

David Godschalk

Computer Related Occupational Deviance

SOZIALWISSENSCHAFT

David Godschalk

Computer Related Occupational Deviance

Ein Mehr-Ebenen-Modell
zur Erklärung und Prävention

Deutscher Universitäts-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.

Dissertation Universität Hamburg, 2006

1. Auflage Januar 2007

Alle Rechte vorbehalten

© Deutscher Universitäts-Verlag | GWV Fachverlage GmbH, Wiesbaden 2007

Lektorat: Brigitte Siegel / Anita Wilke

Der Deutsche Universitäts-Verlag ist ein Unternehmen von Springer Science+Business Media.
www.duv.de



Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, 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.

Umschlaggestaltung: Regine Zimmer, Dipl.-Designerin, Frankfurt/Main
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier
Printed in Germany

ISBN 978-3-8350-0661-4

**Für meine Eltern,
Hillegonda und Marcel Godschalk**

Vorwort

Bei der Realisierung dieser Arbeit haben mich verschiedene Personen unterstützt.

Mein Dank geht in erster Linie an Prof. Dr. Sebastian Scheerer – er hat mir das Promotionsvorhaben ermöglicht und mich mit fachlichen Hinweisen bei der Verfassung dieser Dissertation stets motivierend unterstützt. Herrn Prof. Dr. Fritz Sack danke ich für die Erstellung des Zweitgutachtens.

Den Teilnehmern des Examenskolloquiums vom Aufbaustudium Kriminologie der Universität Hamburg möchte ich für anregende und spannende Diskussionen sowie kritische Auseinandersetzungen im Rahmen meiner Vorträge danken.

Ein herzliches Dankeschön geht auch an meinen Schwiegervater Karl sowie an meinen Kollegen Markus für ihre Durchsicht der Arbeit.

Meiner Frau danke ich für ihre guten Deutschkenntnisse und ihre Hilfe bei der Umschiffung so mancher sprachlicher Klippen. Annemie hat es mir mit ihrer Unterstützung und Geduld überhaupt erst ermöglicht, das Projekt nebenberuflich zu verfolgen.

Besonderer Dank gilt meiner kleinen Tochter Sarah. Vor dem Hintergrund begrenzter zeitlicher Ressourcen fiel es mit dem Wissen um ihre anstehende Geburt wesentlich leichter, Zwischentiefs und Motivationslöcher beim Verfassen der Arbeit zu überwinden. Später spornte sie mich fröhlich strampelnd zum Schreiben an und erlaubte es mir zumindest ab und zu, nachts durchzuschlafen.

David Godschalk

Abstract

Das vorliegende Werk betrachtet abweichendes Verhalten Unternehmensangehöriger mit Bezug zu Informations- und Kommunikationssystemen. Die unternehmenspragmatisch ausgelegte Begriffsdefinition umfasst dabei sowohl Rechtsverstöße, d. h. Computersabotage, Betrug und Geheimnisverrat, als auch nicht kriminalisierte, aber doch unternehmensschädigende Verhaltensweisen wie etwa die missbräuchliche private Nutzung eines betrieblich zur Verfügung gestellten Internetzugangs. Die Aufmerksamkeit der breiten Öffentlichkeit, in der Wissenschaft und in Unternehmen, richtet sich in erster Linie auf außerhalb der Unternehmensgrenzen zu lokalisierende Bedrohungen durch Virenprogrammierer oder Hacker. Computerbezogene Delikte werden jedoch in der Mehrzahl der Fälle von den eigenen Mitarbeitern begangen. Vor allem die schwerwiegenden Schädigungen lassen sich zunehmend auf ‚autorisierte‘ Systemanwender zurückführen.

Zur Klärung der Ursachen und Entstehungsbedingungen von ‚Computer Related Occupational Deviance‘ wird zunächst ein Erklärungsmodell konstruiert, welches über eine Makro-, Meso- und eine Mikroebene die drei analysierten Schichten Gesellschaft, Unternehmung und Individuum miteinander in Verbindung bringt und die Entstehung abweichender Verhaltensweisen prozesshaft als logische Kette aufeinander folgender Wirkungen interpretiert. Eine wichtige Erkenntnis besteht darin, dass steigende Komplexität und Spezifität organisationsinterner Strukturen und Prozesse infolge einer Individualisierung, Rationalisierung und Technologisierung der Unternehmensumwelt in Verbindung mit rational und opportunistisch agierenden Akteuren die Gefahr der Entstehung von Systemschwachstellen und damit das Viktimisierungsrisiko eines Unternehmens erhöhen. Dessen systematische Reduktion zum Ziel hat der Präventionsteil der Arbeit. Nach einem Vergleich verschiedener Risikoanalyseverfahren wird die Szenarioanalyse als geeignete Methode zur Aufdeckung und Behebung von Sicherheitslücken beschrieben. Darüber hinaus werden in Ergänzung bekannter Referenzwerke für die in der Unternehmenspraxis beliebten Grundschutz-Ansätze unter konsequenter Fortführung der dem konstruierten Erklärungsmodell zugrunde liegenden rationalistischen Logik Vorschläge im Sinne heuristischer Handlungsempfehlungen abgeleitet. Die Maßnahmen zielen darauf ab, die Wahrscheinlichkeit abweichenden Verhaltens durch Verschlechterung des wahrgenommenen Kosten-Nutzen-Verhältnisses von Tatgelegenheiten zu reduzieren.

