

Chaos Computer Club Zürich
c/o Cave Germinal
Soodring 36
8134 Adliswil

30. Juni 2009

Bundesamt für Justiz
Fachbereich Internationales Strafrecht
3003 Bern

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

Sehr geehrte Damen
Sehr geehrte Herren

Wir vom Chaos Computer Club Zürich¹ möchten uns hiermit an der Vernehmlassung zur Ratifizierung des Übereinkommens des Europarats zur Bekämpfung der Cyberkriminalität beteiligen.

Als Zürcher Ableger des Chaos Computer Clubs², einem Verein von Hackern im konstruktivsten (ursprünglichen³) Sinne, möchten wir uns speziell anlässlich der Einführung eines “Hacking”-Paragrafen in Art. 143^{bis} StGB äussern.

Generell anerkennen wir die Notwendigkeit gegen insbesondere organisierte Cyberkriminelle vorzugehen, die ohne ethische Grundsätze⁴ in Computersysteme einbrechen, nur um ihre (vermeintliche) Überlegenheit zu demonstrieren oder gar destruktiv und/oder mit Bereicherungsabsichten auf diesen Systemen zu wirken.

Zuallerst begrüßen wir entsprechend, dass aus Abs. 1 die Floskel

¹Präsenz des CCCZH, 29.06.2009: <http://www.ccczh.ch/>

²Präsenz des CCC, 29.06.2009: <http://www.ccc.de/>

³Ursprünge des Hackerbegriffs, 29.06.2009: <http://stallman.org/articles/on-hacking.html>

⁴Hackerethik des CCC e. V., 29.06.2009: <http://www.ccc.de/hackerethics?language=de>

ohne Bereicherungsabsicht gestrichen werden soll, da es paradox erscheint, dass Leute, die aus Neugierde in ein System einbrechen, bestraft werden mögen, während dagegen Täter *mit Bereicherungsabsicht* potenziell straffrei bleiben.

Ebenfalls begrüßen wir, dass die Schweiz nicht dabei ist den “Hacking”-Paragrafen in voller Montur einzuführen, womit es offensichtlich, anders als etwa in Deutschland, zu keiner generellen Anti-Toolsregelung kommt. Eine solche würde Unternehmen im IT-Sicherheitsbereich akut gefährden, die Forschung lähmen und eine Bestrafung für all jene bedeuten, die sich gerne vertieft mit Technik beschäftigen und ihre Resultate preisgeben.

Problematisch im letztgenannten Zusammenhang erscheint aber die Gummiformulierung im Abs. 2 von Art. 143^{bis}, die Menschen mit Freiheitsstrafe bedroht, welche *Passwörter, Programme oder andere Daten* zur Verfügung stellen, falls angenommen werden muss, dass diese zum Zweck einer Straftat nach Abs. 1 von Art. 143^{bis} Verwendung finden.

Wir fragen uns - was geschieht, wenn dies nicht die Intention ist und die Informationen dennoch für solche Zwecke verwendet werden? Wird in solchem Falle nicht Forschungsfreiheit, gar die Pressefreiheit eingeschränkt und überhaupt die Sicherheit von IT-Systemen untergraben, falls nur jemand davon destruktiven Gebrauch macht?

Die Formulierung müsste in die Richtung angepasst werden, dass das Verfügbarmachen solcher Informationen nur dann strafbar ist, wenn diese geeignet sind ein ganz bestimmtes System anzugreifen und nicht eine generelle Menge von Systemen. Wir anerkennen die gute Absicht sogar dieser Überlegung Rechnung getragen zu haben, wie dies im Erläuternden Bericht zur Vorlage⁵ zu lesen ist.

Im Sinne davon einer anderen Gerichtspraxis entgegen zu wirken, schlagen wir dennoch die folgende Formulierung von Art. 143^{bis} Abs. 2 vor:

⁵Erläuternder Bericht auf Seite 13, 29.06.2009: http://www.admin.ch/ch/d/gg/pc/documents/1722/Vorlage_Bericht.pdf

Wer Passwörter, Programme oder andere Daten, von denen er weiss oder annehmen muss, dass sie zu dem in Absatz 1 genannten Zweck verwendet werden sollen, in Verkehr bringt oder zugänglich macht, *um ein klar bestimmtes Datenverarbeitungssystem anzugreifen*, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Damit gedenken wir einer behördlichen Willkür vorzubeugen, die dann und wann Informationen für strafbar erklärt, in anderen Fällen dann aber wieder nichts unternimmt. Wir sehen damit viel eher als gesichert an, dass eine Person sich ihrer Tat bewusst ist, wenn sie Anleitung dafür gibt ein bestimmtes System anzugreifen, anstatt, wenn sie sich für eine Tat verantworten muss, die sich auf eine Unmenge von Systemen (weltweit) bezieht und der Angriff dazu von einer unbestimmten Anzahl mehr oder weniger fähigen Personen ausgeführt werden kann.

Wir bedanken uns bestens unseren Überlegungen Beachtung zu schenken.

Freundliche Grüsse

Hernani Marques, für den
CCCZH