

Inhaltsverzeichnis

Abkürzungsverzeichnis	XVII
1. Einleitung	2
1.1. Einbettung der Arbeit	2
1.2. Herleitung der Fragestellung	4
1.3. Bisherige Bearbeitung	6
1.4. Methode	6
1.5. Übersicht	7
2. Industrielle Revolutionen	9
3. Digitalisierung	14
3.1. Informationstechnologie und Informationstechnik	15
3.2. Computer und Netzwerke	15
3.3. Das Internet: Ein Fundament mit Schwächen	19
3.4. Ubiquitäres Computern	20
3.5. Internet of Things	21
3.6. Industrial Internet of Things	23
4. Industrie 4.0: Sicherungsgegenstand und Schadenspotential	25
4.1. Vierte industrielle Revolution: Industrie 4.0?	26
4.2. Automatisierung und Digitalisierung der Produktion als Dogma einer Industrie 4.0	28
4.3. Das Aufbrechen hierarchisch gesteuerter Automatisierung	29
4.3.1. Die Automatisierungspyramide	30
4.3.1.1. Das Enterprise Resource Planning System (ERP), Produktionsplanung und -steuerung (PPS) und Advanced Planning and Scheduling (APS)	32
4.3.1.2. Das Manufacturing Execution System (MES)	33
4.3.1.3. Cyber Physical Systems (CPS)	34
4.3.1.3.1. CPS und Kognition	36
4.3.1.3.2. CPS und künstliche Intelligenz	36
4.3.1.3.3. Künstliche Intelligenz im Kontext von Varianz, Virtualisierung und Simulation für die Produktion der Industrie 4.0	37
4.3.1.4. Bedeutung der zentralen Systeme	39
4.3.2. Die Durchbrechung der Automatisierungspyramide: Die Ablösung tradierter Informationsflüsse	41
4.4. Neue Dienste, neue Anwendungsfelder	42
4.5. Big Data (Massendatenverarbeitung)	44
4.6. Macht, Industrie, Daten und die besondere Rolle Chinas im IoT	46

4.6.1. Einhegung durch Märkte	47
4.6.2. Konfliktpotenzial	48
4.6.3. Konzernmacht (Abhängigkeit von Infrastruktur, Know-How)	50
4.7. Verletzlichkeit der Datenverarbeitung	53
4.8. Bedeutung der Sicherheitsmechanismen in der Industrie 4.0	57
5. Potentielle Angreifer	61
5.1. (Fremd-)Staatliche Akteure	62
5.1.1. Geostrategische Lage	62
5.1.2. Militär	67
5.1.3. Nachrichtendienste	69
5.1.4. Anbieter von Spionagesoftware	71
5.2. Nichtstaatliche Akteure	72
5.2.1. Konkurrenten	72
5.2.2. „Skript Kiddies“	73
5.2.3. Professionelle Angreifer und Angriffsdienste	74
5.2.4. Überwachungs- und Auswertungsdienste	79
5.2.5. Arbeitgeber	81
5.3. Fazit	82
6. Schutzaufgaben	83
6.1. Allgemein	83
6.2. Technische Sicherheit	84
6.3. Sicherheit durch den Staat	86
6.3.1. Theoretische und ideengeschichtliche Vorlagen staatlicher Sicherheit (Staatszweck)	86
6.3.1.1. Hobbes: Staatszweck Gewaltmonopol und Sicherheit	87
6.3.1.2. Locke: Staatszweck Freiheit vor dem Staat und Schutz des Eigentums	88
6.3.1.3. Rousseau: Staatszweck Freiheit und Widerstandspflicht	89
6.3.1.4. Kant: Freiheit als Staatszweck und Sicherheit als Mittel dazu	90
6.3.1.5. Fazit: Staatszweck Sicherheit für Freiheit und Freiheit durch Sicherheit	90
6.3.2. Verortung von Sicherheit im modernen Verfassungsstaat	91
6.3.2.1. Staatsaufgaben	92
6.3.2.2. Staatsziele	93
6.3.2.3. Strukturprinzipien	97
6.3.2.4. Grundrechte	97
6.3.2.4.1. Beschränktes Gewaltmonopol des Staates durch Grundrechtsvorrang	99
6.3.2.4.2. Sicherheit und Sicherheitsfacetten	100

