

Erhöhung der Informationssicherheit durch das Strafrecht?

Laut einer Umfrage eines führenden internationalen Wirtschaftsprüfungsunternehmens betrachtet die Mehrheit der Schweizer Firmen Cybercrime als eines der grössten Zukunftsrisiken. Massnahmen zum Schutz kritischer Informationsinfrastrukturen und der Information schlechthin gewinnen damit auf allen Ebenen an Bedeutung. In letzter Zeit rückt auch der strafrechtliche Schutz immer mehr ins Zentrum der internationalen Diskussion.

Von Wolfgang Straub*

■ Das Strafrecht dient primär der Abschreckung und damit der Verhinderung von Angriffen auf Informationssysteme. Allerdings dürften nur die wenigsten Hacker vor ihrer Tat das Strafgesetzbuch konsultieren. Ein gezieltes Ausnutzen von straf- und zivilrechtlichen Lücken ist immerhin in Bereich der Wirtschaftsspionage durch konkurrierende Unternehmen denkbar. Prävention setzt nicht nur griffige Strafnormen voraus sondern vor allem breite Information über die Effizienz der Strafverfolgung (z.B. Medienberichterstattung über die Verurteilung von Computerdelinquenten).

Angriffe via Internet erfolgen häufig aus dem Ausland. In diesen Fällen stellen sich stets Fragen nach dem anwendbaren Recht und nach den zuständigen

Strafverfolgungsbehörden.

Die Antworten werden durch nationales Recht gegeben und fallen derzeit keineswegs einheitlich aus, was die grenzüberschreitende Strafverfolgung erheblich erschwert. Diese Problematik kann nur durch internationale Rechtsvereinheitlichung und

verbesserte Kooperation bei der Strafverfolgung entschärft werden.

Cybercrime Convention des Europarats

Im Rahmen des Europarats, dem neben den EU-Ländern zahlreiche weitere Staaten (darunter auch die Schweiz) angehören, wurde am 23. November 2001 die Cybercrime Convention aus-

gehandelt (<http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185>). Diese verpflichtet die Mitgliedstaaten, strafrechtliche Vorschriften zum Schutz von Informationssystemen, gegen Kinderpornografie und Missbrauch geistigen Eigentums zu erlassen. Zu verbieten sind auch die Herstellung und Verbreitung von technischen Mitteln zur Begehung von Computerdelikten (insbesondere Hackersoftware). Das Übereinkommen enthält zudem detaillierte Vorschriften über die Speicherung von im Hinblick auf die Strafverfolgung relevanten Daten sowie über die internationale Zuständigkeit und Rechtshilfe. Die Cybercrime Convention sieht vor, dass juristische Personen wie Kapitalgesellschaften und Vereine für Delikte zur Rechenschaft gezogen werden können, welche von Geschäftsleitungsmitgliedern für sie begangen wurden. Juristische Personen sollen auch für mangelhafte Kontrolle ihrer Mitarbeiter im Hinblick auf derartige Delikte haften. Da in einigen Ländern nur Menschen, nicht aber Firmen strafrechtlich verfolgt werden können, lässt das Übereinkommen den Mitgliedstaaten die Wahl, ob sie straf-, zivil- oder verwaltungsrechtliche Sanktionen vorsehen, doch müssen diese Massnahmen abschreckend, wirkungsvoll und angemessen sein. In der Schweiz wurde im Dezember 2002 eine generelle Neuregelung der strafrechtlichen Verantwortlichkeit von Unternehmen beschlossen.

Im Rahmen des Aktionsplans eEurope hat die EU-Kommission inzwischen einen Vorschlag für einen Rahmenbeschluss über Angriffe auf Informationssysteme erarbeitet. Damit sollen die Vorgaben der Cybercrime Convention des Europarats in den EU-Ländern einheitlich umgesetzt werden. Der Vorschlag betrifft im Gegensatz zur Euro-

paratskonvention nur die Strafbarkeit von Angriffen auf Informationssysteme und die Strafverfolgung. In diesen Bereichen geht er teilweise aber mehr ins Detail.

Koordinierte Bekämpfung der Internetkriminalität

Obwohl die Opfer eines Internetangriffs ein Interesse daran haben, die Täter möglichst rasch und kostengünstig auffindig zu machen, zögern sie oft, die Strafverfolgungsbehörden einzuschalten. Mitunter kennen sie die strafrechtlichen Möglichkeiten zu wenig. Prozesse bringen aber auch die Gefahr mit sich, dass der Sachverhalt an die Öffentlichkeit dringt, was das Image des betroffenen Unternehmens schädigen kann. Das Strafrecht kann seine Abschreckungsfunktion allerdings nur erfüllen, wenn die Opfer von Angriffen vermehrt mit den Strafverfolgungsbehörden kooperieren.

Die Cybercrime Convention soll insbesondere die Effizienz grenzüberschreitender Zusammenarbeit der Strafverfolgungsbehörden im Bereich Internetkriminalität wesentlich verbessern. Die Kompetenz zur Verfolgung von Internetdelikten liegt grundsätzlich bei den Kantonen. Der Bund hat aber per 1.1.2003 eine Koordinationsstelle zur Bekämpfung der Internetkriminalität geschaffen (www.cybercrime.admin.ch). Diese dient als Anlaufstelle für Meldungen von Privaten, berät die kantonalen Untersuchungsbehörden und soll in Zukunft auch selbst aktiv nach strafbaren Inhalten im Internet suchen. Opfern von Angriffen kann sie vor allem dann wertvolle Dienste leisten, wenn zwar



Was bringt das Strafrecht den Betroffenen?

