 Der Blick auf die klassische SAP-Sicherheitsarchitektur	54
2.2 Security by Default	55
2.3 Integration von Sicherheitsanforderungen in den Entwicklungsprozess	58
2.4 SAP BTP: Sicherheit mit neuer Softwaregeneration	60
2.4.1 SAP und die OWASP Top 10	61
2.4.2 SAP-Sicherheitskonzepte für die Cloud	65

- 2.5 Grundlage: die Arbeit mit dem Security Audit Log 68**
- 2.6 SAP Enterprise Threat Detection 72**
- 2.7 SAP Code Vulnerability Analyzer: Schutz des kundeneigenen Codes 74**
 - 2.7.1 Get Clean: vorhandenen ABAP-Code prüfen 75
 - 2.7.2 Stay Clean: Sicherheitsrichtlinien für die ABAP-Programmierung 75
- 2.8 Das neue SAP Security Dashboard 76**
- 2.9 SAP Cloud ALM für das Security Monitoring 77**
- 2.10 Die wichtigsten SAP-Sicherheitsrichtlinien 81**
 - 2.10.1 SAP Security Baseline 81
 - 2.10.2 SAP-Empfehlungen für Sicherheitsdienste 82
 - 2.10.3 Empfehlungen der SAP Community 83

3 Wie kommen Hacker an die erforderlichen Informationen? 85

- 3.1 Nutzung von Suchmaschinen und Foren 86**
 - 3.1.1 Hacking von Passwörtern 86
 - 3.1.2 Erstellung von Entwicklerschlüsseln 89
 - 3.1.3 Weitere Suchbegriffe 91
- 3.2 Nutzung von Künstlicher Intelligenz 92**

4 Was brauchen Hacker für On-Premise-Systeme? Ein Werkzeugkasten 99

- 4.1 Piraten auf Beutezug: Bug Bounty 100**
- 4.2 Das Werkzeug Nummer 1: Dokumentation 103**
- 4.3 Die Kali-Linux-Distribution 104**
- 4.4 Der neue Klassiker im Arsenal: PowerShell 106**
- 4.5 Rot gegen Blau: Werkzeuge für Angriff und Verteidigung 107**
 - 4.5.1 Zielanalyse 107
 - 4.5.2 Netzwerkerkennung und -analyse mit Nmap 111

4.5.3	Servererkennung und -analyse mit Metasploit	114
4.5.4	Burp Suite, der SAP-Angriff über das Web	119
4.5.5	SAP und das HTTP Request Smuggling	119
4.5.6	Kommerzielle Werkzeuge im Bereich SAP	123
4.5.7	Werkzeuge zur Verteidigung von SAP-Systemen	123

5 Was brauchen Hacker für die SAP-Cloud? Mehr für den Werkzeugkasten 127

5.1	Besonderheiten in den Verantwortlichkeiten bei Sicherheitstests und ethischen Hacks in der Cloud	128
5.2	Reconnaissance	129
5.3	Die Top 4 der Angriffswerkzeuge für die Cloud	135
5.3.1	PortSwigger Burp Suite	135
5.3.2	PowerShell	136
5.3.3	Postman	138
5.3.4	Nmap	142
5.4	Angriffe auf die Identitäts- und Zugriffsverwaltung	143
5.4.1	Angriff auf Identitäten	144
5.4.2	Werkzeuge für IAM-Angriffe	147
5.5	Angriffe auf APIs	148
5.6	Container- und Kubernetes-Sicherheit	151
5.7	Rechtheausweitung und Persistenz-Werkzeuge	154
5.8	Zugang zu Exploit-Datenbanken und Schwachstellen	156

6 Erstes Ziel: das Netzwerk 161

6.1	Neue Netzwerkarchitekturen	161
6.2	Die Grundlagen: Netzwerk, Switches, Router und Firewalls	165
6.2.1	Das ISO/OSI-Referenzmodell	165
6.2.2	Verschlüsselung der Netzwerkverbindungen mit SNC	169
6.2.3	Firewall in der SAP-Umgebung	170
6.2.4	SAP Web Dispatcher	173

