

**FHZ Fachhochschule Zentralschweiz**  
**HSW Hochschule für Wirtschaft Luzern**

Einführungsarbeit

# **Cyber-Kriminalität**

## **Prophylaxe und Bekämpfung**

Winter-/Sommersemester 2002/2003

Autoren:

Samuel Dissler  
Mario Studhalter  
Eric Stübi  
Philipp Zumstein

14. März 2003

**FHZ Fachhochschule Zentralschweiz**  
**HSW Hochschule für Wirtschaft Luzern**  
**FHW Diplomstudiengang Wirtschaftsinformatik**

Einführungsarbeit

# **Cyber-Kriminalität**

## **Prophylaxe und Bekämpfung**

Winter-/Sommersemester 2002/2003

Autoren:

Samuel Dissler  
Hiltenberg  
6110 Wolhusen  
041 / 490 46 49  
dissler@arcmedia.ch

Mario Studhalter  
Horwerstrasse 78  
6010 Kriens  
041 / 310 20 86  
mario.studhalter@gmx.ch

Eric Stübi  
Bürgenstockhöchi 6  
6403 Küssnacht  
041 / 850 12 30  
eric\_stuebi@freesurf.ch

Philipp Zumstein  
Postfach 133  
6362 Stansstad  
041 / 610 24 56  
philippzumstein@dplanet.ch

Dozentin:

Ursula Sury  
Zentralstr. 9  
6002 Luzern  
Tel. 041 227 58 58  
usury@hsw.fhz.ch

14. März 2003

## Management Summary

Die Computertechnologie entwickelt sich rasant und die Anzahl Internetuser wächst weiterhin exponentiell. Das Informations- und Kommunikationsbedürfnis des Menschen scheint in ungeahnte Dimensionen vorzustossen. Um dieser Nachfrage gerecht zu werden, wurden elektronische Datennetze erstellt, welche eine einfache Kommunikation und den schnellen Zugriff auf Informationen ermöglichen. Dieser einfache Zugriff und die globale Struktur bewirkt wiederum, dass das World Wide Web immer mehr genutzt wird und die Datenmenge zunimmt.

Die weltweite Vernetzung bringt auch Gefahren mit sich. Genauso wie die Technologie sich entwickelt, nimmt auch die Cyber-Kriminalität rasant zu. Neuen, bisher unbekanntem Herausforderungen sehen sich Strafverfolgungsbehörden gegenübergestellt. Da für Cyber-Kriminalität keine geografischen oder politischen Grenzen bestehen, sind die Strafverfolgungsbehörden gezwungen, neue Wege zu beschreiten. Um die Cyber-Kriminalität zu bekämpfen ist eine internationale Koordination gefordert. Daneben stellt die rasante Entwicklung der Cyber-Kriminalität auch hohe Ansprüche an die Gesetzgeber. Sie sind gefordert, eine einheitliche Rechtsgrundlage zu schaffen. Es darf nicht sein, dass Straftäter Rechtslücken ausnützen und das Internet missbrauchen.

Cyber-Kriminalität ist eine Herausforderung mit internationaler Dimension. Die Aktivitäten zur Vorbeugung und Verfolgung von Internetdelikten sind jedoch von Staat zu Staat recht unterschiedlich.

Die vorliegende Arbeit basiert grösstenteils auf Informationen aus dem Internet und wird mit ausgiebigen Befragungen und Interviews ergänzt. Als Grundlage dienen vor allem vorhandene Untersuchungen und Berichte, insbesondere die des Bundesamtes für Polizei. Fachleute und Verantwortliche, die sich intensiv mit dem Thema Cyber-Kriminalität auseinandersetzen, haben aufschlussreiche Informationen zur Arbeit beigesteuert.

Während dem Recherchieren haben sich die Befürchtungen mehr und mehr bewahrheitet, dass noch viel zu wenig gegen Cyber-Kriminalität unternommen wird. In den kommenden Jahren ist mit einer massiven Zunahme der Straftaten zu rechnen. Besonders gefährdet sind die kleinen und mittleren Unternehmen sowie private Internetuser. Der Staat, die Kantone und Organisationen sind gefordert Aktivitäten zur Bekämpfung und Prävention zu verstärken. Ausserdem müssen sich die Führungspositionen der Unternehmen ihrer Abhängigkeit von Computernetzwerken bewusst werden. Es gilt dort vor allem die nötigen Mittel frei zu machen und in die Sicherheit zu investieren. Die Abhängigkeit vom Netz wird oft nicht realisiert und es braucht wohl zuerst einschneidende Ereignisse, bevor entsprechende Schutzmassnahmen getroffen werden.

Die Staaten müssen enger zusammenarbeiten und eine internationale Rechtsharmonisierung anstreben. Die Aus- und Weiterbildung von Fachkräften muss weiter vorangetrieben und unterstützt werden, um der wachsenden Gefahr Paroli zu bieten.

Um nicht ein Opfer der Cyber-Kriminalität zu werden, muss sich letztendlich jeder Einzelne schützen. Viele Unternehmungen und private Internetuser sind jedoch kaum oder gar nicht geschützt. Ebenfalls sollten sich die Internetuser nicht nur als Konsument sehen, sondern sich wie ein Bürger der Netzgemeinschaft verhalten.

## Vorwort

Wir danken allen Personen recht herzlich, die uns während dem Planen, Recherchieren, Schreiben sowie dem Korrigieren tatkräftig unterstützt haben. Ohne die Mitarbeit dieser Personen wäre es nicht möglich gewesen, eine Arbeit zu verfassen, welche Sie heute in der Hand halten.

Allen voran möchten wir unserer begleitenden Dozentin, Frau Ursula Sury, danken, welche uns während der ganzen Arbeit unterstützend zur Seite gestanden und uns mit wertvollen Tipps weitergeholfen hat.

Unser Dank richtet sich auch an Herr Henauer und Frau Bollman von der nationalen Koordinationsstelle für Internet-Kriminalität (KOBIK), die uns bei einem interessanten Gespräch in Bern wertvolle Informationen geliefert haben.

Ebenso möchten wir uns bei Herrn Roland Portmann für das aufschlussreiche Gespräch bedanken.

In unserer Arbeit wird der Einfachheit halber immer nur in der männlichen Person geschrieben. Alle Aussagen gelten jedoch sinngemäss auch für das weibliche Geschlecht.

# Inhaltsverzeichnis

<b>MANAGEMENT SUMMARY .....</b>	<b>3</b>
<b>VORWORT.....</b>	<b>4</b>
<b>INHALTSVERZEICHNIS.....</b>	<b>5</b>
<b>1 EINLEITUNG .....</b>	<b>7</b>
<b>1.1 Problemstellung.....</b>	<b>7</b>
<b>1.2 Begriffsdefinition .....</b>	<b>7</b>
<b>1.3 Kriminalitätsformen.....</b>	<b>8</b>
1.3.1 Im weiteren Sinne .....	8
1.3.2 Im engeren Sinne .....	9
<b>1.4 Tätergruppen.....</b>	<b>9</b>
<b>1.5 Schadenpotenzial .....</b>	<b>10</b>
<b>2 BEKÄMPFUNG.....</b>	<b>12</b>
<b>2.1 Rechtliche Grundlage .....</b>	<b>12</b>
2.1.1 Rechtslage in der Schweiz .....	12
2.1.2 Convention on Cybercrime .....	13
<b>2.2 Strafverfolgung .....</b>	<b>15</b>
2.2.1 Problematik.....	15
2.2.2 Zuständigkeit .....	16
2.2.3 Strafrechtliche Verantwortlichkeit von ISP .....	16
2.2.4 Koordinationsstelle zur Bekämpfung der Internet-Kriminalität .....	18
2.2.5 Forensics .....	19
2.2.6 Datenschutz.....	20
<b>3 PROPHYLAXE .....</b>	<b>22</b>
<b>3.1 Warum ist Schutz wichtig?.....</b>	<b>22</b>
3.1.1 Gefahren für Unternehmungen.....	22
3.1.2 Gefahren für Privatanwender .....	23
3.1.3 Unschuldiger Täter .....	23
<b>3.2 Prophylaktische Aktivitäten .....</b>	<b>24</b>
3.2.1 Erziehung der „Cyber-Citizen“ .....	24
3.2.2 Projekte International.....	24
3.2.2.1 USA - <i>cybercrime.gov</i> .....	24
3.2.2.2 EU - <i>Aktionsplan für mehr Sicherheit im Internet</i> .....	25
3.2.2.3 <i>Interpol</i> .....	26
3.2.2.4 <i>Aktivitäten in Deutschland</i> .....	26
3.2.3 Aktivitäten in der Schweiz.....	26
<b>3.3 IT-Sicherheit im Unternehmen .....</b>	<b>28</b>
3.3.1 Sicherheit der Informationstechnologie .....	28
3.3.2 Technische Möglichkeiten .....	29
3.3.3 US-Statistik der Sicherheitstechnologien .....	30
3.3.4 Sensibilisierung des Managements.....	31

---

<b>3.4</b>	<b>Schutz im privaten Bereich</b> .....	<b>31</b>
3.4.1	Tools .....	31
3.4.2	Schutz der Privatsphäre .....	32
3.4.2.1	<i>Datensammler im Netz</i> .....	32
3.4.2.2	<i>Persönliche Angaben</i> .....	33
<b>4</b>	<b>ERGEBNISSE UND AUSBLICK</b> .....	<b>34</b>
<b>5</b>	<b>DISKUSSION</b> .....	<b>36</b>
	<b>LITERATURVERZEICHNIS</b> .....	<b>37</b>
	<b>INTERVIEWVERZEICHNIS</b> .....	<b>40</b>
	<b>ANHANG</b> .....	<b>41</b>
	<b>EIDESSTATTLICHE ERKLÄRUNG</b> .....	<b>45</b>

# 1 Einleitung

Das folgende Kapitel soll einen ersten Überblick über die Thematik der Cyber-Kriminalität verschaffen. Dabei werden u.a. die verschiedenen Kriminalitätsformen und Tätergruppen sowie das mögliche Schadenpotenzial durch die Cyber-Kriminalität aufgezeigt.

## 1.1 Problemstellung

Seit der Einführung des Personal-Computers entwickelt sich die Computertechnologie in grossen Schritten. Durch die weltweite Vernetzung im vergangenen Jahrzehnt hat sich der Umgang mit Informationen grundlegend verändert: Informationen sind nun ohne grossen Aufwand schnell und kostengünstig nahezu jederzeit und überall fast jedem zugänglich. Dieses exponentielle Wachstum der Informationstechnologie ist weiterhin voll im Gang. Ebenso ist in den letzten Jahren die Anzahl Internetuser rasant gewachsen und wird gemäss Studien im Jahr 2005 die 1 Milliarde Grenze überschreiten (vgl. Abbildung 1<sup>1</sup>). Das Internet erfreut sich immer grösserer Beliebtheit.

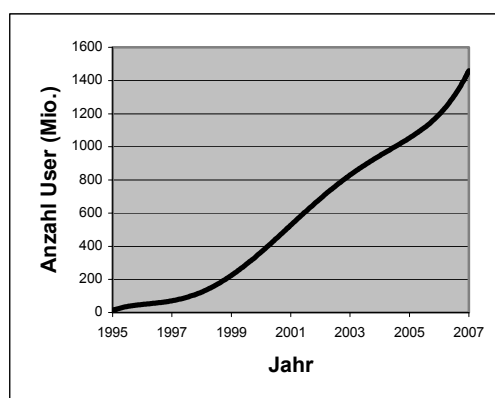


Abbildung 1: Entwicklung der Internetuser

Doch wie im realen Leben gibt es im virtuellen Raum des Internets auch Schattenseiten. Ständig liest man in den Medien neue Berichte über Kinderpornographie im Internet oder bösartige Computerviren. Die Cyber-Kriminalität verbreitet sich immer mehr. Doch das Internet ist kein rechtsfreier Raum. Die Gesetze gelten auch im virtuellen Raum.

Die vorliegende Arbeit beschäftigt sich mit dem Thema Cyber-Kriminalität. Zum einen gibt die Arbeit einen Überblick über die derzeit wichtigsten Kriminalitätsformen. Ebenso zeigt sie die Arbeit den aktuellen Stand der Bemühungen zur Bekämpfung der Cyber-Kriminalität auf nationaler sowie internationaler Ebene. Zugleich wird aufgezeigt, wie sich Privatpersonen sowie Unternehmungen prophylaktisch gegen diese Bedrohung schützen sollten. Aufgrund der gesammelten Fakten wird versucht, Lücken und Handlungsbedarf der Schweiz im Kampf gegen den Cyberkriminalismus aufzuzeigen.

## 1.2 Begriffsdefinition<sup>2</sup>

Auf den ersten Blick unterscheidet sich Cyber-Kriminalität von anderer Kriminalität einzig dadurch, dass sie mittels neuer Informationstechnologien begangen wird.

Gemäss Marcel Alexander Niggli, Professor für Strafrecht an der Universität Freiburg, gibt es bei dieser neuen Kriminalitätsform jedoch fundamentale Veränderungen. Zum einen ist da die Schwierigkeit,

<sup>1</sup> Global Internet Statistic, 2003 / Internet Users will top 1 billion in 2005, 2003

<sup>2</sup> vgl. Niggli, 2002, S. 6-8

dass bei einer Tathandlung via Internet nicht klar ist, wo genau das Delikt verwirklicht wird. Veröffentlicht beispielsweise jemand Anleitungen zum Herstellen von Computerviren, wird es praktisch unmöglich herauszufinden, wo genau dieser Täter handelte. Aufgrund dieser Problematik ergibt sich gemäss A. Niggli auch ein Problem für die Zuständigkeit sowie der Strafverfolgung. Grundsätzlich sei nämlich bei einem Internet-Delikt bei Aufnahme der Ermittlungen nicht bekannt, wo die Tat ausgeführt wurde. Der zweite grosse Teilbereich, durch welchen sich Cyber-Kriminalität von anderen Kriminalitätsformen unterscheidet, betrifft die Frage der Teilnahme. Für die Verwirklichung eines Deliktes via Internet müssen nämlich grundsätzlich immer mehrere Personen beteiligt sein. Ein Internet-Delikt setzt sich gemäss Prof. Niggli mindestens vier bzw. fünf involvierte Personen voraus: den Täter, dessen Zugangsprovider, den Zugangsprovider des Opfers und das Opfer selbst, sowie verschiedene zwischen den Zugangs Providern bestehenden Network-Provider. Zur Strafbarkeit von Zugangs- und Hosting-Provider hat in jüngster Zeit eine rege Diskussion stattgefunden (vgl. Kapitel 2.2.3 Strafrechtliche Verantwortlichkeit von ISP).

Zusammenfassend lässt sich sagen, dass Cyber-Kriminalität aufgrund dieser Veränderungen eine neue, grosse Herausforderung darstellt.

In der Literatur stösst man immer wieder auf verschiedene Begriffe wie Cybercrime, Internet-Kriminalität, Netzwerk-Kriminalität oder High-Tech-Kriminalität. Alle diese Begriffe meinen aber eigentlich dasselbe. Im weiteren Verlauf dieser Arbeit wird der Einfachheit halber für die gesamte Problematik nur noch der Begriff Cyber-Kriminalität verwenden.

## 1.3 Kriminalitätsformen

Spricht man von Cyberkriminalismus, denken die Meisten höchstwahrscheinlich als erstes an bösartige Computerviren oder Kinderpornografie. Doch das Internet kann noch für eine Vielzahl von weiteren Straftaten missbraucht werden. Im folgenden werden die Formen des Cyber-Kriminalismus in zwei Bereiche unterteilt.

### 1.3.1 Im weiteren Sinne<sup>3 4</sup>

Zu diesem Bereich werden die herkömmlichen Straftaten, die neu mit dem Internet begangen werden, gezählt. Es handelt sich hierbei nicht um neue Formen der Kriminalität, sondern um herkömmliche Straftaten, welche mit dem neuen Medium Internet begangen werden. Zu diesem Bereich gehören beispielsweise:

- Harte Pornografie
- Urheberrechtsverletzungen
- Gewaltdarstellungen
- Aufruf zu Gewalttaten
- Verbreitung von rassendiskriminierendem oder rechtsextremem Gedankengut
- Abwicklung von Betrugsgeschäften

---

<sup>3</sup> vgl. Kronig, 2002, S.8-10

<sup>4</sup> vgl. Bündnis 90/Die Grünen, 2001, S.3-6

Die genannte Aufzählung ist nicht abschliessend. Schliesslich können Computernetze auch als Tatwerkzeuge für eine Vielzahl anderer unerlaubter Handlungen – von der Beleidigung bis zur Geldwäsche – verwendet werden. Bei Kinderpornografie oder Rassismus ermöglicht das Internet nun, dass unerlaubte Abbildungen oder Informationen schnell und einfach einer grossen Anzahl von Leuten global zugänglich gemacht werden können.

