

Unternehmenseigene Ermittlungen

Recht – Kriminalistik – IT

Von

Birgit Galley

Dr. Ingo Minoggio

Prof. Dr. Marko Schuba

unter Mitarbeit von

Dr. Barbara Bischoff

Hans-Wilhelm Höfken

ERICH SCHMIDT VERLAG

Bibliografische Information der Deutschen Nationalbibliothek

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

Weitere Informationen zu diesem Titel finden Sie unter
[ESV.info/978 3 503 16530 8](http://ESV.info/978_3_503_16530_8)

Gedrucktes Werk: ISBN 978 3 503 16530 8
eBook: ISBN 978 3 503 16531 5

Alle Rechte vorbehalten.

© Erich Schmidt Verlag GmbH & Co. KG, Berlin 2016
www.ESV.info

Dieses Papier erfüllt die Frankfurter Forderungen der Deutschen Nationalbibliothek
und der Gesellschaft für das Buch bezüglich der Alterungsbeständigkeit
und entspricht sowohl den strengen Bestimmungen der US Norm Ansi/Niso
Z 39.48-1992 als auch der ISO-Norm 9706.

Satz: Herbert Kloos, ES-Editionssupport, Berlin
Druck und Bindung: Druckerei Strauss, Mörlenbach

Inhaltsverzeichnis

Abbildungsverzeichnis	XIII
1. Unternehmenseigene Ermittlungen – Modeerscheinung oder Modell für die Zukunft? (Minoggio)	1
1.1 Eigene Untersuchungen als Ausfluss genereller Überwachungspflichten	2
1.2 Erhöhte Aufklärungspflicht im Konfliktfall	6
1.3 Auswirkungen auf die Unternehmenskultur	11
1.4 Positive Publizitätswirkung bei negativer Presse	12
2. Abgrenzung der eigenen Untersuchungen (Galley/Minoggio) ...	15
2.1 Die anlassbezogene, unternehmenseigene Untersuchung (Minoggio)	15
2.2 Keine „unabhängige Untersuchung“ nach nordamerikanischem Vorbild (Minoggio)	17
2.3 Keine Ermittlungen ohne Anfangsverdacht (Galley)	21
2.3.1 Sehen oder Suchen	21
2.3.2 Eigene Kontrollen versus eigene Ermittlungen	22
2.3.3 Anfangsverdacht durch Kontrollen	23
2.3.4 Vom Anfangsverdacht zur Ermittlung	25
2.4 Mitarbeiter-Überprüfung (Galley)	26
2.4.1 Vor dem Beschäftigungsverhältnis	26
2.4.2 Während des Beschäftigungsverhältnisses	27
2.5 Geschäftspartner-Überprüfung (Galley)	28
2.5.1 Geschäftsanbahnungsphase	28
2.5.2 Anlassabhängige Überprüfung	30
2.5.3 Evaluierung durch Dritte	31
2.6 Eigene Untersuchung als Bestandteil von Anti-Fraud-Management-Programmen (Galley)	32
2.6.1 Anti-Fraud-Strategie	33
2.6.2 Kosten-Nutzen-Analyse	34
2.6.3 Täterverhalten	36
3. Entstehung und Beginn von eigenen Ermittlungen (Galley/Minoggio)	41
3.1 Notwendigkeit von eigenen Ermittlungen (Galley)	41
3.2 Anlass für eigene Ermittlungen (Galley)	44

