Cloud Security in der Praxis

Leitfaden für sicheres Softwaredesign und Deployment

DAS INHALTS-VERZEICHNIS

Inhalt

Einleitung **11**

1 Prinzipien und Konzepte **15**
Least Privilege 16
Defense in Depth 16
Zero Trust 17
Threat Actors, Diagramme und Trust Boundaries 18
Delivery-Modelle für Cloud-Services 22
Das Cloud Shared Responsibility Model 22
Risikomanagement 26
Zusammenfassung 27
Übungen 29

2 Schutz und Management von Data Assets **31**
Identifizieren und Klassifizieren von Daten 31
Beispiele für Stufen der Datenklassifikation 32
Relevante Anforderungen aus Gesetzen oder aus Branchenvorgaben 34
Data Asset Management in der Cloud 35
Cloud-Ressourcen taggen 36
Daten in der Cloud schützen 38
Tokenisieren 38
Verschlüsselung 38
Zusammenfassung 46
Übungen 47

3 Schutz und Management von Cloud Assets **49**
Unterschiede zur klassischen IT 49
Arten von Cloud Assets 50
Compute Assets 51
Storage Assets 57

Network Assets . . . 62
Asset Management Pipeline . . . 63
Beschaffungslecks . . . 64
Verarbeitungslecks . . . 65
Tool-Lecks . . . 66
Erkenntnislecks . . . 66
Cloud Assets taggen . . . 67
Zusammenfassung . . . 68
Übungen . . . 69

4 Identity and Access Management . . . 71
Unterschiede zu klassischer IT . . . 73
Lebenszyklus von Identität und Zugriff . . . 74
Anforderung . . . 76
Genehmigen . . . 76
Erzeugen, löschen, zuweisen oder zurückziehen . . . 77
Authentifizierung . . . 77
Cloud IAM Identities . . . 78
Business-to-Consumer und Business-to-Employee . . . 78
Multifaktor-Authentifizierung . . . 79
Passwörter, Passphrasen und API-Schlüssel . . . 83
Shared IDs . . . 85
Federated Identity . . . 85
Single Sign-On . . . 86
Instanz-Metadaten und Identitätsdokumente . . . 88
Secrets Management . . . 90
Autorisierung . . . 94
Zentrale Autorisation . . . 95
Rollen . . . 96
Revalidieren . . . 97
Bringen wir alles in der Beispielanwendung zusammen . . . 99
Zusammenfassung . . . 101
Übungen . . . 103

5 Vulnerability Management . . . 105
Unterschiede zu klassischer IT . . . 106
Verletzliche Bereiche . . . 108
Datenzugriff . . . 109
Anwendung . . . 109
Middleware . . . 112
Betriebssystem . . . 113
Netzwerk . . . 114
Virtualisierte Infrastruktur . . . 114
Physische Infrastruktur . . . 114

Schwachstellen finden und beheben 115
Network Vulnerability Scanner 116
Agentenlose Scanner und Configuration Management Systems 118
Agentenbasierte Scanner und Configuration Management Systems 119
Cloud Workload Protection Platforms 121
Containerscanner 121
Dynamic Application Scanner (DAST) 122
Static Application Scanner (SAST) 123
Software Composition Analysis Tools (SCA) 123
Interactive Application Scanner (IAST) 124
Runtime Application Self-Protection Scanner (RASP) 124
Manuelle Code-Reviews 124
Penetration Tests 125
User Reports 126
Beispieltools für das Vulnerability und Configuration Management 127
Risikomanagementprozess 129
Metriken beim Vulnerability Management 130
Tool Coverage 130
Mean Time to Remediate 131
Systeme/Anwendungen mit offenen Schwachstellen 131
Anteil der Falsch-Positiven 132
Anteil der Falsch-Negativen 132
Vulnerability Recurrence Rate 132
Change Management 133
Bringen wir alles in der Beispielanwendung zusammen 134
Zusammenfassung 137
Übungen 138

6 Netzwerksicherheit 141
Unterschiede zu klassischer IT 141
Konzepte und Definitionen 143
Zero Trust Networking 143
Allowlists und Denylists 143
DMZs 145
Proxies 145
Software-Defined Networking 146
Network Functions Virtualization 146
Overlay Networks und Kapselung 146
Virtual Private Clouds 147
Network Address Translation 148
IPv6 149

Netzwerkverteidigung bei der Beispielanwendung 150
Verschlüsselung auf dem Transportweg 151
Firewalls und Netzwerksegmentierung 154
Administrativen Zugriff erlauben 161
Network Defense Tools 165
Egress-Filter 169
Data Loss Prevention 172
Zusammenfassung 173
Übungen 174

7 Erkennen, reagieren und wiederherstellen 177
Unterschiede zur klassischen IT 178
Was soll überwacht werden? 179
Zugriff privilegierter User 181
Logs aus Verteidigungstools 183
Logs und Metriken von Cloud-Services 187
Logs und Metriken von Betriebssystemen 188
Middleware-Logs 188
Secrets-Server 189
Ihre Anwendung 189
Wie soll überwacht werden? 190
Aggregation und Aufbewahrung 190
Logs parsen 191
Suchen und korrelieren 192
Alerting und automatisierte Response 193
Security Information and Event Managers 194
Threat Hunting 196
Auf einen Vorfall vorbereiten 196
Team 197
Pläne 198
Tools 200
Auf einen Vorfall reagieren 201
Cyber Kill Chains und MITRE ATT&CK 202
Die OODA-Schleife 203
Cloud-Forensik 205
Unautorisierten Zugriff blockieren 205
Datenabzug und Command and Control stoppen 206
Wiederherstellen 206
IT-Systeme erneut deployen 206
Benachrichtigungen 207
Lessons Learned 207
Beispielmetriken 207

Toolbeispiele für Erkennung, Reaktion und Wiederherstellung 208
Erkennung und Reaktion in einer Beispielanwendung 209
Die Schutzsysteme überwachen 210
Die Anwendung überwachen 211
Das Administrationsteam monitoren 212
Die Audit-Infrastruktur verstehen 212
Zusammenfassung 213
Übungen 215

Anhang: Lösungen zu den Übungen 217

Index 223