Dr. Jürgen-Peter Graf
Richter am Bundesgerichtshof

76133 Karlsruhe
Herrenstraße 45a
Telefon: 0721-159-0
www.internet-strafrecht.de

Stellungnahme zur öffentlichen Anhörung des Rechtsausschusses des Deutschen Bundestages am 21. März 2007 in Berlin

zum Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität (BT-Drs. 16/3656)

I. Allgemeines

Die Vorschläge des Gesetzentwurfs betreffen im Wesentlichen Sachverhalte, welche in der Praxis teilweise schon seit längerer Zeit als regelungsbedürftig angesehen wurden (z.B. Strafbarkeit des Hacking), teilweise erst durch neuere technische Entwicklungen sich als problematisch erwiesen haben.
Allerdings ist dabei in den Blick zu nehmen, dass im Zeitalter internationaler Datennetze es auch neugeschaffenen Strafvorschriften an Wirksamkeit fehlt, wenn Taten im Ausland begangen werden und damit eine Geltung des deutschen Strafrechts gemäß §§ 3 ff. StGB ausscheidet. Für einen wirksamen Schutz besonderer Rechtsgüter wird daher auch eine entsprechende Erstreckung des deutschen Strafrechts nach § 5 StGB auf Auslandstaten zu erwägen sein, nachdem im Zusammenhang mit den Diskussionen um Änderungen im Urheberrecht bereits in der Vergangenheit einige Softwareproduzenten und -vertreiber ihren Sitz aus Europa wegverlegt haben.

II. Zu den einzelnen Änderungsvorschlägen

1. Änderung des § 202 a StGB

Die Vorschrift in ihrer bisherigen Form war praxisuntauglich, weil sie von einem Idealbild eines Hackers ausging, das in Wirklichkeit wohl kaum existiert. Die Vorstellung, dass ein Täter allein zur Überprüfung seines Könnens oder der Sicherheit eines Zugangs diesen „hackt“, ohne dann den weiteren Schritt der Überprüfung der Funktion des „gefundenen“ Zugangs vorzunehmen, dürfte kaum der Realität entsprechen. Auch wegen der fehlenden Versuchsstrafbarkeit gab es daher einen quasi rechtsfreien Raum vom Beginn einer Hacking-Aktivität (welche ebenfalls bereits den Schutz der Daten kompromittieren konnte) bis zum erfolgreichen Verschaffen von Daten. Eine dementsprechende Einlassung war einem Täter praktisch nicht zu widerlegen. Im Übrigen ist es wenig überzeugend, wenn es einem Systemadministrator durch entsprechende Konfiguration des Zugangs zu einem Daten-

system möglich ist, die Strafbarkeit eines „Eindringlings“ dadurch zu erreichen, dass diesem unvermittelt Systemdaten präsentiert werden und damit ein Verschaffen bereits objektiv vorliegt.

Die vorgesehene Änderung entspricht der grundsätzlichen Strafwürdigkeit des „Hacking“ und somit auch dem Schutzbedürfnis für gesicherte Datenzugang. Die teilweise gegen eine solche Änderung vorgebrachten Einwände, wonach dann beispielsweise auch von den Medien unterstützte oder eventuell sogar in Auftrag gegebene und finanzierte „Überprüfungen“ von Datensystemen (bspw. Online-Banking-Systeme) strafbar wären, vermögen nicht zu überzeugen; die „Auftragshacker“ können sich für solche Fälle ohne weiteres der Zustimmung der Inhaber der Daten versichern, so dass sie somit nicht unbefugt handeln. Im Übrigen sind solche „Sicherheits-Checks“ bereits nach geltendem Recht strafbar (vgl. MünchKommStGB/Graf § 202 a Rn80).

Die in der Stellungnahme des Bundesrats vorgebrachten Bedenken bezüglich einer Ausweitung der Strafbarkeit auf eher alltägliche Fälle (MP3-Player oder Passworte für Pay-TV) betreffen nicht die vorgeschlagene Änderung; vielmehr waren solche Fälle – sofern sie überhaupt die weiteren Voraussetzungen erfüllen – bereits nach der gegenwärtigen Rechtslage tatbestandsmäßig im Sinne von § 202 a StGB. Allerdings dürften sich die angemeldeten Zweifel dadurch relativieren, dass § 202 a nur auf Strafantrag hin verfolgt werden kann (§ 205 Abs. 1) und dies grundsätzlich auch künftig so vorgesehen ist.