3.2.1	Unternehmen in der Opferperspektive	44
3.2.2	Unternehmen in der Täterperspektive	47
3.2.3	Auslöser für Krisen	49
3.3	Fraud-Risk-Management (Galley)	50
3.3.1	Internes Kontrollsystem	50
3.3.2	Risikomanagement	52
3.3.3	Bestandteile eines Fraud-Risk-Managements	54
3.4	Hinweisgebersysteme (Galley)	67
3.4.1	Ablauf von Hinweisgebersystemen	68
3.4.2	Whistleblower versus Hinweisgeber	76
3.4.3	Interne oder externe Hinweise	79
3.4.4	Schutzbedürfnisse von Hinweisgebern	80
3.4.5	Anforderungen an Hinweisgebersysteme	81
3.4.6	Arten von Hinweisgebermöglichkeiten	84
3.5	Öffentlichkeit und Medien (Galley)	92
3.5.1	Kommunikation vom Unternehmen	93
3.5.2	Kommunikation ins Unternehmen	94
3.5.3	Kommunikation über das Unternehmen	95
3.6	Nationale und internationale Ermittlungs- und Aufsichtsbehörden (Minoggio)	95
4.	Das Untersuchungsteam – wer macht eigentlich was? (Galley)	99
4.1	Kriminalistische Aufgaben	99
4.1.1	Verantwortungsverteilung im Unternehmen	99
4.1.2	Ermittlungsführung im Unternehmen	105
4.1.3	Interne Revision oder Jahresabschlussprüfer	107
4.2	Unternehmenseigene Ermittlungen mit externer Expertise	109
4.2.1	Einbindung von Unternehmensangehörigen	110
4.2.1.1	Geschäftsleitung	110
4.2.1.2	Aufsichtsrat	111
4.2.1.3	Ermittlungsabteilung	111
4.2.1.4	Interne Revision	111
4.2.1.5	Rechtsabteilung	112
4.2.1.6	Sonstige Mitarbeiter	112
4.2.2	Einbindung von Unternehmensexternen	113
4.2.2.1	Detekteien	113
4.2.2.2	Verdeckte Ermittler	114
4.2.2.3	Spezialisten	114
4.3	Exkurs: Sofortmaßnahmen im Verteidigungsfall	115

5.	Der Beginn der eigenen Untersuchung (Minoggio)	119
5.1	Auftraggeber der unternehmenseigenen Untersuchung	121
5.2	Inhalt und Umfang des Untersuchungsgegenstandes	125
5.3	Zusammenarbeit mit Strafverfolgern	128
5.3.1	Keine Pflicht zur kooperativen Zusammenarbeit	128
5.3.2	Einzelfallentscheidung über die Zweckmäßigkeit einer Zusammenarbeit	129
5.3.3	Ratschläge für die Zusammenarbeit	132
5.4	Umgang mit Presse und Öffentlichkeit	134
5.4.1	Erstes Ziel: Keine Berichterstattung	134
5.4.2	Professionelle Unterstützung bei der PR-Arbeit in der Krise	137
5.4.3	Der richtige Umgang mit der Öffentlichkeit	139
5.4.4	Nur im Ausnahmefall: Einsatz rechtlicher Gegenmittel	140
6.	Sachverhaltsermittlung (Galley/Minoggio)	143
6.1	Gestaltung der Rahmenbedingungen durch vorherige Vereinba- rungen (Minoggio)	145
6.2	Eilbedürftigkeit der eigenen Untersuchung (Minoggio)	147
6.3	Beteiligungsrechte des Betriebsrates (Minoggio)	150
6.3.1	Mitbestimmung bei der Einführung von Verhaltensrichtlinien für die Untersuchung	151
6.3.2	Mitbestimmung bei der Durchführung der Untersuchung	153
6.3.3	Mitbestimmung bei den Konsequenzen aus der Untersuchung	155
6.4	Aufklärungsförderung durch Amnestieregelungen (Minoggio)	156
6.5	Kriminalistische Fallbearbeitung (Galley)	159
6.5.1	Erster Angriff (Galley)	160
6.5.2	Hypothesen und Ermittlungsstrategien (Galley)	160
6.5.3	Datenanalyse (Galley)	162
	6.5.3.1 Betriebliche Daten	162
	6.5.3.2 Daten aus Überwachungen	164
6.5.4	Dokumentenanalyse (Galley)	166
6.5.5	Personenbeweise – Interviews und Befragungen (Galley/Minoggio)	168
	6.5.5.1 Grundlagen zu Interviews und Befragungen (Galley) ...	168
	6.5.5.2 Informationsgespräche (Galley)	170
	6.5.5.3 Durchführung von Interviews (Galley)	171
	6.5.5.4 Befragung eigener Mitarbeiter (Galley)	182
	6.5.5.5 Rechtliche Ausformung und Grenzen der Mitarbeiter- befragung (Minoggio)	183
	6.5.5.5.1 Zum Inhalt des Auskunftsanspruches	184
	6.5.5.5.2 Schweigerechte des Arbeitnehmers	187

