

Edith Huber *Hrsg.*

Sicherheit in Cyber-Netzwerken

Computer Emergency Response
Teams und ihre Kommunikation



Springer VS

Sicherheit in Cyber-Netzwerken

Edith Huber (Hrsg.)

Sicherheit in Cyber-Netzwerken

Computer Emergency Response
Teams und ihre Kommunikation

Herausgeber
Edith Huber
Krems, Österreich

Die Studie wurde finanziert durch die Forschungsförderung der Programmlinie KIRAS, Programmlinie 4, Förderung 2013 vom Bundesministerium für Verkehr, Innovation und Technologie, abgewickelt durch die österreichische Forschungsförderungsgesellschaft m.b.H FFG.



ISBN 978-3-658-09057-9

ISBN 978-3-658-09058-6 (eBook)

DOI 10.1007/978-3-658-09058-6

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 2015

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 Fachmedien Wiesbaden ist Teil der Fachverlagsgruppe Springer Science+Business Media (www.springer.com)

Inhalt

Vorwort	
<i>Sonja Stefl</i>	11
Einleitung	
<i>Edith Huber</i>	15
1 Organisation, Rahmenbedingungen und Kommunikation bei CERTs	
<i>Otto Hellwig</i>	23
1.1 Einleitung	23
1.2 CERTs und ihre Struktur	24
1.2.1 Prinzipielle CERT Beschreibung	24
1.2.2 Dienste eines CERT	27
1.2.3 Der RFC 2350	32
1.2.4 Rahmenbedingungen von CERTs	33
1.2.4.1 Gründung	33
1.2.4.2 Finanzierung	34
1.2.4.3 Constituency (Zielgruppe)	35
1.2.4.4 Globale Ziele des CERT (Mission Statement).....	36
1.2.4.5 Services des CERT	38
1.2.4.6 Aktionsmöglichkeiten.....	40
1.3 Beitrag der CERTs zur IT-Sicherheit organisationsintern, national und global	42
1.4 CERT: Policies und Organisation.....	44
1.4.1 Policies.....	44
1.4.2 Organisation.....	47
1.4.2.1 Organisatorische Grundkonstruktion	48
1.4.2.2 Aufbau- und Ablauforganisation	51
1.5 Kommunikation von CERTs	54
1.5.1 Ziele von Kooperationen.....	54
1.5.2 Kooperationsplattformen von CERTs.....	56
1.5.3 Vertrauen und rechtliche Rahmenbedingungen	59
1.5.4 CERT: Gemeinsame Projekte	60

1.5.5	CERT: Status Kooperation	62
1.6	Zusammenfassung	63
2	Standardisierte Datenaustauschformate	
	<i>Philipp Amann, Markus Huber, Timo Mischitz</i>	67
2.1	Einleitung	67
2.2	Austauschformate für Sicherheitsempfehlungen.....	67
2.2.1	Sicherheitslücken und Schwachstellen	68
2.2.2	Sicherheitsempfehlungen.....	69
2.3	Austauschformate für Gefährdungsindikatoren.....	71
2.3.1	OpenIOC (Incident Object Description and Exchange Format)	71
2.3.2	Cyber Observable eXpression (CybOX).....	72
2.4	Austauschformate für Sicherheitsvorfälle	73
2.4.1	Incident Object Description Exchange Format (IODEF).....	73
2.4.2	APWGs Spezifikation für das Erfassen von Phishing-Attacken.....	74
2.4.3	Real-time Inter-network Defense (RID)	74
2.4.4	Structured Threat Information eXpression (STIX)	75
2.4.5	Extended Abuse Reporting Format (X-ARF)	76
2.5	Gegenüberstellung der verschiedenen Austauschformate	77
2.6	Standardisierte Datenformate bei österreichischen CERTs.....	78
2.7	Zusammenfassung	78
3	Softwareunterstützung für die Behandlung von Sicherheitsvorfällen	
	<i>Markus Huber</i>	81
3.1	Einleitung	81
3.2	Datenquellen für Sicherheitsvorfälle	82
3.2.1	Interne Datenquellen.....	82
3.2.2	Externe Datenquellen.....	82
3.3	Software für die automatisierte Bearbeitung von Sicherheitsvorfällen ...	84
3.3.1	Megatron.....	85
3.3.2	Collective Intelligence Framework (CIF).....	86
3.3.3	AbuseHelper	86
3.3.4	Model-based Analysis of Threat Intelligence Sources (MANTIS) Framework	87
3.3.5	Inhouse Entwicklungen.....	87
3.4	Systeme für die Behandlung von Vorfällen.....	88
3.4.1	Issue-Tracking-Systeme.....	88
3.4.2	Incident-Tracking-Systeme.....	89
3.5	Diskussion	89
3.6	Zusammenfassung	90

