

Inhaltsübersicht

Abkürzungsverzeichnis.....	XVII
-----------------------------------	-------------

1 Einführung.....	1
1.1 Problemstellung	1
1.2 Zielsetzung	9
1.3 Gang der Untersuchung	11
2 Definitionen / Grundlagen.....	15
2.1 Unternehmen des Maschinen- und Anlagenbaus.....	15
2.2 Technik und Technologie	18
2.3 Innovation	21
2.4 Informationsabfluss durch Industriespionage	24
2.5 Dienstleistungen.....	32
3 Identifizierung von speziellen Risiken von E-Service- Angeboten.....	43
3.1 Besondere Merkmale der Konstellation	43
3.2 E-Services Wertschöpfungsketten	45
3.3 Modellierung des Geschäftsprozesses	52
3.4 Angriffe auf Unternehmensdaten in E-Service-Prozessen.....	68
3.5 Risiken im Bereich der technischen Sicherheit.....	75
3.6 Risiken im Bereich der organisatorischen Sicherheit.....	89
3.7 Risiko von Vertrauens- und Kontrollverlust	92
3.8 Zwischenergebnis	96
4 Schutzzumfang und Grenzen der normativen Regelungen zum Schutz von Unternehmensdaten	99
4.1 Subsidiarität rechtlicher Maßnahmen?.....	99
4.2 Schutz von Unternehmensdaten.....	104
4.3 Schutzlücken – Handlungsbedarfe - Fazit.....	246

5	Ansatzpunkte für präventive Schutzmaßnahmen.....	251
5.1	Ansatzpunkte für technischen Schutz und ihre Grenzen	252
5.2	Verzahnung von rechtlichen und technisch-organisatorischen Schutzmaßnahmen	275
5.3	Zwischenergebnis	311
6	Prozesssicherheit durch staatliches Handeln	315
6.1	Aufklärung.....	315
6.2	Normierung	316
6.3	Standardisierung	328
6.4	Zertifizierung	330
6.5	Zwischenergebnis	333
7	Fazit	337
7.1	Zusammenfassung der Arbeit.....	337
7.2	Ausblick und weiterer Handlungsbedarf	347
7.3	Schlusswort.....	348
	Literaturverzeichnis.....	351

Gliederung

Abkürzungsverzeichnis.....	XVII
----------------------------	------

1 Einführung.....	1
1.1 Problemstellung	1
1.2 Zielsetzung	9
1.3 Gang der Untersuchung	11
2 Definitionen / Grundlagen.....	15
2.1 Unternehmen des Maschinen- und Anlagenbaus	15
2.2 Technik und Technologie	18
2.3 Innovation	21
2.4 Informationsabfluss durch Industriespionage	24
2.4.1 Information	24
2.4.2 Wissen/ Know-how	26
2.4.3 Industriespionage/ Piraterie	29
2.5 Dienstleistungen.....	32
2.5.1 Stellenwert und Charakteristika	32
2.5.2 Rolle der IKT	36
2.5.3 Besonderheiten von E-Services	40
3 Identifizierung von speziellen Risiken von E-Service- Angeboten.....	43
3.1 Besondere Merkmale der Konstellation	43
3.2 E-Services Wertschöpfungsketten	45
3.3 Modellierung des Geschäftsprozesses	52
3.3.1 Methode	53
3.3.2 Notation	56
3.3.2.1 Standardnotation	57
3.3.2.2 Gantt-Diagramm	57
3.3.2.3 Ereignisgesteuerte Prozessketten (EPK)	58
3.3.2.4 Industrielles Service Blueprinting (ISB)	58
3.3.2.5 Business Process Modeling Notation (BPMN)	62
3.3.2.6 Bewertung	62

