
Inhaltsverzeichnis

1	Künstliche Intelligenz – gekommen, um zu bleiben	1
1.1	Herausforderungen vertrauenswürdiger KI	4
1.2	Ziel und Eingrenzung des Buches	5
1.3	Inhaltlicher Aufbau	7
2	Grundlagen der Vertrauenswürdigkeit von KI	9
2.1	Geltungsbereich für die Betrachtung der Vertrauenswürdigkeit	16
2.2	Dimensionen der Vertrauenswürdigkeit	22
2.3	Differenzierung von KI-Eigenschaften zu OT und IT	27
2.4	KI Governance Modelle	30
3	Risiken von KI	33
3.1	Sicherheitsbetrachtung Klassische KI vs. Foundation Modelle	33
3.2	Bewertung der Vertrauenswürdigkeit von KI-Anwendungen	35
3.3	Risikotaxonomie von KI	38
3.4	Produkt- und Organisations-Perspektive	41
4	Überblick über laufende KI-Regulierungsinitiativen	49
4.1	Internationale Initiativen	49
4.2	Europäische Initiativen	54
4.3	Nationale Initiativen	60
4.4	Ein Vergleich mit den USA	67
5	Gesetzliche Vorgaben in der EU	75
5.1	EU AI Act	76
5.1.1	Risikoklassen und Transparenzpflichten für GPAI	81
5.1.2	Rollen entlang der KI-Wertschöpfungskette	86
5.1.3	Europäische KI-Governance Struktur und AI Office	87
5.1.4	Erste Schritte für Unternehmen zur AI Act Compliance	88
5.2	Weitere KI relevante Gesetze	90

6	KI-Standards und -Frameworks	99
6.1	Systematik	100
6.2	ISO-Standards	104
6.3	Europäische Frameworks der ENISA und ETSI	107
6.4	Das Framework for AI Cybersecurity Practices	110
6.5	Weitere Frameworks und Best Practices	115
7	Das Zusammenspiel von KI und IT-Security	131
7.1	Cybersecurity of AI – IT-Sicherheit für KI	132
7.2	Cybersecurity by AI – IT-Sicherheit durch KI	139
7.3	AI in Cybersecurity – Angriffe durch KI	143
7.4	Umsetzung einer KI-Initiative in der CISO-Organisation	146
8	Best Practices – Ein Leitfaden zur KI-Governance	151
8.1	Strategie und Ziele	153
8.2	Organisation	164
8.3	Use Case und Lifecycle Management	177
8.4	Konformität	182
9	Vorschläge für KI-Regulierungsansätze des BSI	185
9.1	KI-Sicherheit im BIS-IT-Grundschutz	187
9.1.1	KI-Grundschutzbausteine	188
9.1.2	Neuer BSI-Standard 200-5	191
9.2	Personenzertifizierung für KI	191
10	Sektorspezifische Betrachtung von KI-Sicherheit	197
10.1	Financial Services	200
10.2	Insurance	203
10.3	Public Sector	204
10.4	Automotive	208
10.5	Healthcare	210
10.6	Energy	214
11	Synthese	217
11.1	Zusammenfassung	217
11.2	Diskussion und kritische Reflektion	220
11.3	Ausblick und weiterführende Arbeiten	223

Anlage 1: KI-Regulierungsinitiativen (Auszug)	227
Anlage 2: LLM Security Checkliste	241
Anlage 3: KI-Security-Risiken über den KI-Lebenszyklus	247
Anlage 4: Auswirkungen von KI auf die Informationssicherheit.	255
Anlage 5: KI-Anwendungen in der Cloud-Sicherheit	257
Anlage 6: KI-Anwendungen im GRC	259
Anlage 7: KI-Anwendungen in SOC's	261
Anlage 8: KI-Start-Checkliste	263
Anlage 9: KI-Vertrauens-Checkliste	265
Literatur.	267