6.5.5.5.3	Hinzuziehung eines Rechtsbeistandes bei der Befragung	192
6.5.5.5.4	Belehrungspflichten	194
6.5.5.6	Befragungen von Hinweisgebern (Galley)	195
6.5.5.6.1	Hinweisgeber und Informanten	196
6.5.5.6.2	Anonyme Gesprächspartner	197
6.5.5.7	Befragung von Zeugen (Galley)	197
6.5.5.8	Befragung von Tatverdächtigen (Galley)	199
6.5.5.9	Gespräche mit Beschuldigten/Tätern (Galley)	200
6.5.5.10	Protokollierung der Interviews (Galley)	203
6.5.6	Kriminaltechnik (Galley)	203
6.6	Dokumentation (Galley)	204
6.6.1	Dokumentenmanagement	205
6.6.1.1	Anforderungen an Dokumentation	205
6.6.1.2	Datenbanken zur Ermittlungsunterstützung	210
6.6.1.3	Strukturierung der Arbeitspapiere	214
6.6.1.3.1	Aufbau einer Akte	214
6.6.1.3.2	Referenzierung von Arbeitsunterlagen	216
6.7	Grenzen unternehmenseigener Ermittlungen (Galley)	220
6.7.1	Ermittlungen durch Unternehmensangehörige	220
6.7.2	Glaubwürdigkeit	221
6.7.3	Verschwiegenheit	221
6.7.4	Zeugnisverweigerungsrecht	222
6.7.5	Beschlagnahmefreiheit	223
7.	IT-Forensik (Schuba)	227
7.1	Grundlagen der IT-Forensik	228
7.1.1	Hintergrund zur IT-Forensik	228
7.1.1.1	Definition der Forensik und IT-Forensik	228
7.1.1.2	Geschichte der Forensik und IT-Forensik	229
7.1.2	Digitale Spuren und Beweismittel	230
7.1.2.1	Das Locard'sche Prinzip	231
7.1.2.2	Das Locard'sche Prinzip am „Tatort IT-System“	231
7.1.2.3	Besonderheiten digitaler Beweismittel	233
7.1.2.4	Anti-Forensik	236
7.1.3	Bedeutung der IT-Forensik	241
7.1.3.1	Zunahme digitaler Datenspuren	241
7.1.3.2	Zunahme von Fällen mit digitalen Spuren von Relevanz	242
7.1.4	Täter, Ermittler und Kunden	245
7.1.4.1	Täter	245

7.1.4.2	Durchführung von Angriffen auf IT-Systeme	251
7.1.4.3	Ermittler und Kunden	254
7.1.5	Mögliche Untersuchungsgegenstände	255
7.1.5.1	Computer	255
7.1.5.2	Externe Speichermedien	256
7.1.5.3	Mobiltelefone	257
7.1.5.4	Drucker und Kopierer	258
7.1.5.5	Netzwerkgeräte	258
7.1.5.6	Cloud	259
7.1.6	Probleme und Grenzen der IT-Forensik	260
7.1.6.1	Schnelle Änderung von Hardware und Software	260
7.1.6.2	Menge der gefundenen Daten	261
7.1.6.3	Datenkodierung und Datenverschlüsselung	261
7.1.6.4	Datenverlust	262
7.1.6.5	Viele Täter	262
7.2	Allgemeine Vorgehensweise der IT-Forensik	262
7.2.1	Ermittlungsmethoden	263
7.2.1.1	Live Response	263
7.2.1.2	Post-Mortem Analyse	265
7.2.2	Reaktion auf Vorfälle	268
7.2.2.1	Ereignisse und Sicherheitsvorfälle	269
7.2.2.2	Prozessbeteiligte	270
7.2.2.3	Incident Response Prozess	272
7.2.2.3.1	Vorbereitung	272
7.2.2.3.2	Erkennung und Analyse	273
7.2.2.3.3	Eingrenzung, Beseitigung und Wiederherstellung	275
7.2.2.3.4	Erfahrungen	275
7.2.3	Gerichtsverwertbares Sammeln digitaler Beweise	276
7.2.3.1	CFSAP-Modell	276
7.2.3.2	Investigative Process	277
7.2.3.2.1	Alarm oder Anschuldigung	278
7.2.3.2.2	Güterabwägung	278
7.2.3.2.3	Tatortsicherung	278
7.2.3.2.4	Identifizierung/Beschlagnahme	281
7.2.3.2.5	Sicherung	282
7.2.3.2.6	Bergung	282
7.2.3.2.7	Auswertung	282
7.2.3.2.8	Reduktion	283
7.2.3.2.9	Analyse	283
7.2.3.2.10	Bericht	284
7.2.3.2.11	Be- und Überzeugeng	284

