Auswirkungen von § 202c StGB auf die IT-Landschaft in Deutschland

Roland Beil, André Borngräber, Stefan Wolf

FHTW Berlin

Kurzfassung

Das vorliegende Paper beschäftigt sich mit § 202c StGB, dem so genannten Hacker-Paragraphen. Es untersucht die Auswirkungen auf die deutsche IT-Landschaft durch die detaillierte Auseinandersetzung mit den Gesetzestexten und dem Aufzeigen der Reaktionen der deutschen IT-Sicherheits-Szene.

1. Einleitung

Dieses Papier befasst sich mit § 202c StGB. Der Paragraph mit der Bezeichnung „Vorbereitung des Abfangens und Ausspähens von Daten“ ist Teil des Abschnitts 15: „Verletzung des persönlichen Lebens- und Geheimbereichs“ des Strafgesetzbuches der Bundesrepublik Deutschland und wird umgangssprachlich auch „Hacker-Paragraph“ genannt.

Bei seinem Inkrafttreten im Sommer 2007 hat der Paragraph eine große Unsicherheit bei Personen ausgelöst, die im Arbeitsfeld der IT-Sicherheit tätig sind. In diesem Paper soll den Auswirkungen seiner Einführung und damit auch dieser Unsicherheit auf den Grund gegangen werden.

Dazu wird zu Anfang in Kapitel 2 der Werdegang der Änderung des Strafrechts vorgestellt, das so genannte 41. Strafrechtsänderungsgesetz. Der Hintergrund dieses Gesetzes bzw. der Motivation dahinter wird in Kapitel 3 auf den Grund gegangen.

Im Kapitel 4 folgt zur Klärung der Ausgangssituation der Gesetzestext von § 202c StGB sowie der Vollständigkeit halber von §§ 202a und b StGB, zusammen mit einer grundlegenden Interpretationen der Texte.

Eine kritische Auseinandersetzung mit dem Inhalt des Gesetzes folgt im Kapitel 5, das ebenfalls die Auswirkungen betrachtet. Das Kapitel 6 stellt beschäftigt sich mit der Online-Durchsuchung und ihrem Zusammenhang mit dem vorgestellten Paragraphen.

Das Resümee fasst die gewonnenen Erkenntnisse zusammen und zeigt Möglichkeiten auf, die bestehende Situation zu verbessern.

2. Geschichtlicher Abriss zu §202c StGB

Dieses Kapitel soll einen Überblick über den Werdegang des Paragraphen geben. Betrachtet wird zuerst das Briefgeheimnis, das durch die Gesetzesänderung erweitert wird. Danach wird die Cybercrime-Convention des Europarates vorgestellt. Sie stellt den Ausgangspunkt für die Änderung dar. Die Umsetzung in Deutsches Recht wird anschließend betrachtet, bevor auf die Motivation dieser neuen Strafrechtsänderung eingegangen wird.

2.1 Das Briefgeheimnis

Den Ursprung von § 202c StGB bildet das so genannte Briefgeheimnis. Es soll den Schutz vor Indiskretion für Schriftstücke[1] sicherstellen und sieht eine bis zu einjährige Freiheitsstrafe für Verstöße vor. Eine Verletzung des Briefgeheimnisses durch unbefugtes Lesen von E-Mails erfolgt in dieser Form zunächst nicht, da E-Mails von § 202 StGB nicht berücksichtigt werden.

2.2 Cybercrime-Convention des Europarates

Im Zuge der immer stärker aufkommenden Kriminalität im Internet verabschiedete der Europarat, als erste internationale Organisation am 8. November 2001, eine Cybercrime-Convention. Auf dieser Basis sollen Gesetze und Vorgehensweisen zur Bekämpfung verschiedener Arten kriminellen Verhaltens gegen Computersysteme, Netzwerke und Daten beschlossen werden.

Unterzeichnet wurde die Konvention anfangs jedoch nur von einigen Mitgliedern des Europarates[2] und denjenigen Staaten, die bereits aktiv am Entwurf der Cybercrime-Convention mitgewirkt haben. Letztere sind beispielsweise die USA, Kanada, Japan und Südafrika.

Am 24. Februar 2005 wurde auf Grund dieser Convention ein Rahmenbeschluss 2005/222/JI[3] über Angriffe auf Informationssysteme erstellt, durch welchen sich die Mitgliedstaaten dazu verpflichtet, schwere Formen dieser Kriminalität unter Strafe zu stellen.

