Bundesrat **Drucksache** **676/1/06**

20.10.06

Empfehlungen R - FJ - In - K - Wi
der Ausschüsse

zu **Punkt ...** der 827. Sitzung des Bundesrates am 3. November 2006

Entwurf eines ... Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität (... StrÄndG)

A.

Der **federführende Rechtsausschuss** (R),
der **Ausschuss für Innere Angelegenheiten** (In) und
der **Wirtschaftsausschuss** (Wi)
empfehlen dem Bundesrat,

zu dem Gesetzentwurf gemäß Artikel 76 Abs. 2 des Grundgesetzes wie folgt Stellung zu nehmen:

R
In

1. Zum Gesetzentwurf insgesamt

   a) Der Bundesrat stimmt der Bundesregierung in ihrer Auffassung zu, dass das geltende Computerstrafrecht verbessert werden muss. Die Defizite des geltenden Rechts, die unter anderem durch die rasche Fortentwicklung der modernen Kommunikationsmöglichkeiten bedingt sind, sind in der Begründung des Regierungsentwurfs zutreffend dargestellt.

   b) Der Bundesrat weist jedoch zugleich darauf hin, dass die Gefahr besteht, durch eine weite Tatbestandsfassung ein Spektrum von Handlungsweisen in die Strafbarkeit einzubeziehen, die das Verdikt der Strafbarkeit nicht verdienen. Diese Problematik, die bereits das geltende Recht betrifft und die der Regierungsentwurf im Grundsatz nicht verkennt, ist noch nicht überzeu-

...

Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln
Telefon: (02 21) 97 66 83 40, Telefax: (02 21) 97 66 83 44
ISSN 0720-2946

gend gelöst. In diesem Zusammenhang weist der Bundesrat beispielhaft auf Folgendes hin:

aa) Mit der Neufassung des § 202a StGB soll das Phänomen des "Hacking" besser erfasst werden. Soweit das "Hacking" im eigentlichen Sinn, also das unbefugte Eindringen in fremde Computersysteme durch Missbrauch der modernen Kommunikationsmöglichkeiten, in Frage steht, bestehen auch keine Bedenken in Bezug auf die Strafwürdigkeit und Strafbedürftigkeit. Jedoch reicht die Strafbarkeit weit über solche Konstellationen hinaus. Dies ist vor allem darauf zurückzuführen, dass der Entwurf auf den Zugang zu Daten abstellt, kaum aber noch elektronische Geräte existieren, die ohne Datenspeicherung und -verarbeitung auskommen. Beispielsweise würde sich nach dem Entwurf wohl strafbar machen, wer sich Zugang zu dem von seinem Kind verschlossenen MP3-Player verschafft, um die darauf gespeicherten Musikstücke anzuhören. Dies würde jedenfalls dann gelten, wenn das Kind durch den Verschluss auch verhindern will, dass ein Dritter hört, welche Musik er konsumiert. Ebenfalls strafbar machen würde sich der Jugendliche, der sich das von seinen Eltern an einem (vermeintlich) sicheren Ort verwahrte Passwort für nicht jugendfreie Sendungen im Pay-TV verschafft und sich verbotener Weise eine solche Sendung ansieht. Es handelt sich dabei lediglich um Beispiele aus einer nicht überschaubaren Palette von Handlungen, die unter den neuen Tatbestand fallen würden. Der Umstand hat Auswirkungen auch auf die Reichweite des vorgeschlagenen § 202c StGB-E, der an § 202a StGB anknüpft.

   Es erscheint nicht überzeugend, in diesem Zusammenhang auf die Möglichkeit der Verfahrenseinstellung nach Opportunitätsgrundsätzen zu verweisen.

bb) In § 202c StGB-E sollen Vorbereitungshandlungen unter Strafe gestellt werden. Auch insoweit verfolgt der Regierungsentwurf in Übereinstimmung mit dem umzusetzenden Rahmenbeschluss wichtige Anliegen, namentlich, um der Verbreitung von "Hacker-Tools" entgegenzuwirken. Jedoch ist der Tatbestand abermals sehr weit geraten. Auch im Hinblick darauf, dass bezüglich der vorbereiteten Tat bedingter Vorsatz ausreicht, würden künftig wohl unter anderem die folgenden Verhaltensweisen in die Strafbarkeit einbezogen:

