Forschungsstelle Recht im DFN
ITM, -Zivilrechtliche Abteilung-
Westfälische Wilhelms-Universität Münster
Leonardo-Campus 9
48149 Münster

Telefon: 0251/83-38600
Telefax: 0251/83-38601
E-Mail: recht@dfn.de

Stellungnahme

zum Regierungsentwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität vom 20. September 2006

Einleitung

Seit dem 20. September 2006 liegt ein Regierungsentwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität vor.[1] Das Gesetz dient der Umsetzung des Übereinkommens des Europarats über Computerkriminalität und der Umsetzung des Rahmenbeschlusses 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme. Die Forschungsstelle Recht im Deutschen Forschungsnetz nimmt zu dem vorliegenden Entwurf wie folgt Stellung:

Zusammenfassung

Der Handlungsspielraum des nationalen Gesetzgebers ist durch die Vorgaben des Europaratsübereinkommens und des Rahmenbeschlusses stark eingeschränkt. Dennoch sieht die Forschungsstelle Recht im Deutschen Forschungsnetz im Rahmen der europäischen Vorgaben Korrekturbedarf.

1. Das Ausspähen von Daten (§ 202a StGB-E) sollte auf solche Daten bezogen werden, die durch eine Zugangssicherung gesichert sind. Auf das Merkmal einer *„besonderen“* Zugangssicherung sollte verzichtet werden. Es erweckt nämlich den Eindruck, maßgebliches Abgrenzungskriterium der Vorschrift sei die Höhe des Schutzgrades der Sicherung. Dieses Kriterium ist jedoch angesichts der schnell voranschreitenden Technik konturlos und zur Abgrenzung ungeeignet.

2. Zur Vermeidung der Überkriminalisierung von Bagatellfällen sollte der Tatbestand des Abfangens von Daten (§ 202b StGB-E) auf solche Tathandlungen beschränkt werden, die in der Absicht vorgenommen werden, sich unbefugt Daten aus einer nichtöffentlichen Übermittlung

[1] Abrufbar im Volltext unter: http://www.bmj.bund.de/media/archive/1317.pdf.

zu verschaffen. Das Tatbestandsmerkmal der nichtöffentlichen Übermittlung bedarf zu Vermeidung von Auslegungsschwierigkeiten einer gesetzlichen Definition.

3. Der Tatbestand des Vorbereitens des Ausspähens und Abfangens von Daten (§ 202c Abs. 1 Nr. 2 StGB-E) ist viel zu weit gefasst. Die Kriminalisierung des Verschaffens von Computerprogrammen, die objektiv dazu geeignet sind, Straftaten nach § 202a und § 202b StGB-E zu begehen, ist kriminalpolitisch bedenklich. Durch eine derartige Regelung wird großen Teilen der IT-Sicherheitsbranche die Handlungsgrundlage entzogen. Der Gesetzgeber sollte daher von der ihm zustehenden Möglichkeit eines Vorbehalts nach Art. 6 Abs. 3 des Übereinkommens des Europarates über Computerkriminalität Gebrauch machen.

4. Im Falle der Umsetzung des § 202c Abs. 1 Nr. 2 StGB-E bedarf die gesamte Vorschrift eines Korrektivs. Sie sollte im subjektiven Tatbestand auf solche Handlungen beschränkt werden, die in der Absicht der Begehung einer Straftat nach § 202a und § 202b StGB-E vorgenommen werden.

5. Die Strafbarkeit des Phishings sollte im Gesetz ausdrücklich geregelt werden. Rechtstechnisch ließe sich dies mit einer Versuchsstrafbarkeit im Falle des § 202c Abs. 1 Nr. 1 StGB-E erreichen. Zur Vermeidung einer Überkriminalisierung von Bagatellfällen sollte eine Versuchsstrafbarkeit aber nur bei Berücksichtigung der unter 4. vorgeschlagenen Einschränkung des Tatbestandes angeordnet werden.