2.3 Strafrechtliche Umsetzung in Deutschland

Um diesem Beschluss Folge zu leisten, entstand innerhalb Deutschlands ein Gesetzentwurf zur Änderung des Briefgeheimnisses. Der wachsende Datenverkehr durch weltweite IT-Kommunikation wurde ins geltende Recht in Form von § 202c StGB mit aufgenommen.

---

1 Vgl. [StGB] § 202

2 Mitglieder des Europarates, welche die Cybercrime-Konventionen unterschrieben haben:
Albanien, Armenien, Belgien, Bulgarien, Deutschland, Estland, Finland, Frankreich, Griechenland, Großbritannien, Italien, ehem. Jugoslawische Republik Mazedonien, Kroatien, Moldavien, Niederlande, Norwegen, Polen, Portugal, Österreich, Rumänien, Spanien (vorbehaltlich eines Referendums), Schweden, Schweiz, Ukraine, Ungarn und Zypern

3 vgl. [DeBuTa-2007] A. Problem

Am Ende des Jahres 2006 äußerten die Bundesländer noch ihre Bedenken gegen den Gesetzentwurf zur Verschärfung und Ergänzung des unter dem Pseudonym "Hackerparagraphen" bekannten Gesetzes[1]. Bereits damals wiesen Sachverständige auf die Gefahr hin, dass durch die weite Tatbestandserfassung auch legale Handlungsweisen, beispielsweise ausgeübt durch Sicherheitsberater, Administratoren und Entwickler, kriminalisiert werden.

Trotz erheblicher Kritik passierte die Änderung des Strafgesetzbuches zur Bekämpfung der Computerkriminalität am 25. Mai 2007[2] den Bundestag und am 6. Juli 2007[3] den Bundesrat ohne weitere Debatten. Am 11. August 2007 trat der Paragraph in Kraft.

3. Motivation für das 41. Strafrechtänderungsgesetz[4]

Im Folgenden soll der Nutzwert der Gesetzesänderung im Rahmen der Umsetzung der Cybercrime-Convention des Europarates dargestellt werden. Dabei werden Änderungen am § 202 StGB in ihrer Gesamtheit betrachtet.

Die rasanten Fortschritte im Bereich der Informationstechnologie bieten ein breites Spektrum neuer Möglichkeiten, aber auch des Missbrauchs, der vor den Grenzen der Staaten nicht halt macht. Im Zuge der Gesetzesänderung soll ein Mindeststandard für Strafvorschriften gegen den Missbrauch festgelegt werden.

Durch Angleichung der einzelstaatlichen Strafvorschriften gegen Angriffe auf Informationssysteme soll die Zusammenarbeit zwischen den Justiz- und Strafverfolgungsbehörden verbessert werden. Beispiele für das breite Spektrum neuer Möglichkeiten zum Missbrauch sind Computerviren, digitale trojanische Pferde, logische Bomben und Würmer. Insbesondere komplexe Angriffe gegen moderne Informationsstrukturen, wie Distributed-Denial-of-Service-Attacken, verursachen hohe Schäden.

Auch kriminelle, extremistische und terroristische Gruppen nutzen moderne Informations- und Kommunikationstechnologien verstärkt für ihre Zwecke. So werden gerade im Internet die Taten vielfach grenzüberschreitend begangen, was zur Folge hat, dass die Lokalisierung und Identifizierung von Straftaten erschwert wird. Häufig nutzen dabei Straftäter auch Unterschiede in den nationalen Rechtsordnungen aus, um der Strafverfolgung und Bestrafung zu entgehen oder diese zumindest erheblich zu behindern.

4. Erläuterungen zum Gesetzestext

Dieses Kapitel beschäftigt sich mit dem Gesetzestext von § 202c StGB. Zunächst wird der Text an sich vorgestellt und kurz erläutert. Danach wird auf die Paragraphen eingegangen, die in dem Gesetzestext erwähnt werden. Diese Beziehungen werden ebenfalls kurz erläutert. Abschließend werden Paragraphen genannt und besprochen, die auf § 202c StGB verweisen.

---

1 vgl. [heise-2007a] Bundesrat billigt verschärfte Hackerparagraphen

2 vgl. [GI]

3 vgl. [eRecht-2007] Bundesrat winkt "Hackerparagraph" § 202c StGB durch

4 vgl. [StrÄndG-2007]

4.1 Der Gesetzestext von §§ 202a, b und c[1]

§ 202a Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202b Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c StGB Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder

2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

4.2 Inhalt des Gesetzestextes

Als Umsetzung der Richtlinie des Europarates werden speziell mit Hilfe von § 202c StGB Vorbereitungshandlungen unter Strafe gestellt.