3.3.2.7	Beispielservice: vorbeugende Wartung und kontinuierliche Optimierung	64
3.3.2.8	Eignung für die Darstellung nicht-funktionaler Anforderungen	67
3.4	Angriffe auf Unternehmensdaten in E-Service-Prozessen	68
3.5	Risiken im Bereich der technischen Sicherheit	75
3.5.1	Angriffe auf die IT-Sicherheit	75
3.5.2	Schwachstellen Automatisierungstechnik und automatisierte Datenübertragung	85
3.6	Risiken im Bereich der organisatorischen Sicherheit	89
3.7	Risiko von Vertrauens- und Kontrollverlust	92
3.8	Zwischenergebnis	96
4	Schutzzumfang und Grenzen der normativen Regelungen zum Schutz von Unternehmensdaten	99
4.1	Subsidiarität rechtlicher Maßnahmen?	99
4.2	Schutz von Unternehmensdaten	104
4.2.1	Internationale und supranationale Regelungen	107
4.2.1.1	Europarecht	108
4.2.1.1.1	Europarat	108
4.2.1.1.2	EGMR	108
4.2.1.1.3	Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr	109
4.2.1.1.4	Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (2002/58/EG) – eCommerce-RL	110
4.2.1.1.5	Entwurf der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte	110

4.2.1.1.6	Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung	111
4.2.1.1.7	Datenschutzgrundverordnung (DSGVO)	113
4.2.1.2	OECD	114
4.2.1.3	Vereinte Nationen (UN)	115
4.2.1.4	WTO	115
4.2.1.5	Revidierte Berner Übereinkunft (RBÜ)	118
4.2.1.6	Welturheberrechtsabkommen (WUA)	120
4.2.1.7	WIPO Copyright Treaty (WCT)	120
4.2.2	Grundrechte	121
4.2.2.1	Fernmeldegeheimnis	121
4.2.2.2	Berufsfreiheit	128
4.2.2.3	Unverletzlichkeit der Wohnung	131
4.2.2.4	Eigentumsgarantie	132
4.2.2.5	Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	139
4.2.2.6	Informationelle Selbstbestimmung	145
4.2.2.7	Konkurrenzen	151
4.2.3	Anwendbares Datenschutzrecht	153
4.2.3.1	Bundesdatenschutzgesetz (BDSG)	162
4.2.3.2	Telekommunikationsgesetz (TKG)	163
4.2.3.3	Telemediengesetz (TMG)	165
4.2.3.4	Fazit zum Datenschutzrecht	166
4.2.4	Urheberrechtsgesetz (UrhG)	168
4.2.4.1	Schutz von Geschäftsprozessen	169
4.2.4.2	Schutz von Datenbanken	172
4.2.4.3	Fazit zum Urheberrechtsgesetz	183

4.2.5	Gesetz gegen unlauteren Wettbewerb (UWG)	184
4.2.5.1	Nachahmung unter Nutzung unredlich erlangter Kenntnisse oder Unterlagen - § 4 Nr. 9c UWG	186
4.2.5.2	Behinderung von Mitbewerbern - § 4 Nr. 10 UWG	189
4.2.5.3	Zu widerhandlung gegen eine gesetzliche Vorschrift - § 4 Nr. 11 UWG	193
4.2.5.3.1	§ 4 Nr. 11 UWG i. V. m. § 17 Abs. 2 Nr. 1 UWG - Betriebsspionage	193
4.2.5.3.2	§ 4 Nr. 11 UWG i. V. m. § 18 Abs. 1 UWG	197
4.2.5.4	Schutz unternehmerischer Leistung - §§ 1, 3 Abs. 1 UWG	199
4.2.5.5	Fazit zum UWG	203
4.2.6	BGB	203
4.2.6.1	Schutzrechte an Betriebs- und Servicedaten	204
4.2.6.1.1	Daten als eigentumsfähige Sachen	204
4.2.6.1.2	Zuordnung über das Eigentum am Trägermedium	206
4.2.6.1.3	Zuordnung von Daten wie im BDSG	207
4.2.6.1.4	Zuordnung nach dem Skripturakt - § 903 BGB analog	209
4.2.6.1.5	Abstrakte rechtliche Zuweisung über § 903 BGB analog	211
4.2.6.1.6	Verwertungsrecht des Datenerzeugers de lege ferenda	213
4.2.6.1.7	Fazit zur Zuweisung von Daten	216
4.2.6.2	Charakter von (Unternehmens-) Wissen	217
4.2.6.3	Ausgestaltung des Schutzes im BGB	221
4.2.6.3.1	§ 823 Abs. 1 BGB	221
4.2.6.3.2	§ 823 Abs. 2 BGB	225
4.2.6.3.3	§ 826 BGB	227
4.2.6.3.4	§ 812 BGB – Eingriffskondition	229
4.2.6.3.5	§ 687 Abs. 2 BGB – angemessene Eigengeschäftsführung	234