2. Einfügung eines § 202 b StGB

Die neue Vorschrift des § 202 b soll offenbar unter anderem § 202 a dahingehend ergänzen, dass die Verschaffung von Daten während einer Datenübermittlung auch dann strafbar ist, wenn diese bei der Übermittlung nicht besonders gesichert (im Regelfall verschlüsselt) sind. Diese Ergänzung erscheint sinnvoll, wobei allerdings das weitere Abgrenzungskriterium der „nichtöffentlichen“ Datenübermittlung unklar bleibt. Dies dürfte sicherlich bei sogenannten VPN-Übermittlungen (Virtual Private Network) gegeben sein

und gleichfalls bei Übertragungen in firmen- oder behördeninternen Intranets. Diesbezüglich wird allerdings regelmäßig bereits nach geltendem Recht Strafbarkeit nach § 202 a vorliegen. Sofern „Nichtöffentlichkeit“ jedoch bedeutet, dass beispielsweise auch die Übertragung von Emails erfasst sein soll, dann wäre eine entsprechende Klarstellung erforderlich. Allerdings wird dann die Abgrenzung insgesamt schwierig, wann und welcher Internet-Verkehr überhaupt noch „öffentlich“ ist.

Ein geeigneter Anknüpfungspunkt könnte demgegenüber sein, statt auf nichtöffentliche Datenübermittlung abzustellen besser das Abfangen personenbezogener Daten als strafbar zu erfassen. Damit wären nicht nur Email-Übertragungen sondern auch Online-Banking-Vorgänge, Abgabe von Auktionsgeboten oder jegliche Online-Bestellungen oder –Buchungen geschützt.

Zudem hätte eine entsprechende Regelung den Vorzug, dass hierbei auch Zweifel beseitigt würden, ob die Benutzung sogenannter „offener“ und unverschlüsselter WLAN-Netze strafbar ist, weil die Frage der „Öffentlichkeit“ letztlich vom Betreiberwillen abhängig ist. Auch wenn ein Betreiber keine entsprechende Vorstellung hat, weil er nicht erkennt, dass „sein“ Netzwerk ohne Verschlüsselung und damit unsicher ist, wird er deshalb nicht automatisch eine „öffentliche“ Datenübertragung zulassen wollen. Da dies jedoch für Außenstehende nicht erkennbar ist, müssten sie immer damit rechnen, sich nach der beabsichtigten Vorschrift strafbar zu machen, was letztlich einen Rückschritt hinter die gegenwärtige Rechtssituation darstellen würde. Soweit aber nur personenbezogene Daten dem Schutzbereich unterfallen würden, wäre die bloße Nutzung des Internets mittels unverschlüsselter WLAN-Netze weiterhin erlaubt.

Das weiterhin von der Vorschrift unter Strafe gestellte Verbot des Abfangens von Daten mithilfe von elektromagnetischen Strahlen einer Datenverarbeitungsanlage dürfte zwar im Regelfall bereits nach geltendem Recht strafbar sein; eine ausdrückliche Regelung des Sachverhalts in der neuen Vorschrift erscheint jedoch auch zur Vermeidung möglicher Strafbarkeitslücken in besonderen Einzelfällen sachgerecht.

3. Einfügung eines § 202 c StGB

Die Vorschrift ist mit der Vorverlagerung der Strafbarkeit auf Vorbereitungshandlungen zwar nicht unproblematisch, erscheint aber insgesamt erforderlich, um gerade der Verbreitung sogenannter Hacker-Kits oder Viren/Trojaner-Kits – für welche keine sinnvolle Notwendigkeit unter Computer-Usern besteht - entgegen zu wirken. Einer zu weiten Ausuferung des Tatbestands sollte mit dem Erfordernis der objektiven Zweckbestimmung ausreichend entgegengewirkt werden können. Auch wenn die Vielzahl solcher Passworte und Tools in allgemein zugänglichen Bereichen des Internets verfügbar ist, sind auch heute noch viele Nutzer zu einer entsprechenden Suche nicht in der Lage oder haben Sorge vor einer Infektion mit Viren und bleiben damit auf die Verbreitung mittels Datenträgern als Beilage zahlreicher Computerzeitschriften angewiesen. Auch wenn solche Softwareprogramme (allerdings deutlich sichtbar auf der Titelseite hervorgehoben) dort regelmäßig mit dem Hinweis veröffentlicht werden, allein zur Information der Leser über mögliche Gefahrenpunkte zu dienen, werden sie wohl regelmäßig für Interessierte einen Kaufanreiz darstellen, um diese Tools dann auch auszuprobieren. Mit der vorgesehenen Verbotsnorm dürfte solchen Verbreitungen künftig entgegengewirkt werden, weil jede Redaktion zumindest damit rechnen muss, dass die Software teilweise auch zur Begehung strafbarer Handlungen benutzt werden wird.

Allerdings dürfte die präventive Wirkung einer solchen Regelung sich deswegen „in Grenzen halten“, weil die Mehrzahl solcher Passworte und Tools auf Datenspeichern im Ausland vorrätig gehalten wird, sodass ohne eine entsprechende Änderung der Zuständigkeit deutscher Ermittlungsbehörden (vgl. oben I.) solche Zuwiderhandlungen nicht verfolgt werden können.

4. Ergänzung des § 205 StGB

Die Aufrechterhaltung des Erfordernisses eines Strafantrags für die §§ 202 a, 202 b ist zu befürworten; dies gilt ebenso für die Möglichkeit der

Bejahung des öffentlichen Interesses an einer Strafverfolgung, um gerade auch in Fällen hoher wirtschaftlicher Schäden eine Straftat sanktionieren zu können, bspw. wenn damit auch Auswirkungen für die Wirtschaftspolitik der Bundesrepublik Deutschlands verbunden waren (vgl. MünchKommStGB/Graf § 205 Rn 1).