Im einzelnen:

§ 202a StGB-E (Ausspähen von Daten)

Nach geltendem Recht ist das Ausspähen von Daten tatbestandsmäßig, wenn sich der Täter Daten verschafft, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind (§ 202a Abs. 1 StGB). Nach dem Regierungsentwurf soll es nicht mehr darauf ankommen, ob sich der Täter die Daten verschafft hat; es genügt, dass er sich unbefugt Zugang zu ihnen verschafft. Diese Neuregelung ist zu begrüßen. Das bisherige Merkmal des Verschaffens von Daten ist zur Gewährleistung eines umfassenden Integritätsschutzes der Computersysteme ungeeignet. Ausweislich der Gesetzesbegründung zu dem geltenden Tatbestand des § 202a StGB sollte das bloße Eindringen in fremde Computersysteme straflos bleiben.[2] Dabei wurde jedoch verkannt, dass das durch § 202a StGB geschützte Rechtsgut – nämlich das formelle Geheimhaltungsinteresse des Verfügungsberechtigten – bereits bei einem Eindringen in das Computersystem gefährdet ist, da in der Regel dem Zugangverschaffen auch eine Kenntnisnahme der geschützten Daten folgt. In der Literatur wird dieser Unstimmigkeit mit einer weiten Auslegung des Tatbestandes begegnet, nach der bereits die Absicht, den Inhalt der gesicherten Daten zur Kenntnis zu nehmen,[3] zur Tatbestandsverwirklichung ausreichend ist. Nach dem nunmehr vorliegenden Gesetzesentwurf bedarf es dieses Korrektivs nicht mehr.

Ferner ist die Beschränkung des bisherigen strafrechtlichen Schutzes auf die formelle Verfügungsbefugnis des Inhabers der Daten[4] nicht mehr zeitgemäß. Angesichts der zunehmenden Gefährdung der mit dem Internet verbundenen Rechner bedarf es eines umfassenden Integri-

[2] BT-Drs. 10/5058, S. 28 ff.
[3] *Hoyer*, in: SK-StGB, Stand Oktober 2005, § 202a Rdnr. 13.
[4] So *Lenckner/Winkelbauer*, CR 1996, 483 (485).

tätsschutzes. Dieser wird durch die Vorverlagerung des Strafrechtsschutzes auf die Tathandlung des Zugangverschaffens gewährleistet.

An dem Erfordernis einer „besonderen" Zugangssicherung hält der Entwurf fest. Dies entspricht Art. 2 Abs. 2 des EU-Rahmenbeschlusses[5], wonach die Mitgliedsstaaten beschließen können, dass die Verschaffung des Zugangs nur bei einer Verletzung von Sicherheitsmaßnahmen unter Strafe gestellt ist. **Auf das Erfordernis einer *„besonderen"* Zugangssicherung sollte der Gesetzgeber jedoch verzichten und stattdessen allein darauf abstellen, ob die Daten durch eine Zugangssicherung gesichert sind und sich der Täter Zugang unter Überwindung einer Zugangssicherung verschafft hat.** Damit würde ein Gleichlaufen mit der Vorschrift des § 202 StGB erreicht, die das Briefgeheimnis schon dann schützt, wenn das Schriftstück verschlossen ist. Auch hier bedarf es keiner Überwindung *„besonderer"* Sicherungsvorkehrungen. Der Begriff der *„besonderen"* Zugangssicherung erweckt zudem den Eindruck, es müsse sich um eine von den Daten trennbare Sicherung handeln, womit die Verschaffung des Zugangs zu verschlüsselten Daten nicht tatbestandsmäßig wäre. Deren Erfassung vom Tatbestand des § 202a StGB wird heute mit der ansonsten bestehenden Schutzlosigkeit während des Übertragungsvorgangs begründet.[6] Der vom Regierungsentwurf vorgesehene Tatbestand des Abfangens von Daten (§ 202b StGB-E) wird jedoch gerade diese Strafbarkeitslücke schließen, so dass nach dem derzeit vorliegenden Entwurf verschlüsselte Daten außerhalb des Übertragungsvorgangs nicht geschützt wären.