Inhaltsverzeichnis

Vorwort	VII
Abstract	IX
Inhaltsverzeichnis	XI
Abkürzungsverzeichnis	XV
Abbildungsverzeichnis	XIX
Tabellenverzeichnis	XXI
1 Einleitung und theoretische Grundlagen	1
1.1 Problemstellung	1
1.2 Stand der Forschung und Forschungsbeitrag	4
1.3 Erklärung abweichenden Verhaltens	8
1.4 Aufbau der Arbeit	14
2 Wirtschaftskriminalität	19
2.1 Historische Entwicklung	19
2.1.1 Zwischen Mittelalter und Moderne	20
2.1.2 ‚Entdeckung‘ der White-Collar Kriminalität durch Sutherland	21
2.1.3 Die Zeit nach Sutherlands Pionierrede	23
2.1.4 Ansteigende Aufmerksamkeit	24
2.1.5 Die Moderne	25
2.2 Merkmale	27
2.2.1 Situative Tatmerkmale	27
2.2.2 Täterprofil	30
2.2.3 Rationalisierung wirtschaftskrimineller Handlungen	32
2.3 Definitiorische Eingrenzung und Entstehung	35
2.3.1 Definitionszweck und Konkretisierungsgrad	35
2.3.2 Problematik einer Legaldefinition	37
2.3.3 Occupational Crime als Makrophänomen	38
2.3.4 Logik der Aggregation	39
2.4 Bedeutung aus gesellschaftlicher Sicht	42
2.4.1 Kriminalität im Hell- und Dunkelfeld	43
2.4.2 Schadensarten und Problematik von Schadensschätzungen	45
2.4.3 Schadensumfang	47
3 Computerkriminalität	51
3.1 Historische Entwicklung	51
3.1.1 Anbruch des Computerzeitalters	52
3.1.2 Entdeckung des Makrophänomens	54
3.1.3 Die Hacker-Subkultur	55
3.1.4 Ansteigende Aufmerksamkeit und Kriminalisierung	56
3.2 Sicherheitseigenschaften von ITK-Systemen	60
3.2.1 Die EDV im Kriminalitätsgeschehen	60
3.2.2 Bedeutung von Informationen	63
3.2.3 Sicherheitsgrundlagen in der Informationstechnologie	65
3.2.4 Strukturelemente	68

3.3	Merkmale	71
3.3.1	Vorsätzlichkeit der Handlung	72
3.3.2	Tätertypologie	73
3.3.3	Täterbezogene Merkmale	75
3.3.4	Systembezogene Merkmale	77
3.3.5	Merkmale des Tathergangs	78
4	Computer Related Occupational Deviance	83
4.1	Betrachteter Gegenstandsbereich	83
4.1.1	Abweichendes und kriminelles Verhalten	84
4.1.2	Zusammenhang zwischen Wirtschafts- und Computerkriminalität	86
4.1.3	Empirische Indikatoren der Konvergenz beider Deliktformen	87
4.1.4	Definition von CROD	89
4.1.5	CROD als Mesophänomen	91
4.2	Deliktformen	94
4.2.1	Kategorisierung	94
4.2.2	Betrug	97
4.2.3	Verrat von Geschäftsgeheimnissen	98
4.2.4	Missbräuchliche Nutzung von ITK-Diensten	102
4.2.5	Sabotage	106
4.2.6	Diebstahl von Hardware	109
4.2.7	Diebstahl von Software	110
4.2.8	Taxonomie	112
4.3	Bedeutung aus Unternehmenssicht	114
4.3.1	Ausgaben für IT-Sicherheit	114
4.3.2	Verzerrte Wahrnehmung von Insiderdelikten	116
4.3.3	Strategische Bedeutung von Informationen und ITK-Systemen	118
4.3.4	Kosten und Häufigkeit von Schadensfällen	119
4.3.5	Ansprüche der Stakeholder	121
5	Handlungstheorie	123
5.1	Bewertungskriterien	123
5.1.1	Anforderungen an eine Handlungstheorie	123
5.1.2	Menschenmodelle	124
5.2	Verschiedene kriminologische Theorien im Vergleich	125
5.2.1	Theorieklassen	126
5.2.2	Soziale Lern-, Anomie- und Straintheorien	126
5.2.3	Rationalistische Theorien	128
5.2.4	Vorbehalte gegenüber rationalistischen Theorien	130
5.3	Rational Choice Ansatz	132
5.3.1	Ökonomische Grundlagen	132
5.3.2	Rationalität menschlichen Verhaltens – Erklärungsgehalt der Theorie	134
5.3.3	Beitrag zur Erklärung abweichenden Verhaltens	138
5.3.4	Bewertung der Eignung als Handlungstheorie	141
6	Ursachenanalyse	145
6.1	Entscheidungskalkül (Mikroebene)	145
6.1.1	Ziele und Präferenzen	145
6.1.2	Alternativen	147
6.1.3	Subjektiv erwarteter Nutzen	149