Des Weiteren kann das Internet missbraucht werden, um kriminelle Taten zu verabreden und ihre Ausführung zu koordinieren. Besonders schwerwiegend sind dabei Delikte, die dem Bereich der „organisierten Kriminalität“ zuzurechnen sind, etwa dem internationalen Waffen- und Rauschgifthandel.

### 1.3.2 Im engeren Sinne<sup>5</sup>

Neben den herkömmlichen Straftaten, welche neu mit den Mitteln der Informationstechnologie begangen werden, umfasst die Cyber-Kriminalität ganz spezifische, neue Deliktsformen:

- Unbefugte Datenbeschaffung
- Unbefugtes Eindringen in ein Datenverarbeitungssystem (z.B. Hacking<sup>6</sup>)
- Datenbeschädigung (z.B. Cracking<sup>7</sup>)
- Betrügerischer Missbrauch einer Datenverarbeitungsanlage
- Erschleichen einer automatisiert erbrachten Leistung

Cyber-Kriminalismus beinhaltet eine Vielzahl von Delikten und muss auf einer breiten Front bekämpft werden.

## 1.4 Tätergruppen<sup>8</sup>

Gemäss dem strategischen Analysebericht „Cyber-Kriminalität“ vom Bundesamt für Polizei lassen sich die Täter, welche Informationsstrukturen angreifen, in drei grobe Kategorien einordnen:

- **Cyber-Kriminalität:** In dieser Kategorie sind häufig Einzeltäter aktiv. Allerdings sind auch im Bereich des Betruges oder Geldwäscherei Aktivitäten organisierter Gruppen wahrscheinlich. Bereicherungsabsichten und Sabotage sind häufige Motive für die kriminellen Taten.
- **Cyber-Terrorismus:** In erster Linie sind in dieser Kategorie ideologisch-politisch motivierte Gruppierungen aktiv. Bei solchen Angriffen steht vielfach politische Erpressung im Vordergrund. Häufige Ziele solcher Attacken sind Regierungen oder anders gesinnte Gruppierungen. Bis jetzt sind nur Einzelfälle solcher Angriffe bekannt. In dieser Arbeit wird nicht näher auf das Problem des Cyberterrorismus eingegangen.

---

<sup>5</sup> vgl. Anhang, Artikel 143, 143<sup>bis</sup>, 144<sup>bis</sup> und 147

<sup>6</sup> Hacker suchen nach Sicherheitslücken, um Anwender und Hersteller auf diese aufmerksam zu machen.

<sup>7</sup> Cracker hacken sich in fremde Systeme zur eigenen Bereicherung ein oder beschädigen Daten auf diesen Systemen.

<sup>8</sup> vgl. Cyberkriminalität – Die dunkle Seite der Informationsrevolution, 2001

- **Information Warfare:** Staaten, welche elektronische Angriffe gegen andere Länder führen, zählen zu dieser Kategorie. Bis jetzt sind aber noch keine solchen Fälle bekannt. Information Warfare wurde aber bereits in mit konventionellen Mitteln geführten Konflikten unterstützend eingesetzt. Dass diese Art „Cyberwar“ in Zukunft aber immer wichtiger wird, zeigt US-Präsident Bush. Gemäss Berichten in den Medien habe er angeordnet, Grundlagen und Regeln für Cyber-Angriffe zu entwickeln<sup>9</sup>. Bei einem Cyberangriff würden beispielsweise die für das Militär bedeutsamen Computersysteme durch Cracken oder Versendung von Viren gezielt lahm gelegt, um einen strategischen Vorteil zu erlangen. Der Bereich Information Warfare wird in dieser Arbeit ebenfalls nicht näher behandelt.

## 1.5 Schadenpotenzial

Das Schadenpotenzial im Bereich der Cyber-Kriminalität ist sehr schwierig einzuschätzen. Zum einen ist es beispielsweise schwierig, den entstandenen Schaden genau zu eruieren und betragsmässig zu beziffern. Andererseits bleiben viele Angriffe auf Informationsinfrastrukturen verborgen, weil sie überhaupt nie gemeldet werden. Der Hauptgrund dafür ist sicherlich einmal die Furcht vor einem Imageverlust. Bei einer Hacking-Attacke auf eine Bank ist beispielsweise der unmittelbare Schaden durch den Angriff sehr gering im Vergleich zum entstehenden Imageverlust, falls der Angriff publik wird. Ein weiterer Grund für das Nichtmelden der Cyber-Delikte an die Behörden könnte sein, dass wenig Geschädigte an eine effiziente strafrechtliche Verfolgung der Täter glauben. Angezeigte Delikte werden in der Schweiz jedoch meistens aufgeklärt.<sup>10</sup>

Doch der entstehende Schaden durch Cybercrime ist enorm. Einige Analysten haben versucht, die durch Viren verursachten Schäden zu beziffern. Folgende Zahlen sollen einen groben Eindruck vermitteln, welche Schäden durch Cyberkriminalismus verursacht werden können:

- Gemäss ComputerEconomics soll der Ende Januar 2003 ausgebrochene Wurm „SQLSlammer“ Schäden bis zu 1 Milliarde US-Dollar und der im Jahr 2000 in Umlauf geratene „I love you“-Virus Schäden von 7.7 Milliarden verursacht haben.<sup>11</sup>
- Das FBI und das Computer Security Institute (CSI) beziffern in ihrer Computerverbrechens-Statistik den durchschnittlichen Schaden pro Einrichtung im Jahr 2002 mit rund 2 Millionen US-Dollar. Zu diesen Einrichtungen zählen grosse amerikanische Konzerne und Regierungseinrichtungen sowie Universitäten.<sup>12</sup>

Diese Zahlen sind nur grobe Schätzungen. Die Dunkelziffer wird noch weit höher liegen.

Aus der Computerverbrechens-Statistik von FBI und CSI, welche rund 500 Unternehmen befragte, geht weiter hervor, dass die gemeldeten Attacken und Missbrauchsformen breit gestreut sind. Die grösste Schwachstelle liegt in den Internetverbindungen. 74 Prozent bezeichneten dies als häufige Angriffsstelle. Ebenso berichteten 40 Prozent von Systemeintrüben von ausserhalb, weitere 40 Pro-

---

<sup>9</sup> vgl. Rötzer, 2003

<sup>10</sup> Interview Roland Portmann, 19.02.2003

<sup>11</sup> vgl. Brauch, 2003

<sup>12</sup> vgl. Krempf, 2002

zent berichteten vom Lahmlegen ihrer Internetverbindungen durch DoS-Attacken<sup>13</sup>. Auch Probleme mit Computerviren gehören zum Alltag: 85 Prozent der Antwortenden haben mit diesen Rechner-Schädlingen zu kämpfen. Interessant ist ebenfalls, dass 87 Prozent der Teilnehmenden dieser Studie einen „Missbrauch von Netzzugangsprivilegien“ durch Mitarbeiter beklagen, worunter u.a. das Herunterladen von pornografischem Material oder illegaler Software gemeint ist. Aus diesem Bericht geht auch hervor, dass die Bedrohung nicht nur von Aussen (sprich Internet), sondern grösstenteils auch von den eigenen Mitarbeitern kommt. Da sich die Mitarbeiter physisch hinter der Firewall befinden, können sie gewollt oder ungewollt grossen Schaden verursachen. Diese Bedrohung gilt es also im Sicherheitskonzept miteinzubeziehen.<sup>14 15</sup>

Für die Schweiz fehlen solche detaillierte Studien. Es ist anzunehmen, dass Firmen deutlich grössere Probleme mit der Computer-Sicherheit haben, als sie tatsächlich nach aussen zugeben.

---

<sup>13</sup> Denial of Service: Verweigerung der Dienstleistung oder Verfügbarkeit; Sammelbegriff für alle Cracker Attacken auf die Dienstleistung von zentralen Systemen.

<sup>14</sup> vgl. Krempel, 2002

<sup>15</sup> vgl. Computer Security Institute, 2002, S. 7

## 2 Bekämpfung

Die folgenden Kapitel befassen sich mit den gesetzlichen Grundlagen sowie der Problematik bei der Strafverfolgung auf nationaler und internationaler Ebene.

### 2.1 Rechtliche Grundlage

Eine erfolgreiche Bekämpfung der Cyber-Kriminalität setzt Rechtsgrundlagen voraus, welche der heutigen Technologie angepasst sind.

#### 2.1.1 Rechtslage in der Schweiz<sup>16</sup>

Die neuen Deliktformen der Cyber-Kriminalität stellen ein Problem für die Rechtssetzung dar. In der Schweiz liegen die rechtlichen Grundlagen zur Verfolgung von Computerdelikten jedoch bereits vor.

Das Schweizerische Strafgesetzbuch (StGB) deckt folgende Straftatbestände ab (siehe Gesetzesartikel im Anhang):

- Unbefugte Datenbeschaffung (Artikel 143 StGB)
- Unbefugtes Eindringen in ein Datenverarbeitungssystem (Artikel 143<sup>bis</sup> StGB)
- Beschädigung von Daten (Artikel 144<sup>bis</sup> StGB)
- Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Artikel 147 StGB)
- Erschleichen einer Leistung (Artikel 150 StGB)
- Herstellen und Inverkehrbringen von Materialien zur unbefugten Entschlüsselung codierter Angebote (Artikel 150<sup>bis</sup> StGB)

StGB Art. 143, 143<sup>bis</sup> und 147 können nur dann angewandt werden, wenn die Daten gegen unbefugten Zugriff besonders gesichert sind.<sup>17</sup>

Bisher bekannte Kriminalitätsformen, die neu auch mit dem Internet begangen werden, deckt das Schweizerische Strafgesetzbuch unter anderen mit folgenden Gesetzesartikeln ab:

- Gewaltdarstellung (Artikel 135 StGB)
- Betrug (Artikel 146 StGB)
- Pornografie (Artikel 197 StGB)
- Ehrverletzungen (Artikel 173 ff, StGB)
- Rassendiskriminierung (Artikel 261bis StGB)
- Verletzung des Geschäftsgeheimnisses (Artikel 162 StGB)

---

<sup>16</sup> vgl. Kronig, 2002, S.8-10

<sup>17</sup> vgl. Sury, 2002

## 2.1.2 Convention on Cybercrime<sup>18</sup>

Der Europarat hat in den letzten vier Jahren an einer Konvention gearbeitet, um den Herausforderungen der Cyber-Kriminalität zu begegnen. Dieser weltweit erste Text soll das Internet und die Sicherheit der Nutzer gewährleisten - falls das scheitert, wäre das Entwicklungspotenzial des Internets ernsthaft bedroht.

### Geschichte

Der Europarat hat 1989 eine erste Empfehlung über Cyber-Kriminalität verabschiedet, 1995 folgte eine weitere über Verfahrensfragen. In der zweiten Empfehlung wurde der Gedanke einer internationalen Vereinbarung über Computer-Kriminalität entwickelt. Im Bewusstsein der Gefahren dieses Phänomens hat das Europäische Komitee für Verbrechensbekämpfung (CDPC) Professor H.W.K. Kaspersen mit einer Studie beauftragt. In seinem Bericht hat Professor Kaspersen eine Konvention über Gesetze, Strafverfahren und internationale Instrumente empfohlen.

Im Februar 1997 hat das Ministerkomitee des Europarates einen Expertenausschuss über Straftaten im Internet mit der Ausarbeitung eines verbindlichen Rechtsinstruments beauftragt. Fragen wie Straftaten, die Durchsetzung von Sanktionen auch auf internationaler Ebene und die Rechtsprechung im Zusammenhang mit Cyber-Kriminalität sollten geprüft werden.

### Erster Entwurf

Im April 2000 wurde der Entwurf des Textes bekannt gegeben - äusserst ungewöhnlich bei internationalen Rechtstexten - und im Internet veröffentlicht, um Computer-Spezialisten und Internet-Benutzer Kommentare zu ermöglichen. Die Parlamentarische Versammlung förderte die Diskussion, in dem sie eine Anhörung mit internationalen Fachleuten im März 2001 veranstaltete.

Auf Wunsch des Ministerkomitees beriet auch die Parlamentarische Versammlung über den Text und stimmte mit einigen Änderungsanträgen in ihrer Sitzung im April 2001 für den Text.

### Inhalt

Die europäische Cybercrime-Konvention (ETS-No.: 185) heisst mit offiziellem Titel: "Convention on Cybercrime (Convention sur la cybercriminalité)" und ist unter <http://conventions.coe.int> auf englisch und französisch, zusammen mit einer aktuellen Liste aller Länder welche die Convention bereits unterzeichnet oder ratifiziert haben, abrufbar.

Sie soll Straftaten im Zusammenhang mit neuen Technologien definieren. Methoden der polizeilichen Untersuchungen, Ermittlungen und der internationalen Kommunikation festlegen.

Die Konvention verfolgt drei Ziele:<sup>19</sup>

- Rechtsangleichung bei sämtlichen Mitgliederstaaten
- Gegenseitige Hilfe/Rechtshilfe bei Ermittlungen
- Aufbau eines Informations-Netzwerkes gegen Cyber-Kriminalität

---

<sup>18</sup> vgl. Council of Europe, 2003

<sup>19</sup> Interview KOBİK, 15.01.2003

## Unterzeichnung

„Cyber-Kriminalität und Cyber-Terrorismus sind ernste Herausforderungen unserer Gesellschaft. Diese Konvention bietet die erste koordinierte und internationale Antwort auf diese Herausforderung“, sagte der Stellvertretende Generalsekretär des Europarates, Hans Christian Krüger, bei der Feierstunde zur Unterzeichnung der Konvention.

Die Konvention über Cyber-Kriminalität wurde am 23. November 2001 im ungarischen Parlamentsgebäude in Budapest von 26 Mitgliedsländern des Europarates, darunter auch die Schweiz, und den vier Nichtmitgliedsländern unterzeichnet, die an ihrer Ausarbeitung beteiligt waren (Kanada, Japan, Südafrika und die USA). Dieser verbindliche Vertrag wird zu einem späteren Zeitpunkt auf Einladung des Ministerkomitees auch anderen Staaten zur Unterzeichnung vorgeschlagen werden. Er tritt in Kraft, wenn ihn mindestens fünf Staaten ratifiziert haben. Mindestens drei von ihnen müssen Mitgliedsländer des Europarates sein. Den aktuellen Stand der Unterzeichnung sehen sie in der Tabelle 1.

Stand der Unterzeichnung der Cyber-Konvention (27. Februar 2003)

	Anzahl Staaten	
	Mitglieder im Europarat	Total
Unterzeichnet	29	33
Unterzeichnet und ratifiziert	2*	2*

\* Albanien, Kroatien

www.coe.int

Tabelle 1: Stand Unterzeichnung Cyber-Konvention

Krüger sagte, dass die Konvention die nationalen Gesetzgebungen verstärken werde. Sie werde den Staaten die Möglichkeit geben, gegen Straftaten im Internet vorzugehen, vor allem auch in Verbindung mit der Bekämpfung des Terrorismus. Die Konvention werde weiterentwickelt werden und rasch Zusatzprotokolle erhalten, um im internationalen Zusammenhang neuen Herausforderungen gewachsen zu sein, sagte der Stellvertretende Generalsekretär.

Das Ministerkomitee könnte auch bald die Konvention durch Bestimmungen über die Versendung und Dekodierung von Terrorbotschaften durch das Internet verstärken. Ein Expertenausschuss sei eingesetzt worden, um binnen Jahresfrist ein Zusatzprotokoll über rassistische und fremdenfeindliche Propaganda im Internet auszuarbeiten. Derartige Propaganda soll als Straftat eingestuft werden.