Der gerade auf Dienstreise befindliche "Täter" (Angehöriger einer Behörde oder eines Unternehmens) übermittelt einer Schreibkraft sein Passwort, weil er dringend eine E-Mail aus seinem E-Mail-Postfach benötigt. Er rechnet dabei damit und nimmt billigend in Kauf, dass sich die Schreibkraft bei weiteren Gelegenheiten mit seinem Passwort "einloggt" und sich so den Zugang zu nicht für sie bestimmten Daten verschafft (was sie dann nicht tut).

Der besonders vergessliche und auch etwas nachlässige "Täter" (Angehöriger einer Behörde oder eines Unternehmens) vermerkt sein Passwort im Nahbereich seines Computers. Er rechnet damit und nimmt in Kauf, dass etwa eine Reinigungskraft das Passwort findet und sich damit einloggt (was sie dann nicht tut).

Dem lässt sich nicht überzeugend entgegenhalten, dass es in solchen Fällen an der Überwindung der Zugangssicherung durch den "Haupttäter" fehlen würde, weil der Zugang zu den Daten demjenigen, der über das Passwort verfügt, keinen erheblichen zeitlichen oder technischen Aufwand mehr bereitet (vgl. Einzelbegründung zu § 202a StGB-E, BR-Drs. 676/06, S. 14). Eine solche Interpretation kann schon deswegen nicht richtig sein, weil § 202c StGB-E in Bezug auf das Passwort sonst immer leer laufen würde. Die diesbezügliche Passage in der Entwurfsbegründung ist wohl in dem Sinn zu verstehen, dass die Überwindung der Zugangssicherung ohne Kenntnis des Passworts erheblichen Aufwand bereiten muss.

cc) § 303a StGB ist überaus heftiger Kritik aus nahezu dem gesamten Schrifttum ausgesetzt (vgl. etwa Tröndle/Fischer, § 303a, Rnr. 4 mit zahlreichen Nachweisen). So wirft die Frage der Verfügungsberechtigung über die jeweiligen Daten vor allem in vernetzten Systemen kaum überwindliche Auslegungsprobleme auf (vgl. hierzu LK-Tolksdorf, § 303a, Rnr. 7, 8 ff.). Es ist zu befürchten, dass die Vorschrift in der gegenwärtigen Fassung einer verfassungsrechtlichen Prüfung nicht standhalten würde.

dd) § 303b StGB soll auf den privaten Bereich erweitert werden. Damit ist auch eine erhebliche Ausdehnung der Strafbarkeit verbunden. Dieser Umstand erhält dadurch besonderes Gewicht, dass der Begriff der Datenverarbeitung auf Grund der bei elektronischen Geräten fortschrei-

tenden Digitalisierung eine Vielzahl von Geräten erfasst (dazu schon oben a). Lediglich Beispiele sind Videorekorder, Hifi-Anlagen, Fernsehgeräte oder Navigationssysteme bis hin zu Wasch- und Spülmaschinen oder etwa programmierbaren Elektroherden. Die Störung des Betriebs auch solcher Geräte kann nach der neuen Vorschrift strafbar sein, wenn die Datenverarbeitung für den Berechtigten von wesentlicher Bedeutung ist. Im Extremfall kann damit selbst die Beeinträchtigung des Betriebs einer Wasch- oder Spülmaschine unter den Tatbestand der Computersabotage subsumiert werden.

c) Der Bundesrat bittet, im weiteren Verlauf des Gesetzgebungsverfahrens nach Lösungen zu suchen, mit denen die vorgenannten Probleme ausgeräumt oder zumindest vermindert werden. Er hält dies auch vor dem Hintergrund der derzeitigen tatsächlichen Entwicklung für zwingend geboten: Beispielsweise rechnet eine deutsche Staatsanwaltschaft auf Grund entsprechender Ankündigung eines Rechteinhabers damit, dass wegen der illegalen Verbreitung von lediglich vier Computerspielen über das Internet noch in diesem Jahr über 200 000 Urheberrechtsverstöße bei ihr angezeigt werden. Bei anderen Staatsanwaltschaften wurden in der jüngsten Vergangenheit bereits mehrere 10 000 Fälle angezeigt. Den in dem Entwurf beschriebenen Verhaltensweisen kann unter Umständen eine ähnliche Breitenwirkung zukommen. Auch angesichts dessen muss zumindest eine auf die der Strafe würdigen und bedürftigen Handlungen begrenzte Tatbestandsfassung angestrebt werden.