4 Prozesse und Werkzeuge zur Veröffentlichung von Sicherheitsempfehlungen
Markus Huber 91

4.1 Einleitung 91

4.2 Grundprozess für die Erstellung von Sicherheitsmeldungen 92

4.2.1 Datensammlung 92

4.2.2 Risikobewertung 94

4.2.3 Veröffentlichung 95

4.2.4 Feedback 96

4.3 Taranis 96

4.3.1 5-Phasen von Taranis 96

4.3.2 Benutzeroberfläche 98

4.3.3 Risikobewertung 100

4.3.4 Verbesserungsmöglichkeiten 101

4.4 Textmining 101

4.4.1 Aufbereitung von Informationen für Textmining 102

4.4.2 Methoden für Clusteranalyse 102

4.4.3 Bündelung von mehrsprachigen Nachrichtenquellen 103

4.5 Crowdsourcing 104

4.6 Diskussion 105

4.7 Zusammenfassung 105

5 Wissensmanagement und Kommunikation bei CERTs
Edith Huber, Bettina Pospisil 107

5.1 Rahmenbedingungen eines Wissensmanagements bei CERTs 107

5.2 Systemisch bedingte Variablen, die Kommunikation und Kooperation beeinflussen 107

5.2.1 Kooperationsbereitschaft 108

5.3 Beeinflussende Faktoren auf der Makroebene 109

5.4 Variablen aus der klassischen Vertrauensforschung 112

5.4.1 Ad Integrität 112

5.4.2 Ad Kompetenz 113

5.4.3 Ad Erreichbarkeit 114

5.4.4 Ad Loyalität 114

5.4.5 Ad Verlässlichkeit 115

5.5 Spezielle Variablen aus dem Sicherheitsbereich 115

5.5.1 Ad Diskretion 115

5.5.2 Ad Reputation 116

5.5.3 Variablen, die bei einem internationalen Austausch von Wissen relevant sind 116

5.6	Modellierung des Vertrauensaufbaus	116
5.6.1	Theoretische Vorüberlegungen	116
5.6.2	Modellierung anhand der empirischen Studie.....	117
5.6.3	Kommunikation auf der Mikroebene.....	118
5.6.4	Wahl der Kommunikationsmittel.....	119
5.6.4.1	Einfluss auf die Kommunikation	119
5.6.4.2	Einflüsse der Organisation auf das Kommunikationsverhalten	119
5.6.4.3	Persönlichkeitsfaktoren, die die Kommunikation beeinflussen	120
5.6.5	Lösungen selber suchen... ..	120
5.7	Zusammenfassende Thesen	120
5.7.1	Allgemeine Tendenzen bzgl. Wissensmanagements	121
5.7.2	Kommunikation	121
5.7.2.1	Wunsch nach Regeln	121
5.7.2.2	Persönliche Einflussfaktoren	121
5.7.2.3	Organisationale Einflussfaktoren.....	122
5.7.2.4	Vertrauen als Schlüssel zur Zusammenarbeit.....	122
5.7.3	Ausblick.....	123
6	Anforderungen an die Modellierung der Kommunikation von CERTs	
	<i>Otto Hellwig</i>	125
6.1	Einleitung	125
6.2	Problemstellung.....	125
6.3	Literaturübersicht über Anforderungen von CERTs.....	126
6.3.1	Artikel mit anthropologischem Ansatz	127
6.3.2	Studie European Early Warning and Response System (EWRS)	128
6.3.3	ENISA-Studie CERT Operational Gaps and Overlaps	129
6.3.4	Gescheiterte CERTs.....	130
6.3.5	Stufenmodell von Nolan	130
6.4	Modellierungsansätze	131
6.4.1	Ansatz in der Masterthesis von Sebastiaan Tesink	132
6.4.2	Ziel/Szenario Ansatz	132
6.4.3	Modellierungsüberlegungen am Beispiel der von Timo Mischitz vorgeschlagenen Handlungsempfehlungen für ein Schul-CERT.....	136
6.5	Einschätzung und Outlook	138
6.6	Zusammenfassung	140