Im übrigen ist unklar, wann im Falle des Eindringens über das Internet eine *„besondere"* Zugangssicherung vorliegt. Die meisten Systeme werden derzeit standardmäßig über eine Firewall-Technik geschützt. Durch diese ist für den Angreifer von außen ausreichend dokumentiert, dass ein Eindringen in das System unerwünscht ist. Durch die Verwendung des Begriffs der *„besonderen"* Zugangsicherung wird implementiert, dass die Höhe des Schutzgrades der Zugangssicherung das entscheidende Abgrenzungskriterium sei. Angesichts der schnell voranschreitenden Technik ist dieses Kriterium zur Einschränkung des Tatbestandes ungeeignet. Bei der standardmäßigen Verwendung einer Firewall stehen weiterhin zahlreiche Ports offen, die es dem geübten Angreifer ohne besonderen technischen oder zeitlichen Aufwand ermöglichen, Zugriff auf das geschützte System zu erlangen. Für einen darüber hinausgehenden Schutz bedarf es weitergehender Fachkenntnisse, die dem durchschnittlichen Internet-Nutzer nicht zur Verfügung stehen.

Eine Überkriminalisierung ist bei dieser Fassung des Tatbestandes nicht zu befürchten. Tätigkeiten wie das **Port-Scanning,** bei dem der Angreifer die Ein- und Ausgänge eines Computers abtastet, um offene Zugänge auf dem Zielrechner aufzuspüren, werden weiterhin nicht vom Tatbestand erfasst. Die hierbei übermittelten Daten sind nicht durch eine Zugangssicherung geschützt; sie befinden sich außerhalb des geschützten Systems. Gleiches gilt für **Ping-Scans,** bei denen abgefragt wird, ob der Inhaber einer bestimmten IP-Adresse gerade online ist.

Auch der Zugriff auf frei zugängliche Daten ist nicht tatbestandsmäßig. Ruft der Täter von einem betriebsbereiten PC Daten ab, wird sein Verhalten vom Tatbestand erst dann erfasst, wenn er eine Zugangssicherung wie etwa ID und Kennwort-Abfrage überwindet. Dies stellt nach Auffassung der Forschungsstelle Recht im Deutschen Forschungsnetz bereits heute strafwürdiges Unrecht dar.

[5] Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme.
[6] *Lenckner,* in: Schönke/Schröder, 27. Aufl. 2006, § 202a Rdnr. 8.

Auf das Erfordernis der *„besonderen“* Zugangssicherung sollte daher verzichtet werden.

§ 202b StGB-E (Abfangen von Daten)

Der nach dem Regierungsentwurf vorgesehene Tatbestand des Abfangens von Daten erfasst die Verschaffung von Daten aus einer nichtöffentlichen Datenübermittlung unter Anwendung technischer Hilfsmittel. Durch die Einführung der Vorschrift sollen Übertragungsmöglichkeiten wie etwa E-Mail, VoIP oder Internet-Chats geschützt und bestehende Strafbarkeitslücken während des Übermittlungsvorgangs geschlossen werden. Damit trägt der Entwurf der zunehmenden Bedeutung alternativer Kommunikationsmittel Rechnung und ergänzt den nach § 201 StGB bestehenden Schutz des nichtöffentlich gesprochenen Wortes.