## Kritik<sup>20</sup>

Vor allem als die ersten Entwürfe der Convention on Cybercrime veröffentlicht wurden, meldeten sich eine ganze Reihe von Bürgerrechtsorganisationen zu Wort. Man rügte in einem offenen Brief an den Europarat die unangemessene Erweiterung der Überwachungsmöglichkeiten und bat darum die Konvention nicht zu verabschieden.

Die Bürgerrechtsorganisationen aus den USA, Australien, Kanada, Südafrika und Europa kritisieren in ihrem Brief vom 18. Oktober 2000 unter anderem folgende Punkte:

- Die Konvention widerspräche dem "etablierten Normen zum Schutz des Einzelnen".
- Die "Befugnis der Polizei der nationalen Regierungen" werde unangemessen erweitert.
- Die "Entwicklung von Sicherheitstechniken für Netzwerke" werde behindert.

<sup>20</sup> vgl. Rötzer, 2000

- Die "Verantwortung der Regierung bei künftiger Strafverfolgung" werde herabgesetzt.
- Die Verpflichtung der Internetprovider, die Nutzungsdaten ihrer Kunden speichern zu müssen, gefährde die Privatsphäre und die Menschenrechte der Internetuser.

Auch die Art, wie der Entwurf für die Konvention zustande gekommen ist, wird von den Bürgerrechtsorganisationen kritisiert:

- "Polizeibehörden und mächtige private Interessen, die ausserhalb des Rahmens der demokratischen Verantwortung handeln, haben versucht, durch ein nicht-öffentliches Verfahren Regeln zu etablieren, die zu einer bindenden Gesetzgebung werden. Wir sind der Meinung, dass dieses Vorgehen das Erfordernis der Transparenz verletzt und dem demokratischen Entscheidungsprozess widerspricht."

Allgemein fordern die unterzeichnenden Organisationen, dass neue Rechte für Strafverfolgungsbehörden nur unter sorgfältiger Berücksichtigung der Menschenrechtsabkommen eingeführt werden sollten, was bei dieser Konvention nicht in ausreichendem Masse geschehen sei.

## 2.2 Strafverfolgung

In folgenden Kapiteln wird auf die schwierige Strafverfolgung, die Problematik der Zuständigkeit sowie die Strafrechtliche Verantwortlichkeit der Internet-Service Provider (ISP) eingegangen. Des weiteren wird das Spannungsfeld zwischen elektronischer Beweissicherung und Datenschutz erwähnt.

### 2.2.1 Problematik<sup>21</sup>

Die Verfolgung von Straftaten im Internet zeigt sich recht schwierig. Dies hat verschiedene Gründe im Bereich der Technologie sowie der Strafverfolgung.

#### Technologie:

- Das Internet bietet viele Angriffspunkte.
- Örtliche und zeitliche Gebundenheit besteht nur in sehr begrenztem Mass. Zum Beispiel kann ein Schweizer Autor sein Angebot auf einem Server in Russland platzieren.
- Der Internetbenutzer verfügt über eine relativ hohe Anonymität. Zum Beispiel kann ein Internetuser unter falscher Identität E-Mails versenden dank Freemail-Angeboten. Auch kann ein Internetuser z.B. im Internet-Cafe anonym das Internet nutzen.
- Nicht alle elektronischen Angriffe werden publik.
- Die Sensibilität der Bedrohung ist in der Privatwirtschaft und Verwaltungen zum Teil noch gering.

#### Strafverfolgung:

- Die finanziellen und personellen Ressourcen zum Aufbau und zur Umsetzung von Schutzmassnahmen sowie für die Strafverfolgung sind im Vergleich zu anderen Kriminalitätsformen noch recht bescheiden.
- Die Frage nach der Verantwortung der Internet-Provider ist nicht abschliessend geklärt.

---

<sup>21</sup> vgl. Niggli, 2002

- Sperren von illegalen Angeboten lassen sich dank der globalen Struktur des Internets leicht umgehen.
- Die Rechtslage ist in vielen Staaten unterschiedlich.
- Die internationale Zusammenarbeit zwischen Strafverfolgungsbehörden ist noch nicht ausreichend.
- Rechtshilfeverfahren dauern oft länger als die Beweise bei den Providern im Zielland elektronisch gespeichert bleiben.

### 2.2.2 Zuständigkeit<sup>22</sup>

Während die rechtlichen Instrumente zur Verfolgung von Cyber-Kriminalität vorhanden sind, stellen die mit dem Internet begangenen Delikte die Strafverfolgungsbehörden vor grosse Herausforderungen. Die klassische Unterscheidung von Tätigkeits- und Erfolgsdelikt gerät unter Druck, weil bei Tathandlungen via Internet nicht immer klar ist, wo genau das Delikt ausgeführt wird. Auch beim Erfolg kann man nicht immer anknüpfen, da dieser möglicherweise weltweit eintreten kann.

Diese Situation macht jede Strafverfolgungsbehörde, die sich verantwortlich fühlt oder durch Anzeige verantwortlich wird, auch zuständig. Für die Schweiz heisst das, dass sie grundsätzlich für alle Delikte, die über das Medium Internet begangen werden, zuständig wird. Gemäss Artikel 346 StGB sind auf nationaler Ebene die Behörden des Ausführungsortes zur Verfolgung verpflichtet. Wenn allerdings der Erfolg nur in der Schweiz eingetreten ist, sind die Behörden des Erfolgsortes für die Verfolgung verantwortlich. Da bei Internetdelikten der Ausführungsort meistens längere Zeit nicht bekannt ist, wird man sich auf den Erfolg stützen. Bei Delikten die einen Erfolg kennen wie z.B. Cracking oder Datenbeschädigung ändert sich hier nicht viel. Anders dagegen bei Tathandlungen die keinen Erfolg im Sinne des Tatbestands kennen wie z.B. bei Äusserungsdelikte. Definiert man den Erfolg jedoch noch breiter, so wird zumindest bei den klassischen Äusserungsdelikten wie z.B. Pornografie oder Gewaltdarstellung gemäss Artikel 346 Abs. 2 StGB diejenige Behörde zuständig, wo die Untersuchung angehoben wird. Gerade in solchen Fällen streiten sich die Kantone um die Zuständigkeit, da sich niemand verantwortlich fühlt.

Ein zweiter grosser Unterschied wobei sich Cyber-Kriminalität von anderen Kriminalitätsformen unterscheidet, betrifft die Frage der Teilnahme. Cyber-Kriminalität ähnelt dem Pressestrafrecht, weil bei einem Delikt grundsätzlich immer mehrere Personen beteiligt sind. Insbesondere die Strafbarkeit von Zugangs und Hosting-Providern bleibt in der Schweiz noch offen, weil unklar bleibt, ob die klassischen Regeln der Teilnahme anzuwenden sind gemäss Artikel 24 f. StGB oder das Pressestrafrecht Artikel 27 f., Artikel 322<sup>bis</sup> StGB (siehe folgendes Kapitel).

### 2.2.3 Strafrechtliche Verantwortlichkeit von ISP<sup>23</sup>

Die Problematik der strafrechtlichen Verantwortlichkeit von Internet-Service-Providern (ISP) wurde in der Schweiz erstmals deutlich, als die Bundespolizei im Juli 1998 in einem Rundschreiben an die ISP, unter Hinweis auf ihre mögliche Strafbarkeit, die Sperrung von verschiedenen Websites mit rassen-diskriminierenden Inhalten verlangte. Weil die ISP mit dem Risiko der Strafbarkeit konfrontiert wurden, löste das Rundschreiben bei den Empfängern starke Reaktionen aus. Es war nur annähernd klar,

<sup>22</sup> vgl. Niggli, 2002

<sup>23</sup> vgl. Strafrechtliche Verantwortlichkeit der Internet Service Provider - Gesetzgeber gefordert, 2003

unter welchen Bedingungen ein ISP nach schweizerischem Strafrecht für illegale Inhalte tatsächlich strafbar war. Deshalb wurde umgehend eine Kontaktgruppe gebildet, welche einen Ausgleich zwischen den Interessen der Behörden des Bundes sowie der ISP anstrebte. Die Bundespolizei beauftragte das Bundesamt für Justiz ein Gutachten zu erstellen, weil die Rechtslage unklar war. Das Gutachten kam zum Schluss, dass ISP grundsätzlich für illegale Inhalte im Internet strafrechtlich verantwortlich seien und zwar auch in der Funktion als Access-Provider, und dies selbst dann, wenn sich die illegalen Inhalte auf Servern im Ausland befinden. Auf der Gegenseite anerkannte das Gutachten auch, dass die ISP wegen der ungeheueren und nicht überschaubaren Datenmenge im Internet nicht voraussetzungslos für alle illegalen Inhalte verantwortlich gemacht werden können. Das Gutachten versuchte deshalb Rahmenbedingungen zu definieren, unter denen ein ISP strafrechtlich verantwortlich ist. Basierend darauf formulierte die Bundespolizei in ihrem Positionspapier<sup>24</sup> das von den ISP geforderte Verhalten bei öffentlichen Diensten:

### **Access-Provider<sup>25</sup>**

Liegen dem Access-Provider konkrete Hinweise einer Strafverfolgungsbehörde auf vermutlich illegale Netzinhalte vor, sind Sperrungen - soweit zumutbar - zu erwarten.

Eigenes, aktives Suchen nach strafrelevanten Inhalten im Internet ist allein schon auf Grund der sich täglich ändernden und zunehmenden Datenmenge weder sinnvoll noch Erfolg versprechend und kann deshalb nicht erwartet werden.

### **Hosting-Provider<sup>26</sup>**

Detaillierten und konkreten Hinweisen auf illegale Web-Inhalte und Newsgroups hat der Hosting-Provider nachzugehen. Findet er solche Inhalte, sind diese zu löschen oder zumindest deren Abrufbarkeit zu sperren.

Angesichts der im Vergleich zu den reinen Access-Providern deutlich näheren Anbindung an den Content-Provider, ist mindestens die stichprobeweise Kontrolle verdächtigter Content-Provider zu erwarten.

Bezüglich Dateien auf FTP-Servern<sup>27</sup>, auf welchen die freie Datenablage ermöglicht ist, ist Hinweisen nachzugehen, sofern die Dateien mit branchenüblicher Software gelesen werden können.

### **Online-Service-Provider<sup>28</sup>**

Je nach Ausgestaltung ihrer Dienste stellen Online-Service-Provider Content-, Hosting- oder Access-Provider dar, weshalb die Frage ihrer strafrechtlichen Verantwortung nach diesen Funktionen zu beantworten ist.

Aus Sicht des Verband Inside Telecom (VIT), welcher die Interessen von schweizerischen Telekommunikationsdienstleistungsunternehmen vertritt, war die Strafbarkeit von Access-Providern sowie die formulierten Verhaltensgrundsätze für ISP nicht zumutbar und auf der Grundlage des geltenden

---

<sup>24</sup> vgl. Die Strafrechtliche Verantwortung von Internet Service Providern, 2000, S. 13

<sup>25</sup> Zugangsvermittler zum Internet

<sup>26</sup> Stellen Speicherplatz auf Web-Servern zur Verfügung

<sup>27</sup> Protokoll für den Dateitransfer; Dienst des Internets

<sup>28</sup> Bieten proprietäre Dienste an (insbesondere Datenangebote), nehmen Funktion von ISP wahr.

Rechts nicht haltbar. Der VIT hatte deshalb ein Zweitgutachten<sup>29</sup> in Auftrag gegeben. Das Zweitgutachten bestätigt, dass das Positionspapier der Bundespolizei und dessen Grundlage, das Gutachten des Bundesamt für Justiz, keine verlässliche Grundlage zur Beurteilung des Verhaltens der ISP unter strafrechtlichen Gesichtspunkte darstellte. Die Schweizer Behörden würden es sich einfach machen, wenn sie die Access-Provider verurteilen, die manchmal gesetzeswidrige Inhalte transportieren. Es müssen die Täter verhaftet und verurteilt werden, welche strafbare Inhalte generieren.

Im Vergleich zu den restlichen europäischen Staaten sowie den USA, machen sich Access-Provider in der Schweiz strafbar, wenn sie illegale Inhalte transportieren. Gemäss der am 4. Mai 2000 verabschiedeten E-Commerce-Richtlinie der EU ist eine Verantwortlichkeit bei Durchleitung von gesetzeswidrigen Inhalten ausgeschlossen.

Ein aktuelles Beispiel zeigt, dass in der Schweiz nach wie vor völlige Unklarheit besteht bezüglich der Verantwortlichkeit von ISP. Die Untersuchungsrichterin des Kantons Waadt verlangte am 11. Dezember 2002 die Sperrung von drei im Ausland gehosteten Websites mit ehrverletzenden Inhalten. Die meisten der betroffenen Provider haben sich umgehend entschieden gegen diese Verfügung Beschwerde einzulegen. Mit der Begründung, dass die angeordnete Sperrung nutzlos ist und der Zugang zu den illegalen Inhalten nicht verhindert werden kann. Weiter beurteilen die Provider die Verfügung auch aus rechtlichen Gründen anfechtbar, da die gesetzliche Basis fragwürdig scheint. Die Schweizer Provider fühlen sich gegenüber den Providern in der EU benachteiligt, da in der EU mit der E-Commerce-Richtlinie die Verantwortlichkeit von ISP geklärt ist. Jedoch wird voraussichtlich im Frühling 2003 die von Bundesrätin Ruth Metzler eingesetzte Expertenkommission „Netzwerkriminalität“ ihren Bericht zur Revision des Strafgesetzbuches beenden und damit den Grundstein legen um die Diskriminierung zu beseitigen.<sup>30</sup>

## 2.2.4 Koordinationsstelle zur Bekämpfung der Internet-Kriminalität<sup>31</sup>

Eine Interkantonale Arbeitsgruppe zur Bekämpfung des Missbrauchs der Informations- und Kommunikationstechnik (BEMIK) befasste sich seit Juni 2000 mit der Koordination im Bereich Internet-Kriminalität. Ende Januar 2001 erschien der Bericht, worin die Arbeitsgruppe eine Reihe konkreter Massnahmen zur raschen Verbesserung der teils sehr unbefriedigenden Situation vorschlug. Auf Basis dieses Berichts hat das Eidgenössische Justiz- und Polizeidepartement und die Konferenz der kantonalen Justiz- und Polizeidirektoren beschlossen, bei der Bekämpfung gemeinsam vorzugehen. Aus der BEMIK kam neu die nationale Koordinationsstelle zur Bekämpfung der Internet-Kriminalität (KOBIK) hervor, die Anfang Januar 2003 ihren Dienst aufgenommen hat.

Die KOBIK ist die zentrale Anlaufstelle für Personen, die verdächtige Inhalte aus dem Internet melden möchten. Auf der Website [www.cybercrime.admin.ch](http://www.cybercrime.admin.ch) können die Meldungen online übermittelt werden. Ebenfalls ist die KOBIK Ansprechpartner gegenüber ausländischen Strafverfolgungsbehörden. Finanziert wird die Koordinationsstelle zu zwei Dritteln von den Kantonen und zu einem Drittel vom Bund. Dabei werden die Dienstleistungen der Stelle nur jenen Kantonen angeboten, welche sich an den Kosten auch tatsächlich beteiligen. Hinweise auf strafbare Handlungen werden allerdings den zuständigen Behörden auf jeden Fall mitgeteilt. Der KOBIK steht ein Personalbestand von neun Per-

<sup>29</sup> vgl. Niggli, Riklin, Stratenwerth, 2001

<sup>30</sup> vgl. Untersuchungsrichter verlangt von Schweizer Access-Providern Sperrung von Websites.

<sup>31</sup> vgl. Koordinationsstelle Internet-Kriminalität, 2003

sonen zu. Im Vergleich zum Ausland scheint dies als viel zu wenig. Es muss jedoch beachtet werden, dass die ausländischen Behörden zumeist nicht nur für die Koordination verantwortlich sind, sondern auch Ermittlungen durchführen müssen.

Zu den Hauptaufgaben der KOBİK gehören folgende Punkte:

- **Monitoring**  
Recherchen im Internet zum Erkennen strafbarer Missbräuche ohne konkreten Tatverdacht sowie erste Bearbeitung der eingehenden Verdachtsmeldungen wie Ortung der Urheberschaft zur Bestimmung der Zuständigkeit (Prüfung ob ein Bezug zur Schweiz besteht).
- **Clearing**  
Juristische Prüfung der strafrechtlichen Relevanz eingegangener Verdachtsmeldungen, Koordination mit laufenden Verfahren und Überweisung des Dossiers an die örtlich und sachlich zuständige Strafverfolgungsbehörde im In- und Ausland.
- **Analyse**  
National angelegte Analysen der Cyber-Kriminalität: Kontinuierliche Situationsanalyse Schweiz, fallübergreifende Darstellung der deliktischen Vorgehensweisen und der Tatmittel, Statistiken und Trends.

