economiesuisse

Bundesamt für Justiz
Fachbereich Internationales Strafrecht
3003 Bern

07. Juli 2009

Vernehmlassung zur Genehmigung und Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität

Sehr geehrte Damen und Herren

Mit Schreiben vom 16. März 2009 haben Sie uns aufgefordert, zur Vernehmlassung „Genehmigung und Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität" (ECC) Stellung zu nehmen. Wir danken Ihnen für die Möglichkeit zur Meinungsäusserung. Die Vernehmlassung haben wir mit unserer Arbeitsgruppe Informationsgesellschaft im Rahmen unserer Rechtskommission behandelt.

Zusammenfassung
Die Wirtschaft unterstützt das Vorgehen gegen Computer- und Netzwerkkriminalität. Gerade wegen der raschen technologischen Entwicklung brauchen Unternehmer Rechtssicherheit und Rechtsschutz.

economiesuisse begrüsst die internationale Zusammenarbeit bei der Bekämpfung von Computerkriminalität. Allerdings hat die Europarats-Konvention über die Cyberkriminalität (ECC) einen sehr weiten Geltungsbereich und dehnt die Rechtshilfe-Verpflichtungen auch auf Delikte ausserhalb der EDV-Delikte aus. Die Rechte der Betroffenen müssen weiterhin gewahrt bleiben. Ferner soll die Gelegenheit genutzt werden, die heutigen Bestimmungen zu den Informatikdelikten an die technologische Entwicklung anzupassen. Dabei sollen auch die heutigen Unsicherheiten betreffend Netzwerkkriminalität beseitigt werden. Die vom Bundesrat 2008 sistierten Arbeiten an der entsprechenden Vorlage sind wieder aufzunehmen. In Bezug auf die internationale Amts- und Rechtshilfe ist ein angemessener Rechtsschutz vorzusehen. Die Vorlage ist besser auf das geltende Bankkundengeheimnis abzustimmen.

Die Ratifizierung der ECC ist nicht dringend. Es bestehen bereits heute ausgebaute Zusammenarbeitsverträge. Daher darf die Umsetzung nicht unter einem verfehlten Zeitdruck erfolgen.

economiesuisse
Hegibachstrasse 47
Postfach CH-8032 Zürich
Telefon +41 44 421 35 35
Telefax +41 44 421 34 34

Verband der Schweizer Unternehmen
Fédération des entreprises suisses
Federazione delle imprese svizzere
Swiss Business Federation
www.economiesuisse.ch

Allgemeine Bemerkungen

Die Attacken auf Computer und Netzwerke haben in den letzen Jahren zugenommen. Daraus lässt sich eine Professionalisierung im Bereich der Cyberkriminalität schliessen. Wir erachten das Übereinkommen als wichtig, sehen dieses als Chance, den technologischen und technischen Begriffen des Cyberzeitalters gerecht zu werden und unterstützen Bestrebungen zur Schaffung von Rechtssicherheit und Rechtsschutz. Die Bekämpfung erfolgt in erster Linie mit technischen Mitteln. Angriffe auf Systeme und nichtautorisierte Zugriffe auf Computer und Netzwerke sind vor allem durch technische Massnahmen anzugehen und zu verhindern. Die Bedeutung dieses Übereinkommens darf daher nicht überschätzt werden. Es braucht auch in der Infrastruktur und den technischen Mitteln in anderen Ländern eine Verbesserung. Dabei liegt die Verantwortung vor allem bei den Betreibern von Computersystemen.

Dem Strafrecht und der Strafprozessordnung kommen im Bereich der Cyberkriminalität eine subsidiäre Funktion zu. Meist befinden sich die Täter nicht im eigenen Land, sondern agieren ausserhalb der Landesgrenzen. Daher ist die Zusammenarbeit unter den verschiedenen Ländern wichtig, da sich der Wohnsitz, der Aufenthaltsort und der Handlungsort oft nicht in der Schweiz, sondern in unterschiedlichen Ländern befindet.

Die Unterzeichnung der Konvention ist jedoch nicht dringlich. Wichtige Länder wie Grossbritannien und Schweden haben sie noch nicht unterzeichnet. Auch verfügt die Schweiz bereits über ein dichtes Netz zur Gewährung der Rechtshilfe. Dieses wirkt auch bei der Cyberkriminalität. Andererseits verpflichtet die Konvention auch zur Rechtshilfe gegenüber Ländern, bei denen ein wirksames Gegenrecht nicht voll gewährleistet ist. Umso wichtiger ist der Rechtsschutz für die von einer Massnahme Betroffenen.