Das Internetstrafrecht dient primär der Prävention durch Abschreckung. Es kann diesen Zweck allerdings nur erfüllen, wenn die Opfer von Angriffen vermehrt bereit sind, die Strafverfolgungsbehörden einzuschalten. Zusammen mit der Koordinationsstelle Internetkriminalität können diese den Betroffenen vor allem bei der Tatrekonstruktion und bei der Suche nach den Tätern Unterstützung bieten.



Verdachtsmomente bestehen, aber noch zu wenig konkrete Anhaltspunkte für eine Strafanzeige vorhanden sind.

Schadenersatzansprüche

Angriffe auf Informationssysteme können insbesondere Datenverlust, Leistungsausfall oder unkontrollierte Systemreaktionen verursachen. Diese führen teilweise ihrerseits zu Sach- und Personenschäden. Sie können aber auch Forderungen Dritter wegen Leistungsausfall oder Verzögerungen auslösen. In welchen Fällen die Geschädigten Anspruch auf Schadenersatz haben, beurteilt sich nach den Grundsätzen des Zivilrechts.

- Zivilprozesse gegenüber privaten Hackern usw. sind finanziell meist unergiebig.
- Schwerwiegende Versäumnisse von Mitarbeitern (z.B. Systemadministratoren) können Schadenersatzansprüche auslösen. Dem rechtlichen Vorgehen gegen Arbeitnehmer stehen allerdings oft betriebliche, finanzielle und juristische Überlegungen entgegen.
- Sicherheitslücken in Hard- und Softwarekomponenten oder beim Erbringen von IT-Dienstleistungen (z.B. durch Outsourcingpartner oder Application Service Provider) können zu Gewährleistungs- und Schadenersatzansprüchen führen. Hier zahlt sich eine sorgfältige Analyse und Verteilung der Risiken bei der Vertragsgestaltung aus.
- Haben Geschäftsleitung, Verwaltungsräte und Revisoren die Organisation angemessener Massnahmen zur Informationssicherung bzw. deren Überprüfung vernachlässigt, können sie von den Aktionären für den Scha-

den, welcher dem Unternehmen entstanden ist, zur Rechenschaft gezogen werden.

- Unter Umständen bestehen Ansprüche der direkt oder indirekt Geschädigten gegenüber Versicherungen.

Trotz der verschiedenen möglichen Grundlagen für Schadenersatzansprüche ist es in der Schweiz bis-

her praktisch nie und in der EU nur selten zu gerichtlichen Entscheidungen über Schadenersatz wegen ungenügender IT-Sicherheit gekommen. Dies hängt insbesondere mit rechtlichen Unsicherheiten, Beweisschwierigkeiten und Prozesskostenrisiken zusammen.

Ergänzung des Strafrechts durch das Zivilrecht?

Die Opfer von Angriffen auf Informationssysteme haben hauptsächlich drei Interessen:

- Sie müssen den Ablauf rekonstruieren, um die betreffende Sicherheitslücke zu schliessen.
- Sie möchten weitere Angriffe durch dieselbe Person oder Organisation vermeiden.

- Sie wollen finanziellen Ersatz für die erlittenen Schäden.

Das Zivilrecht kann das Strafrecht im Bereich der Schadensprävention vor allem dadurch ergänzen, dass es Sicherheitsverantwortliche (insbesondere IT-Hersteller, Dienstleister, Administratoren, Geschäftsleitungsmitglieder und Verwaltungsräte) zur Durchführung geeigneter Sicherheitsmassnahmen zwingt. Diese Funktion wird aufgrund der zahlreichen offenen Rechtsfragen, und der damit verbundenen Prozessrisiken bisher allerdings noch unvollkommen erfüllt.

Was bringt die Cybercrime Convention der Schweiz?

Kann das Strafrecht die Informationssicherheit verbessern? Allein durch Verbote lässt sich die Informationssicherheit kaum erhöhen. Das Strafrecht kann seine Abschreckungsfunktion nur erfüllen, wenn die Opfer von Angriffen vermehrt die Strafverfolgungsbehörden einschalten. Eine rasche Umsetzung der Cybercrime Convention sollte die Effizienz der grenzüberschreitenden Strafverfolgung erhöhen und den Betroffenen einen Anreiz geben, vermehrt auch strafrechtlich gegen Angriffe via Internet vorzugehen.

*Dr. Wolfgang Straub, LL.M., ist Rechtsanwalt in Bern. Er ist Mitglied des Beirates der Stiftung InfoSurance.

Wo steht die Schweiz?

Die Schweiz hat die Cybercrime Convention des Europarats zwar unterzeichnet, aber noch nicht ratifiziert. Dieser Schritt wird voraussichtlich erst innerhalb der nächsten Jahre erfolgen, da die notwendige Anpassung prozessrechtlicher Bestimmungen mit der Vereinheitlichung des Strafprozessrechts auf Bundesebene koordiniert werden soll. Das schweizerische Strafrecht enthält aber bereits heute spezifische Normen gegen verschiedene Computerdelikte:

- **Unbefugtes Eindringen** in ein Datenverarbeitungssystem (Art. 143bis StGB)
- **Datenbeschädigung**, Herstellung und Verbreitung von Programmen zur Datenbeschädigung, d.h. insbesondere Viren (Art. 144bis StGB)
- **Betrügerischer Missbrauch** von Datenverarbeitungsanlagen (Art. 147 StGB)
- **Weitere Bestimmungen des Strafgesetzbuches** befassen sich mit Delikten, welche sowohl mithilfe von Computern als auch auf andere Weise begangen werden können (z.B. Kinderpornografie).

Ob die Ratifikation der Cybercrime Convention einen Ausbau der bestehenden Straftatbestände erfordert, wird derzeit kontrovers diskutiert. Sie sollte aber vor allem eine verbesserte Zusammenarbeit bei der grenzüberschreitenden Strafverfolgung bringen.