

# Inhalt

1.	<b>Einführung</b>	7
2.	<b>Geschichte der Wirtschaftsspionage</b>	11
2.1	Industriespionage, wie es sie schon immer gab	11
2.2	Spionage gestern und heute	16
2.2.1	ICE contra TGV	18
2.2.2	Der Fall LÓPEZ	18
2.2.3	Geschmähtes Unternehmen ENERCON	19
2.2.4	Ha'efrati erschüttert die israelische Wirtschaft	19
2.2.5	Wuhan Lili bei VALEO	21
2.3	Abgrenzung Wirtschaftsspionage vs. Konkurrenzausspähung	22
2.4	Worüber die deutschen Geheimdienste ungen sprechen	25
3.	<b>Das Bedrohungsspektrum in Deutschland</b>	31
3.1	Ausländische Geheimdienste	33
3.1.1	USA	34
3.1.2	Russland	39
3.1.3	China	43
3.1.4	Sonstige	47
3.2	Illegale Praktiken der Konkurrenz	52
3.2.1	Fingierte Bewerbungsgespräche oder Scheinbewerber	53
3.2.2	Interne Mitarbeiterzeitschriften und vorgetäuschte Journalisten	55
3.2.3	Messen- und Veranstaltungen	58
3.2.4	Weitergabe vertraulicher Angebote durch Kunden und Lieferanten	60
3.3	Produktpiraterie	62
3.4	Bedrohung durch die Organisierte Kriminalität	64
3.5	Das Risiko der Expansion in neue Märkte	68
3.5.1	Informationsabfluss bei der Einreise	68
3.5.2	Das Risiko eines Parallelwerkes	70
3.5.3	Ausländische Mitarbeiter	72
3.5.4	Die dritte Schicht	74
3.5.5	Abfluss bei ausländischen Behörden	76
4.	<b>Industriespionage – ein unternehmerisches Risiko?</b>	79
4.1	Der Faktor Mensch, das größte Risiko	80
4.1.1	Interne Täter	82
4.1.2	Leichtfertigkeit und Angeberei	85

4.1.3	Wechsel von Mitarbeitern . . . . .	89
4.2	Social Engineering . . . . .	92
4.3	Umgang mit Daten und Informationen . . . . .	99
4.4	Anmeldung von Patenten . . . . .	107
4.5	Besondere Gefahren auf Geschäftsreisen im Ausland . . . . .	109
4.5.1	Socializing . . . . .	109
4.5.2	Vermeintlich freundliche Geschäftspartner . . . . .	111
4.5.3	Das Risiko Datenträger . . . . .	114
4.5.4	Kommunikation im Ausland . . . . .	117
4.5.5	Sicherheit im Hotel . . . . .	120
4.6	Risiken bei der Öffentlichkeitsarbeit . . . . .	122
<b>5.</b>	<b>Baulich organisatorische Schwachstellen</b> . . . . .	<b>127</b>
5.1	Objektsicherheit ist der einfachste Schutz vor Informationsverlust . . . . .	127
5.2	Die Zugangsmöglichkeiten ins Unternehmen . . . . .	130
5.3	Die Sicherung sensibler Bereiche . . . . .	131
5.4	Angriffe an der Außenhaut (HPM-Angriffe) . . . . .	132
5.5	Die Gefahr durch fremde Personen im Unternehmen . . . . .	134
5.6	Zutritts- bzw. Zugriffsberechtigungskonzepte . . . . .	135
<b>6.</b>	<b>Moderne Technik macht Vieles möglich</b> . . . . .	<b>139</b>
6.1	Die täglichen Fallen bei EDV und TK-Anlagen . . . . .	140
6.2	Wie leicht es ist, Datenspeicher und Protokolle auszulesen . . . . .	142
6.3	Key ghost/key logger . . . . .	144
6.4	Das Risiko von IP, WLAN, HotSpots und Bluetooth . . . . .	148
6.5	Service- und Supportverträge, Externe Zugänge . . . . .	151
6.6	Der Umgang mit Passwörtern . . . . .	154
<b>7.</b>	<b>Wenn der Ernstfall kommt, sollte man schnell handeln</b> . . . . .	<b>157</b>
7.1	Krisenmanagement oder die richtige Strategie . . . . .	158
7.2	Die Stunde der Security- und IT-Abteilungen . . . . .	162
7.3	Ermittlungen durch externe Spezialisten . . . . .	163
7.4	Sweep zum Auffinden von illegalen Abhöreinrichtungen . . . . .	165
<b>8.</b>	<b>Präventiver Ansatz für Informationsschutz</b> . . . . .	<b>173</b>
8.1	Risiko- und Schwachstellenanalyse . . . . .	173
8.2	Loyalität der Mitarbeiter schafft Sicherheit . . . . .	175
8.3	Beteiligung, Sensibilisierung und Vorbildfunktion . . . . .	178
8.4	Wichtige Regularien und Vorkehrungen . . . . .	181
8.5	Sicherheitsstrukturen im Unternehmen . . . . .	183
8.6	Informationsschutz auf Auslandsreisen . . . . .	184
	<b>Stichwortverzeichnis</b> . . . . .	<b>189</b>