5. Ergänzung des §§ 303 b StGB

Die Ausweitung des Tatbestands auch auf private Nutzer entspricht der allgemeinen Bedeutung der Computertechnik für jedermann und der Erkenntnis, dass auch Privatpersonen erheblich geschädigt werden können, wenn beispielsweise wichtige Aufzeichnungen, Finanz- oder Buchungsunterlagen durch einen Eingriff vernichtet oder gelöscht werden.

Auch die Einführung von besonders schweren Fällen des Computersabotage erscheint für die unter Absatz 4 aufgeführten Fälle gerechtfertigt und die vorgesehene Strafandrohung gerechtfertigt.

III. Fälle des „Phishing“ oder gleichgelagerte Sachverhalte

In der Begründung des Gesetzentwurfs gibt es keinen Hinweis dazu, ob Fälle des bloßen „Phishing“ – ohne Weiterverwendung der erlangten Zugangsdaten bei erfolgreichem „Phishing“ – erfasst werden sollen. Allerdings ergibt sich aus der Presseerklärung des BMJ vom 20. Sept. 2006 anlässlich der Beschlussfassung über den Gesetzentwurf im Bundeskabinett, dass nach Auffassung der Bundesregierung Sachverhalte des „Phishing“ bereits nach gegenwärtigem Recht strafbar seien (vgl. Graf NStZ 2007, 129 ff. Fn 5). Diese Auffassung wird nochmals bestätigt in der Gegenäußerung der Bundesregierung zur Stellungnahme des Bundesrats (BT-Drs. S. 34).

Nach Ansicht des Unterzeichners sind demgegenüber zahlreiche Fälle des „Phishing“, welche in der Vergangenheit erfolgt sind, aber auch derzeit immer

noch auftauchen, nach gegenwärtiger Rechtslage nicht strafbar. Insoweit darf ich auf den beigefügten Kurzaufsatz in der NStZ 2007, 129 ff. verweisen.

Allerdings ist dies in der vorliegenden Literatur nicht unbestritten, wobei Ansätze über eine Strafbarkeit nach §§ 202 a, 263 oder 269 StGB verfolgt werden. Für derartige Überlegungen kommt es jedoch immer auf den jeweiligen Einzelfall an, wobei eine Vermögensgefährdung im Sinne von § 263 StGB in Angelegenheiten des Online-Banking eher bejaht werden könnte als beispielsweise beim „Phishing“ von Account-Daten, denen ein Vermögenswert schwerer zugewiesen werden kann, so dass es damit erst Recht an einer Vermögensgefährdung fehlen dürfte.

Auch eine vorgeschlagene Anwendung des § 269 StGB dürfte vielfach daran scheitern, dass es an der erforderlichen Garantiefunktion fehlen dürfte. Zumindest erscheint es wenig nachvollziehbar, wenn der Urheber der „Phishing“-Attacke durch geschickte Formulierungen der Massen-Email eine Strafbarkeit vermeiden kann.

Letztlich sollte bereits aufgrund der bestehenden Zweifel an einer allgemeinen Strafbarkeit eine ausdrückliche Regelung vorgesehen werden, um jeden Zweifel am gesetzgeberischen Willen auszuräumen und klarzustellen, dass solche Sachverhalte strafwürdig und daher auch strafbar sind. Dabei erscheint es sinnvoll und notwendig, nicht nur die Bereiche des Online-Banking zu erfassen, sondern aus allgemeinen Erwägungen jegliche Fälle des „Phishing“, auch wenn diese telefonisch oder schriftlich erfolgen. Eine Beschränkung einer Strafbarkeit nur auf eine Begehung mittels Datenübertragung im Internet dürfte zu einer Verlagerung der Handlungen auf die bezeichneten anderen Bereiche führen; zudem wäre eine solche Differenzierung weder angemessen noch in ihrer Notwendigkeit erklärbar. Insoweit sollte auch, da nach diesem Vorschlag nicht nur elektronische Daten betroffen sind, eine eigenständige Strafvorschrift geschaffen werden, welche aber aufgrund des Schwerpunktes der angesprochenen Sachverhalte durchaus im 15. Abschnitt des StGB angesiedelt werden kann.

Eine Regelung könnte, wie folgt, lauten:

§ 202 d

Betrügerische Erlangung von Passworten oder sonstigen Zugangsdaten

Wer es unter Vortäuschung einer falschen Identität unternimmt, durch schriftliche oder elektronische Mitteilungen sowie sonstige Möglichkeiten der Telekommunikation andere Personen zur Herausgabe von geheim zu haltenden Informationen, insbesondere Passworten oder sonstigen Zugangsdaten, zu veranlassen, welche den Zugang zu Daten- und Mediendiensten oder deren Benutzung ermöglichen, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.