- 6.3 SAP-Landschaft analysieren** 174
 - 6.3.1 Tier 1: SAP-GUI-Client und SAP Fiori 175
 - 6.3.2 Tier 1: Zugang aus dem Internet und Übergang ins Intranet 176
 - 6.3.3 Tier 2: Übergang vom Intranet zur SAP-Tier 180
 - 6.3.4 Tier 3: die SAP-Systeme 182
- 6.4 Virtuelle Netzwerke und Software-defined Networking** 183
 - 6.4.1 Die Idee einer neuen offenen Netzwerkarchitektur 186
 - 6.4.2 Sicherheit im Software-defined Networking 187
 - 6.4.3 Software-defined Networking als zentrales Element bei Cloud-Anbietern und Hyperscalern 188
- 6.5 Angriffe auf das Netzwerk in On-Premise-Landschaften** 190
 - 6.5.1 Angriff auf ein VPN 191
 - 6.5.2 Angriffe auf das Netzwerk jenseits des VPNs 193
 - 6.5.3 Angriffe auf die Web- und RFC-Ports der SAP-Server 194
- 6.6 Angriff auf das Netzwerk über die Cloud** 196
- 6.7 Grundlegende Mitigation gegen Netzwerkangriffe** 197

7 Einmal im Netzwerk, werden die Passwörter gehackt: Passwortschutz 199

- 7.1 Technologie und Logik von Passwortprüfungen** 200
- 7.2 Technische Implementierung der Passwörter im SAP-System** 203
- 7.3 Wie kommen Hacker an die Passwort-Hashes?** 209
- 7.4 Angriff auf die Passwörter bzw. Hashes** 213
- 7.5 Werkzeuge: John the Ripper, Hashcat und die Cloud** 214
- 7.6 Verwendung von Wörterbüchern und Regeln beim Angriff** 219
- 7.7 Gegenmaßnahmen: starke Passwörter, sichere Hashes und Single Sign-on** 221
 - 7.7.1 Nutzung eines sicheren Hash-Algorithmus 222
 - 7.7.2 Bereinigung alter Hash-Werte 226
 - 7.7.3 Passwort-Policy einführen 228
 - 7.7.4 Single Sign-on anstelle lokaler Passwörter nutzen 231

8 Welche SAP-Standardfunktionen können Hacker ausnutzen? 235

8.1 Verstecken eigenentwickelter ABAP-Programme	235
8.1.1 Anlegen von ABAP-Programmen in öffentlichen Namensräumen	236
8.1.2 Anlegen von ABAP-Programmen in SAP-Namensräumen	239
8.2 Funktionen ohne Berechtigungsprüfung	242
8.3 Aufruf von Funktionsbausteinen über das Reporting	244
8.4 RFC-Verbindungen pflegen ohne SM59-Berechtigung	245
8.5 Ändern nicht änderbarer Tabellen	249
8.6 Quelltexte pflegen ohne Versionierung	252
8.7 Daten in der SAP-HANA-Datenbank mit ABAP manipulieren ...	255
8.8 Löschen von Protokollen	258
8.8.1 Löschen von Security-Audit-Log-Protokollen	259
8.8.2 Löschen von Tabellenänderungsprotokollen	259
8.8.3 Löschen von Änderungsbelegen	260
8.8.4 Löschen der Versionshistorien	261

9 Angriff auf das SAP-System: Schutz von Remote Function Calls 263

9.1 Grundlagen von Remote Function Call	264
9.1.1 RFC-Bibliotheken	265
9.1.2 Beispiel für ein Programm zum Aufruf eines RFC-Funktionsbausteins	267
9.2 Mögliche Angriffe per Remote Function Call	270
9.2.1 Zugriff über eine Citrix-App	271
9.2.2 Orchestrierung von RFC-Angriffen per GitHub	272
9.2.3 Angriffe über Windows PowerShell	273
9.2.4 Angriffe mit Microsoft Excel	276
9.3 Blue Team: Schutz der RFC-Verbindungen	277
9.3.1 Technische Komponenten der RFC-Verbindungen	277
9.3.2 RFC-Berechtigungen verstehen und einsetzen	280