In §202a StGB „Ausspähen von Daten“ geht es um den unbefugten Zugang zu Daten. Absatz 2 dieses Paragraphen definiert ebenfalls, dass als Daten nur solche gemeint sind, „*die elektronisch, magnetisch der sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.*“.[2]

Um einer Überkriminalisierung vorzubeugen beschränkt sich der Begriff Daten in diesem Zusammenhang laut dem Gesetzentwurf auf solche, bei denen „*Vorkehrungen getroffen*

1 vgl. [STGB]

2 Vgl. [STGB] § 202a Abs. 2

sind, den Zugang auf Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren.“[1] Diese Festlegung ist insofern wichtig, als dass andere Paragraphen, beispielsweise § 303a StGB, darauf Bezug nehmen.

In § 202b StGB „Abfangen von Daten“ wird das Abfangen von Daten aus einer nichtöffentlichen Datenübermittlung oder den elektromagnetischen Abstrahlungen einer Datenverarbeitungsanlage behandelt. Darunter fällt z. B. das so genannte „Sniffing“, zu Deutsch etwa „schnüffeln“. Dabei fängt man innerhalb eines Netzwerkes Datenpakete ab, die eigentlich für andere Computer bestimmt sind. Dadurch kann man Rückschlüsse auf die Existenz anderer Computer in diesem Netzwerk ziehen und auch mit Hilfe eines Entschlüsselungsalgorithmuses Zugangscodes erlangen. Elektromagnetische Abstrahlungen gehen vor allem von Monitor- oder nicht, bzw. schlecht abgeschirmten Netzwerkkabeln aus. Anhand dieser Abstrahlungen ist es ebenfalls möglich, den Datenverkehr nachzuvollziehen.

Um die Tragweite des Paragraphen richtig einzuschätzen ist es wichtig hervorzuheben, dass er ein abstraktes Gefährdungsdelikt behandelt. D. h., dass es beim Durchführen einer Straftat nach § 202c StGB nicht um die Verletzung eines Rechtsgutes geht und es demzufolge auch keinen Geschädigten gibt. Unter Strafe gestellt wird vielmehr die Schaffung einer Gefahr.

Wer also Passwörter, Zugangscodes oder aber Computerprogramme, mit denen diese beschaffbar sind, in irgendeiner Weise zur Verfügung stellt, macht sich strafbar.

Diese „Hacker-Tools“ genannten Computerprogramme werden im Gesetzentwurf folgendermaßen näher definiert: „*Erfasst werden insbesondere die so genannten Hacker-Tools, die bereits nach der Art und Weise ihres Aufbaus darauf ausgelegt sind, illegalen Zwecken zu dienen und die aus dem Internet weitgehend anonym geladen werden können.*“[2] Weiter heißt es „*Das Programm muss aber nicht ausschließlich für die Begehung einer Computerstraftat bestimmt sein. Es reicht, wenn die objektive Zweckbestimmung des Tools auch die Begehung einer solchen Straftat ist.*“[3]

Im Absatz 2 wird auf § 149 Abs. 2 und 3 StGB verwiesen, die sich im Abschnitt 8 „Geld- und Wertzeichenfälschung“ befinden. Diese behandeln das Aufgeben, also nicht weiter verfolgen, einer Tat nach § 149 StGB „Vorbereitung der Fälschung von Geld und Wertzeichen“ und die damit einhergehende Aufhebung der Bestrafung. Wer also die Vorbereitung einer Straftat nach § 202a und § 202b StGB aufgibt und dafür Sorge trägt, dass die teilweise vorbereitete Straftat nicht zu Ende geführt werden kann, wird nicht bestraft.

4.3 Referenzen auf § 202c StGB

Weiterhin tauchen Verweise zum untersuchten Paragraphen im Abschnitt 27 „Sachbeschädigung“ des StGB in §§ 303a und b auf. In § 303a StGB „Datenveränderung“ wird die Veränderung (löschen, unterdrücken, unbrauchbar machen) von Daten behandelt.

In § 303b StGB „Computersabotage“ wird das Stören einer Datenverarbeitungsanlage unter Strafe gestellt. Das kann durch Veränderung von Daten nach § 303a StGB, durch das

---

1 Vgl. [StrÄndG-2007] S. 13, Abs. 1

2 Vgl. [StrÄndG-2007] S. 17, Ziffer 2

3 Vgl. [StrÄndG-2007] S. 19, Ziffer 3

Zerstören der Datenverarbeitungsanlage oder eines Datenträgers oder durch das Eingeben oder Übermitteln von Daten mit der Absicht, anderen einen Nachteil zuzufügen, herbeigeführt werden.

