

Dirk Fleischer

Wirtschaftsspionage

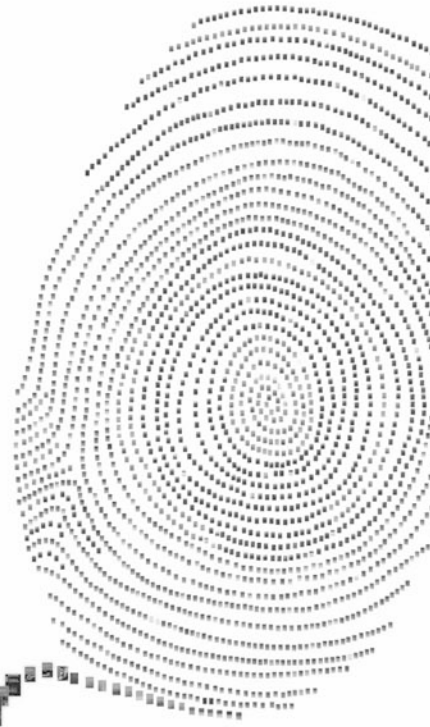
Phänomenologie – Erklärungsansätze –
Handlungsoptionen

Wirtschaftsspionage

Lizenz zum Wissen.




Sichern Sie sich umfassendes Technikwissen mit Sofortzugriff auf tausende Fachbücher und Fachzeitschriften aus den Bereichen: Automobiltechnik, Maschinenbau, Energie + Umwelt, E-Technik, Informatik + IT und Bauwesen.

Exklusiv für Leser von Springer-Fachbüchern: Testen Sie Springer für Professionals 30 Tage unverbindlich. Nutzen Sie dazu im Bestellverlauf Ihren persönlichen Aktionscode **C0005406** auf www.springerprofessional.de/buchaktion/



**Jetzt
30 Tage
testen!**

Springer für Professionals.
Digitale Fachbibliothek. Themen-Scout. Knowledge-Manager.

-  Zugriff auf tausende von Fachbüchern und Fachzeitschriften
-  Selektion, Komprimierung und Verknüpfung relevanter Themen durch Fachredaktionen
-  Tools zur persönlichen Wissensorganisation und Vernetzung

www.entschieden-intelligenter.de

Springer für Professionals

 Springer

Dirk Fleischer

Wirtschaftsspionage

Phänomenologie – Erklärungsansätze –
Handlungsoptionen

Dirk Fleischer
Schulzendorf, Deutschland

ISBN 978-3-658-11988-1 ISBN 978-3-658-11989-8 (eBook)
DOI 10.1007/978-3-658-11989-8

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Springer Vieweg

© Springer Fachmedien Wiesbaden 2016

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag, noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen.

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Vieweg ist Teil von Springer Nature

Die eingetragene Gesellschaft ist Springer Fachmedien Wiesbaden GmbH

*Danke für meine Arbeitsstelle,
danke für jedes kleine Glück.
Danke für alles Frohe, Helle und für die Musik.*

Kirchenlied von Martin Gotthard Schneider (1961)

Abkürzungsverzeichnis

a.a.O.	am angegebenen Ort
ADR	Accord européen relatif au transport international des marchandises Dangereuses par Route; Europäisches Übereinkommen über die internationale Beförderung gefährlicher Güter auf der Straße
AEO	Authorised Economic Operator
AG	Aktiengesellschaft
AktG	Aktiengesetz
ATZüV	Atomrechtliche Zuverlässigkeitsüberprüfungs-Verordnung
BAFIN	Bundesanstalt für die Finanzdienstleistungsaufsicht
BayObLG	Bayrisches Oberstes Landesgericht
BetrVG	Betriebsverfassungsgesetz
BfV	Bundesamt für Verfassungsschutz
BGH	Bundesgerichtshof
BilMoG	Bilanzrechtsmodernisierungsgesetz
BKA	Bundeskriminalamt
BReg.	Bundesregierung
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT	Bundestag
BV	Betriebsvereinbarung
CIA	Central Investigation Agency
CIFAS	Credit Industry Fraud Avoidance Service; heute bekannt als National Fraud Database
CSO	Chief Security Officer
d. h.	das heißt
Drs.	Drucksache
DV	Datenverarbeitung
DVD	Digital Video Disk
ebd.	ebenda

