# Inhaltsverzeichnis

**Teil I Einführung in das Sealed Cloud-Computing**

**1 Herausforderung Datenschutz und Datensicherheit in der Cloud** ..... 3
Hubert A. Jäger, Ralf O. G. Rieken und Edmund Ernst

1.1 Cloud-Computing als Datenverarbeitung im Auftrag ..... 3
1.1.1 Beteiligte und Schutzziele ..... 4
1.1.2 Das rechtliche Konstrukt der Auftragsverarbeitung ..... 8
1.2 Zertifizierung von Cloud-Diensten ..... 10
1.2.1 Auftraggeber und Nutzer einer Zertifizierung ..... 10
1.2.2 Parameter der Vertrauenswürdigkeit einer Zertifizierung ..... 12
1.2.3 Das Problem der Erschwinglichkeit ..... 14
1.3 Die Herausforderung der Insider-Attacken ..... 15
1.3.1 Das Vertrauens-Dilemma ..... 15
1.3.2 Vermeintliche Lösung: Ende-zu-Ende-Verschlüsselung ..... 18
1.3.3 Definition der Betreiber- bzw. Manipulationssicherheit ..... 19
1.4 Sicherheits- und Datenschutzanforderungen im Cloud-Computing ..... 20
1.4.1 Bestehende Kataloge ..... 21
1.4.2 Weitere Anforderungen für eine nachhaltige Digitalisierung ..... 25
Literatur ..... 30

**2 Grundprinzip der Sealed Cloud** ..... 33
Hubert A. Jäger, Ralf O. G. Rieken, Edmund Ernst, Arnold Monitzer, Dau Khiem Nguyen, Jaymin Modi, Sibi Antony, Christos Karatzas, Franz Stark, Jaro Fietz und Lamya Abdullah

2.1 Überblick ..... 33
2.2 Data Clean-up ..... 39
2.2.1 Physikalische und logische Kapselung ..... 39
2.2.2 Der Mechanismus der vorsorglichen Datenlöschung ..... 42
2.2.3 Robustheit gegen Manipulation oder Ausfälle ..... 45



Bibliografische Informationen
http://d-nb.info/1216394156

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

2.3 Schlüsselverteilung ..... 47
2.3.1 Auf die Verteilung der Schlüsssel kommt es an ..... 48
2.3.2 Schlüsselerzeugung und -verwahrung ..... 49
2.3.3 Robuste Gestaltung der Schlüsselverfügbarkeit ..... 51
2.3.4 Gezielte Schlüsselvernichtung ..... 52
2.4 Wartung über gefilterte Schnittstellen ..... 55
2.4.1 Versiegelte und unversiegelte Betriebszustände ..... 55
2.4.2 Zugänge im versiegelten Zustand ..... 57
2.5 Sicherung der Integrität der Sealed Cloud ..... 60
2.5.1 Initialisierungs-, Audit und Versiegelungsprozesse ..... 61
2.5.2 Überprüfung der Softwareintegrität beim Boot ..... 66
2.5.3 Produktion vertrauenswürdiger Software ..... 69
2.6 Verzahnung der Maßnahmenpakete ..... 72
2.7 Alternative & ergänzende Ansätze für Sealed Computing ..... 74
Literatur ..... 78

**Teil II Sicherheit im Cloud-Computing**

**3 Grundsätzliches zu Sicherheit und Datenschutz** ..... 83
Hubert A. Jäger, Ralf O. G. Rieken, Edmund Ernst, Arnold Monitzer, Claudia Seidl, Wilhelm Würmseer und Daniel Kammerer