Hervorzuheben ist, dass in beiden Paragraphen Absätze vorhanden sind, die besagen, dass sowohl der Versuch strafbar ist[1], als auch die Vorbereitung der Straftat nach § 202c StGB.[2]

Der Strafbestand des Störens einer Datenverarbeitungsanlage durch Eingeben oder Übermitteln von Daten ist bspw. durch eine so genannte „Denial of Service" (kurz: DoS) Attacke (auf Deutsch ungefähr: „Dienstverweigerungsattacke") erfüllt. Bei dieser wird ein Zielcomputersystem, in der Regel Server bestimmter Unternehmen oder Organisationen, mit einer überdurchschnittlich großen Menge von Anfragen konfrontiert, sodass dieser seine normalen Aufgaben nicht mehr erledigen kann. Das führt dazu, dass diese Server für einen Zeitraum nicht mehr zu erreichen sind und somit beispielsweise die Webseite des Unternehmens nicht mehr angezeigt werden kann.

Durch die Formulierung „*Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, ...*"[3] soll hervorgehoben werden, dass dieser Paragraphen nicht nur die Datenverarbeitungen von Unternehmen und Organisationen betrifft, sondern auch die von Privatpersonen schützt.

Die letzte Erwähnung von § 202c StGB im Strafgesetzbuch findet im Abschnitt 7 „Straftaten gegen die öffentliche Ordnung" statt: Nach § 129a StGB „Bildung terroristischer Vereinigungen" Abs. 2 wird bestraft, wer eine Vereinigung gründet, deren Zweck es unter anderem ist, Straftaten nach § 303b StGB zu begehen oder anzudrohen, oder wer in einer solchen Vereinigung Mitglied ist. Unter Straftaten nach § 303b StGB gehört, wie bereits erläutert, auch das Vorbereiten der Computersabotage nach § 202c StGB.

Hiermit werden also auch Vereinigungen unter Strafe gestellt, deren Zweck es ist Computerprogramme herzustellen oder zur Verfügung zu stellen, mit deren Hilfe eine Straftat nach § 202a oder § 202b StGB vorbereitet werden kann.

4.4 Schlussfolgerungen zu §§ 202a, b und c StGB

Abschließend kann gesagt werden, dass § 202c StGB den Schutz vor Computerstraftaten unterstützt. Verbreitete Angriffsmöglichkeiten auf Datenverarbeitungsanlagen, die vorher nicht oder nur über Umwege als Straftaten galten, bspw. DoS Attacken, werden nun klar als Computerstraftaten definiert und unter Strafe gestellt.

Allerdings fällt bei der Betrachtung des Gesetzestextes auch eine potenzielle Überkriminalisierung auf. Beispielsweise wird allein die Verfügbarmachung von Computerprogrammen, mit deren Hilfe unter anderem das Aushorchen einer Datenverarbeitungsanlage möglich ist, unter Strafe gestellt. Genauso wird das präventive Untersuchen von Computersystemen auf ihre Sicherheit hin kriminalisiert, sofern dies nicht vom Betreiber des Systems in Auftrag gegeben wurde.

---

1 Vgl. [STGB] § 303a Abs. 2 und § 303b Abs. 3

2 Vgl. [STGB] § 303a Abs. 3 und § 303b Abs. 5

3 vgl. [STGB] § 303b Abs. 1

Auf diese Weise wurden in der Vergangenheit viele Sicherheitslücken entdeckt, z. B. die Lücke in der T-Com-Datenbank „OBSOC“ (Online Business Solution Operation Center) vom Chaos Computer Club und mit deren Hilfe man Kunden- und Unternehmensdaten über das Internet einsehen und verändern konnte.[1]

5. Die Auswirkungen der Gesetzesänderung

In diesem Kapitel werden die Auswirkungen von § 202c StGB abgegrenzt. Wie bereits beschrieben, führte der Paragraph schon vor seiner Einführung zu einer großen Unsicherheit bei IT-Sicherheitsexperten, Softwareentwicklern und Webseitenbetreibern. Das liegt vor allem daran, dass er unklare Formulierungen enthält, die verschiedene Interpretationen zu bestimmten Sachverhalten zulassen. Insgesamt kann man sagen, dass die Arbeit von IT-Sicherheitsbeauftragten auf diese Weise zu einer rechtlichen Grauzone geworden ist.

Das soll zunächst anhand von einigen beispielhaften Szenarien gezeigt und die Gründe dafür herausgestellt werden. Danach wird das daraus resultierende Problem der Überkriminalisierung vertieft. Abschließend werden einige der direkten Folgen der Einführung des Paragraphen aufgezeigt.