Begründung (nur für das Plenum):

Der Entwurf wirft Probleme auf, die im weiteren Gesetzgebungsverfahren noch gelöst werden müssen.

Wi 2. Zu Artikel 1 Nr. 3 (§ 202c StGB)

Der Bundesrat bittet, im weiteren Verlauf des Gesetzgebungsverfahrens zu prüfen,

a) ob die aktuelle Ausgestaltung des § 202c StGB-E beim gutwilligen Umgang mit allgemeinen Programmier-Tools, -sprachen oder sonstigen Softwareprogrammen sowie "Hacker-Tools" zur Sicherheitsüberprüfung

von IT-Systemen ausreichend vor einer ungewollten Kriminalisierung schützt und

b) ob der § 202c StGB-E um eine konkrete Aufnahme des Tatbestandes des "Phishing" (Versuch, per E-Mail den Empfänger durch irrezuführende und manipulierte Angaben und Inhalte zur Herausgabe von Zugangsdaten und Passwörtern zu bewegen) erweitert werden kann.

Begründung (nur für das Plenum):

zu a:

Ausweislich der Begründung sollen "nur Hacker-Tools", nicht aber "allgemeine Programmier-Tools, -sprachen oder sonstige Anwendungsprogramme" unter den objektiven Tatbestand der Vorschrift fallen. Damit dürften etwa Antivirensoftware und andere Sicherheitsprogramme ausgenommen sein. Da aber die Zweckbestimmung im Tatbestand objektiviert zu betrachten ist, beinhaltet die derzeitige Formulierung des Tatbestandes ein großes Risiko, dass Rechtsanwender auch die genannten Instrumente kriminalisieren könnten. Ferner beschaffen und benutzen etwa IT-Sicherheitsexperten und andere vorsorgliche IT-Anwender Programme, die manche Rechtsanwender durchaus als "Hacker-Tools" einordnen könnten. Daraus erwachsende Unsicherheiten und Risiken treffen sowohl die IT-Unternehmen als Anbieter von Produkten und Dienstleistungen für IT-Sicherheit als auch alle Wirtschaftsunternehmen, die ihre betrieblichen IT-Infrastrukturen und –Anwendungen durch entsprechende IT-Sicherheitsvorkehrungen schützen.

zu b:

Die Telekommunikations- und Internet-Wirtschaft klagt über hohe immaterielle und materielle Schäden, die den seriösen Unternehmen der Branche durch Imageverluste sowie auf Grund von durch "Phishing" ausgelöste Leistungs- und Qualitätsprobleme entstehen.

Die Zahl der "Phishing-Attacken" und die dadurch verursachten Schäden steigen in erheblichem Umfang. Eine Erhebung des Branchenverbandes BITKOM bei den Landeskriminalämtern hat ergeben, dass die Zahl der "Phishing-Opfer" im ersten Halbjahr 2006 um bis zu 50 Prozent gestiegen ist. Der Schaden lag im Durchschnitt bei ca. 4 000 Euro pro Einzelfall.

Da § 202c Abs. 1 Nr. 1 StGB-E bereits einen guten Ansatz für einen entsprechenden "Phishing-Straftatbestand" enthält, wird vorgeschlagen, den bisherigen Entwurf so zu erweitern, so dass er auch eindeutig "Phishing" als Straftatbestand erfasst.

Ferner würde eine solche Regelung auch einen Beitrag zur Verbesserung des Verbraucherschutzes darstellen.

B.

3. Der **Ausschuss für Frauen und Jugend** und
der **Ausschuss für Kulturfragen**
empfehlen dem Bundesrat,

gegen den Gesetzentwurf gemäß Artikel 76 Abs. 2 des Grundgesetzes keine Einwendungen zu erheben.