9.3.3	Unified Connectivity: eine weitere Schutzebene	290
9.3.4	RFC-Sicherheit auf Client-Seite herstellen	290
9.3.5	RFC-Callback-Sicherheit aktivieren	292
9.3.6	RFC-Gateway absichern	294
9.3.7	Verschlüsselung aktivieren	296

10 Manipulation des kundeneigenen Codes: ABAP-Angriffe 299

10.1	Codebeispiele für Angriffe mit ABAP-Code	299
10.1.1	Direkte Zugriffe auf die Datenbank mit dem Befehl »EXEC SQL«	300
10.1.2	Generierung von dynamischem Code	302
10.1.3	Generierung von »verstecktem« Code	303
10.1.4	Umgehung des Mandantenkonzepts	306
10.1.5	Debuggen mit Hauptspeicheränderungen (Radieren)	307
10.1.6	In Quelltexten Benutzernamen hinterlegen	309
10.1.7	Transaktionen aufrufen mit »CALL TRANSACTION«	310
10.2	ABAP-Trojaner und Ransomware	312
10.3	Angriffe auf das Transport Management System mit Upload-Viren	315
10.4	Gegenmaßnahmen gegen ABAP-Angriffe	316
10.4.1	Programmübergreifende Analyse von Quelltexten	316
10.4.2	Scannen eines Transports	326

11 Angriffe auf SAP HANA und die In-Memory-Datenbank 329

11.1	Sicherheitskonzepte für SAP HANA	329
11.2	Penetrationstests für SAP HANA	332
11.3	Angriffe auf den Hauptspeicher	333
11.4	Durchgriffe auf das ABAP-Schema in SAP HANA	335
11.5	Monitoring und Erkennung von Angriffsmustern mit dem SAP HANA Audit Log	338

11.5.1	Speicherung der Audit-Log-Dateien	338
11.5.2	Policies für das SAP HANA Audit Log	341
11.5.3	Best-Practice-Konfiguration für das SAP HANA Audit Log	343
11.5.4	Löschen von Audit-Protokollen	346
11.6	Härtung von SAP HANA	348
11.6.1	Absicherung der Unix-Benutzer	348
11.6.2	Isolierung von Tenants	352
11.6.3	Verschlüsselung von Daten	357
11.6.4	Absicherung der SAP-HANA-Standardbenutzer	362
11.6.5	Skripte zur Analyse der Systemsicherheit	367

12 Angriffe auf die SAP-Cloud-Infrastruktur 373

12.1	Die fünf Säulen der SAP BTP	373
12.1.1	Anwendungsentwicklung und -bereitstellung	376
12.1.2	Automatisierung	377
12.1.3	Integration	378
12.1.4	Daten und Analytics	379
12.1.5	Künstliche Intelligenz	379
12.2	Identity Hacking in der Cloud	379
12.2.1	Der Anmeldeprozess mit Microsoft Entra ID	382
12.2.2	Sicherheitsmechanismen in Entra ID	386
12.2.3	Relevanz von Mimikatz in Hybrid-Umgebungen	387
12.3	API Hacking und die SAP Integration Suite	389
12.3.1	APIs suchen und finden	389
12.3.2	Proxy-Tools für die Analyse und Manipulation von APIs	393
12.3.3	Beispiel einer Hack Session auf die SAP BTP	396

13 Angriffe auf SAP-Cloud-Anwendungen 403

13.1	Ein Cyber-Angriff auf ein fiktives Unternehmen: die Auto&Bahn AG	404
13.1.1	Ein schwarzer Tag der Auto&Bahn AG	404
13.1.2	Was kann man aus diesem Beispiel lernen?	406