Der Tatbestand ist in seiner derzeitigen Fassung zu weit gefasst und führt zu einer Überkriminalisierung von Bagatellfällen. Da die Vorschrift im Gegensatz zu § 202a StGB-E keine Überwindung von Zugangshindernissen erfordert, werden von ihr Fälle erfasst, bei denen sich Computersysteme aufgrund von Standardeinstellungen automatisiert in offene Netze einwählen. Dies betrifft z.B. schwerpunktmäßig den Bereich des Wireless-LAN. Die Kriminalisierung solcher sozialüblichen Verhaltensweisen sollte nach dem Zusatzprotokoll zum Übereinkommen des Europarats über Computerkriminalität vermieden werden.[7] Da eine Beschränkung des Tatbestandes auf Handlungen, die unter Überwindung von Zugangshindernissen vorgenommen werden, nach dem Übereinkommen des Europarats nicht möglich ist, sollte diese im subjektiven Tatbestand vorgenommen werden. **Es sollte dabei darauf abgestellt werden, dass der Täter bei Vornahme der Tathandlung die Absicht hat, sich unbefugt Daten aus einer nichtöffentlichen Datenübermittlung zu verschaffen.** Damit würden nur noch solche Fälle von der Vorschrift erfasst, bei denen der Täter den zielgerichteten Willen hat, sich geschützte Daten zu verschaffen, es ihm also gerade darauf ankommt.

Kritikwürdig ist ferner die fehlende Definition des Tatbestandsmerkmals der nichtöffentlichen Übermittlung. Nach dem Regierungsentwurf stellt die Datenübermittlung im Internet einen der Schwerpunkte des Anwendungsbereichs der Neuregelung dar.[8] Zweifelhaft ist aber, ob es sich bei der Übertragung von Daten im Internet um eine nichtöffentliche Kommunikation handelt. Aufgrund der dezentralen Struktur des Internets ist die Gefahr des missbräuchlichen Mitlesens während des Übertragungsvorgangs evident. Aus diesem Grund wird in der Literatur zum Teil angenommen, die Kommunikation im Internet sei so anfällig und unvollkommen, dass sie einer öffentlichen Kommunikation mit allgemeiner Teilnahmemöglichkeit gleichgestellt werden könne.[9] Dem entspricht auch die Auslegung des Begriffs des nichtöffentlich gesprochenen Wortes in § 201 Abs. 2 Nr. 2 StGB, auf die die Begründung des Regierungsentwurfs verweist.[10] Danach sind solche Äußerungen nicht geschützt, die zwar nicht an die Öffentlichkeit gerichtet sind, die aber so erfolgen, dass sie von Dritten ohne besonderes Bemühen mitgehört werden können, und damit faktisch öffentlich sind.[11]

---

[7] Convention on Cybercrime – Explanatory Report - ETS No. 185, Nr. 58.
[8] Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität vom 20. September 2006, S. 15 f.
[9] So zuletzt *Sankol*, MMR 2006, 361 (364).
[10] Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität vom 20. September 2006, S. 16.
[11] *Lenckner*, in: Schönke/Schröder, 27. Aufl. 2006, § 201 Rdnr. 9.

Um der Intention des Gesetzgebers gerecht zu werden, besonders gefährdete Kommunikationsmittel wie das Internet zu schützen, sollte dem Tatbestand ein eigener Absatz mit einer entsprechenden Definition der nichtöffentlichen Kommunikation angefügt werden. Diese sollte allein auf das subjektive Element der vom Absender getroffenen Bestimmung der Daten abstellen. Anbieten würde sich insofern eine Formulierung wie „Nichtöffentlich ist eine Kommunikation, deren Inhalte nach der Bestimmung des Absenders an einen begrenzten Kreis von Personen gerichtet sind".

