

# Die unfassbaren Kriminellen

Für Leute mit kriminellen Potential ist die Informationstechnologie das Paradies – noch, denn die Strafbehörden sind ihnen immer dichter auf den Fersen.

VON UELI GRÜTER

Lange Zeit hatte man den Eindruck, die Informatik und das Internet als Teil davon sei ein rechtsfreier Raum. Die Delinquenten, wie zum Beispiel Hacker, waren und sind Leute mit hohem IT-Know-how und wurden darum primär einmal bewundert. Je mehr die Menschen aber von Informatik abhängig sind, desto eher realisieren sie, dass kriminelle Machenschaften in der Informatik unser tägliches Leben bedrohen können. Diese Erkenntnis ist offenbar zwischenzeitlich auch bei den Behörden angekommen. So bezeichnet Armee-Chef André Blattmann den «Cyberwar» als «die aktuell gefährlichste Bedrohung» der Schweiz. Und während die Behörden der Informatikriminalität jahrelang machtlos ausgeliefert waren, rüsten sie mehr und mehr auf und können nun auch Erfolge vorweisen.

## Informatik als kriminelles Biotop

Die Informatik eröffnet Leuten mit krimineller Energie ganz neue Möglichkeiten. Während man bei einem «Offline-Einbruch» Kopf und Kragen riskiert, ist ein Zugriff über Datenleitungen auch anonym möglich. Elektronische Spuren können verwischt werden. Kriminelle machen sich generell die Finger nicht schmut-

zig. Der Einbruch kann sozusagen von zu Hause aus oder auch aus dem fernen Ausland verübt werden. Unter diesen Umständen wird die Informatik geradezu zum kriminellen Biotop, in dem sogar bisher unbescholtene Leute ab und an der Versuchung erliegen.

## Hohe Anforderungen an Strafverfolgungsbehörden

Die grössten Probleme bei der Strafverfolgung von Delikten im IT-Bereich sind primär nicht fehlende Strafnormen, sondern ungenügendes technisches Know-how und Material sowie die Organisation.

Kriminelle waren zwar schon immer kreativ. Jedoch hatte ihre Kreativität in der Regel kürzere Halbwertszeiten. Die Informatik hingegen legt ein extremes Innovationstempo vor, das sich auch Kriminelle zunutze machen. Damit entsteht ein eigentlicher technischer Wettlauf, in dem träge staatliche Organisationen permanent hinterherrennen. Erschwerend kommt hinzu, dass die öffentliche Hand – gerade in der heutigen Zeit – knapp bei Kasse ist und sich teure Informatik gar nicht leisten kann. Allerdings reicht gutes Material alleine sowieso nicht, es braucht auch noch die hellen Köpfe. Diese generieren aber wieder Kosten und ihre fortwährende Ausbildung dauert.

Geschwächt wird die Strafverfolgung im Bereich der Informatik in der Schweiz zusätzlich durch die primär kantonale Organisation. Jeder Kanton hat für sich selber in seinen forensischen Diensten Informatikspezialisten

aufgebaut. Schnell hat sich jedoch gezeigt, dass man der wachsenden Kriminalität in diesem Bereich durch föderale Strukturen nicht Herr werden kann. Sowohl Bund als auch Kantone haben begonnen, ihre Bemühungen gegen die Informatikriminalität zu koordinieren und teilweise an spezialisierte Unternehmen auszulagern. Auf Bundesebene sind für ein koordiniertes Vorgehen gegen die Kriminalität im Internet unter anderem die Schwei-



Die Behörden waren der Informatikriminalität lange machtlos ausgeliefert. Nun rüsten sie mehr und mehr auf.

### IN KÜRZE

- Die IT und das Internet galten lange Zeit als rechtsfreie Räume.
- Die grössten Probleme bei der Strafverfolgung von IT-Delikten sind ungenügendes technisches Know-how und Material sowie die Organisation.
- Im Informatikstrafrecht wird das Recht angewendet, das zur Beurteilung von Offline-Sachverhalten dient.

zerische Koordinationsstelle zur Bekämpfung der Internetkriminalität (Kobik) und die Schweizer Melde- und Analysestelle Informationssicherung (Melani) entstanden. Nach wie vor sind diese jedoch auf die kantonalen Strafverfolgungsbehörden angewiesen, was die Bemühungen schwächt.