7 „Das CERT ist eine Organisation, die lebt“	
<i>Bettina Pospisil</i>	143
7.1 CERT als Organisationseinheit	143
7.1.1 Zielsetzung eines CERTs.....	143
7.1.2 Organisationsstruktur des CERT - Die Rolle in der Großorganisation	144
7.1.3 Die Rolle der Umwelt	146
7.2 CERT als soziales und offenes System	147
7.2.1 Auswirkungen der Umwelt	147
7.2.2 Auswirkungen des Einzelnen.....	148
7.3 CERT als Interaktionssystem	149
7.3.1 Herausbildung von Rollen im CERT	149
7.3.2 Auf die Person kommt es an... ..	150
7.4 Das CERT im übergreifenden Netzwerk.....	150
7.5 Die Rolle der Technik in den CERTs	151
7.6 Positionierung der CERT-Mitarbeiter	152
7.7 Interaktion und Handeln im CERT	153
7.8 Wissensmanagement im CERT	153
7.8.1 Verwaltbarkeit von Wissen.....	153
7.8.2 Personenbezogenes Wissen	154
7.9 Gender im CERT.....	155
7.10 Was hat sich im CERT verändert?.....	156
7.11 Zusammenfassende Thesen	157
7.11.1 Allgemeine Anerkennung notwendig für Zielumsetzung	157
7.11.2 Weitestgehend unabhängiges Selbstbild.....	157
7.11.3 Wunsch nach praxisnahem CERT-Gesetz	157
7.11.4 Handlungen oftmals individuell geprägt.....	158
7.11.5 Zusätzliche Herausforderung durch Doppelrollen	158
7.11.6 Netzwerk-Idee braucht Transparenz	159
7.11.7 Unzureichende Wissensverwaltung hemmt Fortschritt.....	159
7.11.8 Gesellschaftliche Akzeptanz und Zahl der Vorfälle steigt.....	159
7.12 Ausblick	160
AutorInnen	163

Vorwort

Sonja Steßl

Sehr geehrte Leserin, sehr geehrter Leser,

vor knapp einem Vierteljahrhundert wurde in Österreich der erste Computer offiziell mit dem Internet verbunden. Heute leben wir mit dem Internet, im Internet und vom Internet – selbstverständlich, mitunter affirmativ, mitunter kritisch. In den vergangenen Jahrzehnten hat das Internet den Austausch von Informationen beschleunigt und hat damit auch das Kommunikationsverhalten von uns allen grundlegender verändert als vielen bewusst ist.

Die Digitalisierung ist in nahezu allen Lebensbereichen unverzichtbar geworden und bietet Chancen und Partizipation für Privatpersonen, Unternehmen und die öffentliche Verwaltung. Doch diese neu geschaffene, umfassende Vernetzung hat auch viel Raum für Risiken und Bedrohungen geschaffen. Diese entwickeln sich laufend weiter, die Gesellschaft steht fast täglich vor neuen Herausforderungen.

Themen wie der Schutz von geistigem Eigentum, Datenschutz, Schutz kritischer Infrastrukturen und anders erfahren mit der Ausweitung des Cyber Space eine neue Dimension.

Der Staat alleine kann die Herausforderungen nicht bewältigen. Ein Großteil der Internetinfrastruktur ist in privater Hand. Somit ist eine tragfähige Kooperation zwischen Wirtschaft und Staat notwendig, um gemeinsam die Sicherheit im Cyberspace zu gewährleisten. Darüber hinaus können in Zeiten von Cloud-Computing und weltweit verteilter digitaler Prozesse offene Fragen nicht lediglich national beantwortet werden. Es bedarf vielmehr einer internationalen Koordination und konzertierter Aktivitäten. Dafür setze ich mich auch als für die Bereiche IKT und E-Government zuständige Staatssekretärin im Bundeskanzleramt ein. Denn nicht zuletzt spielt das Bewusstsein und Verhalten von Privatpersonen im Netz eine wesentliche Rolle in diesem Kontext, weshalb Information, Ausbildung und Bewusstseinsbildung möglichst breiter Bevölkerungsschichten ein weiterer wesentlicher Aspekt von Cyber Security ist. Das ist auch gesellschaftspolitisch relevant.