Die Koordinationsstelle ist auf der Basis einer Verwaltungsvereinbarung zwischen Bund und Kantonen tätig. In dieser Vereinbarung wird der Bund ermächtigt, im Bereich der Internet-Kriminalität Informations- und Koordinationsaufgaben zu übernehmen. Deswegen kommt bei Delikten mit kantonaler Zuständigkeit weiterhin das kantonale Recht zum Zug. Nur bei Straftaten, welche die innere Sicherheit der Schweiz bedrohen ist das Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) die rechtliche Basis.

Im Interview mit Herrn Henauer und Frau Bollman von der KOBİK konnten wir in Erfahrung bringen, dass von den momentan durchschnittlich 20 eingehenden Meldungen pro Tag, vor allem harte Pornografie, Kreditkartenbetrug und Gewaltdarstellung betreffen.<sup>32</sup>

## 2.2.5 Forensics

Forensics beschäftigt sich mit der elektronischen Beweissicherung bei Straftaten. Hier geht es um das Nachweisen ob eine Straftat begangen wurde und ob diese dem Täter nachgewiesen werden kann. Forensics ist eine neue Herausforderung für die Strafverfolgungsbehörden, da es nicht einfach ist nachzuweisen, dass z.B. eine Datenbank gehackt wurde. Auch Firmen oder Private sind in technischer und organisatorischer Art gefordert, da im Zivilrecht der Geschädigte dem Schädiger nachweisen muss, dass ihm ein Schaden zugefügt worden ist, z.B. wenn ein Konkurrent mittels Cracking Daten zerstört oder durch Hacking Industriespionage betreibt.<sup>33</sup>

---

<sup>32</sup> Interview KOBİK, 15.01.2003

<sup>33</sup> vgl. Sury, 2002

### Vorgehen bei der Spurensuche<sup>34</sup>

Bei der Ermittlung muss vorsichtig vorgegangen werden, da ansonsten Dokumente als Beweisstücke nicht anerkannt werden. Es wäre ja möglich, dass Daten nachträglich oder durch den Ermittlungsvorgang selber verändert wurden.

Als erstes wird meistens direkt vor Ort eine Voruntersuchung vorgenommen, um festzustellen, ob der Computer für das Ausüben unerlaubter Handlungen verwendet wurde. Allerdings ist es nicht einfach einen Verdacht direkt vor Ort abzuwenden, hingegen bestärken klare Indizien den Verdacht auf ein Vergehen. Für diese Untersuchung wird ein zweiter Computer verwendet, der nur lesend auf die Festplatte des verdächtigen Rechners zugreift.

Falls der Computer weiter untersucht werden muss, wird unter Beisein einer oder mehrerer Personen eine Art „Versiegelung“ vorgenommen. Um vorlegen zu können, dass während den Ermittlungen keine Daten manipuliert wurden, wird mit einem speziellen Programm ein Hashcode oder Hashwert (eine Art Prüfsumme, die jedes Bit eines Datenträgers berücksichtigt), berechnet. Die Berechnung des sogenannten digitalen Fingerabdruckes kann bis zu mehreren Stunden dauern.

Danach können die Daten des suspekten Rechners auf einen zweiten Computer kopiert werden ohne an den Originaldaten etwas abzuändern. Dabei wird gleichzeitig der Hashcode der kopierten Daten berechnet, der mit dem des Originals übereinstimmen muss. Erst ab hier können die weiteren Untersuchungen vorgenommen werden.

Nach der Sicherstellung der verdächtigen Daten kann der Computer entweder mitgenommen, versiegelt oder weiter für die Arbeit genutzt werden. Abhängig von der Art des vermuteten Delikts.

Nach den Untersuchungen werden die Berichte erstellt und mit den entsprechenden Dateien auf einem separaten Medium abgelegt.

## 2.2.6 Datenschutz

Datenschutz, der Schutz der Privatheit oder "Privacy", ist ein Grundrecht unserer liberalen Rechts- und Gesellschaftsordnung. Die Europäische Menschenrechtskonvention und die Bundesverfassung garantieren das Recht auf Datenschutz, welches eine Reaktion ist auf die rasante Entwicklung der Informations- und Kommunikationstechnologien seit den sechziger Jahren des vergangenen Jahrhunderts.

Das schweizerische Datenschutzgesetz (DSG) beinhaltet klare Richtlinien, die beim Erstellen einer Datenbank von Persönlichkeitsdaten befolgt werden müssen. Grundsätzlich gilt.<sup>35</sup>

- Personendaten dürfen nicht wider Treu und Glauben erhoben werden (z.B. durch absichtliche Täuschung)
- Institutionen dürfen Personendaten nur insoweit erheben/bearbeiten, als dass sie für die geschäftlichen Aufgaben unentbehrlich sind.

---

<sup>34</sup> vgl. Kronenberg, 2002

<sup>35</sup> vgl. Universität Bern, 2003

- Wird der Zweck der Datenbearbeitung geändert, muss im Voraus die ausdrückliche Zustimmung der betroffenen Person eingeholt werden.
- Löschen nicht mehr benötigter Daten.
- Falls Personendaten an Dritte weitergegeben werden oder regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet und wenn für die Bearbeitung keine gesetzliche Pflicht besteht, muss die Datensammlung beim eidg. Datenschutzbeauftragten angemeldet werden, soweit die betroffene/n Person/en keine Kenntnis davon haben.
- Jede Person, deren Daten in einer Datensammlung bearbeitet werden, hat das Recht, über alle diese Daten Auskunft zu erhalten. Dies geschieht in der Regel kostenlos.

Ebenfalls regelt das schweizerische Datenschutzgesetz die Wahl eines Eidgenössischen Datenschutzbeauftragten ([www.edsb.ch](http://www.edsb.ch)) welcher insbesondere folgende Aufgaben hat:<sup>36</sup>

- Aufsicht über Bundesorgane
- Aufsicht über Privatpersonen
- Beratung von privaten Personen
- Unterstützung und Beratung der Organe des Bundes und der Kantone
- Stellungnahme zu Rechtsvorlagen des Bundes
- Zusammenarbeit mit in- und ausländischen Datenschutzbehörden
- Information der Öffentlichkeit
- Führung und Veröffentlichung des Registers der Datensammlungen.

Das Datenschutzgesetz (DSG) setzt die rechtlichen Rahmenbedingungen für den Umgang mit Personendaten fest. Mit zusätzlichen technischen Mitteln zum sicheren Verwalten und Transportieren von Daten kann ein umfassender Datenschutz erreicht werden.

Die wachsende Datenmenge und ihre zunehmende Sensibilität (z.B. Finanz- oder Geninformationen) ist eine wachsende Herausforderung für den Schutz von Personendaten.

Informationen und Daten werden für das Funktionieren unserer Gesellschaft immer wichtiger. Der gesunde Ausgleich zwischen Zugang zu Informationen und Schutz der persönlichen Informationen ist ein wichtiger Bestandteil des Datenschutzes.

Bei dieser schwierigen Gratwanderung überschneiden sich die Anliegen von Bürgerrechtsorganisationen und Strafverfolgungs-Behörden. Die einen setzen sich für den Schutz der Privatsphäre ein, und die anderen sind auf lückenlose Rückverfolgung und Sicherung von Datenspuren angewiesen. Hier gilt es einen gemeinsamen Nenner zu finden!

Angesichts der rasanten Entwicklung im Bereich der Informations- und Kommunikationstechnologien erstaunt es nicht, dass die rechtlichen Grundlagen nicht Schritt zu halten vermögen und deshalb nicht der heutigen technologischen Realität entsprechen.<sup>37</sup>

Unternehmungen, welche maximale Vorkehrungen treffen, um Angriffe nachzuvollziehen und die Beweise in elektronischer Form sicherzustellen, laufen Gefahr, den Datenschutz zu verletzen.<sup>38</sup>

---

<sup>36</sup> vgl. Eidgenössischer Datenschutzbeauftragter, 2003

<sup>37</sup> vgl. Baeriswyl, 2000

<sup>38</sup> vgl. Sury, 2002

## 3 Prophylaxe

*„Der sicherste PC ist der Rechner, der keine Aussenanbindung besitzt, in einem feuersicheren Panzerschrank steht, keine Tastatur hat und ohne Wechsellaufwerke auskommt“.<sup>39</sup>*

Diese Aussage ist zweifelsohne richtig. In der heutigen Zeit brauchen Computer jedoch immer dringender Anbindungen zur Aussenwelt um Datenverbindungen und -austausch zu ermöglichen. Diese Anbindungen werden für die normalen Geschäftsabläufe immer wichtiger - ein erheblicher Teil der Firmen kommt heute ohne Internetanbindung nicht mehr aus. Dazu steigt unaufhörlich die Anzahl der privaten Internetuser. Umso mehr man vernetzt ist, umso vielfältiger sind die Gefahren aus dem Netz.

Nebst allen Anstrengungen zur Bekämpfung der Cyber-Kriminalität kann mit gezielter Prophylaxe bereits viel verhindert werden. In diesem Kapitel werden nationale und internationale Aktivitäten zur Prävention und Massnahmen zur Vorbeugung der Cyber-Kriminalität vorgestellt.

### 3.1 Warum ist Schutz wichtig?

Im weltweiten Netz gibt es viele Gefahren. Insbesondere für Unternehmungen ist es überlebenswichtig, dass sie die virtuellen Bedrohungen ernst nehmen und sich dagegen schützen. Doch auch für Privatpersonen ist es wichtig, dass sie sich der Gefahren bewusst sind und entsprechende Massnahmen treffen.

Im Folgenden werden einige Gefahren für Unternehmungen sowie Privatanwender dargelegt.

#### 3.1.1 Gefahren für Unternehmungen<sup>40</sup>

Die Benutzung von Infrastrukturen der Informationstechnologie (IT) ist heute zu einer betrieblichen Selbstverständlichkeit geworden, nicht aber das Bewusstsein der eigenen Abhängigkeit von Anwendungen, Daten und IT-Systemen. Das Risikopotential und die daraus resultierende Verletzlichkeit wird deshalb oft unterschätzt.

Für ein Unternehmen ist das IT-Bedrohungsbild komplex und beinhaltet mehr als nur Computerviren und fehlende Firewalls. Konkurrenten könnten beispielsweise Wirtschaftsspionage betreiben. Ebenso sind Fälle bekannt, in denen Firmen versuchten, ihre Konkurrenten durch gezielte Attacken lahmzulegen<sup>41</sup>. Eine nichtfunktionierende IT-Infrastruktur hat enorme Folgen für die Unternehmung. Eine weitere grosse Gefahr ist der drohende Imageverlust, falls ein Angriff bekannt würde. Im Extremfall können IT-Zwischenfälle betroffene Unternehmen in ihrer Existenz gefährden. Eine gute IT-Sicherheit in den Unternehmungen ist also überlebenswichtig.

---

<sup>39</sup> vgl. Rittelmeier, 2003

<sup>40</sup> vgl. Arrigoni, 2003

<sup>41</sup> Interview Roland Portmann, 19.02.2003

### 3.1.2 Gefahren für Privatanwender

Obwohl man als Privatanwender normalerweise keine sensiblen Geschäftsdaten auf dem Rechner hat, ist es dennoch wichtig, sich vor den Gefahren des Internet zu schützen. Denn es gibt mit Sicherheit auf jedem privaten Rechner Daten, welche man nicht in fremde Hände geben möchte. Oder es könnte folgendes passieren:

- Datenbeschädigung oder -verlust durch Viren  
(ein Virus löscht Daten auf der Festplatte)
- Finanzielle Schäden durch Dialer<sup>42</sup>  
(ein Dialer wählt sich ohne eigenes zutun auf teure Telefonnummern ein)
- Kreditkartenmissbrauch  
(ein Cracker benutzt eine bei einem Onlinegeschäft eingegebene Kreditkartennummer für eigene Zwecke)
- Verletzung der Privatsphäre  
(ein Hacker liest beispielsweise Steuererklärung oder Bewerbungen)

Ein weiterer, wichtiger Punkt ist der Schutz der Kinder. Im Web gibt es (fast) alles zu sehen. Doch nicht jeder soll alles sehen. Ebenso tummeln sich in Chatrooms oder Newsgroups viele dunkle Gestalten. In diesem Bereich sollte auch Prophylaxe betrieben werden.

### 3.1.3 Unschuldiger Täter

Alle Massnahmen sollten keineswegs nur dazu dienen, nicht zum Opfer zu werden, sondern auch um nicht ungewollt zum Täter zu werden.

Beispielsweise kann der Server einer Unternehmung als Zwischenstation für einen Hacker-Angriff dienen. Als Quelle des Angriffes würde dann die IP-Adresse der Unternehmung dienen. Somit wäre man ungewollt zum Täter geworden.

Oder ein falsch konfigurierter Mailserver eines Unternehmens könnte für einen Fremd-Relay Server bei Spamming<sup>43</sup> missbraucht werden (Spammer → Relay<sup>44</sup> → Opfer). Dabei kann sich der Spammer hinter unschuldigen Tätern (Relay) verstecken. Dazu schickt der Spammer seine Mails nur einmal an das Relay, aber mit einer gigantischen Adressliste. Das missbrauchte Relay macht dann die eigentlich "Arbeit".<sup>45</sup>

Zu beachten gilt ebenfalls, dass bereits der Besitz von kinderpornografischem Material strafrechtlich geahndet wird. Falls man also im Internet auf solche Bilder stösst, sollte man aus diesem Grund keinerlei Material zu Beweis Zwecken speichern oder downloaden! Ebenfalls sollte man gemäss Webauftritt der Koordinationsstelle für Internet-Kriminalität (KOBIK) keinesfalls auf möglicherweise strafbare Anzeigen antworten und nicht aktiv nach strafrechtlich relevanten Internet-Inhalten suchen.<sup>46</sup>

---

<sup>42</sup> Dialer sind Programme, die selbst eine Verbindung ins Internet oder zum Server des Providers aufbauen.

<sup>43</sup> Spamming: Massenversand im Internet mit kommerzieller Absicht.

<sup>44</sup> Als Mail-Relaying wird das Entgegennehmen und anschließende Weiterleiten einer E-Mail durch ein Rechner-system bezeichnet. Der dafür genutzte Rechner ist dann ein Mailrelay-Rechner, kurz auch Mailrelay.

<sup>45</sup> vgl. MTA's und Fremd-Relaying, 2003

<sup>46</sup> vgl. Koordinationsstelle Internet-Kriminalität

## 3.2 Prophylaktische Aktivitäten

Die Wichtigkeit prophylaktischer Tätigkeiten wurde erkannt. Es werden auf nationaler und internationaler Ebene diverse Anstrengungen unternommen.

### 3.2.1 Erziehung der „Cyber-Citizen“<sup>47</sup>

So wie den Kindern durch entsprechende Erziehung und Sozialisation die Grundregeln des Zusammenlebens in der „Offline-Welt“ beigebracht werden, so muss man dies selbstverständlich auch in der „Online-Welt“ tun. Dabei kann man davon ausgehen, dass die ethischen Standards der alten traditionellen Welt auch in der neuen Online-Welt zu gelten haben. Letztendlich geht es darum, möglichst jeden Internet-Teilnehmer sich zu einem rücksichts- und verantwortungsvollen „Cyber-Citizen“ entwickeln zu lassen, der wie jeder normale Bürger in der traditionellen Welt auch, einerseits seine freiheitlichen und demokratischen Rechte genießen kann, der sich aber andererseits auch seiner sozialen Verantwortung und seiner entsprechenden Pflichten bewusst ist.