4.2.6.4	Ergebnis, Konkurrenzen und Verjährung	235
4.2.7	Strafrechtlicher Schutz.....	237
4.2.7.1	§ 202a StGB	238
4.2.7.2	§ 202b StGB	239
4.2.7.3	§ 303a StGB	239
4.2.7.4	§ 303b StGB	240
4.2.7.5	§ 263a StGB	241
4.2.7.6	§§ 17, 18 UWG	244
4.2.7.7	Ergebnis zum strafrechtlichen Schutz	245
4.3	Schutzlücken – Handlungsbedarfe - Fazit.....	246
5	Ansatzpunkte für präventive Schutzmaßnahmen	251
5.1	Ansatzpunkte für technischen Schutz und ihre Grenzen	252
5.1.1	Bereitstellung/ Vorhaltung von Servicedaten	253
5.1.1.1	Produktionsnetzwerk.....	253
5.1.1.2	Maschinensteuerung.....	255
5.1.1.3	Chip.....	255
5.1.1.4	Einplatinencomputer	256
5.1.1.5	Datenspeicherung in der Cloud	257
5.1.2	Schutz für gespeicherte Servicedaten	259
5.1.2.1	Verschlüsselung	259
5.1.2.2	Digitale Signaturen	262
5.1.2.3	Dongle/ Security-Token.....	263
5.1.2.4	Trusted Platform Module (TPM)	264
5.1.3	Schutz der Kommunikationswege	264
5.1.3.1	Techniker vor Ort	265
5.1.3.1.1	Kabelgebundener Zugriff.....	266
5.1.3.1.2	WLAN.....	266
5.1.3.1.3	RFID.....	267
5.1.3.2	Fernzugriff auf Daten	270
5.1.3.2.1	VPN.....	270
5.1.3.2.2	Cloud-basierte Fernwartung	271
5.1.3.3	Industrial Rights Management (IRM)	272
5.1.4	Grenzen technischer Lösungsansätze	273
5.2	Verzahnung von rechtlichen und technisch-organisatorischen Schutzmaßnahmen	275
5.2.1	Recht und Organisation	275

5.2.1.1	Zugangskontrolle zu Datenverarbeitungsanlagen	277
5.2.1.2	Zutrittskontrolle	278
5.2.1.3	Speicherkontrolle	279
5.2.1.4	Benutzerkontrolle	279
5.2.1.5	Zugriffskontrolle	279
5.2.1.6	Übermittlungskontrolle	279
5.2.1.7	Eingabekontrolle	281
5.2.1.8	Auftragskontrolle	281
5.2.1.9	Transportkontrolle	282
5.2.1.10	Verfügbarkeitskontrolle	282
5.2.1.11	Organisationskontrolle	283
5.2.2	Schutz im Produktionsnetzwerk	288
5.2.3	Bereitstellung in der Maschinensteuerung	291
5.2.4	Chip	303
5.2.5	Einplatinencomputer	305
5.2.6	Cloud	306
5.2.6.1	Speicherung von Daten	307
5.2.6.2	Cloud-basierte Fernwartung	308
5.2.7	IRM	309
5.3	Zwischenergebnis	311
6	Prozesssicherheit durch staatliches Handeln	315
6.1	Aufklärung	315
6.2	Normierung	316
6.2.1	IT-Sicherheitsgesetz	317
6.2.2	Anpassung des BGB	318
6.2.3	Anpassung des BDSG	321
6.2.4	Anlage zu § 9 Satz 1 BDSG als Leitbild für alle elektronisch ausgetauschten Daten	323
6.2.5	Patentierung von Service-Prozessen	325
6.3	Standardisierung	328
6.4	Zertifizierung	330
6.5	Zwischenergebnis	333

7	Fazit	337
7.1	Zusammenfassung der Arbeit	337
7.2	Ausblick und weiterer Handlungsbedarf	347
7.3	Schlusswort	348
	Literaturverzeichnis.....	351