### Strafrecht und Informatikkriminalität

Grundlage jeder staatlichen Aktivität gegen die Informatikkriminalität bilden strafrechtliche Normen, die es entweder schon gab oder aber für Delikte im Bereich Informatik neu geschaffen wurden. Dabei ist das Strafrecht darauf ausgerichtet, Straftaten zu ahnden, die Täter zu bestrafen und dadurch diese selbst und andere davon abzuhalten, Straftaten zu verüben. Nicht im Vordergrund steht der finanzielle Ausgleich für allfälligen Schaden. Die Voraussetzungen, jemanden zu bestrafen, müssen im Gesetz klar definiert sein. Ein Delikt muss tatbestandsmässig sein, also dem im Gesetz umschriebenen Fehlverhalten in allen Punkten entsprechen und entweder vorsätzlich oder, wenn vorgesehen, fahrlässig begangen worden sein. Dazu muss das Verhalten rechtswidrig sein, es darf nicht aus Notwehr oder Notstand (zum Beispiel der Einbruch in eine SAC-Hütte, um dem Erfrierungstod zu entgehen) erfolgen und das Opfer darf nicht eingewilligt haben. So sind chirurgische Eingriffe in der Regel nicht rechtswidrig, da der Patient zur unvermeidlichen Körperverletzung sein Einverständnis gegeben hat. Schlussendlich muss der Täter schuldhaft gehandelt haben, was voraussetzt, dass er in der Lage ist, das Unrecht einzusehen und sich entsprechend der Einsicht zu verhalten. Dies ist zum Beispiel bei einer geistigen Behinderung oft nicht gegeben.

### Informatikdelikte

Informatikdelikte sind Straftaten, bei denen die Informatik selber das Ziel ist (z.B. die Zerstörung von IT-Systemen), bei denen die Infor-

#### DER AUTOR

Ueli Grüter, LL.M., ist Rechtsanwalt in Zürich und Luzern und Dozent an der Hochschule Luzern mit Spezialgebiet Kommunikations- und Technologierecht. In der Serie

«Informatikrecht für die Praxis» führt Grüter in 13 Folgen kurz und verständlich durch die rechtlichen Grundlagen in der Informatik und zeigt die rechtlichen Stolpersteine. Mit der letzten Folge erscheint die Serie dann auch als E-Book.



## DATENSCHUTZ MIT BISS

*Bis vor wenigen Tagen war der Datenschutz in der Schweiz weitgehend ein Löwe ohne Zähne. Nun hat das Bundesgericht aber dem Löwen ein stattliches Gebiss verpasst. Was ist geschehen und was heisst dies für die Zukunft?*

Obwohl das Schweizerische Datenschutzgesetz fast 20 Jahre alt ist, war nicht bekannt, wie stark der Staat die Selbstbestimmung des Einzelnen über seine eigenen Daten schützt. Die Medien haben zwar das Datenschutzgesetz als Massstab genommen und immer wieder Verstösse aufgedeckt. Der Eidgenössische Datenschutzbeauftragte, der für die Aufsicht der Bearbeitung von Daten durch Private zuständig ist, hatte jedoch keine griffigen gesetzlichen Mittel oder zu wenig personelle Ressourcen, um dem Datenschutz zum Durchbruch zu verhelfen. Damit hatten Verstösse gegen das Datenschutzgesetz in der Regel keine rechtlichen Konsequenzen. Die Revision des Datenschutzgesetzes sowie der Bundesjustiz zeigt nun aber offenbar seine Wirkung. Dazu kommt eine immer lebhaftere Diskussion des Datenschutzes in der Bevölkerung und in den Medien, angeheizt durch ein hemmungsloses und nimmersattes Datensammeln durch Unternehmen wie Google.