5.1 Szenarien für die Anwendung von § 202c StGB

Die hier vorgestellten Szenarien sollen verschiedene Situationen schildern, die seit der Einführung des Paragraphen eine rechtliche Grauzone darstellen.

Als erstes Szenario soll der Besitz eines Tools betrachtet werden, dass in die Kategorie „Hacker-Tools“ fällt. Exemplarisch wird von einem „Sniffer“ ausgegangen. Damit ist es möglich, Datenpakete aus einem Funknetzwerk zu empfangen, darunter auch Daten die eigentlich für andere Empfänger bestimmt sind. Mit Hilfe dieser Datenpakete und einem weiteren Tool kann dann der Zugangscode des Funknetzwerks entschlüsselt werden, was es einem Angreifer ermöglicht, in das Netz einzudringen.

Man ist damit also im Besitz eines Computerprogramms, mit dem eine Straftat nach § 202b StGB (Abfangen von Daten) begangen werden kann. § 202c StGB stellt allerdings nur das Herstellen, sich oder einem anderen Verschaffen, Verkaufen, einem anderen Überlassen, Verbreiten oder sonstiges Zugänglichmachen unter Strafe. Somit ist der bloße Besitz nicht strafrechtlich relevant.

Das nächste Szenario geht vom gleichen Tool aus, allerdings befindet es sich diesmal nicht im Besitz, sondern wird erst beschafft. Es wird davon ausgegangen, dass es sich auf einer ausländischen Internetseite befindet, ein Open Source Programm und unter einer GNU Public License (GPL) für jedermann frei zugänglich ist. Das Tool soll aus Interesse an seiner Arbeitsweise heruntergeladen werden. Durch das Herunterladen aus dem Internet scheint mit dem Beschaffen der Software also der Tatbestand zur Ausübung einer Straftat nach § 202c StGB erfüllt.

In einem weiteren Szenario wird davon ausgegangen, dass ein Student eines Informatik-Studiengangs im Rahmen einer Lehrveranstaltung „IT-Sicherheit in der Praxis“ einen

---

1 vgl. [DS]

Portscanner programmiert. Damit können Computer gescannt werden, um zu erfahren, ob sie offene, also nicht gesicherte Ports besitzen. Diese offenen Ports könnten dann zum Eindringen in das Computersystem und dem unbefugten Ausspähen von Daten nach § 202a StGB genutzt werden. Durch Herstellen eines Computerprogramms, durch das diese Straftat möglich ist, ist wiederum der Tatbestand der Vorbereitung erfüllt. Der Student scheint sich, damit also strafbar zu machen.

Zusätzlich zur Herstellung wird nun angenommen, dass der Student sein Programm per E-Mail an einige Kommilitonen schickt. Damit erfüllt er den Tatbestand des Verbreitens von „Hacker-Tools“ und scheint sich strafbar zu machen.

Das nächste Szenario geht davon aus, dass das vom Studenten hergestellte Programm als besonders gute Lösung vom Dozenten der Lehrveranstaltung auf einen Universitätsserver hoch geladen und mit Einverständnis des Studenten unter einer Open Source Lizenz frei verfügbar gemacht wird. Der Student handelt anscheinend illegal, da er durch das Überlassen eines Hacker-Tools an einen anderen eine Straftat vorbereitet haben könnte. Des Weiteren ergibt sich durch das Zugänglichmachen der Software auf dem Universitätsserver ebenfalls eine Straftat, für die die Universität, der Dozent oder der Leiter des Hochschul-Rechenzentrums rechtlich belangt werden könnte.

Im letzten Szenario wird davon ausgegangen, dass der Hersteller des Tools es selber im Internet unter einen Open Source Lizenz zur Verfügung stellt, die Lizenz allerdings um einen Eintrag erweitert, der lautet: „Das Programm darf nicht zur Vorbereitung einer Straftat nach §§ 202a oder 202b StGB benutzt werden“. Auch hierbei ist es rechtlich unklar, ob man durch einfaches Einfügen eines solchen Zusatzes der Möglichkeit einer Bestrafung entgehen kann.

5.2 Gründe für die rechtliche Grauzone

Alle aufgeführten Szenarien haben gemeinsam, dass die beschriebenen Handlungen in keiner Weise einen kriminellen Hintergrund haben, aber trotzdem als Vorbereitung zu einer Straftat nach §§ 202a oder 202c StGB illegal scheinen. Die Formulierung „scheinen“ wird hier, wie auch in den Szenarien verwendet, um die unsichere Rechtslage zu verdeutlichen.