6.1.4 Beschränkte Rationalität	151
6.2 Missbrauchsgelegenheiten (Mesoebene)	154
6.2.1 IT-Sicherheitsverantwortliche	154
6.2.2 Transaktionskostenökonomik	156
6.2.3 Organisatorische Reibungsverluste	157
6.2.4 Opportunismus und Spezifität	161
6.2.5 Komplexität und beschränkte Rationalität	163
6.2.6 Informationsverkeilung	166
6.3 Gesamtgesellschaftliche Rahmenbedingungen (Makroebene)	168
6.3.1 Individualisierung und Rationalisierung	168
6.3.2 Markt- und Wettbewerbsdruck	170
6.3.3 Technologisierung	171
6.4 Das Gesamtmodell im Überblick	174
7 Prävention	175
7.1 Notwendigkeit aus Unternehmenssicht	176
7.1.1 Gesellschaftliche Träger der Verbrechenskontrolle	176
7.1.2 Arten der Verbrechensbekämpfung	177
7.1.3 Grenzen staatlicher Präventionsbemühungen	178
7.2 Risikoanalyseverfahren	180
7.2.1 Klassische Analyseverfahren	181
7.2.2 Bewertung klassischer Verfahren	182
7.2.3 Alternative Verfahren	186
7.2.4 Szenarioanalyse	189
7.3 Grundschutzmaßnahmen	191
7.3.1 Information technology – Code of practice for information security management	192
7.3.2 IT-Grundschutzhandbuch	193
7.3.3 Grundschutz im Kontext von CROD	194
7.4 Reduktion von Tatgelegenheiten	195
7.4.1 Komplexitätsabbau	195
7.4.2 Spezifitätsreduktion	199
7.4.3 Zentralisierung der Datenhaltung	201
7.4.4 Sicherheitsschulungen	205
7.5 Nutzenreduktion	209
7.5.1 Vertrauensaufbau	209
7.5.2 Vermeidung arbeitsplatzbezogener Risiken	213
7.6 Kostenerhöhung	216
7.6.1 Sicherheitspolicy	216
7.6.2 Sicherheitsgrundsätze	219
7.6.3 Beschämenseiten	220
8 Schlussbetrachtung	223
8.1 Zusammenfassung	223
8.2 Ausblick	226
Literaturverzeichnis	229

Abkürzungsverzeichnis

AC	Audit Commission
AO	Abgabenordnung
AktG	Aktiengesetz
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BSI	British Standards Institution oder Bundesamt für Sicherheit in der Informationstechnik
CCTA	Central Computer and Telecommunications Agency
CERT/CC	Computer Emergency Response Team Coordination Center
CIO	Chief Information Officer
COBOL	Common Business Oriented Language
CPU	Central Processing Unit
CRAMM	CCTA Risk Analysis and Management Method
CRM	Customer Relationship Management
CROD	Computer Related Occupational Deviance
CSI	Computer Security Institute
DBMS	Datenbankmanagementsystem
DFÜ	Datenfernübertragung
DOS	Disk Operation System
DSL	Digital Subscriber Line
DTI	Department of Trade and Industry
E-Mail	Electronic Mail
EDV	Elektronische Datenverarbeitung
EITO	European Information Technology Observatory
EMF	Enhanced Metafile
Eniac	Electronic Numerical Integrator and Calculator
ERP	Enterprise Ressource Planning
EstG	Einkommensteuergesetz
EU	Expected Utility
FBI	Federal Bureau of Investigation
FORTRAN	Formula Translation
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	GmbH Gesetz
GG	Grundgesetz
GVG	Gerichtsverfassungsgesetz
HGB	Handelsgesetzbuch

HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IM	Instant Messaging
IP	Internet Protocol
IRC	Internet Relay Chat
ISO	International Organization for Standardization
IT	Informationstechnologie
ITK	Informations- und Telekommunikationstechnologie
JPEG	Joint Photographic Experts Group
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
LAN	Local Area Network
MARION	Méthodologie d'Analyse des Risques Informatiques et d'Optimisation par Niveau
MIS	Management Informationssystem
MPAA	Motion Picture Association of America
NORAD	North American Aerospace Defense Command
ODBC	Open Database Connectivity
OEM	Original Equipment Manufacturer
OS	Operating System
PDA	Persönlicher Digitaler Assistent
PDF	Portable Document Format
PIM	Personal Information Management
PIN	Persönliche Identifikationsnummer
PC	Personal Computer
PKS	Polizeiliche Kriminalstatistik
RIAA	Recording Industry Association of America
ROI	Return on Investment
SEU	Subjective Expected Utility
SHTTP	Secure Hypertext Transfer Protocol
SQL	Structured Query Language
SRI	Stanford Research Institute
SSO	Single Sign On
StÄndG	Steueränderungsgesetz
StGB	Strafgesetzbuch
TAN	Transaktionsnummer
TCP/IP	Transmission Control Protocol / Internet Protocol
TDDSG	Teledienstdatenschutzgesetz

TDG	Teledienstegesetz
TDSV	Telekommunikations-Datenschutz-Verordnung
TKG	Telekommunikationsgesetz
UrhG	Urheberrechtsgesetz
USV	Unterbrechungsfreie Stromversorgung
UWG	Gesetz gegen den unlauteren Wettbewerb
USB	Universal Serial Bus
VoIP	Voice over IP
WAN	Wide Area Network
WiKG	Wirtschaftskriminalitätsgesetz
WLAN	Wireless Local Area Network
WWW	World Wide Web

Abbildungsverzeichnis

Abb. 1-1: Das Grundmodell der soziologischen Erklärung.....	11
Abb. 1-2: Makro-Kontext, soziale Gebilde und die Mikroebene der Akteure sozialen Handelns	13
Abb. 1-3: Aufbau der Arbeit.....	14
Abb. 1-4: Phasen der Modellbildung und zugehörige Kapitel	15
Abb. 2-1: Entdeckung und Verfolgung unternehmensschädigender Handlungen	40
Abb. 3-1: Computerkriminalität als Bedrohung der IT-Sicherheit.....	67
Abb. 3-2: Elemente eines Informations- und Telekommunikationssystems	68
Abb. 4-1: Abweichendes und kriminelles Verhalten.....	85
Abb. 4-2: Schnittmenge von Wirtschaftskriminalität und Computerkriminalität	87
Abb. 4-3: Deliktformen der Wirtschaftskriminalität – Erwartung in den nächsten fünf Jahren.....	89
Abb. 4-4: CROD – Eingrenzung des Gegenstandsbereichs	90
Abb. 4-5: Taxonomie von CROD.....	112
Abb. 4-6: Absolute und relative Zunahme der Ausgaben für IT-Sicherheit in West-Europa in den Jahren 2002 bis 2005	115
Abb. 4-7: Anteil der Unternehmen mit mindestens einem computerbezogenen Missbrauchsfall (eigene Mitarbeiter und Unternehmensfremde) im vergangenen Jahr	120
Abb. 6-1: Nutzenfunktion eines risikoaversen Entscheiders	149
Abb. 6-2: Anteil der outgesourceten Funktionen im Bereich der Informationssicherheit	155
Abb. 6-3: Anzahl der dem CERT/CC jährlich gemeldeten softwarebezogenen Sicherheitslücken.....	165
Abb. 6-4: Informationsunsicherheit als Folge organisatorischen Versagens	167
Abb. 6-5: Entwicklung der ITK-Ausgaben im Verhältnis zum Bruttoinlandsprodukt in Deutschland	172
Abb. 6-6: Mehr-Ebenen-Modell zur Erklärung von CROD	174
Abb. 7-1: Szenarioanalyse zur Prävention von CROD	190
Abb. 7-2: Faktoren, die auf das Sicherheitsverhalten der Anwender einwirken	207
Abb. 8-1: Übersicht Grundschutzmaßnahmen	226

Tabellenverzeichnis

Tab. 2-1: Schadenstaxonomie wirtschaftskrimineller Handlungen	45
Tab. 3-1: Täterbezogenes Fehlverhalten und Rollen der EDV im Rahmen der Computerkriminalität	64
Tab. 4-1: Formen abweichenden Verhaltens mit Bezug zur EDV	96
Tab. 4-2: Deliktformen von CROD und Merkmale der Tatbegehung.....	113