3.1 Was steckt hinter dem Begriff Sicherheit? ..... 83
3.1.1 Der junge Begriff des Datenschutzes ..... 84
3.1.2 Datenschutz als Antagonist der Sicherheit ..... 87
3.1.3 Wir sagen Sicherheit und meinen Freiheit von Angst ..... 89
3.2 Grundsätzliche technische Optionen für Sicherheit ..... 91
3.2.1 Hohe Barrieren ..... 92
3.2.2 Tarnen und Täuschen ..... 93
3.2.3 Überwachung ..... 94
3.2.4 Modularisierung und Automatisierung ..... 94
3.3 Grundsätzliche organisatorische Optionen für Sicherheit ..... 95
3.3.1 Strafandrohung ..... 96
3.3.2 Sorgfalt und Rechenschaftspflicht ..... 96
3.3.3 Gewaltenteilung ..... 97
3.4 Grundsätze sicherheitstechnischer Gestaltung ..... 99
3.4.1 Privacy & Security by Design ..... 99
3.4.2 Fehlertolerantes Design & Privacy by Default ..... 100
3.4.3 Stand der Technik nutzen ..... 101
3.5 Zusammenwirken mehrerer Maßnahmen in Prozessen ..... 108
3.5.1 Kombination mehrerer Maßnahmen ..... 108
3.5.2 Dynamische Abläufe ..... 110

3.6 Das Dilemma des Verteidigers ... 111
3.6.1 Sicherheit kann nicht bewiesen werden ... 111
3.6.2 Komplexität zwingt zur Kooperation ... 111
3.6.3 Psychologische und soziologische Aspekte des Vertrauens ... 113
3.7 Vertrauensmodelle ... 115
3.7.1 Idealisierende Modelle ... 115
3.7.2 Holistische Modelle/Zero-Trust-Modelle ... 117
Literatur ... 118

**4 Modellierung der Sicherheit im Cloud-Computing** ... 121
Hubert A. Jäger, Ralf O. G. Rieken, Edmund Ernst und Jaro Fietz

4.1 Grundwerte der Informationssicherheit ... 121
4.1.1 Gängige Modellierung der Verfügbarkeit ... 123
4.1.2 Probabilistische Modellierung der Vertraulichkeit ... 124
4.2 Definition der ideal sicheren Cloud ... 125
4.3 Modellierung der möglichen Angriffe ... 126
4.3.1 Angriffsbäume ... 126
4.3.2 Der ideale Angreifer ... 127
4.3.3 Modellierung der Erfolgswahrscheinlichkeit des Angriffs ... 128
4.4 Der Angriffsbaum beim Cloud-Computing ... 130
4.4.1 Überblick ... 130
4.4.2 Angriffe von außen ... 131
4.4.3 Angriffe von innen ... 142
4.4.4 Angriffe über Zulieferkomponenten ... 149
4.4.5 Angriffe durch staatliche Akteure ... 153
4.4.6 Andere Angriffe (gegen die Verfügbarkeit) ... 155
4.5 Einfluss des menschlichen Verhaltens ... 156
4.5.1 Nutzersorgfalt und benutzerfreundliche Sicherheit ... 157
4.5.2 Loyalität der Mitarbeiter des Cloud-Dienstes ... 158
4.5.3 Sorgfalt und Whistleblowing bei Anbietern & Lieferanten ... 159
4.6 Anlaysemöglichkeiten durch das probabilistische Modell ... 160
4.6.1 Schwachstellen- und Sensitivitätsanalyse ... 161
4.6.2 Systemvergleiche ... 162
Literatur ... 165

**5 Wie viel Sicherheit ist genug?** ... 167
Hubert A. Jäger, Ralf O. G. Rieken und Arnold Monitzer

5.1 Der Begriff der Datensouveränität ... 167
5.1.1 Vernetzung mit Lieferanten, Kunden und Mitbewerbern ... 168
5.1.2 Der Begriff der Usage Control ... 169
5.1.3 Datenschutzkonforme Data Economy ... 174

5.2 Die Technologiedividende ..... 175
5.3 Der Trend zu Sealed/Confidential Computing ..... 177
5.4 Kriterien für die Anwendungen von Sealed Cloud ..... 179
5.4.1 Kriterien der Compliance ..... 179
5.4.2 Wirtschaftliche Kriterien ..... 180
5.4.3 Mögliche Kontraindikationen ..... 181
5.5 Einbettung der Sealed Cloud in Multi-Cloud-Strategien ..... 181
5.5.1 Versiegelte Anonymisierung – unversiegelte Analyse ..... 182
5.5.2 Organisationsverschulden mit Schutzspektrum vermeiden ..... 184
Literatur ..... 185