- 13.2 SAP-Cloud-Anwendungen** 408
- 13.3 Die wichtigsten Angriffsvektoren auf Cloud-Anwendungen** 409
 - 13.3.1 Phishing und Social Engineering 409
 - 13.3.2 Identity, Brute-Force- und Credential-Stuffing-
Angriffe 410
 - 13.3.3 Man-in-the-Middle-Angriffe 412
 - 13.3.4 Angriffe auf APIs 412
 - 13.3.5 Exploits und Softwareschwachstellen 413
 - 13.3.6 Denial-of-Service- und Distributed-Denial-of-Service-
Angriffe 414
 - 13.3.7 Bedrohungen durch Insider 414
 - 13.3.8 Datenextraktion durch Malware 415
- 13.4 Sicherheitskonzept für SAP-Fiori-Anwendungen in
der Cloud** 416
 - 13.4.1 Cross-Site-Scripting-Angriffe durch Viren in
SAP-Fiori-Anwendungen 418
 - 13.4.2 Schutz gegen Angriffe auf SAP-Fiori-Apps 419
- 13.5 Hybrider SAP-Hack mit der Burp Suite** 422
- 13.6 Google Dork für einen API-Angriff** 428
- 13.7 Die Gefährlichkeit des Protokoll-Schmugglers** 429
- 13.8 Juristische Rahmenbedingungen von SAP-Systemen und
-Anwendungen in einer Hyperscaler-Cloud** 432

- 14 Ransomware: Ablauf eines Angriffs** 437

- 14.1 Die Dynamik des Erfolgs von Ransomware-Akteuren** 438
- 14.2 Was kann man aus diesem Ablauf lernen?** 448

- 15 Berechtigungsbasierter Penetrationstest** 451

- 15.1 Berechtigungsbasierter Penetrationstest vs. klassische
Berechtigungsanalyse** 452
- 15.2 Technische Voraussetzungen und Vorbereitung** 457
 - 15.2.1 Auswahl der Benutzer oder Rollen 457
 - 15.2.2 Zugang zum Qualitätssicherungssystem 459

15.2.3	Das Problem der laufenden Einstellungen	460
15.2.4	Erstellen von Testbenutzern	462
15.3	Voranalyse	462
15.3.1	Aufbau einer Datenbank zur Analyse von Berechtigungen	464
15.3.2	Abgleich der Berechtigungen zwischen Produktiv- und Qualitätssicherungssystem	467
15.3.3	Anzahl der vergebenen Transaktionen im Vergleich zur Gesamtanzahl und der Anzahl der Transaktionen pro Modul	470
15.3.4	Analyse der vergebenen Tabellenzugriffsberechtigungen	473
15.3.5	Auswahl geeigneter Testkandidaten für den Penetrationstest	478
15.4	Ablauf des berechtigungsbasierten Penetrationstests	480
15.4.1	Vorbereitungsphase	480
15.4.2	Durchführung der Voranalyse	481
15.4.3	Testdurchführung, Dokumentation und Berichterstattung	481
15.4.4	Nachbereitung und Follow-up	483
15.5	Wo sind die Kronjuwelen? Besonders interessante Angriffsziele	484
15.5.1	Stammdaten in der Finanzbuchhaltung (Modul FI)	484
15.5.2	Stammdaten im Personalwesen (Modul HCM)	491
16	Angriffe gegen mobile Anwendungen	495
16.1	Beispielanforderung: eine mobile App zur Krankmeldung	496
16.2	Netzwerkarchitektur für den mobilen Zugriff auf SAP-Systeme	497
16.2.1	OData-Services und Anbindung an On-Premise- Systeme	498
16.2.2	Erweiterung um Drittanbieterdienste in der Cloud und als On-Premise-Systeme	499
16.3	Grundlegende Überlegungen zur Sicherheit einer mobilen Anwendung auf der SAP BTP	500
16.4	Angriffe auf die mobile Landschaft	505
16.4.1	Wireless Access Point	505