Vorbehalte

Mit verschiedenen Vorbehalten soll nach dem Entwurf die Schweizer Rechtslage besser berücksichtigt werden. Zu den vorgeschlagenen Vorbehalten nimmt economiesuisse wie folgt Stellung:

- *Art. 3*: „Hacking" bezeichnet ein Aktivwerden, bei welchem über ein Netzwerk in ein Datensystem eingedrungen wird. Die vorgesehene Einschränkung zum Artikel auf Taten in unrechtmässiger Bereicherungsabsicht erscheint nicht zweckmässig. Dieser Artikel 3 sollte ohne Einschränkungen übernommen werden. Eine Bereicherungsabsicht liegt oft nicht vor.
- *Art. 7*: Die vorgesehene Einschränkung erscheint uns nicht sinnvoll. Die Tat sollte strafbar sein, ohne dass der Täterschaft Absicht des Erlangens eines ungerechtfertigten Vorteils nachgewiesen werden muss. Eine Fälschung von Banknoten ist auch schon strafbar, ohne dass die gefälschten Exemplare in Umlauf gebracht werden.
- *Art. 17*: Bei diesem Artikel ist nach unserer Auffassung ein Vorbehalt im Sinne einer Präzisierung der Aufbewahrungspflicht von sechs Monaten für Daten anzubringen, die zur Teilnehmeridentifikation erforderlich sind, welche auch für den internen Kommunikationsdienst gelten.
- *Art. 18b Abs. 1*: Dieser Artikel ist vollumfänglich abzulehnen. Es dürfen nicht Verkehrsdaten vor Abschluss eines Rechtshilfeverfahrens ins Ausland geliefert werden. Bereits die Bekanntgabe einer Gegenpartei kann das Bankgeheimnis verletzen.

Strafprozessrecht

Das geltende Strafprozessrecht und die einschlägigen Sondererlasse erfüllen die Anforderungen der ECC und gehen teilweise gar darüber hinaus. Es stellt schon heute weitgehende Mittel und Verfahren zur Identifizierung und Verfolgung der Täter zur Verfügung.

Rechtshilfe

Die Europaratskonvention hat einen überaus grossen Geltungsbereich betreffend der erfassten Straftaten, der sich vor allem bei der Rechtshilfe auswirkt. Gemäss Art. 25 (I) muss Rechtshilfe nach den Bestimmungen der Konvention in allen Fällen gewährt werden, bei denen Beweise in elektronischer Form vorhanden sein können. Dies trifft nicht nur auf eigentliche Computerdelikte sondern etwa auch auf andere Wirtschaftsdelikte wie beispielsweise Insiderhandel, Geldwäscherei, Verletzung von Immaterialgüterrechten oder Wettbewerbsverstösse zu. Entsprechend greifen auch die in der Konvention vorgesehenen provisorischen Sicherungsmassnahmen.

Grundsätzlich begrüssen wir eine wirksame und rasche Rechtshilfe. Diese darf aber nicht zulasten der betroffenen Parteien gehen, indem diesen keine oder nur ungenügende Rechtsmittel gegen die Weiterleitung ihrer Daten ins Ausland zur Verfügung stellen. Einerseits darf gemäss Art. 25 Abs. 4 des Übereinkommens die Verweigerung der Rechtshilfe nicht alleine damit legitimiert werden, dass die betroffene Straftat ein fiskalisches Delikt darstellt. Andererseits sollen Verkehrs- und Übermittlungsdaten in gewissen Fällen umgehend, wenn möglich sogar in Echtzeit weitergeleitet werden. Dieses Rechtshilfeverfahren ist mit der aktuellen Ausgestaltung des schweizerischen Bankkundengeheimnisses nicht vereinbar und daher zu überarbeiten.

Die von der ECC vorausgesetzte Ermittlungskompetenz verlangt, dass die Behörden bei irgendeinem Delikt Informationssysteme durchsuchen können. Dies muss auch in Echtzeit geschehen können. Die von der ECC vorausgesetzten Ermittlungsbefugnissen gehen ausserordentlich weit. Vor allem im Bereich der Wirtschaftskriminalität ist keine strafbare Handlung mehr vorstellbar, ohne dass Mittel, Techniken oder Instrumente zum Einsatz kommen, welche in einem Cyberzusammenhang stehen.

