

LEHRBUCH

Edith Huber

# Cybercrime

Eine Einführung



Springer VS

---

# Cybercrime

---

Edith Huber

# Cybercrime

Eine Einführung



Springer VS

Edith Huber  
Donau-Universität Krems  
Krems an der Donau, Österreich

ISBN 978-3-658-26149-8                      ISBN 978-3-658-26150-4 (eBook)  
<https://doi.org/10.1007/978-3-658-26150-4>

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

Springer VS

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2019

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 allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jedermann benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des jeweiligen Zeicheninhabers sind zu beachten.

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. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Springer VS ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.

Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

---

# Vorwort

Computerkriminalität oder Cybercrime ist ein Phänomen der modernen Welt, der Welt der Informationen und Daten. Mit der Einführung und Nutzung der Informations- und Telekommunikationstechnologien hat sich Grundlegendes geändert. Smartphones, Tablets und Computer erleichtern unsere Alltagsgeschäfte, das Arbeiten und das Kommunizieren miteinander, jedoch mit dem Einzug der Technologien in die Unternehmenswelt haben sich Prozesse, Produkte, Organisationen und Geschäftsmodelle verändert. Eine Veränderung mit Chancen aber auch mit Risiken für die Unternehmen genauso wie für jeden Einzelnen.

Innerhalb der vergangenen 25 Jahre hat sich als Antwort auf diese Veränderung eine Cybercrime-Industrie entwickelt, die sich der Schwächen der Nutzer und der Schwachstellen der Systeme bedient, um sich illegal zu bereichern. Diese Entwicklung ist eine Herausforderung für Exekutive, Justiz, Schulen, Firmen und Staaten und letztendlich für jeden Einzelnen, denn jeder kann Opfer von Cybercrime werden. Das hier vorliegende Buch beschäftigt sich mit den Profilen von Opfern und Tätern, den unterschiedlichen Arten von Cybercrime und wie man sich letztendlich schützen kann.

Krems an der Donau, Österreich

Edith Huber

---

## Danksagung

An dieser Stelle möchte ich mich bei all jenen bedanken, die mich bei der Erstellung des Buches unterstützt haben, vor allem Mag. Heike Strumpen für das Lektorat und viele kritische Reflexionen, Bettina Pospisil, MA für jahrelange gemeinsame Forschungen, Dr. Wolfgang Haidegger, Dr. Otto Hellwig, Gregor Langer, der Firma Integral Markt- und Meinungsforschungs GmbH und Joachim Dostal.

---

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	1
<b>2</b>	<b>Von der Online-Kriminalität zu Cybercrime – eine historische Entwicklung</b>	5
2.1	Überblick	5
2.2	Die Entwicklung der virtuellen Gesellschaft	5
2.2.1	Vom Festnetz zum intelligenten Netz	7
2.2.2	Das Smartphone und internetfähige Endgeräte	8
2.3	Telekommunikationsnutzung (Internetnutzung)	10
2.4	Neue Kommunikationsformen	11
2.5	Online-Kriminalität	14
2.6	Cybercrime in Österreich	16
2.6.1	Cybercrime-Delikte an Unternehmen	17
2.7	Zusammenfassung	18
	Literatur	19
<b>3</b>	<b>Cybercrime</b>	21
3.1	Überblick	21
3.2	Das Problem einer eindeutigen Definition	22
3.2.1	Andere Länder andere Sitten	23
3.2.2	Unterschiedliche Wissenschaften, unterschiedliche Welten	24
3.3	Differenzierung nach der Art der Attacke	26
3.3.1	Opportunistische und zielgerichtete Attacken	26
3.3.2	Räuberische und marktorientierte Attacken	27
3.4	Zusammenfassung	28
	Literatur	28

<b>4</b>	<b>Relevante Akteure im Umfeld der Cyber-Kriminalität</b>	31
4.1	Überblick	31
4.2	Die Perspektive der Täter	31
4.2.1	Hacking	32
4.2.2	Der Hacker	33
4.2.3	Die Erstellung eines Täterprofils im Bereich Cybercrime	38
4.2.4	Delikte	39
4.2.5	Formation	41
4.2.6	Motive	42
4.2.7	Art des Angriffs	43
4.2.8	Angriffsort	51
4.3	Die Perspektive der Opfer	51
4.4	Regulatoren und Government	55
4.5	Internationale Organisationen in Bezug auf Cybercrime	56
4.5.1	Die vereinten Nationen	56
4.5.2	Der Europarat	56
4.5.3	Arbeitsgruppe der G8 – ‚High Tech Crime‘	57
4.5.4	CERTs – Computer Emergency Response Teams	57
4.5.5	Privatwirtschaftliche IT-Sicherheitsdienstleister	58
4.6	Zusammenfassung	58
	Literatur	59
<b>5</b>	<b>Aspekte der Kriminologie</b>	63
5.1	Überblick	63
5.2	Forensische Psychologie	63
5.2.1	Täterprofilung	64
5.3	Kriminologische Theorien in der Soziologie und Psychologie	66
5.3.1	Die Gesellschaft und die Kriminalität	67
5.3.2	Lerntheorie im Anwendungsfeld von Cybercrime	68
5.3.3	Merkmalstheorien von Kriminalität	69
5.3.4	Etikettierungsansatz – Labelling-Ansatz	69
5.3.5	Zur Ontogenese aggressiven Verhaltens im Cyberspace	70
5.3.6	Die moralische Entwicklung nach Kohlberg	71
5.3.7	Routine activity theory – eine Erklärung für Viktimisierung	71
5.4	Zusammenfassung	72
	Literatur	72