Das hat offenbar auch dem Eidgenössischen Datenschutzbeauftragten neuen Drive gegeben. Dieser hat das Verhalten eines Piratenjägers auf dem Internet beanstandet und die Sache bis vor Bundesgericht gezogen. Und dieses hat soeben entschieden, dass es Privaten nicht erlaubt ist, im Internet verdeckt nach IP-Adressen von Personen zu suchen, die urheberrechtlich geschützte Inhalte vornehmlich in Tauschbörsen zwar legal herunterladen, jedoch oft auch gleichzeitig illegal Musik, Filme und anderes uploaden. Damit hat das Bundesgericht, wie vom Gesetz eigentlich vorgesehen, die Interessen von Privaten bezüglich der Selbstbestimmung über ihre Daten klar höher gewichtet als die wirtschaftlichen Interessen der Musik- und Filmindustrie. Zudem hat das Bundesgericht, nachdem dies schon die Datenschutzkommission respektive das heutige Bundesverwaltungsgericht bezüglich E-Mail-Adressen getan hat, den Begriff der persönlichen Daten, die durch das Datenschutzgesetz geschützt sind, ausgedehnt. Denn nun fallen auch die IP-Adressen darunter.

Damit ist eine verdeckte Ermittlung durch Private im Internet nicht mehr zulässig. Aber auch die Strafverfolgungsbehörden können bei Delikten des Urheberrechts, um die es bei der Internet-Piraterie primär geht, weder jetzt noch in naher Zukunft verdeckt nach IP-Adressen und entsprechenden Uploads suchen. Weder das aktuell geltende Gesetz zur verdeckten Ermittlung noch die neue, ab 1. Januar 2011 geltende Strafprozessordnung führen Delikte des Urheberrechts als Gegenstand der verdeckten Ermittlung auf.

Wenn jetzt da und dort in Hinblick auf die Internet-Piraterie nach einer Gesetzesänderung gerufen wird, ist dies nicht angezeigt, denn sowohl das Datenschutzgesetz wie das Urheberrechtsgesetz, aber auch die Bundesstrafprozessordnung wurden erst vor kurzem revidiert – in vollem Bewusstsein der Risiken, die das Internet birgt.

Auch wenn der Entscheid des Bundesgerichts mit einer knappen Mehrheit der Bundesrichter zustande gekommen ist und es sich um eine Premiere und damit um keine gefestigte Rechtsprechung handelt, gehen Juristen davon aus, dass der Entscheid für den Datenschutz in der Schweiz, und möglicherweise sogar in ganz Europa, wegweisend ist. Dies vor allem auch für die zahlreichen Beschwerden, die gegen Google hängig sind. Google muss sich also warm anziehen. Nach einem heissen Datenschutz-Sommer wird es nun Winter.

Weitere Infos u.a. unter [www.edoeb.admin.ch](http://www.edoeb.admin.ch)

matik als Tatwerkzeug dient (z.B. Betrug mittels Manipulation von Informatiksystemen) oder bei denen die Informatik Hilfsmittel ist (z.B. mit dem Computer verfasste Drohbrieft).

Im schweizerischen Strafrecht gibt es nur wenige Straftatbestände respektive Gesetzesartikel, die neu erlassen wurden und ausschliesslich auf Informatikdelikte ausgerichtet sind. Wie sonst im Informatikrecht wird auch im Informatikstrafrecht das Recht angewendet, das bereits zur Beurteilung von Offline-Sachverhalten dient. Ausserordentlich ist also nicht das Recht, sondern die Sachverhaltsumgebung.

Zu den spezifischen Informatikdelikten – also Straftatbestände, die mindestens teilweise direkt mit der Informatik verbunden sind – gehören die unbefugte Datenbeschaffung, das unbefugte Eindringen in ein Datensystem, die Datenbeschädigung, der betrügerische Miss-

brauch einer Datenverarbeitungsanlage, die Erschleichung einer Leistung, die eine Datenverarbeitungsanlage erbringt, sowie die Fälschung von elektronischen Urkunden. Dazu kommen die unspezifischen IT-Delikte. Diese Straftaten können zwar durch die Informatik begünstigt werden, sind aber nicht darauf angewiesen. Dazu gehören die Verletzung von Immaterialgüterrechten (insbesondere Urheberrechte), unlauterer Wettbewerb, die Verletzung von Schweigepflichten, Pornographie, unerlaubte Glücksspiele, die Verletzung der Geheim- und Privatsphäre sowie die Rassendiskriminierung. ■