Sicherheit und Vertrauen im Internet sind wertvolle Güter. Es gilt sie zu schützen, so wie man andere Standortfaktoren schützt. Die Politik ist sich dieser Verantwortung bewusst und hat bereits 2008 das Government Computer Emergency Response Team (govCERT) etabliert und einen nationalen CERT-Verbund 2011 im Bundeskanzleramt institutionalisiert. Dadurch wurden rechtzeitig wesentliche operative Akzente gesetzt. Diese Strukturen haben sich bewährt und sind zu einem beständigen Grundpfeiler zur Aufrechterhaltung der digitalen Sicherheit geworden. Durch ein qualitativ hochwertiges Service ist es uns in Österreich gelungen, die CERT-Strukturen als fixe Anlaufstellen im Falle von IKT-Sicherheitsvorfällen für die öffentliche Verwaltung und der Privatwirtschaft zu etablieren. Im Falle einer Kompromittierung erhalten Betroffene hier Rat und Hilfe. Dabei profitieren sie auch an der internationalen Verflechtung der CERTs, die einen kontinuierlichen, internationalen Informationsaustausch mit anderen Betroffenen ermöglicht. So entsteht Wissen um Best Practice und um effiziente Lösungsmöglichkeiten.

Diese Strukturen und Prozesse sind beispielgebend für andere Bereiche. Der CERT-Verbund dient als Plattform für österreichische CERTs, um die Kommunikation zwischen den einzelnen Organisationen zu initiieren und das Vertrauen zu festigen. Bereits etablierte CERTs geben Erfahrungen und Lessons Learned über die Aufbauphase von Strukturen und Prozessen an neue Mitglieder weiter.

Ziel dieser Plattform ist auch Spezialexpertise, die bisher nicht in allen CERT-Organisationen vorhanden war, zu identifizieren und für alle Beteiligten nutzbar zu machen. Auf Basis der CERT-Verbund Initiative sind auf diese Weise zum Beispiel Schulungsmöglichkeiten für neue Teams entstanden, um Spezialwissen über die Behandlung von IKT-Sicherheitsvorfällen von erfahrenen CERTs vermittelt zu bekommen.

Eine Voraussetzung für positive Effekte aus einem Netzwerk ist Vertrauen. Vertrauen ist ein wesentlicher Faktor in der CERT-Community, damit ein reibungsloses Miteinander in der Vorfallsbehandlung sicherstellt ist.

In den vergangenen Jahren ist eine Vielzahl von Computer Emergency Response Teams entstanden. Sie gewährleisten die Widerstandsfähigkeit der von uns täglich genutzten Netze. Es gibt bereits viele Studien über Strukturen und technische Prozesse aus dem CERT-Komplex. Das Thema des multidisziplinären Zusammenhalts der CERT-Community ist ein neuer Aspekt, dem die vorliegende wissenschaftliche Arbeit zu Grunde liegt. Diese Studie geht der Frage nach, welche Parameter erfüllt sein müssen, um die Kommunikation zu verbessern, und geht dabei im Detail auf die Organisationsstrukturen, Prozesse, Kommunikationsstrukturen und Persönlichkeitsvariablen der CERTs ein.

Ich freue mich, Ihnen hiermit die Ergebnisse dieser spannenden und interessanten Arbeit präsentieren zu dürfen und bedanke mich im Namen der politischen

Spitze im Bundeskanzleramt herzlich bei den beteiligten WissenschaftlerInnern, die hier großartige Arbeit geleistet haben. Die Ergebnisse dieses Projektes werden uns in Zukunft helfen, CERT-Services noch besser und effektiver gestalten zu können und somit die digitale Welt für alle Beteiligten sicherer zu machen.