Diese wird dadurch geschaffen, dass Formulierungen wie „*Wer eine Straftat [...] vorbereitet, indem er [...]*“ im Gesetzestext gewählt wurden. Das Wort „*indem*“ kann hierbei auf 2 Arten verstanden werden. Einmal kann die Vorbereitung der Straftat bereits darin liegen, dass man sich ein Hacker-Tool verschafft, ganz egal aus welcher Motivation heraus. Auf der anderen Seite kann die Formulierung so ausgelegt werden, dass sie die Vorbereitung zu einer Straftat näher eingrenzen soll, indem sie die Tätigkeiten, die als Vorbereitung gelten, näher definiert.

Genauso unklar ist die Abgrenzung, ab wann sich eine Handlung als Vorbereitung auslegen lässt. Im zweiten beschriebenen Szenario, indem ein Hacker-Tool von einer ausländischen Internetseite beschafft wird, geschieht dies aufgrund von allgemeinem Interesse an der Arbeitsweise solcher Tools. Wenn es nun beschafft wird, weil man sich speziell für das Eindringen in fremde Netzwerke interessiert, ist das dann schon die Vorbereitung zu einer Straftat? Beschafft man sich das Tool mit dem Ziel ins Funknetzwerk des Nachbarn einzudringen, ist die Vorbereitungshandlung hingegen recht eindeutig. Die genannten

Varianten sind aber nicht eindeutig gegeneinander abgrenzbar, da der Wille des Tatverdächtigen nicht festgestellt werden kann.

Der Begriff des Computerprogramms ist ebenfalls noch nicht eindeutig im deutschen Recht definiert. Er taucht im Urheberrecht auf, allerdings sind diese Definitionen nicht für Computerstraftaten geeignet. In § 202c StGB ist die Rede von „*Computerprogrammen, deren Zweck die Begehung einer solchen Tat ist, ...*“. Der Zweck eines Computerprogramms ist allerdings nie eindeutig festzustellen. Die Gesellschaft für Informatik begründet diese Tatsache, „*... weil Computerprogramme keinen Zweck haben. Selbst wenn der Entwickler einen bestimmten Zweck intendiert, können sie immer missbraucht werden.*“[1]

Die Unsicherheiten zur Rechtslage in Problematiken der IT-Sicherheit basiert also in unklaren Formulierungen im Gesetzestext von § 202c StGB.

5.3 Das Problem der Überkriminalisierung

Diese Unsicherheiten haben dazu geführt, dass sich in der deutschen IT- Landschaft ein Gefühl der Überkriminalisierung verbreitet hat. Viele IT-Sicherheitsexperten sind sich nicht mehr sicher, ob sie sich in einem legalen Rahmen bewegen und sehen daher ihre Existenz bedroht. Sie sehen durch die Gesetzesänderung die Meinung bestätigt, dass die Verantwortlichen für den Entwurf wenig Kompetenz auf dem Gebiet der Computertechnik haben.

In einem Entwurf des Bundestages zum Strafrechtsänderungsgesetz wird erklärt, dass es zu keiner Überkriminalisierung von IT-Sicherheitsexperten kommen soll:

> „Das ist nicht der Fall, wenn das Computerprogramm beispielsweise zum Zwecke der Sicherheitsprüfung, zur Entwicklung von Sicherheitssoftware oder zu Ausbildungszwecken in der IT-Sicherheitsbranche hergestellt, erworben oder einem anderen überlassen wurde, …“.[2]

Da diese Stellungnahme zu der Problematik allerdings nicht bindend für Gerichte ist, ändert sie nichts an dem Vorhandensein der rechtlichen Grauzone.

Auch die Aussage des BSI, verstärkt zertifizierte IT-Sicherheitsexperten auszubilden, wird von der Fachwelt mit Kritik aufgenommen.[3] Es wird eine Monopolisierung der IT-Sicherheitskompetenz befürchtet.

Eine weitere skurrile Auslegung von § 202c StGB in Verbindung mit § 303b StGB und § 129a Abs. 2 StGB ergibt, dass der Chaos Computer Club als „terroristische Vereinigung“ gelten könnte.[4]

---

1 vgl. [GI]

2 Vgl. [DeBuTa-2006 S.19]

3 Vgl. [CCC-2007b]

4 Vgl. [PC WELT]

5.4 Direkte Folgen durch die Einführung des Paragraphen

Viele Personen, die im Feld der IT-Sicherheit tätig sind, haben mehr oder weniger drastische Wege eingeschlagen, um aus der beschriebenen unsicheren Rechtslage zu entkommen.