Strafrecht

Das materielle Strafrecht mit seinen am 1. Januar 1995 in Kraft getretenen Bestimmungen im Bereich „Computerstrafrecht" vermag den Erfordernissen der Konvention über weite Strecken zu genügen. Anpassungsbedarf besteht vor allem in Bezug auf den Straftatbestand des unbefugten Eindringens in ein Datenverarbeitungssystem und die Begriffsbestimmung des sogenannten „Hackings".

Hingegen entsprechen die heute im Strafgesetzbuch verwendeten Begriffe zu den Computerdelikten der Technologie der 80er Jahre und tragen der heutigen Situation keine Rechnung mehr. Ein Grossteil des geschäftlichen und privaten Informationsverkehrs wird heute über mobile Kleingeräte abgewickelt. Es wäre daher von Vorteil, wenn in allen Gesetzen ein einheitlicher Grundbegriff verwendet würde, welcher alle Kommunikations- und Datenübermittlungsmöglichkeiten umfasst. Die Ratifizierung der Konvention soll daher genutzt werden, die Bestimmungen der heutigen Situation anzupassen, wie dies etwa auch Österreich getan hat. Dabei muss auch gewährleistet werden, dass künftigen Entwicklungen Rechnung getragen wird.

Zu diesen notwendigen Arbeiten gehören eine Überprüfung der geltenden Strafnormen zur Computerkriminalität und namentlich die Frage der Netzwerkkriminalität. Hier liegen die Vorarbeiten vor. Die Vorlage aus dem Jahre 2004 soll im Sinne der Vernehmlassungsergebnisse von 2005 weitergeführt werden. Der Entscheid des Bundesrates von 2008, die weit fortgeschrittenen Arbeiten nicht weiter zu verfolgen, trägt den Anliegen der Branche nach einer Verbesserung der Rechtssicherheit nicht Rechnung. Wir sind gerne bereit, an diesen Arbeiten aktiv und konstruktiv mit konkreten Vorschlägen mitzuwirken.

Durch die Schaffung objektiver Strafbarkeitsbedingungen wie das Aufweisen einer Zugriffssicherung kann der Gesetzgeber eine sicherheitsbewusste Haltung fördern und bewirken. Unter dem Begriff „Hacking", wie in Art. 143bis verwendet, verstehen wir ein bewusstes und versuchtes Beschaffen von Passwörtern und Zugangsdaten, eine Unterbindung von Diensten oder unerlaubtes Abfangen von Daten. Das Eindringen in eine Datenverarbeitungseinrichtung stellt einen Eingriff in die Privatsphäre dar, welche auch die geschäftliche Geheimsphäre betrifft. Anders umschrieben handelt es sich hier um einen „virtuellen, elektronischen Hausfriedensbruch".

Das Beschaffen und Anbieten von Eindringhilfen („Phishing", „Pharming") ist grundsätzlich verboten. Jedoch dürfen bei Art. 143bis nicht die wirkungsvollen Instrumente zur Sicherung von Datenverarbeitungsvorrichtungen gegen unbefugten Zugang vergessen werden. Um überhaupt solche Produkte entwickeln zu können, müssen Programmierer ein Sicherungsprogramm entwickeln um anschliessend zu testen, ob ihr Sicherungsprogramm die nötige Wirkung aufweist. Somit sollten diese „Vorfeldtatbestände" nicht unter Strafe stehen. Allerdings dürfte dies schon durch den Rechtfertigungsgrund der Einwilligung des Verletzten gewährleistet sein, was eine spezielle Bestimmung erübrigen könnte.

Durch unbefugtes Eindringen und Datenbeschaffen können auch Daten im Computer und im System verändert oder beschädigt werden. Es geht primär um die Erhaltung und Wahrung der Funktionsfähigkeit von Computer und Netzwerken. Wir verweisen bei der Verwendung und Beschreibung der technischen Begriffe auf das Informationspapier von ISSS (Information Security Society Switzerland) und des ECC (European Computer Crime Convention) Arbeitskreises.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und die Berücksichtigung unserer Anliegen. Wir sind zudem gerne bereit, bei der Überarbeitung der Strafbestimmungen und der Frage der Netzwerkkriminalität mitzuwirken. Gerne stehen wir Ihnen für weitere Informationen zur Verfügung.

Freundliche Grüsse
economiesuisse

Dr. Pascal Gentinetta
Vorsitzender der Geschäftsleitung

Thomas Pletscher, lic. iur.
Mitglied der Geschäftsleitung