Einleitung

Edith Huber

Kaum ein Tag vergeht, an dem die Medien nicht von einem neuen Abhörskandal, Cyberangriff oder einen Internetmissbrauch berichten. Die neue Informationstechnik macht es möglich. Ein ständiges Immer-erreichbar-Sein hat in den letzten Jahren unser Kommunikationsverhalten maßgeblich verändert. Dabei ist die Kommunikation in Netzwerken ein wesentlicher Bestandteil unserer Gesellschaft geworden. Die hier durchgeführte Studie „CERT – Kommunikation“¹ beschäftigt sich mit den sicherheitsrelevanten Herausforderungen einer Kommunikation und Wissenstransfer in CERTs. Dabei stehen Fragen nach ‚schutzwürdiger Informationen und Kommunikation‘, ‚Internetkriminalität‘ und vor allem der ‚Vertrauenswürdigkeit der Kommunikatoren und in sicherheitsrelevanten Netzwerken‘ und ‚dem sinnvollen Austausch von Wissen‘ im Vordergrund.

Man darf es nicht leugnen, in den letzten 25 Jahren hat sich unser Kommunikationsverhalten massiv verändert. Kaum eine andere Technologisierung hat in den vergangenen Jahren das Leben der Menschen so intensiv verändert. Mit stärker werdender Vernetzung, Digitalisierung und Automatisierung sind immer mehr Angriffsflächen auf Information und Kommunikation gegeben. Die Tagesmedien sind voll von Meldungen über Abhörskandale, Cyberangriffen und Internetkriminalität. Diese Entwicklung beeinflusst auch massiv das Kommunikationsverhalten innerhalb der CERTs.

Ein wesentliches Ziel dieses Forschungsprojektes ist es das Kommunikationsverhalten in sicherheitsrelevanten Bereichen – also in CERTs - zu verbessern. Dem Bedarf einer Zusammenarbeit wird sowohl vom österreichischen Staat (siehe Digitale Agenda) und von der Europäischen Kommission schon seit langem propagiert und gefordert. (Kommission, 2014) Dabei ist es jedoch unerlässlich die Grundlagen und Ursachen dieser Entwicklung aufzuzeigen.

1 Die Studie wurde finanziert durch die Forschungsförderung der Programmlinie KIRAS, Programmlinie 4, Förderung 2013 vom Bundesministerium für Verkehr, Innovation und Technologie, abgewickelt durch die österreichische Forschungsförderungsgesellschaft m.b.H FFG

Cybercrime in Österreich

Ein Betrachtungsgegenstand von CERTs ist es auch kriminelle Angriffe auf IKT zu dokumentieren und zu melden. Damit einher lässt sich die Diskussion im Zusammenhang mit Computerkriminalität und Cyberterrorismus nicht verhindern. Betrachtet man die Diskussionen der letzten Jahre, so muss man festhalten, dass es immer wieder unklar ist, was nun konkret unter dem Bereich ‚Cybercrime‘ zu subsumieren ist.

Die Definition des Begriffs ‚Cybercrime‘ ist abhängig von dessen Verwendung und vor allem der jeweiligen Rechtslage der einzelnen Länder. Eine begrenzte Menge von Definitionen bezieht sich jedoch auf die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und dessen Systeme. (UNODC, 2013) Bisher werden in Österreich folgende Deliktsarten unter dem Bereich ‚Cybercrime‘ im StGB gelistet:

- §§ 118a: Wiederrechtlicher Zugriff auf ein Computersystem
- 119: Verletzung des Telekommunikationsgeheimnisses
- 119a: Missbräuchliche Abfangen von Daten
- 126a: Datenbeschädigung
- 126b: Störung der Funktionsfähigkeit eines Computers
- 126c: Missbrauch von Computerprogrammen
- 148a: Betrügerischer Datenverarbeitungsmissbrauch
- 225a: Datenfälschung

In den vergangenen Jahren kamen noch hinzu:

- 207a: Kinderpornographie (Pornographische Darstellung Minderjähriger)
- 208a: Anbahnung von Sexualkontakten zu Unmündigen (seit Jänner 2012) (Kriminalstatistik, 2013)

Der Schaden, den Cybercrime anrichtet, beträgt laut einer Studie des Center for Strategic and International Studies in Österreich alleine 0,41% des Bruttoinlandsproduktes. (APA, 2014)

