RESEARCH

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

Springer VS

*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


Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

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

# Inhalt

# 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 erfahrenden 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 WissenschafterInnenn, 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) Bislang 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** | | 352 | 181 | 452 | 176 | 741 | 250 | 2.268 | 456 | 1.737 | 310 |
| § 118a StGB | Wiederrechtlicher Zugriff auf Comutersysteme | 62 | 28 | 79 | 23 | 172 | 40 | 229 | 55 | 391 | 67 |
| § 119a StGB | Missbräuchliche Abfangen von Daten | 10 | 4 | 9 | 3 | 30 | 16 | 21 | 7 | 10 | 5 |
| § 126a StGB - Vergehen | Datenbeschädigung | 73 | 42 | 81 | 40 | 70 | 38 | 296 | 43 | 196 | 51 |
| § 126a StGB - Verbrechen | Datenbeschädigung | 1 | - | 4 | 1 | 2 | - | 6 | 5 | 2 | 2 |
| § 126b StGB - Vergehen | Störung der Funktionsfähigkeit eines Computers | 7 | 1 | 11 | 3 | 8 | 2 | 645 | 5 | 470 | 10 |
| § 126b StGB - Verbrechen | Störung der Funktionsfähigkeit eines Computers | - | - | 14 | - | 13 | 3 | 57 | 1 | 34 | 2 |
| § 126c StGB | Missbrauch von Computerprogrammen | 56 | 21 | 78 | 29 | 88 | 26 | 163 | 35 | 171 | 37 |
| § 148a StGB - Vergehen | Betrügerischer Datenverarbeitungsmissbrauch | 113 | 63 | 127 | 35 | 309 | 86 | 806 | 270 | 421 | 106 |
| § 148a StGB - Verbrechen | Betrügerischer Datenverarbeitungsmissbrauch | 18 | 15 | 32 | 27 | 12 | 7 | 6 | 1 | 5 | 2 |
| § 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 - Vergehen | Kinderpornographie | 450 | 412 | 279 | 255 | 467 | 411 | 525 | 489 | 483 | 423 |
| § 207a StGB - Verbrechen | Kinderpornographie | 13 | 11 | 36 | 34 | 35 | 29 | 47 | 46 | 68 | 57 |
| § 208a StGB | Anbahnung von Sexualkontakten zu Unmündigen | - | - | - | - | - | - | 44 | 32 | 65 | 49 |
| Internetbetrug | | 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** | | 205 | 101 | 262 | 128 | 385 | 130 | 344 | 147 | 202 | 91 |
| § 118a StGB | Wiederrechtlicher Zugriff auf Comutersysteme | 26 | 13 | 16 | 6 | 31 | 13 | 40 | 18 | 41 | 26 |
| § 119a StGB | Missbräuchliche Abfangen von Daten | 4 | 3 | 6 | 3 | - | - | 7 | 2 | 2 | 2 |
| § 126a StGB - Vergehen | Datenbeschädigung | 45 | 23 | 81 | 50 | 40 | 21 | 61 | 42 | 44 | 27 |
| § 126a StGB - Verbrechen | Datenbeschädigung | 3 | 1 | 7 | 4 | 2 | 2 | 1 | - | 1 | - |
| § 126b StGB - Vergehen | Störung der Funktionsfähigkeit eines Computers | 11 | - | 6 | 3 | 5 | 1 | 4 | 1 | 4 | 1 |
| § 126b StGB - Verbrechen | Störung der Funktionsfähigkeit eines Computers | - | - | - | - | - | - | - | - | - | - |
| § 126c StGB | Missbrauch von Computerprogrammen | 32 | 18 | 26 | 6 | 45 | 9 | 38 | 13 | 34 | 14 |
| § 148a StGB - Vergehen | Betrügerischer Datenverarbeitungsmissbrauch | 78 | 38 | 86 | 23 | 210 | 49 | 177 | 60 | 64 | 15 |
| § 148a StGB - Verbrechen | Betrügerischer Datenverarbeitungsmissbrauch | 2 | 2 | 8 | 7 | 51 | 35 | 9 | 5 | 5 | 3 |
| § 225a StGB | Datenfälschung | 4 | 3 | 26 | 26 | 1 | - | 7 | 6 | 7 | 3 |
| **Cyber Crime im weiteren Sinn** | | 114 | 97 | 1.532 | 1.076 | 2.884 | 2.225 | 2.510 | 1.799 | 3.089 | 2.370 |
| § 207a StGB - Vergehen | Kinderpornographie | 99 | 91 | 330 | 300 | 232 | 204 | 490 | 426 | 844 | 751 |
| § 207a StGB - Verbrechen | Kinderpornographie | 15 | 6 | 12 | 10 | 8 | 8 | 14 | 7 | 18 | 8 |
| § 208a StGB | Anbahnung von Sexualkontakten zu Unmündigen | - | - | - | - | - | - | - | - | - | - |
| Internetbetrug | | - | - | 1.163 | 746 | 2.612 | 2.003 | 1.976 | 1.359 | 2.206 | 1.600 |
| Sonstige Straftaten im Internet | | - | - | 27 | 20 | 32 | 10 | 30 | 7 | 21 | 11 |
| **Cyber Crime GESAMT** | | 319 | 198 | 1.794 | 1.204 | 3.269 | 2.355 | 2.854 | 1.946 | 3.291 | 2.461 |

Abb. 1: Kriminalstatistik 2013 - BMI Wien