6.3.2.4.3. Schutzpflichten.....	103
6.3.3. Sicherheit und Freiheit in der Informationsgesellschaft	108
6.4. Industrie 4.0-Perspektive der IT-Sicherheit	111
6.5. IT-Sicherheit durch den Staat?	112
6.5.1. Das „Computergrundrecht“ oder das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“	113
6.5.2. IT-Sicherheitslücken	115
6.5.3. Einfachgesetzliche Ausprägungen der IT-Sicherheit	116
6.6. Freiheitsschutz.....	120
6.6.1. Menschenwürde	121
6.6.2. Die freie Entfaltung der Persönlichkeit	121
6.6.3. Die informationelle Selbstbestimmung	122
6.6.4. Datenschutz und einfachgesetzliche Ausprägungen des Schutzes personenbezogener Daten	125
7. IT-Sicherheit für ein Industrie 4.0-Szenario.....	128
7.1. Kundenindividuelle Produktion: Sichere Prozesse	129
7.1.1. Produktentstehung.....	129
7.1.2. Produktionsplanung.....	130
7.1.3. Produktion	133
7.1.4. Service.....	135
7.2. Fernwartung von Produktionsanlagen: Sichere Dienste	136
7.3. Technologiedatenmarktplatz: Sichere Daten	137
7.4. Visueller Security-Leitstand: Sichere Vernetzung.....	139
8. IT-Sicherheitsmaßnahmen und Datenschutz in Industrie 4.0	141
8.1. Konkordanz durch Technikgestaltung	141
8.2. Methode KORA: Konkretisierung rechtlicher Anforderungen.....	142
8.3. Relevanz der nationalen und unionalen Grundrechte.....	143
9. Verfassungsrechtliche Vorgaben	148
9.1. Fundament und vitale Voraussetzung zur Grundrechtswahrnehmung	148
9.1.1. Die Würde des Menschen	148
9.1.2. Recht auf Leben (geistige) und körperliche Unversehrtheit	149
9.2. Beruf, Unternehmen und Eigentum	150
9.2.1. Beruf und Unternehmen.....	150
9.2.2. Eigentum	154
9.3. Rechtsgrundsätze und Rechtsdurchsetzung.....	158
9.3.1. Gleichheit vor dem Gesetz	158

9.3.2 Zugang zu den Gerichten und effektiver Rechtsschutz.....	159
9.3.3. Rechtliches Gehör	161
9.3.4 Verhältnismäßige Beschränkungen von Grundrechten.....	162
9.4. Selbstbestimmter (und fernvermittelter) Informationsumgang.....	163
9.4.1. Informationelle Selbstbestimmung und (Fern-)Kommunikation.....	164
9.4.2. Schutz der Integrität und Vertraulichkeit informationstechnischer Systeme.....	170
9.5 Chancen und Risiken für die verfassungsrechtlichen Vorgaben.....	172
9.5.1. Chancen einer it-sicheren Industrie 4.0.....	173
9.5.1.1. Fundament und vitale Voraussetzungen zur Grundrechtswahrnehmung.....	173
9.5.1.2. Beruf, Unternehmen und Eigentum	175
9.5.1.3. Rechtsgrundsätze und Rechtsdurchsetzung	179
9.5.1.4. Selbstbestimmter (und fernvermittelter) Informationsumgang.....	181
9.5.2. Risiken einer it-sicheren Industrie 4.0.....	182
9.5.2.1. Fundament und vitale Voraussetzungen zur Grundrechtswahrnehmung.....	183
9.5.2.2. Beruf, Unternehmen und Eigentum	186
9.5.2.3. Rechtsgrundsätze und Rechtsdurchsetzung	190
9.5.2.4. Selbstbestimmter (und fernvermittelter) Informationsumgang.....	191
10. Anforderungen	203
10.1. A1 Fernmeldegeheimnis.....	203
10.2. A2 Geheimnisschutz	204
10.3. A3 Datenschutz	206
10.4. A4 Schutz der Produktions- und Arbeitsmittel	206
10.5. A5 Rechtssicherheit.....	207
10.6. A6 Mitbestimmung	208
11. Kriterien	209
11.1. K1 Technik- und Organisationssicherheit.....	210
11.2. K2 Vertraulichkeit.....	214
11.3. K3 Integrität	220
11.4. K4 Verfügbarkeit.....	223
11.5. K5 Zurechnung.....	224
11.6. K6 Zweckbindung	228
11.7. K7 Beweisbarkeit	231
11.8. K8 Erforderlichkeit	236
11.9. K9 Transparenz	238
11.10. K10 Souveränität.....	241