---

<b>6</b>	<b>Malware</b> .....	75
6.1	Überblick .....	75
6.2	Definition .....	76
6.3	Methoden und Formen .....	78
6.4	Profiling .....	78
6.4.1	Extrinsische Motive .....	78
6.4.2	Intrinsische Motive .....	80
6.4.3	Persönlichkeitsfaktoren .....	81
6.5	Business Modell .....	83
6.6	Prävention .....	86
6.6.1	Awareness schaffen .....	87
6.6.2	Soziologische Betrachtung .....	88
6.6.3	Psychologische Betrachtung .....	91
6.6.4	Technische Prävention .....	91
6.6.5	Normen, Standards und Gesetze .....	93
6.7	Zusammenfassung .....	96
	Literatur .....	97
<b>7</b>	<b>Identitätsdiebstahl</b> .....	99
7.1	Überblick .....	99
7.2	Definition .....	100
7.3	Methoden und Formen .....	101
7.3.1	Identitätsdiebstahl im eigentlichen Sinn – online .....	102
7.3.2	Identitätsdiebstahl im weiteren Sinn – offline .....	104
7.4	Profiling .....	105
7.4.1	Opfer .....	105
7.4.2	Die Täter .....	106
7.5	Business Modell .....	108
7.6	Prävention .....	109
7.7	Zusammenfassung .....	110
	Literatur .....	112
<b>8</b>	<b>Cyberstalking</b> .....	113
8.1	Überblick .....	113
8.2	Definition .....	113
8.2.1	Cyberstalking im engeren Sinne .....	115
8.2.2	Cyberstalking im weiteren Sinn .....	117
8.3	Methoden und Formen .....	118
8.3.1	Online versus Offline Cyberstalking .....	118
8.3.2	Wie wird cybergestalkt? .....	119
8.3.3	Arten der Kontaktaufnahme .....	121

8.4	Profiling .....	122
8.4.1	Opfer .....	122
8.4.2	Täter .....	125
8.5	Business Modell / Vorgehensmodell .....	130
8.6	Prävention .....	132
8.7	Zusammenfassung .....	132
	Literatur .....	134
<b>9</b>	<b>Kinderpornografie im Internet .....</b>	<b>135</b>
9.1	Überblick .....	135
9.2	Definition .....	136
9.3	Methoden und Formen .....	138
9.3.1	Verteilung, Produktion und Konsum von Kinderpornografie .....	138
9.3.2	Cyber-Grooming .....	140
9.4	Profiling .....	140
9.4.1	Opfer .....	140
9.4.2	Täter .....	142
9.5	Business Modell / Vorgehensmodell .....	144
9.6	Prävention .....	145
9.7	Zusammenfassung .....	146
	Literatur .....	147
<b>10</b>	<b>Cybercrime in Österreich 2006–2016 – Am Fallbeispiel der Stadt Wien .....</b>	<b>149</b>
10.1	Überblick .....	149
10.2	Einleitung und methodischer Ansatz .....	149
10.3	Cybercrime-Fälle, bei denen es zu einer Verhandlung vor Gericht kam .....	151
10.3.1	Der typische Cyber-Kriminelle .....	151
10.3.2	Typ 1: Der Business-Man .....	152
10.3.3	Typ 2: Die Hausfrau .....	152
10.3.4	Typ 3: Der Perspektivlose .....	153
10.3.5	Weitere Trends und Entwicklungen .....	153
10.3.6	Wie gestaltet sich der Tathergang (Modus Operandi)? ..	154
10.4	Cybercrime-Fälle, bei denen es zu keiner Verhandlung vor Gericht kam – die Akten der Staatsanwaltschaft – ungelöste Fälle .....	158
10.5	Zusammenfassung und Fazit .....	161
	Literatur .....	162