Unter dem Begriff „The Cybercitizen Partnership“ (<http://www.cybercitizenship.org>) gibt es in den USA seit kurzer Zeit ein bundesweites, staatlich initiiertes Projekt, welches die Förderung und Verbreitung von diesbezüglichen Programmen und Erziehungskonzepten unterstützt. Die Internet-Teilnehmer (Cyber-Citizens) sollen nicht nur lernen, wie man sich vor eventuellen Angriffen und Gefahren im Netz schützen kann, sondern auch wie man sich selbst den anderen gegenüber verantwortungsbewusst im Netz verhält. Dabei kann auch hier die „goldene Regel“ als Grundorientierung dienen: „Was Du nicht willst, das man Dir tut, das füg auch keinem andern zu.“

### 3.2.2 Projekte International

#### 3.2.2.1 USA - cybercrime.gov

Die „Abteilung für Computerkriminalität und geistiges Eigentum“ (Computer Crime and Intellectual Property Section - CCIPS<sup>48</sup>) der Strafkammer des U.S. Justizministeriums hat mit „cybercrime.gov“ ein umfangreiches und informatives Angebot geschaffen. Dies beinhaltet u.a. allgemeine Informationen zur CCIPS und zur Anzeige von Internetstraftaten. Daneben gibt es Dokumente mit weiterführenden Linkhinweisen zu Themen, die mit Cybercrime im Zusammenhang stehen. Das eigentliche Angebot besteht in der Dokumentensammlung zu den drei Themengebieten „Computercrime“, „Intellectual Property Crime“ und „Cybercrime Documents“. Die ersten beiden Kategorien umfassen Erläuterungen zur jeweiligen Verfahrensweise, Orientierungshilfen, Dokumente, Gesetzestexte und zahlreiche Berichterstattungen zur einschlägigen Rechtsprechung. In der Rubrik „Cybercrime Documents“ befinden sich u.a. Pressemitteilungen, Reden und Leitfäden. Das gesamte Angebot lässt sich zudem individuell an die eigenen Informationsbedürfnisse anpassen. So gibt es z.B. die Möglichkeit, nur für Studenten oder Eltern relevante Texte anzuzeigen. Aber auch ein Opfer der Computerkriminalität oder ein Mitglied der High-Tech-Industrie kann für sich relevante Informationen herausfiltern lassen.<sup>49</sup>

---

<sup>47</sup> vgl. Rüter, 2003

<sup>48</sup> vgl. Computer Crime and Intellectual Property Section (CCIPS), 2003

<sup>49</sup> vgl. Juristisches Internetprojekt Saarbrücken, 2003

### 3.2.2.2 EU - Aktionsplan für mehr Sicherheit im Internet

Die Europäische Union ist seit 1996 eine Vorkämpferin gegen illegale und schädliche Inhalte auf dem Internet. In diesem Zusammenhang wurde der Aktionsplan für mehr Sicherheit im Internet (Safer Internet Action Plan)<sup>50</sup> geschaffen, woraus in den letzten vier Jahren eine Reihe von Projekten entstanden sind. Diese werden von der EU mit 25 Mio. € finanziell unterstützt und gefördert.

Der Aktionsplan verfolgt drei Ziele:

- Schaffung eines europäischen Netzwerks von Hotlines und die Förderung von Selbstregulierung und Verhaltensregeln.
- Entwicklung und Bewertung von Filtersoftware und Filterdiensten sowie die Förderung einer nutzerfreundlichen Inhaltsklassifizierung.
- Aufklärung über die Gefahren des Internets und Förderung von Sensibilisierungsmassnahmen.

Die aktuellen Berichte, News und Informationen rund um den Aktionsplan und der verschiedenen Projekte sind auf der Webseite [www.saferinternet.org](http://www.saferinternet.org) abrufbar.

Wichtigster Beitrag des Aktionsplans zur sichereren Nutzung des Internet zum Kampf gegen illegale Inhalte ist das europäische Meldstellennetz. Die Meldstellen nehmen Klagen der Nutzer über illegale Inhalte entgegen. Nach einer Prüfung der Klage wird diese an die entsprechende Stelle – die Polizei, Internet-Diensteanbieter oder eine andere Meldestelle – weitergeleitet. Derzeit hat das europäische Netz Mitglieder in 11 Ländern, nämlich in Belgien, Dänemark, Deutschland, Frankreich, Irland, Island, den Niederlanden, Österreich, Schweden, Spanien und dem Vereinigten Königreich. Der Verband INHOPE<sup>51</sup>, dem alle Meldestellen angehören, veranstaltet Treffen, gibt Leitlinien bezüglich vorbildlicher Verfahren heraus und ermutigt neue Mitglieder. In den Vereinigten Staaten und in Australien hat er assoziierte Mitglieder.<sup>52</sup>

Der Aktionsplan hatte eine Laufzeit von vier Jahren und endete am 31. Dezember 2002. Als Nachfolgeprogramm wurde von der Europäischen Kommission das eSafe-Programm vorgeschlagen. Die Entscheidung darüber wird noch im Europäischen Parlament und Rat diskutiert. Nach endgültiger Genehmigung soll das Programm im März 2003 beginnen und für zwei Jahre fortgeführt werden.<sup>53</sup>

eSafe besteht aus vier Aktionslinien:

- **Ein sicheres Umfeld**  
Das beinhaltet die Schaffung und Erweiterung des europäischen Netzwerks von Hotlines und die Förderung von Selbstregulierung und Verhaltensregeln.
- **Filtersysteme und Klassifizierung von Internet-Inhalten**  
Das beinhaltet die Bewertung von Filtersoftware und Filterdiensten und die Förderung einer nutzerfreundlichen Inhaltsklassifizierung.
- **Aufklärung**  
Hier kommt es besonders auf die Schaffung eines weitreichenden europäischen Netzwerks und angewandte soziologische Forschung an.

<sup>50</sup> vgl. Safer Internet Action Plan, 2003

<sup>51</sup> <http://www.inhope.org>

<sup>52</sup> vgl. Internet Action Plan follow-up, 2003

<sup>53</sup> vgl. Safer Internet, 2003

- **Programmunterstützung**

Man beabsichtigt, eine engere Verbindung zwischen den einzelnen Aktionslinien herzustellen, z.B. zwischen Hotlines und Aufklärungsaktivitäten oder zwischen Klassifizierung und Selbstregulierung.

### 3.2.2.3 Interpol

Die internationale kriminalpolizeiliche Organisation Interpol<sup>54</sup>, welcher rund 150 Mitgliedsstaaten angehören, informiert auch auf ihrem Webauftritt zum Thema "Information Technology Crime". Hier werden die verschiedenen Risiken im IT-Umfeld erläutert und für Unternehmen und Privatpersonen nützliche Empfehlungen zur Kriminalprävention in Form von Checklisten zur Verfügung gestellt.

### 3.2.2.4 Aktivitäten in Deutschland

In Deutschland gibt es eine Reihe von Webseiten, die sowohl Privatanwender als auch Unternehmen über die Erscheinungsformen der Cyber-Kriminalität und die Gefahren des Internets informieren und aufzeigen, mit welchen Massnahmen ein optimaler Schutz vor den Gefahren erreicht werden kann. Hier sollen exemplarisch ein paar Beispiele vorgestellt werden.

Führend in diesem Zusammenhang ist das Bundesamt für Sicherheit in der Informationstechnik BSI. Auf der Webseite [www.bsi.de](http://www.bsi.de) sind umfassende Informationen über die Internet-Sicherheit, IT-Grundschutz sowie die in den Jahren seiner Tätigkeit erzielten Arbeitsergebnisse abrufbar. Mit dem Internetauftritt [www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de), der sich eher an Privatanwender richtet, sollen Internetnutzer mit leicht verständlichen Texten und kurzweiligen Illustrationen für das Thema „IT-Sicherheit“ sensibilisiert werden. Der Internetauftritt ist eine Weiterentwicklung der CD-ROM „Ins Internet – mit Sicherheit!“, welche über 650'000 mal kostenlos an Bürgerinnen und Bürger verteilt wurde.<sup>55</sup>

Das Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) informiert auf der Webseite [www.polizei.propk.de](http://www.polizei.propk.de) vor allem Eltern und Kinder über die potentiellen Gefahren des Internets sowie mögliche Massnahmen für eine sichere Nutzung. Speziell wird auf den Schutz für Kinder eingegangen.<sup>56</sup>

Interessant für Private wie auch Unternehmungen ist das Portal [www.sicherheit-im-internet.de](http://www.sicherheit-im-internet.de) vom deutschen Bundesministerium für Wirtschaft und Arbeit (BMWA) und des deutschen Bundesministerium des Innern (BMI). Die Plattform bietet ein umfangreiches Angebot zum Thema „Sicherheit im Internet“. Zwei weitere Projekte mit dem Ziel, Straftaten im Internet durch entsprechende Aufklärung zu verhindern sind [computerbetrug.de](http://computerbetrug.de) und [dialerhilfe.de](http://dialerhilfe.de). Das Angebot richtet sich hierbei vor allem an den Privatanwender.<sup>57</sup>

## 3.2.3 Aktivitäten in der Schweiz

Die neu geschaffene Koordinationsstelle zur Bekämpfung der Internet-Kriminalität KOBIK<sup>58</sup> nimmt im Bereich Monitoring und Analyse der Cyber-Kriminalität eine entscheidende Rolle ein. Die beiden Be-

---

<sup>54</sup> <http://www.interpol.int>

<sup>55</sup> vgl. Ins Internet – mit Sicherheit!, 2003

<sup>56</sup> vgl. So schützen Sie sich vor Risiken im Internet, 2003

<sup>57</sup> Die Projekte laufen unter dem Dach des Interessenverband Deutsches Internet e.V. (IDI) in München.

<sup>58</sup> vgl. Kap. 2.2.4 Koordinationsstelle zur Bekämpfung der Internet-Kriminalität

reiche der Koordinationsstelle sind dem Dienst für Analyse und Prävention (DAP) zugeteilt. Aus den Analysetätigkeiten gehen Berichte für verschiedene Empfänger wie Strafverfolgungsbehörden, politische Instanzen oder die Öffentlichkeit hervor. Die Grundlage für die Kooperation im Bereich Prophylaxe der Cyber-Kriminalität ist somit gegeben.

In der Schweiz gibt es eine Vielzahl von Organisationen, die sich mit den Gefahren des Internets und den möglichen Schutzmassnahmen auseinandersetzen. Allgemein gefasst - die Sicherheit um Informationen steht hoch im Kurs.

Eine Stiftung die sich mit diesem Thema befasst ist InfoSurance. Diese hat zum Zweck die Informationssicherheit in der Schweiz zu erhöhen. Dazu sollen

- Entscheidungsträger und Benutzer der Informationstechnologien im öffentlichen und privaten Sektor bezüglich Gefahren und Risiken sensibilisiert werden.
- Organisatorische und technische Voraussetzungen zur Früherkennung von Gefahren, zu ihrer Prävention sowie zur Schadenminderung und -bewältigung geschaffen werden.
- Zusammenarbeit zwischen Wirtschaft, Wissenschaft und Staat gefördert werden.

An der Stiftung sind namhafte Firmen aus der Privatwirtschaft, wie z.B. Microsoft, Siemens, UBS, Swisscom aber auch der Bund beteiligt.

Mit Fragen der Sicherheit in Informationssystemen beschäftigt sich die Fachgruppe Security (FGSec)<sup>59</sup> der Schweizer Informatiker Gesellschaft (SI). Die Fachgruppe unterstützt Kontakte und Erfahrungsaustausch unter den Mitgliedern, und pflegt Kontakte mit anderen nationalen und internationalen Organisationen.

Daneben gibt es noch eine Vielzahl anderer Vereinigungen und Fachgruppen wie

- Stiftung für Datenschutz und Informationssicherheit (SDI)<sup>60</sup>
- Sicherheitsgruppe (SGRP)<sup>61</sup>
- Schweizer Verband der Sicherheit von Informationssystemen (CLUSIS)<sup>62</sup>
- Information Systems Audit and Control Association (ISACA)<sup>63</sup>
- Information Systems Security Association (ISSA)<sup>64</sup>

Prophylaktische Aktivitäten werden auch von den Datenschutzbehörden unternommen. Auf der Webseite des Datenschutzbeauftragten des Kanton Zürich [www.datenschutz.ch](http://www.datenschutz.ch) werden z.B. konkrete Hinweise und Tipps für Anwender zur Verbesserung der Sicherheit im Internet geboten.

Erwähnt werden soll an dieser Stelle die beiden Websites [www.computer-security.ch](http://www.computer-security.ch) und [www.computec.ch](http://www.computec.ch). Sie bieten dem Benutzer viele aktuelle Informationen zu den Themen Computer, Technik und Sicherheit.

---

<sup>59</sup> <http://www.fgsec.ch>

<sup>60</sup> <http://www.privacy-security.ch>

<sup>61</sup> <http://www.sgrp.ch>

<sup>62</sup> <http://www.clusis.ch>

<sup>63</sup> <http://www.isaca.ch>

<sup>64</sup> <http://www.issa-suisse.org>

Im Bereich Aus- und Weiterbildung im Zusammenhang mit Information, Technik und Sicherheit mischt die Schweiz an vorderster Front mit. So bieten Universitäten, Fachhochschulen und private Firmen ein breites Angebot an Studiengängen, Lehrgängen und Kursen zu den genannten Themenbereichen an. An der Hochschule für Wirtschaft in Luzern wird seit kurzem in Zusammenarbeit mit dem Schweizerischen Polizeiinstitut ein speziell für die Strafverfolgungsbehörde ausgelegter Kurs „IT-Ermittler“ angeboten. Der Kurs ist erfolgreich angelaufen und gilt in der Schweiz als einzigartig in diesem Fachbereich.

Nach Recherchen im Internet ist allgemein festzustellen, dass in der Schweiz zur Vorbeugung und Prävention der Cyber-Kriminalität, im Vergleich zum benachbarten Ausland, dem Privatanwender auf dem Internet eher wenig Informationen zur Verfügung gestellt wird. Hier besteht ein dringender Nachholbedarf.

Es ist vor allem zum Schutz der Kinder und Jugendlicher wichtig, dass ihnen die Möglichkeit geboten wird, sich über die Gefahren zu informieren.

### 3.3 IT-Sicherheit im Unternehmen

Information hat heute aus betriebs- und volkswirtschaftlicher Sicht die gleiche Bedeutung wie die klassischen Produktionsfaktoren Arbeit, Kapital und Boden. Für ihren Schutz wird viel Aufwand betrieben, z.B. Arbeitssicherheit, Absicherung von Investitionsrisiken, oder Vorsorge- und Sozialversicherungen.

Der Schutz der wichtigen Ressource Information ist oft nur in Teilbereichen und wenig koordiniert gewährleistet, obwohl Information sehr leicht kopiert, entwendet oder verändert werden kann. Verlust, Manipulation oder Diebstahl von Informationen kann ein Unternehmen existenziell bedrohen.<sup>65</sup>

#### 3.3.1 Sicherheit der Informationstechnologie

Durch den Einsatz von Informationstechnologie als Träger der Informationen und die weltweite Vernetzung von verschiedenen Systemen werden Unternehmensdaten unterschiedlichen Bedrohungen ausgesetzt. Davor gilt es die IT-Systeme zu schützen.

Weder im Leben noch in der Technik kann es eine absolute Sicherheit geben. Aus unternehmerischer Sicht sollte der Begriff IT-Sicherheit als eine zentrale Eigenschaft von Geschäftsprozessen verstanden werden, die durch geeignete technische und organisatorische Massnahmen sicherstellt, dass das Restrisiko für die Organisation auf ein tragbares Mass reduziert wird.<sup>66</sup>

Bevor etwas abgesichert wird, muss geklärt werden, wie, was, wovor abgesichert werden soll. Dieses Wie, Was und Wovor wird als eine Reihe von Entscheidungen in einem Sicherheitskonzept definiert.

IT-Sicherheit ist kein Produkt, sondern ein Managementprozess.

---

<sup>65</sup> vgl. InfoSurance, 2000

<sup>66</sup> vgl. Raepple, 2001, S. 7

### 3.3.2 Technische Möglichkeiten

In den folgenden Kapiteln wird auf ein paar wichtige Hilfsmittel eingegangen, mit welchen das Sicherheitskonzept technisch umgesetzt werden kann.