11.11. K11 (Nicht-)Verkettbarkeit	244
12. Technische Gestaltungsziele	247
12.1. Z1 Stand der Technik	247
12.2. Z2 Konfiguration und Updatefähigkeit (Systeme)	248
12.3. Z3 Sichere Identitäten	249
12.4. Z4 Sichere Identifizierung und Authentisierung	250
12.5. Z5 Sicheres Identitätsmanagement	252
12.6. Z6 Kryptographieeinsatz	253
12.7. Z7 Vertraulichkeitsschutz	253
12.8. Z8 Integritätsschutz	254
12.9. Z9 Aufbau einer Sicherheitsinfrastruktur	255
12.10. Z10 Rollen- und Rechtevergabe (Daten/Systeme)	256
12.11. Z11 Sicherer Zutritt und Zugang (Daten/Systeme)	256
12.12. Z12 sicherer Zugriff (Daten/Systeme)	257
12.13. Z13 Sicherheits- und Vertrauensanker (Daten/Systeme)	258
12.14. Z14 sicheres Dokumentieren (Daten/Systeme)	259
12.15. Z15 Systeme mit Minimalfunktionalität (Systeme)	259
12.16. Z16 Modularer, strukturierter und nachvollziehbarer Aufbau (Daten/System)	260
12.17. Z17 Exportmöglichkeiten / Schnittstellen (Systeme)	261
12.18. Z18 Anonyme Datenverarbeitung (Daten)	261
12.19. Z19 Pseudonyme Datenverarbeitung (Daten)	262
12.20. Z20 Beherrschbarkeit	264
12.21. Z21 Quelloffene Soft- und Hardware (Daten/Systeme)	265
12.22. Z22 Offene Standards (Daten)	266
12.23. Z23 Datenvermeidende und datensparsame Designs (Daten)	266
12.24. Z24 Löschen von Daten (Daten)	266
12.25. Z25 Datenschutzmanagement	267
12.26. Z26 IT-Sicherheitsmanagement	268
12.27. Z27 Auditier- und Revisionsfähigkeit (Systeme/Daten)	269
12.28. Z28 Resilienz	269
12.29. Z29 Anomalieerkennung	272
12.30. Z30 Trennung (Systeme/Daten)	273
13. Technische Gestaltungsvorschläge	275
13.1. Basale Vorschläge	276
13.1.1. V1 Einhaltung des Stands der Technik durch Umsetzung aktueller und einschlägiger Normen und Standards	276

13.1.2. V2 Bedrohungs- und Risikomodellierung.....	278
13.1.3. V3 Up-to-Date-Halten.....	280
13.1.4. V4 Nutzbarmachen von Open Source-Lösungen.....	280
13.1.5. V5 Nutzbarmachen von offenen Standards.....	281
13.1.6. V6 Separieren.....	282
13.1.7. V7 Regelmäßige Datensicherung.....	284
13.1.8. V8 Löschroutine.....	285
13.1.9. V9 Protokollierung.....	288
13.1.10. V10 Schulung.....	291
13.1.11. V11 Modularisierung.....	292
13.2. Vorschläge zur Implementierung von Elementen einer datenschutzgerechten IT-Sicherheitsinfrastruktur.....	293
13.2.1. V12 Implementierung identitätsbasierter Sicherheitsmechanismen und Identitätsmanagement.....	294
13.2.2. Vorüberlegungen zur weiteren Anknüpfung an die Identität.....	298
13.2.2.1. Umsetzung der Zugangs- und Zutritts- und Zugriffskontrolle.....	300
13.2.2.2. Umsetzung des Identity- und Accessmanagements.....	302
13.2.2.3. Pseudonymisierung und Anonymisierung.....	305
13.2.3. V13 Kryptographische Anwendungen.....	309
13.2.3.1. Vertrauliche Speicherung und Kommunikation durch Verschlüsselung.....	309
13.2.3.2. Verbindliche Zuordnung, Integrität sowie Authentizität durch Signaturen.....	311
13.2.3.3. Asymmetrische Kryptosysteme.....	314
13.2.3.3.1. Elemente.....	314
13.2.3.3.2. Schlüsselmanagement.....	315
13.2.3.3.3. Kryptographische Prämisse.....	316
13.2.4. V14 Aufbau initialer Systemsicherheit.....	317
13.2.5. V15 Ausgestaltung von Anomalieerkennungen und Abwehrmechanismen.....	321
13.3. Vorschläge zur dauerhaften Einhaltung und zum Nachweis von Datenschutz und IT-Sicherheit.....	324
13.3.1. V16 Implementierung eines Datenschutzmanagementsystems (DSM).....	324
13.3.2. V17 Implementierung eines Informationssicherheitsmanagements (ISM).....	329
13.3.3. V18 Nachweisen der datenschutz- und it-sicherheitsrechtlichen Maßnahmen.....	334
14. Schlussbetrachtung.....	338
15. Literaturverzeichnis.....	342