et al.	und andere
etc.	et cetera
f.	folgende
ff.	fortfolgende
GenG	Genossenschaftsgesetz
GmbHG	Gesetz betreffend der Gesellschaften mit beschränkter Haftung
GRUR	Gewerblicher Rechtsschutz und Unternehmensrecht
HDD	Hard Drive Disk (Festplatte)
HGB	Handelsgesetzbuch
Hrsg.	Herausgeber
i.e.S.	im engeren Sinn
i.S.d.	im Sinne des
i.Ü.	im Übrigen
i.W.	im Wesentlichen
i.w.S.	im weiteren Sinn
IT	Informationstechnologie
itS	Informationstechnisches System
KontraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KPMG	Klynveld, Peat, Marwick und Goerdeler; Gründen der gleichnamigen Unternehmensberatung
lit.	littera (Buchstabe)
m.w.N.	mit weiteren Nachweisen
MfS	Ministerium für Staatssicherheit
Mio.	Millionen
Mrd.	Milliarden
NFIS	Nationale Initiative für Internet- und Informationssicherheit
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
OLG	Oberlandesgericht
OWIG	Ordnungswidrigkeitengesetz
p.a.	per anno
PKS	Polizeiliche Kriminalstatistik
Rdnr.	Randnummer
RISK	Risiko Identifikation
S.	Seite
SAT	Situational Action Theorie
SchwerbG	Schwerbehindertengesetz
SE	Social Engineering
sog.	sogenannte
StGB	Strafgesetzbuch

SÜG	Sicherheitsüberprüfungsgesetz
u.a.	unter anderem
USB	Universal Serial Bus
UWG	Gesetz gegen den unlauteren Wettbewerb
VDI	Verein Deutscher Ingenieure
vgl.	vergleiche
VW	Volkswagen
z. B.	zum Beispiel
ZStW	Zeitschrift für die gesamte Strafwissenschaft

Inhaltsverzeichnis

1	Einleitung	1
2	Phänomenologie	3
2.1	Unterscheidung zwischen Wirtschaftsspionage und Konkurrenzausspähung	4
2.2	Verflechtung staatlicher und unternehmerischer Ausspähung	5
2.3	Der Innentäter	8
2.3.1	Innentäter im engeren Sinn	8
2.3.2	Innentäter im weiteren Sinn	9
2.3.3	Gefährdungspotential durch Innentäter	10
2.3.4	Motivationslage der Innentäter	11
2.3.5	Innentäter – korrupte Wirtschaftskriminelle?	13
2.4	Phänomenologische Einschätzung der Wirtschaftsspionage	13
2.4.1	Phänomenologische Erkenntnisse zur Spionage	13
2.4.2	Wirtschaftsspionage als Form der Wirtschaftskriminalität	14
2.4.3	Empirische Erkenntnisse	16
2.5	Zwischenfazit	26
3	Die Angriffsmethoden	29
3.1	Kategorisierung von Angriffsarten	29
3.2	Open Source Intelligence (OSINT)	31
3.3	Human Intelligence (HUMINT)	35
3.3.1	Social Engineering	37
3.3.2	Anfälligkeit für Social Engineering	39
3.3.3	Social Engineering – arglistige Täuschung?	40
3.3.4	Social Engineering durch Innentäter	42
3.4	Signal Intelligence (SIGINT)	43
3.5	Kriminalgeographie des Worldwide Web	43
3.5.1	APT Angriffe	44
3.5.2	IT Angriffe durch Innentäter	47
3.6	Zwischenfazit	48