#### Firewalls

Um der drohenden Angriffsgefahr aus dem Internet zu begegnen, werden in den letzten Jahren verstärkt Filtermechanismen, sogenannte Firewalls, eingesetzt, um das lokale Netzwerk oder einen einzelnen Computer zu schützen. Zu diesem Zweck filtern sie den Datenverkehr, der über sie geleitet werden soll. Anhand bestimmter Regeln wird entschieden, welche Datenpakete die Firewall passieren dürfen und welche nicht (vgl. Abbildung 2). Diese Regeln können vom Benutzer der Firewall konfiguriert werden, um eine strenge oder weniger strenge Filterung zu erreichen.

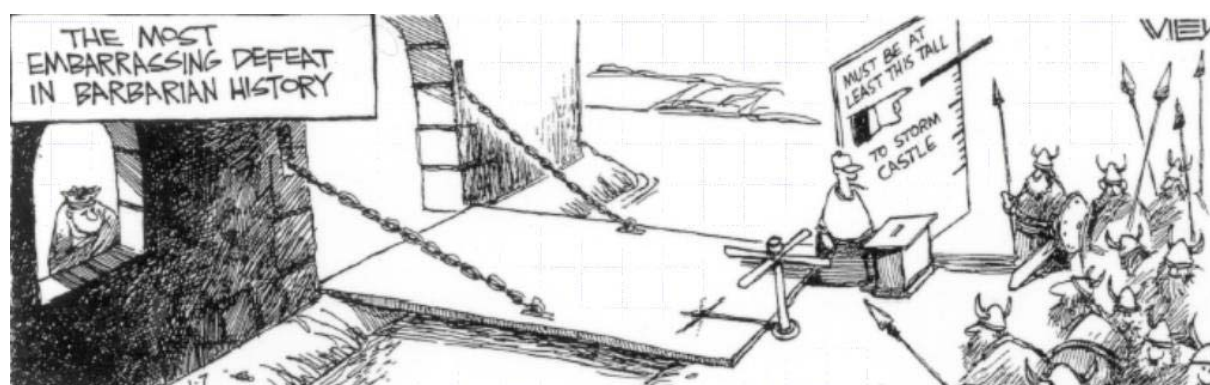


Abbildung 2: „Firewall“<sup>67</sup>

Eine Firewall kann ein Netz gegen Gefahren sichern. Doch dies ist kein Allheilmittel, denn es gibt immer noch Möglichkeiten, das zu sichernde Netz zu schädigen. So erfolgt laut der Studie von FBI/CSI ein Grossteil der Hackerangriffe aus dem eigenen internen Netz, also durch Mitarbeiter<sup>68</sup>. Eine Firewall sichert das zu schützende Netz also primär gegen Gefahren von aussen. Gefahren von innen müssen somit mit anderen Massnahmen bekämpft werden und können zum Teil mit Intrusion Detection Systemen analysiert und abgefangen werden. Mehr dazu im nächsten Kapitel.

Ein externes Netz, wie zum Beispiel das Internet, bringt immer neue Bedrohungen für das interne Netz mit sich. Viele Nutzer verfügen über ausreichende Kenntnisse, um andauernd neue Sicherheitslücken zu finden, die zu neuen Attacken führen können. Eine Firewall schützt nie vollständig gegen alle Bedrohungen. Eine ständige Pflege und Administration der Firewall-Konfiguration ist daher extrem wichtig.

#### Intrusion Detection Systems (IDS)

Die Entwicklung in der IT-Security hat gezeigt, dass reine Firewall-Systeme keinen absoluten Schutz vor Angriffen bieten. Ein grosser Teil der Angriffe kommt von eigenen Mitarbeitern, gegen die eine Firewall nichts ausrichten kann. Besser ist es grundsätzlich mit Angriffen zu rechnen und diese zu erkennen. Hier kommen Intrusion Detection Systeme zum Einsatz. Diese Systeme dienen der Erkennung von Angriffen auf ein Computersystem oder Netzwerk. Sie beobachten den Datenverkehr und

<sup>67</sup> Quelle: W. Cheswick, S. Bellovin: Firewalls and Internet Security, Addison- Wesley, 1994

<sup>68</sup> vgl. Computer Security Institute, 2002

beurteilen anhand von Regeln, ob gerade ein Angriff stattfindet, oder ob ein Angriff stattgefunden hat. Im ersten Fall schlägt ein IDS Alarm und meldet die Angriffe, damit schnell Gegenmassnahmen getroffen werden können. Im zweiten Fall kann der Systembetreuer im Nachhinein den Angriff analysieren.

Intrusion Detection Systeme gewinnen immer mehr an Bedeutung. Es ist damit zu rechnen, dass solche Systeme in Zukunft vermehrt auch in KMU-Betrieben zum Einsatz kommen werden.<sup>69</sup>

### Anti-Virus Software

Die grösste Bedrohung ihres Unternehmens sehen viele Manager in Viren. Die Antivirus-Technologie ist ausgereift, kostengünstig und leicht zu installieren. Nachteilig ist sicherlich, dass eine regelmässige Wartung und Erneuerung zwingend ist.

### Verschlüsselungstechnologien

Oft sollen Daten gesichert und verschlüsselt übertragen werden. Dazu werden Technologien wie SSL, VPN oder PGP eingesetzt.

Daneben gibt es noch eine Vielzahl anderer Technologien, deren Erklärung den Rahmen vorliegender Arbeit sprengen würde.

## 3.3.3 US-Statistik der Sicherheitstechnologien

Eine US-Studie des CSI (Computer Security Institute) zeigt, welche Sicherheitstechnologien von US-Grossunternehmen aus verschiedenen Branchen verwendet werden. Von den 500 befragten Unternehmen im Jahr 2002 setzten 89% Firewalls ein, 60% verwendeten Intrusion Detection Systeme und 90% gaben an, Antivirus-Software zu verwenden.<sup>70</sup>

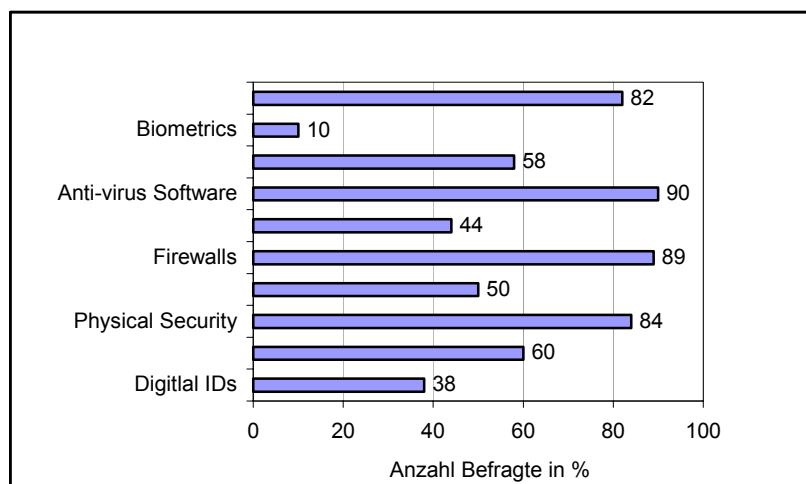


Abbildung 3: Einsatz von Sicherheitstechnologien in US-Grossunternehmen (2002)

<sup>69</sup> Interview Roland Portmann, 19.02.2003

<sup>70</sup> vgl. Computer Security Institute, 2002

### 3.3.4 Sensibilisierung des Managements

Wie bereits erwähnt ist IT-Sicherheit eine Aufgabe des Managements. Grössere Unternehmen besitzen meist eigene professionelle Abteilungen, die sich mit dem Thema der IT-Sicherheit auseinandersetzen und aktiv Forschung in diesem Umfeld betreiben. Diese sind meistens genügend gegen Attacken abgesichert. Problematisch ist die Situation bei kleineren und mittelgrossen Betrieben, wo der IT-Sicherheit noch zuwenig Bedeutung zukommt. Wichtig ist, dass auch hier das Management sich über die Gefahren im Zusammenhang mit der Cyber-Kriminalität bewusst wird, und in der Lage ist, mögliche Risiken zu erkennen und nötigenfalls Schutzmassnahmen zu ergreifen.

Dabei handelt es sich nicht nur um technische Massnahmen. Das Management muss auch die eigenen Mitarbeiter genügend auf Gefahren, wie Social Hacking, aufmerksam machen. Beim passiven Social Hacking versucht der Hacker durch das Ausspionieren des sozialen Umfeldes an Passwörter zu gelangen ohne dabei programmtechnisches Wissen zu haben. Beim aktiven Social Hacking versucht der Hacker durch Angabe einer falschen Identität an Passwörter oder wichtige Unternehmensinformationen zu gelangen ohne dabei ebenfalls programmtechnisches Wissen zu haben. Der Hacker gibt sich z.B. als Administrator des Providers aus und verwendet irgendeinen Vorwand um an das Passwort zu gelangen. Für das Management ist es deshalb von Bedeutung, dass sie ihre Mitarbeiter aufklären und klare Richtlinien herausgeben. Unaufgeklärte Mitarbeiter können ungewollt dem Arbeitgeber grossen Schaden zufügen.<sup>71</sup>

## 3.4 Schutz im privaten Bereich

Die Mehrheit der Internetuser geht sorglos mit Ihren Daten um. Die technischen Möglichkeiten zum Schutz sind jedoch vorhanden - sie müssen nur genutzt werden! Im folgenden werden einige wichtige Tools erläutert, welche jeder Internetuser haben sollte. Zugleich werden einige Tipps zum Verhalten im Internet gegeben, um die Privatsphäre zu schützen.

### 3.4.1 Tools<sup>72</sup>

Wer regelmässig im Internet surft, häufig E-Mail schreibt und Programme runterlädt, dem wird dringend der Einsatz von folgenden Programmen empfohlen:

- **Einen guten Virens Scanner**  
(z.B. McAfee, Norton AntiVirus oder AVG)
- **Eine Firewall und/oder ein Intrusion Detection System (IDS)**  
(z.B. ZoneAlarm oder Norton Personal Firewall)

Je nach Erfahrung des Benutzers empfiehlt sich ein spezieller Trojaner-Scanner<sup>73</sup> oder zusätzliche Tools.

Wie bereits erwähnt, gibt es im Internet nahezu alles zu sehen. Doch die meisten Eltern wollen nicht, dass ihre Sprösslinge die dunklen Seiten des Internets durchstöbern. Filtersysteme versprechen, nur

---

<sup>71</sup> vgl. Social Hacking, 2003

<sup>72</sup> vgl. Schutz im Internet Teil 2, 2003

<sup>73</sup> Trojaner: Programm, welches neben seiner eigentlichen Aufgabe unbemerkt ein Virus transportiert.

das zum Browser durchzulassen, was Eltern oder Administratoren erlauben. Programme wie Cyber-Patrol oder NetNanny erfüllen diese Funktion.<sup>74</sup>

All diese Tools nützen wenig, wenn sie nicht richtig benutzt werden. Hier sind einige Ratschläge, die jeder Internetuser beherzigen sollte:

- Immer auf Programm-Updates achten. Ganz besonders bei den Virenscannern. Ausserdem müssen die Virendatenbanken regelmässig aktualisiert werden.
- Mindestens einmal im Monat das gesamte System mit dem Virenschanner scannen. Häufige Internetuser sollten besser wöchentlich mit den neusten Virensignaturen scannen.
- Darauf achten, dass die aktuellen Sicherheits-Updates für das Betriebssystem installiert sind.
- Beim Download von Programmen ist Vorsicht geboten. Nach Möglichkeit keine Programme aus zweifelhaften Quellen downloaden. Ausserdem vor der Programminstallation unbedingt auf Viren oder Trojaner hin scannen.
- Anhänge von E-Mails sollten nie geöffnet werden, ohne sie vorher gescannt zu haben - besonders bei unbekanntem Absender. Auch wenn es vermeintliche Text-Dateien oder Bilder sind.
- Die Sicherheitseinstellungen des Browser überprüfen. Bei der Standardinstallation sind viele Sicherheitslücken offen (z.B. ActiveX, Java).

### 3.4.2 Schutz der Privatsphäre<sup>75</sup>

Um seine Privatsphäre zu schützen kann jeder einzelne einiges unternehmen. Persönliche Informationen werden viel zu leichtfertig preisgegeben.

#### 3.4.2.1 Datensammler im Netz

Sobald man ins Internet geht, ist es mit der Privatsphäre vorbei. Bereits beim Provider, über den der Internetzugang hergestellt wird, laufen etliche Daten über den Benutzer auf, anhand derer man identifiziert werden könnte. Doch es geht noch weiter. Bei jedem Besuch einer Webseite werden automatisch Daten des Besuchers gespeichert. Das beginnt beim Referrer, der zeigt, auf welcher Webseite der Besucher zuvor war. Beim Betreten der Seite erfährt der Webseitenbetreiber ausserdem die IP-Adresse, er sieht, welchen Browser und welches Betriebssystem der Besucher benutzt und erkennt die Auflösung des Monitors.

Ohne besondere Vorkehrungen werden, ohne es zu merken, ständig wesentlich mehr private Daten ins Internet gesendet als notwendig! Man ist eine Art gläserner Surfer. Abhilfe schaffen da verschiedene Webseiten (beispielsweise [www.anonymsurfen.com](http://www.anonymsurfen.com) oder [www.anonymizer.com](http://www.anonymizer.com)) sowie spezielle Tools (z.B. Steganos Internet Anonym). Dabei wird jeweils durch verschiedene anonyme Proxy-Server die wahre Identität verschleiert.

---

<sup>74</sup> vgl. Kossel, 2003, S. 152-159

<sup>75</sup> vgl. Sicherheit-online.net, 2003

### 3.4.2.2 Persönliche Angaben

Die meisten Daten, die im Internet über einen User bekannt werden, sind weder durch technische Tricks, noch heimlich in Erfahrung gebracht worden - sie wurden vielmehr freiwillig vom Betroffenen herausgegeben. In vielen Fällen ist sich der User dabei überhaupt nicht bewusst, dass er gerade eine Datenbank mit seinen persönlichen Daten regelrecht füttert:

- Onlinegewinnspiele: Eine beliebte Masche, an Daten von Internetsurfern zu kommen. Dabei wird man in der Regel aufgefordert, Name und Mailadresse, womöglich auch die Wohnanschrift einzutragen.
- Free-Mailer. Kostenlose E-Mail- oder SMS-Dienste verlangen bei der Anmeldung häufig sehr viele Angaben, die weit über den Namen hinausgehen. Das Ziel, dem User damit "massgeschneiderte" Werbung anzudienen, wird in der Regel auch gar nicht verschleiert. Fakt ist allerdings auch, dass mit diesen Angaben ein nahezu exaktes Persönlichkeitsprofil des Users erstellt - und weiterverkauft - werden kann.
- Gästebücher und Newsgroups. Eine Datenquelle, die häufig unterschätzt wird. Wenn ein Benutzer in einer Newsgroup einen Beitrag verfasst, bleibt dieser über Jahre hinweg für jedermann abrufbar. In der Suchmaschine Google etwa sind Newsgroup-Beiträge bis ins Jahr 1981 zurück abrufbar und können nach bestimmten Suchkriterien, etwa einer Mailadresse oder einem Namen, abgefragt werden. So ist beispielsweise bekannt, dass manche Arbeitgeber den Namen eines Stellenbewerbers einfach in eine Suchmaschine eingeben - gewisse "Jugendsünden" könnten einem hier sicherlich so manche Chance verbauen. Ein ähnliches Risiko stellen Gästebücher dar. Der Name des Besuchers in Verbindung mit der Mailadresse und persönlichen Angaben stellen ebenfalls eine Fundgrube für Datensammler dar.
- Webseiten. Dank spezieller Editoren kann heutzutage nahezu jeder mit wenigen Handgriffen eine eigene Webseite ins Netz stellen. Was man auf seiner persönlichen Homepage über sich verrät, bleibt jedem selbst überlassen - oft ist es schon zu viel.

Was mit persönlichen Daten geschehen kann, zeigt sich am folgenden Beispiel: Mehr als 105'000 Internetuser hatten bei einem Onlinegewinnspiel ihre Mailadresse angegeben. Gelandet sind diese Adressen letztlich bei ebay, einem Internet Auktions-Portal, wo sie als Packet zum Verkauf angeboten wurden. Ein Käufer könnte diese Adressen nun beispielsweise für Spamming, also den Massenversand von Werbebotschaften per Mail, verwenden.

Man sollte sich also immer genau bewusst sein, welche Daten man wo preisgibt.

