***TeleTrusT* Deutschland e. V.**
Verein zur Förderung der Vertrauenswürdigkeit von Informations- und Kommunikationstechnik
www.teletrust.de

Erfurt, 27. Oktober 2006

# TeleTrusT-Stellungnahme zum Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität (…StrÄndG)

TeleTrusT Deutschland e.V. setzt sich seit nunmehr 17 Jahren für mehr Vertrauenswürdigkeit der Informations- und Kommunikationstechnik, sie verwendende Applikationen und unterstützende Services in Wirtschaft und Verwaltung ein.

Der Entwurf der Bundesregierung zum Strafrechtsänderungsgesetz zur Bekämpfung von Computerkriminalität kann aus unserer Sicht zu einem den veränderten Bedingungen der deutschen Informationsgesellschaft angepassten Rechtsrahmen führen.

TeleTrusT begrüßt ausdrücklich, dass die Bundesregierung ihrer Verantwortung zum Schutz ihrer Bürger nachkommen will. Angesichts des steigenden Aufkommens schädlichen Verhaltens beim Einsatz von Computern in offenen Netzen hat der deutsche Gesetzgeber mit dem vorliegenden Entwurf des StrÄndG nunmehr eine Präzisierung und Ergänzung der bestehenden Strafvorschriften zur Verfolgung von Computerkriminalität eingeleitet.

Es ist grundsätzlich festzustellen, dass für die Beurteilung des Erfolgs dieses Vorhabens die folgenden Rahmenbedingungen angemessen Berücksichtigung finden müssen:

> Erstens ist der Anwendungsbereich deutschen Strafrechts grundsätzlich auf in Deutschland begangene Straftaten begrenzt, das Medium Internet jedoch global verbreitet (insofern greift auch der EU-Rahmenbeschluss, der mit dem Gesetzentwurf für Deutschland umgesetzt werden soll, mit einem auf das Gebiet der Europäischen Union begrenzten Regelungsansatz letztlich zu kurz).
>
> Ferner sollen die Regulierungsmaßnahmen gegen Computerkriminalität die freie Erreichbarkeit und Verfügbarkeit von Informationen nicht über Gebühr einschränken.
>
> Nicht zuletzt sei daran erinnert, dass auch eine strafrechtliche Sanktionierung unerwünschter Handlungen die Durchführung dieser Handlungen nur eingeschränkt eindämmen kann. In gewissem Maße kann Prävention durch Abschreckung erreicht werden.

Die deutsche Gerichtsbarkeit ist politisch unabhängig und hat ihre Tätigkeit allein an den maßgeblichen geltenden Rechtsvorschriften auszurichten. Wenngleich die maßgeblichen Gesetzesbegründungen für die Gerichte keine bindende Wirkung haben, können sie zumindest bei der Auslegung von Gesetzen herangezogen werden.

Für die Stellungnahme von TeleTrusT zum vorliegenden Gesetzgebungsverfahren wurde daher die Begründung zum Gesetzentwurf mit herangezogen; ebenso wurde der unter http://www.medien-internet-und-recht.de/volltext.php?mir_doc_id=398 verfügbare Aufsatz von Ass. Jur. Alexander Schultz „Neue Strafbarkeiten und Probleme ...“ vom 20.09.2006 genutzt.

Keine Berücksichtigung fanden dagegen Erläuterungen zum Gesetzentwurf, die beispielsweise vom BMJ in letzter Zeit kommuniziert worden sind.

Die durch das StrÄndG vorgeschlagenen Änderungen/Ergänzungen von Gesetzen werden in dieser Stellungnahme durch das nachgestellte Kürzel n.N. (nach Novellierung) gekennzeichnet.

## Zu den vorgeschlagenen Gesetzesänderungen im Einzelnen:

Wie bereits dargestellt, begrüßt TeleTrusT das aktuelle StrÄndG und sieht nur wenig Änderungsbedarf.

§ 202c (1) StGB (Strafgesetzbuch) n.N. stellt seiner Zielrichtung nach die Herstellung und Verbreitung sogenannter „Hacker-Tools“ unter Strafe. Dies ist per se nicht zu beanstanden. Problematisch ist allerdings, dass insbesondere auch bei der Entwicklung von Software solche Hackertools zu Zwecken des Tests und der Weiterentwicklung der Sicherheit von Softwarelösungen unentbehrlich sind.
Der Gesetzesentwurf ist unklar formuliert, so dass bei entsprechender Auslegung auch die sachlich nicht zu beanstandende Entwicklung und Verbreitung von Hackertools zu Zwecken der Verbesserung der IT-Sicherheit unter Strafe gestellt würde. Mit anderen Worten sind davon möglicherweise auch Programme betroffen, die nur potentiell gefährliche Funktionen beinhalten und als unverzichtbare Tools beispielsweise von Programmierern und Systemadministratoren im Rahmen ihrer tagtäglichen Arbeit laufend genutzt werden.