§ 202c StGB-E (Vorbereiten des Ausspähens und Abfangens von Daten)

Der Gesetzesentwurf erfasst in § 202c StGB-E bestimmte Vorbereitungshandlungen zu Straftaten nach § 202a und § 202b StGB-E. Damit wird Art. 6 Abs. 1 Buchstabe a Nr. ii des Übereinkommens des Europarats über Computerkriminalität umgesetzt.[12] Nach § 202c Abs. 1 Nr. 2 StGB-E soll das Herstellen oder Verschaffen von Computerprogrammen, deren Zweck die Begehung einer Tat nach § 202a und § 202b StGB-E ist, unter Strafe gestellt werden. Die Forschungsstelle Recht im Deutschen Forschungsnetz hält diese Tatbestandsalternative für zu weit gefasst. Ausweislich der Begründung des Entwurfs soll die objektivierte Zweckbestimmung des Tools maßgeblich sein; ausreichend sei es, wenn diese auf die Begehung einer Straftat nach § 202a oder § 202b StGB-E gerichtet sei.[13] Eine solche objektive Bestimmung des Verwendungszwecks ist jedoch nicht geeignet, allgemeine Programmiertools von denen im Gesetzesentwurf als „Hacking-Tools" bezeichneten Programmen zu unterscheiden. Zur Systemwartung verwendete Programme können auch multifunktional, d.h. sowohl zur Wartung als auch zur Begehung von Straftaten verwendbar sein. Eine generelle Kriminalisierung des Verschaffens solcher Programme gefährdet in großem Umfang die IT-Sicherheit, da die Sicherheitsbranche zwingend auf die Verfügbarkeit derartiger Programme angewiesen ist. **Kriminalpolitisch erwünschenswert wäre es daher, wenn der Gesetzgeber von der in Artikel 6 Abs. 3 des Übereinkommens des Europarats vorgesehenen Möglichkeit eines Vorbehalts gegenüber der Vorschrift des § 202c Abs. 1 Nr. 2 StGB-E Gebrauch machen würde.**

Sollte der Gesetzgeber an der vorgenannten Regelung festhalten, bedarf die Vorschrift eines einschränkenden Korrektivs. Da objektive Kriterien auf Grund der Multifunktionalität der Programme hierzu ungeeignet sind, sollte die Unterscheidung im subjektiven Tatbestand vorgenommen werden. Der Regierungsentwurf trägt diesem Umstand insofern Rechnung, als er nur die Vorbereitung einer Straftat nach § 202a oder § 202b StGB-E als tatbestandsmäßiges Unrecht erfasst. Diese Einschränkung ist nach Auffassung der Forschungsstelle Recht im Deutschen Forschungsnetz nicht weitgehend genug. Vorbereitungshandlungen sind nach der Systematik des Strafgesetzbuches grundsätzlich straflos. Strafwürdiges Unrecht können sie nur darstellen, wenn sie sich auf eine hinreichend konkretisierte Haupttat beziehen. **Um eine solche einschränkende Auslegung zu garantieren, sollte der Tatbestand nur bei Vorliegen von dolus directus ersten Grades in Bezug auf die vorbereitete Tat verwirklicht sein. Es empfiehlt sich daher eine Beschränkung auf solche Handlungen, die in der Absicht vorgenommen werden, eine Straftat nach § 202a oder § 202b StGB-E zu begehen.**

[12] Übereinkommen des Europarats über Computerkriminalität vom 23.11.2001 – ETS No. 185.
[13] Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität vom 20. September 2006, S. 17.

Strafbarkeit des Phishings

Bedenklich erscheint ferner, dass der Gesetzesentwurf eine Strafbarkeit des Phishings nicht angeordnet hat. Nach geltendem Recht ist dessen Strafbarkeit umstritten, wenn es nicht zur Herausgabe oder Verwendung des Passworts oder der PIN/TAN-Nummer kommt. An einer Strafbarkeit nach §§ 263, 263a StGB fehlt es, da der Herausgabe der persönlichen Zugangsdaten noch keine unmittelbare vermögensmindernde Wirkung zukommt. Auch § 269 StGB bietet keinen ausreichenden Schutz.[14] An der Strafwürdigkeit einer Phishing-Attacke bestehen jedoch keine Zweifel, so dass insofern Regelungsbedarf besteht. **Rechtstechnisch ließe sich die Strafbarkeitslücke durch eine auf § 202c Abs. 1 Nr. 1 StGB-E beschränkte Versuchsstrafbarkeit erreichen;** die genannte Vorschrift stellt die Verschaffung von Passworten oder sonstigen Sicherungscodes zur Begehung einer Straftat nach § 202a oder § 202b StGB-E unter Strafe. **Zur Vermeidung von Überkriminalisierungen sollte eine solche Versuchsstrafbarkeit aber nur dann eingeführt werden, wenn die Norm des § 202c Abs. 1 Nr. 1 StGB-E auf subjektiver Seite – wie vorgeschlagen – auf dolus directus ersten Grades beschränkt wird.**