## 4 Ergebnisse und Ausblick

Mit steigender Anzahl Internetuser wird auch die Kriminalität im Internet immer grösser. Deshalb muss in den kommenden Jahren mit einer massiven Zunahme von Straftaten gerechnet werden. Damit in Zukunft Überraschungen ausbleiben, müssen die Firmen, öffentliche Verwaltungen sowie Private Internet-User betreffend Cyber-Kriminalität sensibilisiert werden. Gefordert sind die Firmen, die Kantone, der Staat sowie auch Privatbenutzer. Um sich vor Cyber-Kriminalität schützen zu können, werden immer mehr Kenntnisse über die Technologie vorausgesetzt. Die Technologie, von der sich die Gesellschaft abhängig macht, sollte beherrscht werden.

Vor allem ist das Management von kleineren und mittleren Unternehmungen gefordert, sich mit IT-Sicherheit auseinander zu setzen, da genau diese in den kommenden Jahren vermehrt zur Zielscheibe von Industriespionage oder anderen bösartigen Attacken werden. Die Täter wissen nämlich, dass es normalerweise viel einfacher ist, sich bei KMU's erfolgreich in die Systeme einzuschleichen, und vertrauliche Daten zu beschädigen oder zu entwenden, da solche Unternehmen gegen Attacken meistens zu wenig abgesichert sind. Grossfirmen dagegen haben dieses Problem mehr oder weniger erkannt und investieren viel Geld in die IT-Sicherheit.

Für die Schweiz ist der Kampf gegen die Internet-Kriminalität im Alleingang unmöglich. Gefragt ist eine enge internationale Kooperation und Rechtsharmonisierung. Mit der Unterzeichnung der Convention on Cybercrime ist ein erster wichtiger Schritt bereits getan. Mit der Koordinationsstelle zur Bekämpfung der Internet-Kriminalität (KOBIK) ist eine schweizerische Stelle für die Koordination gegen das Verbrechen im Internet geschaffen. Ebenfalls besteht dank der KOBIK ein Ansprechpartner für das In- und Ausland. Ein Grund zum Handeln besteht jedoch immer noch bezüglich der strafrechtlichen Verantwortlichkeit der Internet Service Provider. Hier könnte sich die Schweiz nach der EU orientieren, welche mit der E-Commerce-Richtlinie dieses Problem weitgehend geklärt hat. Die Anpassung des Rechts muss mit dem Wandel der Technologie mithalten können. Es wäre fatal, wenn in Zukunft weiterhin Unklarheit betreffend strafrechtlicher Verantwortlichkeit der ISP bestehen würde.

Da Täter oft über bessere Computerausrüstung verfügen als ihre amtlichen Verfolger und sie die Anonymität des Internets für ihre Tat geschickt zu nutzen wissen, werden die Kriminellen selten ermittelt und gefasst. Um die Täter zu fassen reicht es also nicht, nur Anpassungen des bestehenden Rechts vorzunehmen. Es muss auch die Aus- und Weiterbildung von Fachkräften noch mehr vorangetrieben werden um den Wissensvorsprung der Täter möglichst klein zu halten. Dies gilt für die Schweiz sowie für alle anderen Länder.

Des Weiteren muss in Zukunft das Spannungsfeld zwischen Datenschutz und Strafverfolgung möglichst fair gelöst werden. Hier gilt es einen Mittelweg zwischen Privatsphäre und Handlungsspielraum der Strafverfolgungs-Behörden zu finden.

Eine Vielzahl von Cyber-Kriminalitätsdelikten wird erst dadurch möglich, dass Internetuser keine oder unzureichende Schutzmassnahmen treffen, weil sie sich der Gefahren des Internets oft nicht bewusst sind. Dies betrifft vor allem Kinder und Jugendliche. Auf nationaler Ebene sollten Projekte zur Prävention und Bekämpfung der Internet-Kriminalität gefördert werden und durch Aufklärungs- und Öffentlichkeitsarbeit das Bewusstsein und die Kenntnis über die Gefahren und Chancen des Netzes verbessert werden.

Alle Anstrengungen zur Verhinderung von Missbrauch werden fehl schlagen, wenn sich die Nutzer lediglich als Konsumenten von Internet-Diensten verstehen, und sich nicht als Netzbürger und Netzbürgerinnen verhalten. In der Frühphase des Internets gab es allgemein beachtete Grundsätze, Sitten und Gebräuche, die einem Missbrauch des Netzes entgegenwirkten, die so genannten „Netiquetten“. Im Zuge der Kommerzialisierung des Netzes und der Entwicklung immer neuer Nutzungsformen scheinen derartige freiwillige Verhaltensregelungen leider verlorengegangen zu sein. Das Internet stellt insofern eine gewaltige Herausforderung an unser Bildungs- und Gesellschaftssystem dar.

Durch den technologischen Fortschritt werden in Zukunft auch mobile Geräte mit drahtlosem Zugang ans Internet von den Gefahren bedroht sein. Die Geräte verfügen über immer mehr Funktionalitäten, wodurch diese komplexer und anfälliger gegen mögliche Hackerangriffe oder Virenattacken werden. Besonders im Unternehmensalltag lauern viele Gefahren, weil dort der Anteil der mobilen Datenkommunikation immer mehr an Bedeutung gewinnt. Bereits heute empfangen Mitarbeiter per Mobiltelefon oder PDA ihre E-Mails und greifen auf Datenbanken und Software des Unternehmens zu. Hier müssen Firmen befürchten, dass Spione sich mit speziellen Software-Tools z.B. via Handy unbemerkt Zugang zu den Unternehmensnetzen verschaffen, diese lahm legen oder Daten klauen. Täter verlieren nie an Kreativität und werden alle Möglichkeiten ausschöpfen, um an ihre Opfer zu gelangen.

Viele Unternehmen haben sich von den Chancen des Internets geradezu abhängig gemacht und könnten ohne das Netz nicht existieren. Diese Abhängigkeit wird nicht nur von den Unternehmen, sondern von der gesamten Gesellschaft unterschätzt. Beunruhigend ist dies vor allem, weil das Internet selbst wiederum vollkommen von technischen Einrichtungen abhängig ist. Durch die Struktur des Internets könnten gezielte Angriffe auf die Hauptknotenpunkte (Network Access Points) zum Kollaps des gesamten Netzes führen. Gemäss einer Studie der University of Notre Dame wäre bei einem Ausfall von nur vier Prozent der Network Access Points das Internet zerstückelt und unbrauchbar<sup>76</sup>. Sollte jemand die Absicht und die nötigen Mittel haben, könnte er das Netz durchaus lahmlegen.

Ein solcher Super-GAU des Internets würde den Benutzern die Wichtigkeit des Netzes und die Abhängigkeit davon vor Augen führen. Spätestens dann würde der Sicherheit in der Informationstechnologie höhere Priorität eingeräumt und ein gerechtfertigter Aufwand betrieben werden.

---

<sup>76</sup> vgl. Rötzer, 2002

## 5 Diskussion

Die vorliegende Arbeit deckt das aktuelle Thema Cyber-Kriminalität auf breiter Ebene ab. Aus der Sicht der Autoren sind die gesetzten Ziele erreicht worden: Die Grundlagen zum Thema Cyber-Kriminalität werden ausführlich erläutert. Dem Leser wird ein Einblick in die Aktivitäten der Schweiz und den europäischen Staaten zur Bekämpfung und Vorbeugung der Cyber-Kriminalität geboten. Der Zusammenhang zu Forensics und das Spannungsfeld zum Datenschutz wird ebenfalls angegangen. In der Arbeit wird explizit darauf verzichtet, die einzelnen Deliktformen im Detail zu beschreiben, und mit Beispielen zu erläutern. Dies hätte den Rahmen vorliegender Arbeit gesprengt.

Das Ermitteln der Anzahl Delikte sowie die Deliktsummen erwies sich als sehr schwierig. Es besteht einerseits eine sehr grosse Dunkelziffer - andererseits werden die Zahlen vertraulich behandelt und der Öffentlichkeit nicht bekannt gegeben. Oft wird zwischen Computerdelikten und Delikten die im Zusammenhang mit dem Internet stehen nicht unterschieden.

Die Problematik Cyber-Kriminalität wurde bisher in der Literatur wenig erwähnt. Als Grundlage für die Informationsbeschaffung diente primär das Internet – unter anderem, weil es mit dem Thema Cyber-Kriminalität in direktem Zusammenhang steht. Sehr aufschlussreiche Informationen konnten bei der KOBIK in Bern gewonnen werden. Aus deren Tätigkeiten werden zukünftig weitere Berichte und Analysen vorgehen.

Die Arbeit zeigt einmal mehr auf, dass Aktivitäten zur Bekämpfung und Prävention in der Schweiz wie auch im Ausland verstärkt werden müssen. Gefordert sind vor allem die Staaten mit der Schaffung einer einheitlichen Rechtsgrundlage.

# Literaturverzeichnis

- Arrigoni, F. (2003). IT-Sicherheit: es muss nicht immer ein Virus sein. Online (25.02.2003):  
[www.bhz.ch/itsicherheit.html](http://www.bhz.ch/itsicherheit.html)
- Baeriswyl, B. (2000). Fakten. Die Zeitschrift für Datenschutz des Kantons Zürich.  
Sondernummer 2/2000.
- Brauch, P. (2003). Teurer Wurm: Das hat SQLSlammer gekostet. Online (01.02.2003):  
[www.heise.de](http://www.heise.de)
- Bundesamt für Polizei. (2001). Cyberkriminalität – Die dunkle Seite der Informationsrevolution.  
Strategischer Analysebericht Oktober 2001.
- Bündnis 90/Die Grünen. (2001). Cybercrime und Bürgerrechte.  
Eine Information der Bundestagsfraktion Bündnis 90/Die Grünen. Berlin.
- Computer Crime and Intellectual Property Section (CCIPS). Online (15.01.2003):  
[www.cybercrime.gov/ccips.html](http://www.cybercrime.gov/ccips.html)
- Computer Security Institute. (2002). 2002 CSI/FBI Computer Crime and Security Survey.  
Vol. 8, No 1. Spring 2002. Online (16.01.2003): [www.fbi.gov](http://www.fbi.gov)
- Council of Europe. Online (12.02.2003):  
[www.coe.int](http://www.coe.int)
- Eidgenössischer Datenschutzbeauftragter. Online (27.02.2003):  
[www.edsb.ch/d/ueberuns/privacypolicy.htm](http://www.edsb.ch/d/ueberuns/privacypolicy.htm)
- Fischer, P. (2002). Informatik-Lexikon für Praxis und Studium.  
Kilchberg: Smartbooks.
- Global Internet Statistics. Online (17.02.2003):  
[www.gltreach.com/globstats](http://www.gltreach.com/globstats)
- Infosurance. (2000). Leitfaden zur Informationssicherheit für Führungskräfte.
- Ins Internet - mit Sicherheit! Neues Sicherheitsportal für Jedermann - Tipps und Tricks.  
Pressemitteilung des Bundesamt für Sicherheit in der Informationstechnik, Bonn.  
Online (07.02.2003): [www.bsi.bund.de/presse/pressinf/bsi\\_buerger.htm](http://www.bsi.bund.de/presse/pressinf/bsi_buerger.htm)
- Internet Action Plan follow-up. Online (16.01.2003):  
[www.europa.eu.int/iap](http://www.europa.eu.int/iap)
- Internet Users will top 1 billion in 2005. Online (24.02.2003):  
[www.c-l-a.com/pr032102.htm](http://www.c-l-a.com/pr032102.htm)
- Juristisches Internetprojekt Saarbrücken. Cybercrime.gov. Online (15.01.2003):  
[www.jura.uni-sb.de](http://www.jura.uni-sb.de)

- Knauff, L. Was ist Mail-Relaying und was ist Missbrauch? Online (25.02.2003):  
[www.uni-halle.de/mailrelay2.html](http://www.uni-halle.de/mailrelay2.html)
- Koordinationsstelle Internet-Kriminalität. Online (21.02.2003):  
[www.cybercrime.admin.ch](http://www.cybercrime.admin.ch)
- Kossel, A. (2003). Feigenblätter fürs Web. c't – magazin für computer technik,  
05/2003, S. 152-159.
- Krempf, St. (2002). Cybercrime beschert US-Firmen spürbare Kosten. Online (18.02.2003):  
[www.heise.de](http://www.heise.de)
- Kronenberg, U. (2002). Spurensuche im IT-Umfeld I. Theorie. IT-Security-Lab HSW.
- Kronig, P. (2002). Bekämpfung der Internet-Kriminalität in der Schweiz.  
Revue, 8/2002, S. 8-10.
- MTA's und Fremd-Relaying. Online (25.02.2003):  
[www.ulm.ccc.de/chaos-seminar/spam/MTA.html](http://www.ulm.ccc.de/chaos-seminar/spam/MTA.html)
- Niggli, M.A. (2002). Internet-Kriminalität.  
Revue, 8/2002, S. 6-8.
- Niggli, Riklin, Stratenwerth. (2001). Die Strafrechtliche Verantwortlichkeit von Internet-Providern.
- Raepple, M. (2001). Sicherheitskonzepte für das Internet. Grundlagen, Technologien und  
Lösungskonzepte für die kommerzielle Nutzung. Heidelberg: dpunkt-Verlag.
- Rittelmeier, H. (2003) Allgemeines zur Firewall. Online (25.02.2003):  
[www.computerbetrug.de](http://www.computerbetrug.de)
- Rittelmeier, H. (2003). 0190-Dialer – Allgemeine Betrachtung. Online (25.02.2003):  
[www.computerbetrug.de](http://www.computerbetrug.de)
- Rochford, O. (2002). Hacken für Dummies.  
Bonn: mitp Verlag.
- Rötzer, F. (2000). Kritik an der Konvention gegen Cyberkriminalität des Europarats.  
Online (12.02.2003): [www.heise.de](http://www.heise.de)
- Rötzer, F. (2002). Die Achillesferse des Internet. Online (02.03.2003):  
[www.heise.de](http://www.heise.de)
- Rötzer, F. (2003). Strategie für den Cyberkrieg. Online (07.02.2003):  
[www.heise.de](http://www.heise.de)
- Rüther, W. Internet und „Cyber-Kriminalität“ eine Herausforderung auch für die Kriminologie.  
Kriminologisches Seminar der Universität Bonn. Online (12.10.2003):  
[www.jura.uni-bonn.de](http://www.jura.uni-bonn.de)

Safer Internet Action Plan. Online (16.01.2003):

[www.europa.eu.int/iap](http://www.europa.eu.int/iap)

Safer Internet - Informationsbrief zur Aufklärung im Rahmen des EU-Programms Sicherheit im Internet. Online (16.01.2003):

[www.saferinternet.org/news/saferde21.htm](http://www.saferinternet.org/news/saferde21.htm)

Schutz im Internet Teil 2. Online (28.02.2003):

[www.trojaner-info.de/report\\_schutz2.shtml](http://www.trojaner-info.de/report_schutz2.shtml)

Schweizerische Bundespolizei. (2000). Die Strafrechtliche Verantwortung von Internet Service Providern, Positionspapier der Bundespolizei.

Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (Stand am 18. Dezember 2001). Die Bundesbehörden der Schweizerischen Eidgenossenschaft. Online (02.03.2002):

[www.admin.ch](http://www.admin.ch)

Sicherheit-Online.net. Surfen Sie – aber sicher. Online (18.02.2003):

[www.sicherheit-online.net](http://www.sicherheit-online.net)

So schützen Sie sich vor Risiken im Internet. Programm Polizeiliche Kriminalprävention der Länder und des Bundes. Online (09.02.2003):

[www.polizei.propk.de/service/sicher/index.xhtml](http://www.polizei.propk.de/service/sicher/index.xhtml)

Social Hacking. Online (05.03.2003):

[www.it-menschen.de/texte/social.htm](http://www.it-menschen.de/texte/social.htm)

Strafrechtliche Verantwortlichkeit der Internet Service Provider – Gesetzgeber gefordert. Zweitgutachten zum Gutachten des Bundesamtes für Justiz. Verband Inside Telecom. Online (21.02.2003):

[www.vit.ch](http://www.vit.ch)

Sury, U. (2002). Forensics.

Mosaic, INFORMATIK • INFORMATIQUE 2/2002.