	Jahr 2009		Jahr 2010		Jahr 2011		Jahr 2012		Jahr 2013	
	angezeigt	aufgeklärt	angezeigt	aufgeklärt	angezeigt	aufgeklärt	angezeigt	aufgeklärt	angezeigt	aufgeklärt
Cyber Crime im engeren Sinn / IT-Delikte										
§ 118a StGB	352	181	452	176	741	250	2.268	458	1.737	310
Wiederrichtlicher Zugriff auf Computersysteme	62	28	79	23	172	40	229	55	391	67
§ 118a StGB - Misbräuchliche Abfragen von Daten	10	4	9	3	30	16	21	7	10	5
§ 126a StGB - Datenbeschädigung	73	42	81	40	70	38	206	43	196	51
§ 126a StGB - Datenbeschädigung	1	-	4	1	2	-	6	5	2	2
Verbrechen										
§ 126b StGB - Störung der Funktionsfähigkeit eines Computers	7	1	11	3	8	2	645	5	470	10
Verbrechen										
§ 126b StGB - Störung der Funktionsfähigkeit eines Computers	-	-	14	-	13	3	57	1	34	2
Verbrechen										
§ 126c StGB - Missbrauch von Computerprogrammen	56	21	78	29	88	26	163	35	171	37
§ 148a StGB - Betrügerischer Datenverarbeitungsmissbrauch	113	63	127	35	309	86	806	270	421	106
Verbrechen										
§ 148a StGB - Betrügerischer Datenverarbeitungsmissbrauch	18	15	32	27	12	7	6	1	5	2
Verbrechen										
§ 225a StGB - Datenfälschung	12	7	17	15	37	32	39	34	37	28
Cyber Crime im weiteren Sinn	9.359	8.614	3.771	2.139	4.196	2.199	8.040	2.351	9.462	4.253
§ 207a StGB - Kinderpornographie	450	412	279	255	467	411	525	489	483	423
Verbrechen										
§ 207a StGB - Kinderpornographie	13	11	36	34	35	29	47	46	68	57
Verbrechen										
§ 208a StGB - Anbahnung von Sexualkontakten zu Unmündigen	-	-	-	-	-	-	44	32	65	49
Innenbereich	8.858	8.174	3.364	1.837	3.441	1.725	6.619	1.746	7.670	3.683
Sonstige Straftaten im Internet	38	17	92	13	253	34	805	38	1.176	41
Cyber Crime GESAMT	9.711	8.795	4.223	2.315	4.937	2.449	10.308	2.807	11.199	4.563

	Jahr 2004		Jahr 2005		Jahr 2006		Jahr 2007		Jahr 2008	
	angezeigt	aufgeklärt	angezeigt	aufgeklärt	angezeigt	aufgeklärt	angezeigt	aufgeklärt	angezeigt	aufgeklärt
Cyber Crime im engeren Sinn / IT-Delikte										
§ 118a StGB	205	101	262	128	385	130	344	147	202	91
Wiederrichterlicher Zugriff auf Computersysteme	26	13	16	6	31	13	40	18	41	26
§ 118a StGB	4	3	6	3	-	-	7	2	2	2
Misbräuchliche Abfragen von Daten	45	23	81	50	40	21	61	42	44	27
§ 126a StGB - Vergehen	3	1	7	4	2	2	1	-	1	-
Datenbeschädigung	11	-	6	3	5	1	4	1	4	1
§ 126b StGB - Verbrechen	-	-	-	-	-	-	-	-	-	-
Störung der Funktionsfähigkeit eines Computers	32	18	26	6	45	9	38	13	34	14
§ 126c StGB - Verbrechen	78	38	86	23	210	49	177	60	64	15
Misbrauch von Computerprogrammen	2	2	8	7	51	35	9	5	5	3
§ 148a StGB - Vergehen	4	3	26	26	1	-	7	6	7	3
Betrügerischer Datenverarbeitungsmissbrauch	114	97	1.532	1.076	2.884	2.225	2.510	1.789	3.089	2.370
§ 225a StGB - Verbrechen	99	91	330	300	232	204	480	426	844	751
Datenfälschung	15	6	12	10	8	8	14	7	18	8
§ 207a StGB - Verbrechen	-	-	-	-	-	-	-	-	-	-
Kinderpornographie	-	-	1.163	746	2.612	2.003	1.976	1.359	2.206	1.600
Kinderpornographie	-	-	27	20	32	10	30	7	21	11
Anbahnung von Sexualkontakten zu Unmündigen	318	198	1.794	1.204	3.288	2.355	2.854	1.846	3.291	2.461
Internetübergriff										
Sonstige Straftaten im Internet										
Cyber Crime GESAMT										

Abb. 1: Kriminalstatistik 2013 - BMI Wien