4	Rechtliche Einordnung	49
4.1	Differenzierung nach Schutzbereichen	50
4.1.1	Schutzbereich der „Wirtschaftsspionage“	50
4.1.2	Schutzbereich der „Wirtschaftsausspähung“	51
4.1.3	Schutzbereich der „Computerdelikte“	51
4.2	Tatbestandliche Voraussetzungen der Wirtschaftsausspähung	53
4.2.1	Betriebs- und Geschäftsgeheimnisse	53
4.2.2	Täterkreis	56
4.2.3	Tathandlungen	57
4.2.4	Geheimnisverrat	58
4.2.5	Geheimnisausspähung	59
4.2.6	Geheimnisverwertung	61
4.3	Tatbestandliche Voraussetzungen der Wirtschaftsspionage	62
4.3.1	Geheimdienst einer fremden Macht	64
4.3.2	Ausüben geheimdienstlicher Tätigkeit	65
4.3.3	Zweckbindung der Handlung	66
4.3.4	Zielrichtung der Handlung	67
4.3.5	Funktionelle Eingliederung des Täters	68
4.4	Tatbestandliche Voraussetzungen der Computerdelikte	68
4.4.1	Datenbegriff	69
4.4.2	Ausspähen und Abfangen von Daten	71
4.4.3	Veränderungen von Daten	74
4.4.4	Computersabotage	75
4.4.5	Computerbetrug	76
4.5	Ausgewählte sonstige relevante Tatbestände	78
4.6	Zwischenfazit	80
5	Kriminologische Erklärungsansätze	81
5.1	Vor den Theorien	82
5.2	Anomietheorie nach Merton	82
5.3	Kontrolltheorie nach Hirschi	84
5.4	White Collar Crime Approach nach Sutherland	86
5.5	Subkulturtheorie 2.0	87
5.5.1	Ursprung	87
5.5.2	Anwendbarkeit im arbeitsplatzbezogenen Kontext	88
5.6	Neutralisationstechniken	90
5.7	Routine Aktivitäts Theorie nach Cohen und Felson	93
5.8	Situational Action Theorie nach Wikström	94
5.9	Leipziger Verlaufmodell nach Schneider	97
5.10	Kriminologische Erkenntnisse zu Cyberkriminellen	100
5.10.1	Gruppendynamische Ansätze	100
5.10.2	Individuelle Ansätze	101
5.11	Zwischenfazit	103

6	Präventionsansätze	105
6.1	RADAR Ansatz	106
6.2	R – Risikobeurteilung	107
6.2.1	Geht es immer nur um „Kronjuwelen“?	107
6.2.2	Verantwortlichkeiten	108
6.2.3	Klassifizierungen	108
6.3	A – Auswahl von Mitarbeitern und Partnern	111
6.3.1	Auswahl von Mitarbeitern	111
6.3.2	Auswahl von Geschäfts- und Kooperationspartnern	118
6.4	D – Durchgängiges Sicherheitskonzept	120
6.4.1	Elemente im Einzelnen	121
6.4.2	Maßnahmenplanung	124
6.5	A – Awarenessbildung	126
6.5.1	Awareness und Capability	126
6.5.2	Organisatorische und personelle Awareness	127
6.6	R – Regelmäßige Auditierung	130
6.7	Zwischenfazit	134
7	Schlussbetrachtung	137
	Literatur	139
	Stichwortverzeichnis	145

Abbildungsverzeichnis

Abb. 2.1	Atomium der Wirtschaftskriminalität	16
Abb. 3.1	Intelligence Circle	30
Abb. 3.2	Ablauf eines Social Engineering Angriffs	37
Abb. 3.3	Tatort Internet	44
Abb. 3.4	Ablauf APT	45
Abb. 4.1	Unterscheidung nach Schutzbereichen	52
Abb. 4.2	Geheimdienstliche Tätigkeit	66
Abb. 4.3	Datenmanipulation	77
Abb. 5.1	Routine Aktivität Theorie	93
Abb. 5.2	Grundkonzept der situativen Handlungstheorie	97
Abb. 5.3	Das Leipziger Verlaufsmodell wirtschaftskriminellen Verhaltens	99
Abb. 6.1	Ebenen der Risikobeurteilung	107
Abb. 6.2	Stufenmodell Zuverlässigkeitsüberprüfungen	112
Abb. 6.3	Auswahlkriterien Wirtschaftspartner	119
Abb. 6.4	Stufenkonzept	120
Abb. 6.5	Elemente eines durchgängigen Sicherheitskonzepts	121
Abb. 6.6	Exemplarische Darstellung eines Sicherheitskonzepts	124
Abb. 6.7	Maßnahmenplanung	125
Abb. 6.8	Security Awareness	126
Abb. 6.9	Zufriedenheit der CSO mit den Rahmenbedingungen	129
Abb. 6.10	Die Generationen, ihr Umfeld	131
Abb. 6.11	Regelkreis des Informationsschutzes	132