Universität Bern. Online (27.02.2003):

<http://visor.unibe.ch/media/summer97/970624b.htm>

Untersuchungsrichter verlangt von Schweizer Access-Providern Sperrung von Websites. Verband Inside Telecom. Online (21.02.2003): [www.vit.ch](http://www.vit.ch)

## Interviewverzeichnis

Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK),  
Herr Henauer, Frau Bollmann, Interview vom 15.01.2003.

Roland Portmann, Wissenschaftlicher Mitarbeiter IT-Security HSW,  
Interview vom 19.02.2003.

# Anhang

## Gesetzesartikel StGB<sup>77</sup>

### Art. 24 (5. Teilnahme. Anstiftung)

<sup>1</sup> Wer jemanden zu dem von ihm verübten Verbrechen oder Vergehen vorsätzlich bestimmt hat, wird nach der Strafandrohung, die auf den Täter Anwendung findet, bestraft.

<sup>2</sup> Wer jemanden zu einem Verbrechen zu bestimmen versucht, wird wegen Versuchs dieses Verbrechens bestraft.

### Art. 25 (Gehilfenschaft)

Wer zu einem Verbrechen oder zu einem Vergehen vorsätzlich Hilfe leistet, kann milder bestraft werden (Art. 65).

### Art. 27 (6. Strafbarkeit der Medien)

<sup>1</sup> Wird eine strafbare Handlung durch Veröffentlichung in einem Medium begangen und erschöpft sie sich in dieser Veröffentlichung, so ist, unter Vorbehalt der nachfolgenden Bestimmungen, der Autor allein strafbar.

<sup>2</sup> Kann der Autor nicht ermittelt oder in der Schweiz nicht vor Gericht gestellt werden, so ist der verantwortliche Redaktor nach Artikel 322bis strafbar. Fehlt ein verantwortlicher Redaktor, so ist jene Person nach Artikel 322bis strafbar, die für die Veröffentlichung verantwortlich ist.

<sup>3</sup> Hat die Veröffentlichung ohne Wissen oder gegen den Willen des Autors stattgefunden, so ist der Redaktor oder, wenn ein solcher fehlt, die für die Veröffentlichung verantwortliche Person als Täter strafbar.

<sup>4</sup> Die wahrheitsgetreue Berichterstattung über öffentliche Verhandlungen und amtliche Mitteilungen einer Behörde ist straflos.

### Art. 135 (Gewaltdarstellungen)

<sup>1</sup> Wer Ton- oder Bildaufnahmen, Abbildungen, andere Gegenstände oder Vorführungen, die, ohne schutzwürdigen kulturellen oder wissenschaftlichen Wert zu haben, grausame Gewalttätigkeiten gegen Menschen oder Tiere eindringlich darstellen und dabei die elementare Würde des Menschen in schwerer Weise verletzen, herstellt, einführt, lagert, in Verkehr bringt, anpreist, ausstellt, anbietet, zeigt, überlässt oder zugänglich macht, wird mit Gefängnis oder mit Busse bestraft.

<sup>1bis</sup> Mit Gefängnis bis zu einem Jahr oder mit Busse wird bestraft, wer Gegenstände oder Vorführungen nach Absatz 1, soweit sie Gewalttätigkeiten gegen Menschen oder Tiere darstellen, erwirbt, sich über elektronische Mittel oder sonstwie beschafft oder besitzt.<sup>2</sup> Die Gegenstände werden eingezogen.<sup>121</sup>

<sup>3</sup> Handelt der Täter aus Gewinnsucht, so ist die Strafe Gefängnis und Busse.

### Art. 143 (Unbefugte Datenbeschaffung)

<sup>1</sup> Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, sich oder einem andern elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind, wird mit Zuchthaus bis zu fünf Jahren oder mit Gefängnis bestraft.

<sup>2</sup> Die unbefugte Datenbeschaffung zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

---

<sup>77</sup> vgl. Schweizerisches Strafgesetzbuch (2001)

**Art. 143<sup>bis</sup> (Unbefugtes Eindringen in ein Datenverarbeitungssystem)**

Wer ohne Bereicherungsabsicht auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.

**Art. 144<sup>bis</sup> (Datenbeschädigung)**

<sup>1</sup>. Wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten verändert, löscht oder unbrauchbar macht, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.

Hat der Täter einen grossen Schaden verursacht, so kann auf Zuchthaus bis zu fünf Jahren erkannt werden. Die Tat wird von Amtes wegen verfolgt.

<sup>2</sup>. Wer Programme, von denen er weiss oder annehmen muss, dass sie zu den in Ziffer 1 genannten Zwecken verwendet werden sollen, herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonst wie zugänglich macht oder zu ihrer Herstellung Anleitung gibt, wird mit Gefängnis oder mit Busse bestraft.

Handelt der Täter gewerbsmässig, so kann auf Zuchthaus bis zu fünf Jahren erkannt werden.

**Art. 146 (Betrug)**

<sup>1</sup> Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, jemanden durch Vorspiegelung oder Unterdrückung von Tatsachen arglistig irreführt oder ihn in einem Irrtum arglistig bestärkt und so den Irrenden zu einem Verhalten bestimmt, wodurch dieser sich selbst oder einen andern am Vermögen schädigt, wird mit Zuchthaus bis zu fünf Jahren oder mit Gefängnis bestraft.

<sup>2</sup> Handelt der Täter gewerbsmässig, so wird er mit Zuchthaus bis zu zehn Jahren oder mit Gefängnis nicht unter drei Monaten bestraft.

<sup>3</sup> Der Betrug zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

**Art. 147 (Betrügerischer Missbrauch einer Datenverarbeitungsanlage)**

<sup>1</sup> Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, durch unrichtige, unvollständige oder unbefugte Verwendung von Daten oder in vergleichbarer Weise auf einen elektronischen oder vergleichbaren Datenverarbeitungs- oder Datenübermittlungsvorgang einwirkt und dadurch eine Vermögensverschiebung zum Schaden eines andern herbeiführt oder eine Vermögensverschiebung unmittelbar darnach verdeckt, wird mit Zuchthaus bis zu fünf Jahren oder mit Gefängnis bestraft.

<sup>2</sup> Handelt der Täter gewerbsmässig, so wird er mit Zuchthaus bis zu zehn Jahren oder mit Gefängnis nicht unter drei Monaten bestraft.

<sup>3</sup> Der betrügerische Missbrauch einer Datenverarbeitungsanlage zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

**Art. 150 (Erschleichen einer Leistung)**

Wer, ohne zu zahlen, eine Leistung erschleicht, von der er weiss, dass sie nur gegen Entgelt erbracht wird, namentlich indem er ein öffentliches Verkehrsmittel benützt, eine Aufführung, Ausstellung oder ähnliche Veranstaltung besucht, eine Leistung, die eine Datenverarbeitungsanlage erbringt oder die ein Automat vermittelt, beansprucht, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.

**Art. 150<sup>bis</sup> (Herstellen und Inverkehrbringen von Materialien zur unbefugten Entschlüsselung codierter Angebote)**

<sup>1</sup> Wer Geräte, deren Bestandteile oder Datenverarbeitungsprogramme, die zur unbefugten Entschlüsselung codierter Rundfunkprogramme oder Fernmeldedienste bestimmt und geeignet sind, herstellt, einführt, ausführt, durchführt, in Verkehr bringt oder installiert, wird, auf Antrag, mit Haft oder Busse bestraft.

<sup>2</sup> Versuch und Helferschaft sind strafbar.

#### **Art. 162 (2. Verletzung des Fabrikations- oder Geschäftsgeheimnisses)**

Wer ein Fabrikations- oder Geschäftsgeheimnis, das er infolge einer gesetzlichen oder vertraglichen Pflicht bewahren sollte, verrät, wer den Verrat für sich oder einen andern ausnützt, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.

#### **Art. 173 (1. Ehrverletzungen. Üble Nachrede)**

<sup>1</sup> Wer jemanden bei einem andern eines unehrenhaften Verhaltens oder anderer Tatsachen, die geeignet sind, seinen Ruf zu schädigen, beschuldigt oder verdächtigt, wer eine solche Beschuldigung oder Verdächtigung weiterverbreitet, wird, auf Antrag, mit Gefängnis bis zu sechs Monaten oder mit Busse bestraft.

<sup>2</sup> Beweist der Beschuldigte, dass die von ihm vorgebrachte oder weiterverbreitete Äusserung der Wahrheit entspricht, oder dass er ernsthafte Gründe hatte, sie in guten Treuen für wahr zu halten, so ist er nicht strafbar.

<sup>3</sup> Der Beschuldigte wird zum Beweis nicht zugelassen und ist strafbar für Äusserungen, die ohne Wahrung öffentlicher Interessen oder sonstwie ohne begründete Veranlassung, vorwiegend in der Absicht vorgebracht oder verbreitet werden, jemandem Übles vorzuwerfen, insbesondere, wenn sich die Äusserungen auf das Privat- oder Familienleben beziehen.

<sup>4</sup> Nimmt der Täter seine Äusserung als unwahr zurück, so kann er milder bestraft oder ganz von Strafe befreit werden.

<sup>5</sup> Hat der Beschuldigte den Wahrheitsbeweis nicht erbracht oder sind seine Äusserungen unwahr oder nimmt der Beschuldigte sie zurück, so hat der Richter dies im Urteil oder in einer andern Urkunde festzustellen.

#### **Art. 174 (Verleumdung)**

<sup>1</sup> Wer jemanden wider besseres Wissen bei einem andern eines unehrenhaften Verhaltens oder anderer Tatsachen, die geeignet sind, seinen Ruf zu schädigen, beschuldigt oder verdächtigt, wer eine solche Beschuldigung oder Verdächtigung wider besseres Wissen verbreitet, wird, auf Antrag, mit Gefängnis oder Busse bestraft.

<sup>2</sup> Ist der Täter planmässig darauf ausgegangen, den guten Ruf einer Person zu untergraben, so ist die Strafe Gefängnis nicht unter einem Monat.

<sup>3</sup> Zieht der Täter seine Äusserungen vor dem Richter als unwahr zurück, so kann er milder bestraft werden. Der Richter stellt dem Verletzten über den Rückzug eine Urkunde aus.

#### **Art. 175 (Üble Nachrede oder Verleumdung gegen einen Verstorbenen oder einen verschollen Erklärten)**

<sup>1</sup> Richtet sich die üble Nachrede oder die Verleumdung gegen einen Verstorbenen oder einen verschollen Erklärten, so steht das Antragsrecht den Angehörigen des Verstorbenen oder des verschollen Erklärten zu.

<sup>2</sup> Sind zur Zeit der Tat mehr als 30 Jahre seit dem Tode des Verstorbenen oder seit der Verschollenerklärung verflossen, so bleibt der Täter straflos.

#### **Art. 177 (Beschimpfung)**

<sup>1</sup> Wer jemanden in anderer Weise durch Wort, Schrift, Bild, Gebärde oder Tätlichkeiten in seiner Ehre angreift, wird, auf Antrag, mit Gefängnis bis zu drei Monaten oder mit Busse bestraft.

<sup>2</sup> Hat der Beschimpfte durch sein ungebührliches Verhalten zu der Beschimpfung unmittelbar Anlass gegeben, so kann der Richter den Täter von Strafe befreien.

<sup>3</sup> Ist die Beschimpfung unmittelbar mit einer Beschimpfung oder Tätlichkeit erwidert worden, so kann der Richter einen oder beide Täter von Strafe befreien.

**Art. 197 (4. Pornographie)**

<sup>1</sup> Wer pornographische Schriften, Ton- oder Bildaufnahmen, Abbildungen, andere Gegenstände solcher Art oder pornographische Vorführungen einer Person unter 16 Jahren anbietet, zeigt, überlässt, zugänglich macht oder durch Radio oder Fernsehen verbreitet, wird mit Gefängnis oder mit Busse bestraft.

<sup>2</sup> Wer Gegenstände oder Vorführungen im Sinne von Ziffer 1 öffentlich ausstellt oder zeigt oder sie sonst jemandem unaufgefordert anbietet, wird mit Busse bestraft. Wer die Besucher von Ausstellungen oder Vorführungen in geschlossenen Räumen im voraus auf deren pornographischen Charakter hinweist, bleibt strafflos.

<sup>3</sup> Wer Gegenstände oder Vorführungen im Sinne von Ziffer 1, die sexuelle Handlungen mit Kindern oder mit Tieren, menschlichen Ausscheidungen oder Gewalttätigkeiten zum Inhalt haben, herstellt, einführt, lagert, in Verkehr bringt, anpreist, ausstellt, anbietet, zeigt, überlässt oder zugänglich macht, wird mit Gefängnis oder mit Busse bestraft. Die Gegenstände werden eingezogen.

<sup>3bis</sup> Mit Gefängnis bis zu einem Jahr oder mit Busse wird bestraft, wer Gegenstände oder Vorführungen im Sinne von Ziffer 1, die sexuelle Handlungen mit Kindern oder Tieren oder sexuelle Handlungen mit Gewalttätigkeiten zum Inhalt haben, erwirbt, sich über elektronische Mittel oder sonstwie beschafft oder besitzt. Die Gegenstände werden eingezogen. 4. Handelt der Täter aus Gewinnsucht, so ist die Strafe Gefängnis und Busse.

<sup>4</sup> Handelt der Täter aus Gewinnsucht, so ist die Strafe Gefängnis und Busse.

<sup>5</sup> Gegenstände oder Vorführungen im Sinne der Ziffern 1–3 sind nicht pornographisch, wenn sie einen schutzwürdigen kulturellen oder wissenschaftlichen Wert haben.

**Art. 261<sup>bis</sup> (Rassendiskriminierung)**

Wer öffentlich gegen eine Person oder eine Gruppe von Personen wegen ihrer Rasse, Ethnie oder Religion zu Hass oder Diskriminierung aufruft, wer öffentlich Ideologien verbreitet, die auf die systematische Herabsetzung oder Verleumdung der Angehörigen einer Rasse, Ethnie oder Religion gerichtet sind, wer mit dem gleichen Ziel Propagandaaktionen organisiert, fördert oder daran teilnimmt, wer öffentlich durch Wort, Schrift, Bild, Gebärden, Tätlichkeiten oder in anderer Weise eine Person oder eine Gruppe von Personen wegen ihrer Rasse, Ethnie oder Religion in einer gegen die Menschenwürde verstossenden Weise herabsetzt oder diskriminiert oder aus einem dieser Gründe Völkermord oder andere Verbrechen gegen die Menschlichkeit leugnet, gröblich verharmlost oder zu rechtfertigen sucht, wer eine von ihm angebotene Leistung, die für die Allgemeinheit bestimmt ist, einer Person oder einer Gruppe von Personen wegen ihrer Rasse, Ethnie oder Religion verweigert, wird mit Gefängnis oder mit Busse bestraft.

**Art. 322<sup>bis</sup> (Nichtverhinderung einer strafbaren Veröffentlichung)**

Wer als Verantwortlicher nach Artikel 27 Absätze 2 und 3 eine Veröffentlichung, durch die eine strafbare Handlung begangen wird, vorsätzlich nicht verhindert, wird mit Gefängnis oder Busse bestraft. Handelt der Täter fahrlässig, so ist die Strafe Haft oder Busse.

**Art. 346 (2. Örtliche Zuständigkeit. Gerichtsstand des Ortes der Begehung)**

<sup>1</sup> Für die Verfolgung und Beurteilung einer strafbaren Handlung sind die Behörden des Ortes zuständig, wo die strafbare Handlung ausgeführt wurde.<sup>246</sup> Liegt nur der Ort, wo der Erfolg eingetreten ist oder eintreten sollte, in der Schweiz, so sind die Behörden dieses Ortes zuständig.

<sup>2</sup> Ist die strafbare Handlung an mehreren Orten ausgeführt worden, oder ist der Erfolg an mehreren Orten eingetreten, so sind die Behörden des Ortes zuständig, wo die Untersuchung zuerst angehoben wurde.

# Eidesstattliche Erklärung

Wir erklären hiermit, dass wir die vorliegende Einführungsarbeit selbstständig, ohne Mithilfe Dritter und nur unter Benutzung der angegebenen Quellen verfasst haben.

Luzern, den 14. März 2003

\_\_\_\_\_  
Samuel Dissler

\_\_\_\_\_  
Mario Studhalter

\_\_\_\_\_  
Eric Stübi

\_\_\_\_\_  
Philipp Zumstein