Die Betreiber der Webseite des Open Source Toolkits „KisMAC“[1] haben ihre Seite beispielsweise auf einen Server im Nachbarland Schweiz portiert. Das Toolkit besteht aus verschiedenen Werkzeugen, mit deren Hilfe man mit einem Mac in Funknetzwerke eindringen kann und fällt dadurch in die Kategorie der „Hacker-Tools“. Um dem Strafbestand der Verbreitung eines solchen Tools zu entgehen, haben sich die Betreiber dem deutschen Rechtsraum entzogen.

Ebenso hat sich der bekannte IT-Sicherheitsexperte Stefan Esser zurückgezogen. Er war einer der Beteiligten an der Initiative „Month of PHP-Bugs“[2], die sich zum Ziel gesetzt hatte, neue Schwachstellen in der beliebten Scriptsprache PHP zu finden. Diese Programmiersprache ist sehr verbreitet und findet sich auf vielen Internetseiten.

Durch das Aufzeigen von Sicherheitslücken in der Scriptsprache soll die Sicherheit im Internet verstärkt werden, da es leichter ist, sich gegen bekannte Lücken wehren zu können als gegen unbekannte. Da das Veröffentlichen dieser Sicherheitslücken aber auch als Vorbereitung zu einer Straftat angesehen werden kann, schloss der Sicherheitsexperte seine deutsche Webseite.

Auf die gleiche Weise hat auch Martin Schmidt reagiert, der auf seinem Blog „#!/bin/blog“ jahrelang über Sicherheitslücken in Unix und Linux Systemen berichtet hat. Er befürchete „*für ein paar peinlich-triviale Scripts, die hier im Blog stecken, mit einem Jahr Freiheitsstrafe rechnen* [zu müssen, d.V,].“[3] und hat daher seinen Blog geschlossen.

Generell ist die Veröffentlichung von Sicherheitslücken in Programmen, aber auch in Programmiersprachen oder Werkzeugen, eine umstrittene Angelegenheit. Professor Jürgen Beyerer, Sprecher des Fraunhofer-Verbundes Verteidigungs- und Sicherheitsforschung, hatte im März dieses Jahres für besonders sensible Bereiche eine Geheimhaltung von neu entdeckten Schwachstellen gefordert.[4]

Einen anderen Weg zur Klärung der ungenauen Rechtslage hat die Firma „VisuKom“ eingeschlagen. Als IT-Sicherheits-Dienstleister berät sie Unternehmen bezüglich der Sicherheit ihrer Datenverarbeitungsanlagen. Dazu werden die Anlagen mit Hilfe von Sicherheitstools getestet, die unter anderem auf der Ausnutzung von bekannten Schwachstellen basieren. Gleichzeitig bietet die Firma auf ihrer Internetpräsenz eine Reihe dieser Tools an, die durch den neuen Paragraphen auch als „Hacker-Tools“ eingestuft werden können.

Durch die Strafbarkeit der Benutzung und Verbreitung der Tools sieht das Unternehmen seine Existenzgrundlage gefährdet. Daher hat der Geschäftsführer Marko Di Filippo stell-

---

1 Vgl. [KISMAC]

2 Vgl. [PHPBUG]

3 Vgl. [BINBLOG]

4 Vgl. [TR] S.72

vertretend für die Firma eine Verfassungsbeschwerde eingereicht.[1] Diese soll Aufklärung bringen, in wie weit die Tätigkeiten des Unternehmens illegal sind.

Einen Schritt weiter ist Michael Kubert gegangen, der auf seiner Internetseite „JavaExploits“[2] verschiedene Hacker-Tools frei zur Verfügung stellt. Er hat vorsichtshalber Strafanzeige gegen sich selbst gestellt um zu klären, ob seine Handlung strafbar nach § 202c StGB ist.[3]

Ebenfalls auf gerichtlichem Weg will Michael Eckert, Chefredakteur des Online-Magazins „Tecchannel“, für Aufklärung sorgen. Er stellte am 17. September 2007 Strafanzeige gegen das Bundesamt für Sicherheit in der Informationstechnik (BSI)[4]. Dadurch soll geprüft werden, inwiefern sich das Bundesamt strafbar macht, indem es auf seiner Internetpräsenz die „BSI Open Source Software Security Suite“ anbietet, deren Bestandteil auch der Passwort-Cracker „Jack The Ripper“ ist[5]. Dieses Tool ermöglicht das Knacken eines Passworts auf verschiedene Arten und fällt damit klar in die Kategorie „Hacker-Tool“. Nachdem die Antwort des Staatsanwalts nicht viel Klarheit gebracht hat, wurde eine Beschwerde am Landgericht Bonn eingelegt[6].