**Teil III Sealed Cloud Anwendungen**

**6 Vertraulicher Datenaustausch** ..... 189
Ralf O. G. Rieken, Hubert A. Jäger, Ansgar Dirkmann und Lars Iclodean

6.1 Anwendungen für firmenübergreifenden Datenaustausch ..... 189
6.2 Zusammenarbeit im Team ..... 191
6.2.1 Herkömmliche Realisierung mit Verschlüsselung ..... 192
6.2.2 Realisierung mit Verschlüsselung und Versiegelung ..... 193
6.2.3 Komfortvorteile resultierend aus Versiegelung ..... 194
6.2.4 Sicherheitsvorteile resultierend aus Versiegelung ..... 195
6.3 Maschine-zu-Maschine-Kommunikation – M2M ..... 196
6.3.1 Kommunikationswege für M2M ..... 196
6.3.2 Anforderungen an ein geeignetes Kommunikationssystem ..... 197
6.3.3 Virtuelle industrielle Datenräume in einer Sealed Cloud ..... 199
Literatur ..... 200

**7 Verwaltung von sensiblen Daten** ..... 201
Ralf O. G. Rieken, Hubert A. Jäger und Sibi Antony

7.1 Speicherung sensibler Daten und Datenschutz ..... 201
7.1.1 Daten für forensische Analysen nach Hackerangriffen ..... 202
7.1.2 Videoüberwachung im öffentlichen Raum ..... 202
7.1.3 Speicherung von Kommunikationsverbindungsdaten ..... 203
7.1.4 Journale zur Tätigkeit privilegierter Administratoren ..... 203
7.1.5 Daten zur Analyse von Compliance-Situationen ..... 203
7.1.6 Was ist allen Beispielen gemeinsam? ..... 203
7.2 Wann sind Daten tatsächlich gespeichert? ..... 204
7.2.1 Klassisches Verständnis des Begriffs „Speichern“ ..... 204
7.2.2 Speichern als zweistufiger Prozess ..... 205
7.2.3 Einfrieren von Daten ..... 205
7.2.4 Auftauen von Daten ..... 205

7.3 Beispiel: Datenschutzgerechte Verwaltung von Data Lakes ..... 206
7.4 Produktives Beispiel: Vorratsdatenspeicherung von Verkehrsdaten ..... 208
7.5 Anlassbezogene Videos ..... 208
Literatur ..... 209

**8 Sealed Computing für allgemeine Anwendungen** ..... 211
Ralf O. G. Rieken, Hubert A. Jäger und Christos Karatzas

8.1 Datenschutzgerechte Analyse von Daten ..... 211
8.1.1 Anwendungsbeispiel: Versicherungen ..... 212
8.1.2 Herausforderung Datenschutz ..... 213
8.1.3 Komplikation ..... 213
8.1.4 Lösung – Grundgedanke ..... 213
8.1.5 Versiegelte Speicherung der Ursprungsdaten ..... 214
8.1.6 Technisch hart codierte Regeln zum Lesen ..... 214
8.1.7 Versiegelte Analyse ohne Personenbezug ..... 215
8.2 Eine versiegelte Plattform für allgemeine Anwendungen ..... 215
8.2.1 Überblick Sealed Platform ..... 217
8.2.2 Komponenten und deren Funktionen ..... 218
8.2.3 Deployment von Anwendungen auf der Sealed Platform ..... 220
8.2.4 Administration der Sealed Platform ..... 223
8.2.5 Schutzgüten für Anwendungen ..... 224
Literatur ..... 225

**Anhang A: Hintergründe und Beispiele zur Modellierung von Cloud-Sicherheit** ..... 227

**Glossar** ..... 233

**Stichwortverzeichnis** ..... 239