Swiss Internet User Group
Postfach 1908
8021 Zürich

siug@siug.ch

An das
Bundesamt für Justiz
Fachbereich Internationales Strafrecht
Bundesrain 20

3003 Bern

Zürich, den 25. Juni 2009

Vernehmlassungsantwort bezüglich der Genehmigung und Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität

Sehr geehrte Damen und Herren

Die SIUG ist eine Non-Profit-Organisation und Initiative der /ch/open, die sich aus Internet-Experten verschiedener Stufen zusammensetzt. Dazu gehören Akademiker aus verschiedenen Fachgebieten, Experten aus dem IT Security-Bereich, selbständige Informatiker und Anwender. Das Ziel der SIUG ist es, sich für eine vernünftige Anwendung, Entwicklung und Reglementierung des Internets und verwandter Technologien einzusetzen, ohne dabei den ursprünglichen offenen Geist und die Tradition des Mediums übermässig einzuschränken.

Gerne folgen wir der Einladung zur Teilnahme am Vernehmlassungsverfahren bezüglich der Genehmigung und Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität und möchten wie folgt Stellung nehmen.

Gemäss Vernehmlassungsentwurf soll dem gültigen (leicht geänderten) Art. 143bis Absatz 1 Strafgesetzbuch

> *Wer auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.*

Absatz 2 zur Seite gestellt werden

> *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, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.*

Wie der Vernehmlassungsentwurf in Kapitel 2.2.5.2 ausführt, ist bereits heute neben dem

Eindringen auch die Herstellung und Verbreitung von Computerviren nach Art. 144bis Ziffer 2 StGB, wie unter Umständen auch der (unvollendete) Versuch oder die Gehilfenschaft, Software herzustellen oder zu verbreiten, welche dem Zwecke der Datenbeschädigung oder -veränderung dienen soll, verboten.

Darüber hinaus soll nun mit dem neu geschaffenen Absatz 2 zusätzlich (und als Offizialdelikt) auch

> *die Bereitstellung von Daten im Internet, mittels welcher grundsätzlich eine Vielzahl von Systemen 'geknackt' werden können, die mit demselben Schutz ausgestattet sind*
> (Kapitel 2.2.5.2 Vernehmlassungsentwurf)

geahndet werden können.

Grundsätzlich lässt sich festhalten, dass sich der Zweck einer Software aus sich selbst nicht eindeutig bestimmen lässt. Ein Programm ist mit einem herkömmlichen Werkzeug vergleichbar. Genauso wie sich Skalpell, Hammer, Brecheisen oder Dietrich für nützliche oder gar lebensrettende Tätigkeiten einsetzen lassen, können sie auch für illegale Absichten verwendet werden.

Die Praxis und auch aktuelle Studien zeigen, dass sich die meisten Angriffe mit alltäglichen und/oder einfachen Programmen ausführen lassen, wie sie mit jedem Betriebssystem mitgeliefert werden. Dazu zählen Webbrowser oder auch das Terminalprogramm Telnet.

Niemand käme auf die Idee, die Verbreitung von Taschenmessern oder Webbrowsern zu verbieten.

Neben diesem offensichtlichen Beispiel, sind aber auch viele andere Programme, welche gemeinhin als „Hackertools“ bezeichnet werden könnten, für die IT (Sicherheits-) Industrie von entscheidender Bedeutung.

Mit sogenannten Portscannern z. B. lassen sich Computer oder ganze Netzwerke nach Diensten abfragen, welche allenfalls eine Angriffsfläche bieten. Ein Angreifer nutzt die so gewonnen Informationen, um einen Einbruch vorzubereiten, der Betreiber der Computer-Anlage, um die Sicherheit zu erhöhen. Vergleichen lässt sich die Tätigkeit mit dem Ferienhausbesitzer, der vor der Abreise an Türen und Fenster rüttelt, um sich zu vergewissern, dass sie auch wirklich verschlossen sind.

Wer mehr Sicherheit benötigt, wird Schlösser, Türen, Gitter etc. einsetzen, welche darauf geprüft sind, ob sie bekannten Einbruchswerkzeugen standhalten. Hier kommen in der Netzwerkwelt „Vulnerability Scanner“ zum Einsatz. Diese Schwachstellenprüfer testen Computer auf unzählige bereits bekannte Sicherheitslücken. Um eine verlässliche Aussage treffen zu können, ob eine allfällige Schwachstelle auch wirklich ausgenutzt werden könnte, muss dies in der Regel auch (automatisiert) versucht werden.

Ein weiteres Beispiel sind Passwortlisten und -Cracker. Mit diesen Hilfsmitteln lassen sich innerhalb eines Unternehmens die Stärke der verwendeten Kennwörter prüfen und auch die Verantwortlichen für das Thema sensibilisieren. Hier wie auch bei Softwareherstellern gilt: Erst wenn eine Lücke nicht nur abstrakt beschrieben, sondern konkret aufgezeigt und bewiesen werden kann, wird sie angemessen ernst genommen.

Eine zusätzliche wichtige Kategorie von Programmen zur Fehlersuche und Qualitätssicherung sind sogenannte Netzwerk-Sniffer. Mit ihnen kann der Datenverkehr aufgezeichnet werden und so Fehler im Netzwerk oder in Protokollimplementierungen festgestellt werden. Aber sie lassen sich auch dazu verwenden, (unverschlüsselte) Passwörter abzuhören und Schwachstellen aufzuspüren.

Um die Sicherheit informationstechnischer Anlagen weiterhin gewährleisten resp. steigern zu können, ist ein ungehinderter Austausch von Informationen zwischen Forschern in Beruf und Lehre, IT Dienstleistern und Kunden zwingend notwendig. Dazugehören auch Studiengänge, Kurse und das Bereitstellen von Beispielcode. Ein Bezug der notwendigen Software von einer vertrauenswürdigen Stelle muss gewährleistet bleiben. Es kann nicht angehen, dass durch Strafandrohung die Sicherheit leidet, während dem sich ein Angreifer, der sich durch das unbefugte Eindringen sowieso strafbar macht, die notwendigen Werkzeuge und Informationen aus dem Ausland beschafft. Hier verkehrt sich die ursprüngliche Absicht des Gesetzes, nämlich Daten zu schützen respektive Computer sicherer zu machen, ins Gegenteil.

Diese mögliche Rechtsunsicherheit gilt es zu vermeiden. Folgerichtig fordert auch die zu Grund liegende Cybercrime-Konvention, dass dieser Artikel nicht so ausgelegt werden darf,

> *als begründe er die strafrechtliche Verantwortlichkeit in Fällen, in denen das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen oder der Besitz nach Absatz 1 nicht zum Zweck der Begehung einer [...] umschriebenen Straftat, sondern beispielsweise zum genehmigten Testen oder zum Schutz eines Computersystems erfolgt.*

Wenn sich der Zweck von Passwörtern, Programmen oder andere Daten nicht eindeutig zuordnen lässt, dürfen sie auch nicht im Zentrum von Strafuntersuchungen stehen. Allenfalls könnte man sich überlegen, ob analog Art. 143bis Absatz 1 Strafgesetzbuch explizit auch der Angriffsversuch in böswilliger Absicht strafbar werden soll.

So wie Crash-Tests in der Automobilindustrie müssen Sicherheitstests für Computer auf einem hohen Niveau möglich bleiben.

Wir hoffen, dass unsere Bedenken angemessen berücksichtigt werden können und stehen für weitere Auskünfte gerne zur Verfügung.

Besten Dank & mit freundlichen Grüssen

Für die Swiss Internet User Group