7.3	IT-Forensik-Techniken für verschiedene IT-Systeme und Anwendungen	284
7.3.1	Clients und Server	285
7.3.1.1	Laptops und Notebooks	285
7.3.1.2	Windows-Forensik	286
7.3.1.3	Linux-Forensik	290
7.3.1.4	Sonderfall: Drucker und Kopierer	291
7.3.2	IT-Forensik von Anwendersoftware	291
7.3.2.1	Webbrowser	291
7.3.2.2	E-Mail	292
7.3.2.2.1	Outlook	293
7.3.2.2.2	Web-E-Mail Clients	293
7.3.2.2.3	Gefälschte E-Mails	293
7.3.3	Netzwerkforensik	294
7.3.4	Mobile Forensik	295
7.3.4.1	Herausforderungen der IT-Forensik mobiler Geräte	296
7.3.4.1.1	Isolation des Geräts	296
7.3.4.1.2	Gerätevielfalt	297
7.3.4.1.3	Datenextraktion	297
7.3.4.1.4	Datendekodierung	298
7.3.4.1.5	Verschlüsselung	298
7.3.4.1.6	Apps	299
7.3.4.2	Existierende Tools	299
7.3.5	Cloud-Forensik	302
7.3.5.1	Herausforderungen der Cloud-Forensik	302
7.3.5.1.1	Cloud-Dienste nicht standardisiert	302
7.3.5.1.2	Kein physikalischer Zugriff auf Cloud-Server	302
7.3.5.1.3	Cloud-Server von mehreren Kunden benutzt	303
7.3.5.1.4	Unterschiede lokale und Cloud-Zeitstempel	303
7.3.5.2	Datensicherung in der Cloud	303
7.3.5.2.1	IaaS-Datensicherung	304
7.3.5.2.2	PaaS-Datensicherung	305
7.3.5.2.3	SaaS-Datensicherung	306
7.4	Zusammenfassung	307
8.	Zwischenberichte und Abschlussbericht der eigenen Untersuchung (Galley/Minoggio)	309
8.1	Grundlagen zum forensischen Bericht (Galley)	309
8.1.1	Zwischenbericht	311
8.1.2	Mündlicher Bericht	315
8.1.3	Schlussbericht	316

8.2	Schutz der Untersuchungskommunikation (Minoggio)	319
8.2.1	Kein genereller Beschlagnahmeschutz	320
8.2.2	Beschlagnahmeverbote nach § 97 StPO für die Untersuchungs- kommunikation	321
8.2.2.1	Schutz von Unterlagen im Unternehmen	321
8.2.2.2	Schutz beim Syndikusanwalt	324
8.2.2.3	Schutz von Unterlagen außerhalb des Unternehmens bei einem Berufsheimnisträger	326
9.	Konsequenzen aus einer eigenen Untersuchung (Galley/Minoggio)	329
9.1	Arbeitsrechtliche Maßnahmen (Minoggio)	330
9.1.1	Die Abmahnung	330
9.1.2	Die Beendigung des Arbeitsverhältnisses	332
9.1.2.1	Die einverständliche Beendigung	332
9.1.2.2	Die außerordentliche Kündigung	333
9.1.2.3	Die ordentliche Kündigung	337
9.2	Schadensersatzansprüche (Minoggio)	338
9.3	Erstattung einer Strafanzeige (Minoggio)	339
9.3.1	Pro und contra Strafanzeige	339
9.3.2	Die erfolgreiche Strafanzeige	340
9.4	Anpassung der Compliance-Maßnahmen (Galley)	341
9.4.1	Bedeutung von Compliance im Geschäftsverkehr	341
9.4.2	Anpassung von Compliance-Strukturen	343
9.5	Wirtschaftliche Konsequenzen – Einfluss auf den Unternehmens- wert (Galley)	345
9.5.1	Betriebswirtschaftliche Vorüberlegungen	345
9.5.2	Finanzielle Auswirkungen von Wirtschaftsstraftaten	346
9.5.2.1	Verbandsgeldbußen	347
9.5.2.2	Vorteilsabschöpfung/Verfall	347
9.5.3	Öffentliche Auftraggeber	348
9.5.3.1	Korruptionsregister	349
9.5.3.2	Steuerliche Unbedenklichkeitsbescheinigungen	349
9.5.4	Betriebswirtschaftliche Schlussüberlegungen	350
	Literaturverzeichnis	351
	Stichwortverzeichnis	369