16.4.2	Single Sign-on und Identity Access Management	507
16.4.3	Gestohlene Cookies	508
16.4.4	Angriffe auf Cloud Connector und SAP-Backend	508
16.4.5	Angriffe auf SAP-Fiori-Anwendungen	508
17	Angriffe aus dem Internet der Dinge	513
17.1	Sicherheit im Internet der Dinge	514
17.2	Sicherheitsebenen des Internets der Dinge	515
17.2.1	Hardware- und Softwareebene des Internets der Dinge	516
17.2.2	Ebene der Daten – Big Data	518
17.2.3	Ebene der Anwendungs- und Produktentwicklung	519
17.2.4	Ebene der Fertigung	519
17.2.5	Ebene des technischen Betriebs	521
17.3	Kryptografie	522
17.3.1	Verschlüsselung auf ASIC und FPGA	523
17.3.2	Beispiel: Kryptografie im eigenen Auto	524
17.3.3	Das Spiel mit dem Zufall	525
17.4	Anatomie eines Industrieanlagen-Hacks	527
17.5	Angriffswerkzeuge für Hardware-Hacks	530
17.5.1	Werkzeuge für RF-Angriffe	530
17.5.2	USB-Angriffe und eine Gummi-Ente	533
17.5.3	Alles in einem: Flipper Zero	536
17.5.4	Weitere Werkzeuge im Hacker-Rucksack	539
17.6	Anatomie eines Hardware-Hacks	539
18	Härtung der SAP-S/4HANA-Plattform	543
18.1	Standardsicherheitsmaßnahmen der ABAP-Plattform	544
18.2	Systemhärtung	546
18.2.1	Security Baseline als Grundlage für eigene Sicherheitsrichtlinien	547
18.2.2	Praktische Vorgehensweise zur Systemhärtung	550

18.3 Benutzer und Berechtigungen im Griff	554
18.3.1 Need-to-know-Prinzip umsetzen	555
18.3.2 Benötigte Anwendungen und Programme ermitteln	556
18.4 Angriffsfläche verringern	564
18.5 Backup und Restore – nicht nur in der Theorie	567
18.5.1 Backups planen	567
18.5.2 Restore testen	568
18.6 Systemhärtung auf Betriebssystemebene	569
18.7 Überwachung des Dateisystems: »auditd« und Muster für die Angriffserkennung	572
18.8 Mitigation bei Angriffen	574

19 Erkennung von Angriffen, Abwehr und Forensik 577

19.1 Anatomie eines Angriffs: das Framework MITRE ATT&CK im SAP-Kontext	578
19.1.1 Wichtige MITRE-ATT&CK-Taktiken	579
19.1.2 Wichtige MITRE-ATT&CK-Techniken	581
19.1.3 Kategorisierung typischer Angriffsmuster	582
19.2 An der Quelle: die wichtigsten Protokolle zur Erkennung von Angriffen	586
19.2.1 Security Audit Log	586
19.2.2 Systemlog	587
19.2.3 Gateway-Logging	588
19.2.4 Logging von Internet Communication Manager und SAP Web Dispatcher	589
19.2.5 Logging des Message-Servers	590
19.2.6 Logging von Datenänderungen in Tabellen	591
19.2.7 Logging von Änderungen an Benutzern und Berechtigungen	592
19.2.8 Logging von Änderungsbelegen	593
19.2.9 Logging des SAProuter	593
19.2.10 Audit Trail für SAP HANA	594
19.2.11 SAP Audit Log für die SAP BTP	595

- 19.3 Microsoft Sentinel als SIEM für SAP-Systeme** 595
 - 19.3.1 Anatomie der Regeln zur Erkennung von Angriffen 600
 - 19.3.2 Beispiel für eine Regeldefinition 603
 - 19.3.3 Investigation und Forensik 607
 - 19.3.4 Threat Hunting: auf der Suche nach dem Fuchs im Hühnerstall 610
 - 19.3.5 Mit Playbooks automatisieren 613
- 19.4 Auf Angriffe reagieren – manuell oder automatisch?** 617
- 19.5 Praxisbeispiele von Angriffen** 618
 - 19.5.1 Datendiebstahl vor dem Jobwechsel 619
 - 19.5.2 Ein Administrator, der nur helfen wollte 620
- 19.6 Alternative SIEM-Lösungen für SAP-Systeme** 621

- Das Autorenteam 625
- Index 627