§ 303b StGB-E (Computersabotage)

Die Neufassung des Tatbestands der Computersabotage dient der Umsetzung von Art. 5 des Europarat-Übereinkommens, der die Erstreckung der Vorschrift auf private Computer- und Informationssysteme vorsieht. Auffallend ist das hohe Strafmaß. Nach Abs. 4 der Vorschrift ist bei der Verwirklichung eines besonders schweren Falles Freiheitsstrafe von sechs Monaten bis zu zehn Jahren vorgesehen. Regelbeispiele sind die Herbeiführung eines Vermögensverlustes großen Ausmaßes, die gewerbsmäßige Begehung oder die Beeinträchtigung der Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder der Sicherheit der Bundesrepublik Deutschland.

Die Neuregelung ist zu begrüßen. Der Entwurf erfasst nunmehr auch das Zusenden von Viren und Würmern gegenüber Privaten, sowie die so genannte Denial of Service Attacke, bei dem die Zugänge zu einzelnen oder zahlreichen Rechnersystemen mit elektronischen Mitteilungen überflutet werden, um diese zu blockieren, was letztlich zu einem partiellen Zusammenbruch der Internetkommunikation führen kann. Insofern bestehen bisher Strafbarkeitslücken.[15] Die vom Tatbestand erfassten Tätigkeiten sind geeignet, großflächige oder gar globale Netzstörungen zu bewirken. Angesichts dieses Gefährdungspotentials erscheint es gerechtfertigt, derartigen Netzstörungen den Status der Kleinkriminalität zu entziehen.

[14] So etwa: *Popp*, NJW 2004, 3517 f.; dagegen: *Buggisch*, NJW 2004, 3519 ff.

[15] Vgl. nur zuletzt: *OLG Frankfurt a.M.*, Beschluss vom 22.5.2005, Az. 1 Ss 319/05, bei dem das Online-Buchungssystem eines Unternehmens aufgrund eines Aufrufs im Internet zeitweise faktisch zusammenbrach. Das Oberlandesgericht sprach den Angeklagten mangels Vorliegens einer Nötigung frei. Im Volltext abrufbar unter: http://www.libertad.de/service/downloads/pdf/olg220506.pdf.

Forschungsstelle Recht im Deutschen Forschungsnetz

Das Deutsche Forschungsnetz (DFN) ist das von der Wissenschaft selbst verwaltete Hochleistungsnetz für Wissenschaft und Forschung in Deutschland. Es verbindet Hochschulen und Forschungseinrichtungen miteinander und unterstützt die Entwicklung und Erprobung neuer Anwendungen für das Internet. Der Verein zur Förderung eines Deutschen Forschungsnetzes e.V. – DFN-Verein – betreibt als anerkannt gemeinnützige Organisation das DFN und stellt seine Weiterentwicklung und Nutzung sicher. Um dies zu gewährleisten setzt sich der DFN-Verein unter anderem für ein rechtssicheres Umfeld bei der Nutzung des DFN in Wissenschaft und Forschung ein. Hierzu hat der DFN-Verein die Forschungsstelle Recht im DFN an der Universität Münster unter Leitung von Prof. Dr. Thomas Hoeren eingerichtet.

Münster, den 6. Dezember 2006

Forschungsstelle Recht im DFN, Ass. jur. Kai Welp (wiss. Mitarbeiter)