Vor diesem Hintergrund und nicht zuletzt auch zur Vermeidung von Rechtsunsicherheit und hieraus resultierenden weiteren Standortnachteile für Deutschland ist § 202c StGB in seiner Formulierung weiter zu präzisieren.

Die Begründung zum vorliegenden Entwurf des StrÄndG schafft auch keine Klarheit:
Einerseits wird ausgeführt, dass allgemeine Programmier-Tools, -Sprachen oder sonstige Anwendungsprogramme von der Regelung ausgenommen seien.
Andererseits wird festgestellt, dass das betreffende Programm nicht ausschließlich für die Begehung einer Computerstraftat bestimmt sein muss.

Dabei greift der Entwurf eines neuen § 202c StGB eine bereits in Zusammenhang mit der Strafbarkeit von Vorbereitungshandlungen für einen Computerbetrug (§ 263 StGB) verwendete Formulierung auf, die da lautet: *„Wer eine Straftat nach (…) vorbereitet, indem er Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt (…)“*. Auch dort hat sich bereits in der praktischen Anwendung das Problem herausgebildet, dass der Zweck bestimmter Computerprogramme nicht dergestalt objektivierbar ist, dass diese zwangsläufig zu rechtswidrigen Zwecken eingesetzt werden. Dies ist ebenso wenig der Fall, wie der Zweck eines Messers (und vieler anderer Werkzeuge) objektivierbar ist; sie können sowohl zu erlaubten als auch zu unerlaubten Zwecken eingesetzt werden. Deshalb wird auch hier mittlerweile vertreten, dass – auch insoweit entgegen der Gesetzesbegründung – nicht auf den vermeintlich objektivierbaren Zweck solcher „Dual-Use-Software“ abgestellt werden soll, sondern darauf, wozu der betroffene Nutzer dieses Computerprogramm einzusetzen gedenkt.

Für diese Auslegung spricht im Ergebnis auch Art. 6 Abs. 2 der Cyber-Crime-Konvention als einem internationalen Abkommen zum Computerstrafrecht, das mit dem StrÄndG auch in Teilen umgesetzt werden soll.

**Im Ergebnis ist das StrÄndG in §202c (1) StGB n.N.** deshalb dahingehend **zu präzisieren**, dass sichergestellt ist, dass die dort unter 1. und 2. beschriebenen Handlungen nicht a priori strafbar sind. Sie könnten daher mit Zweckbindung an zulässige Zwecke, wie z.B. qualitätssichernde Maßnahmen bei der Softwareentwicklung oder zu administrativen Maßnahmen der Datensicherheit in Unternehmen und Behörden, weiter strafverfolgungsfrei betrieben werden. Dies ist im Sinne der konkurrenzfähigen Entwicklung deutscher marktfähiger Produkte und Leistungen der ICT-Branche sowie dem vertrauenswürdigen Betreiben von ICT-Systemen in Wirtschaft und Verwaltung zwingend geboten!

Würde die Herstellung und Verbreitung entsprechender Software-Tools allerdings zum Zwecke der Vorbereitung von Straftaten nach §§ 202a oder 202b StGB n.N. betrieben, stünden sie

unter Strafe. Diese Absicht zur Verwendung bei einer Straftat muss allerdings im konkreten Einzelfall seitens der anklagenden Seite bewiesen werden.

Bei der oben beschriebenen (aus unserer Sicht falschen) Interpretation der derzeitigen Formulierung von § 202c (1) StGB n.N. könnte man die Argumentation sogar dahingehend auf die Spitze treiben, dass es dem Beschuldigten lediglich möglich sei, glaubhaft darzustellen, dass er die in § 202c (1) beschriebenen Handlungen nach 1. oder 2. zwar ausgeführt habe – jedoch **nicht** mit der Absicht, damit Straftaten nach §§ 202a, 202b StGB n.N. vorzubereiten. Dies widerspräche allerdings dem Grundsatz der Unschuldsvermutung im deutschen Strafrecht – wäre also völlig widersinnig.

Parallel zum Gesetzgebungsverfahren, dessen Wirkungsbereich, wie oben beschrieben, beschränkt sein muss, könnte die Bundesregierung wirksame Impulse in anderen Bereichen geben, die effektive Beiträge zur Eindämmung von Computerkriminalität zu leisten in der Lage sind. Hierzu gehört vor allem die möglichst konzertierte Installation von Sicherheitsmechanismen bei möglichst vielen Behörden, aber auch die Förderung derselben bei Netz- und Internet-Providern, Unternehmen, und Bürgern. So könnte Angriffen, die derzeit nachgewiesenermaßen stark mehrheitlich „von außen“ kommen, wirksam begegnet werden. Die Sicherheitskonzepte sind verfügbar – sie müssen nur eingesetzt werden.

Eine Schlüsselstellung (im doppelten Sinn des Wortes) kann hierbei eine flächendeckende Public-Key-Infrastruktur, die einheitliche IDs vergibt und das Schlüsselmanagement betreibt, einnehmen.