6. Streitpunkt: Die Online-Durchsuchung und § 202c StGB

Neben dem § 202c StGB beschäftigt sich dieses Paper auch mit der geplanten Online-Durchsuchung seitens der deutschen Bundesregierung. Die Online-Durchsuchung soll u.a. der Prävention zur Abwehr von Gefahren des internationalen Terrorismus dienen.[7] Informationstechnische Systeme sollen nach Hinweisen oder Beweisen von kriminellen Aktivitäten durchsucht werden.

6.1 Gesetzesgrundlage

Am 21. Dezember 2006 hat der Landtag von Nordrhein-Westfalen als erstes Bundesland mit der Änderung des Verfassungsschutzgesetzes des Landes - trotz massiver verfassungsrechtlicher Bedenken von Sachverständigen - die gesetzliche Grundlage für die Online-Durchsuchung beschlossen. Das Gesetz trat am 30. Dezember 2006 in Kraft.

Eine erste Niederlage musste die Bundesregierung am 5. Februar 2007 einstecken. Der Bundesgerichtshof entschied, dass heimliche Online-Durchsuchungen durch die Polizei unzulässig seien. Für einen solchen Eingriff fehlt die erforderliche Ermächtigungsgrundlage. Derzeit sind nur offene Durchsuchungen erlaubt.[8]

---

1 Vgl. [VISUKOM]

2 Vgl. [JE]

3 Vgl. [SPITBLOG]

4 Vgl. [TECCHANNEL-a]

5 Vgl. [BSI]

6 Vgl. [TECCHANNEL-b]

7 Vgl. [BMI1-2007] S. 1

8 Vgl. [Heise-2007b]

Seit dem 10. Oktober 2007 verhandelt das Bundesverfassungsgericht (BVerfGG) in Karlsruhe Verfassungsbeschwerden gegen die Online-Durchsuchung im Verfassungsschutzgesetz von Nordrhein-Westfalen.[1]

Der Verhandlungsausgang wird mit Spannung verfolgt, da er als Tendenz für eine bundeseinheitliche verfassungsmäßige Einführung der Online-Durchsuchung zu werten ist. Laut Fachkreisen ist mit einem Urteil vor März 2008 nicht zu rechnen.

Für eine Umsetzung der Online-Durchsuchung müsste das Grundgesetz sowie zahlreiche Länder- und Bundesgesetze angepasst werden, um sowohl dem Verfassungsschutz als auch der Landespolizei Zugriff auf informationstechnische Systeme, juristisch zu ermöglichen.

6.2 Begriffsdefinition

Diesem Paper wird folgende Begriffsbestimmung zugrunde gelegt:

> Unter der Online-Durchsuchung wird die versteckte Suche unter Einsatz elektronischer Mittel nach verfahrensrelevanten Inhalten auf informationstechnischen Systemen verstanden, die sich nicht im direkten physikalischen Zugriff der Sicherheitsbehörden befinden, aber über Kommunikationsnetze erreichbar ist.[2]

Der Terminus „informationstechnische Systeme“ umfasst alle gegenwärtigen und zukünftigen Systeme, bestehend aus Hard- und Software, die zur Erfassung, Speicherung, Verarbeitung, Übertragung und Anzeigen von Informationen/Daten genutzt werden können.[3]

Dies bedeutet, dass neben dem heimischen Computer auch Großrechner (z. B. Server), eingebundene externe Datenträger und auch Telekommunikationsgeräte (z. B. Handy, Fax) mit zur Online-Durchsuchung herangezogen werden können. Telekommunikationsinhalte sind aber nicht Gegenstand der Durchsuchung.

6.3 Datenerhebung

Unter Verwendung der RFS (Remote Forensic Software), der offizielle Name der Online-Durchsuchungssoftware, sollen die Daten erhoben werden. Die im Vorfeld definierten Suchabfragen/Suchkriterien[4] sollen die Ermittlungen nach Hinweisen auf dem Zielsystem unterstützen:

- Dateinamen
- bestimmte Dateiendungen/Datentypen
- Eigenschaften/Attribute (Zugriffsdaten, etc.)
- Schlüsselwörter
- bestimmte Verzeichnisse

---

1 Vgl. [BGH2007]

2 Vgl. [BMI1-2007] S. 2

3 Vgl. [BMI1-2007] S.4f

4 Vgl. [BMI2-2007] S. 7

Eine genaue Methode, wie der Bundestrojaner auf dem Zielrechner installiert wird, ist nicht bekannt. Im Internet existieren zahlreiche Theorien, auf die in diesem Paper später eingegangen wird.

Ist Bundestrojaner auf dem Zielsystem installiert, erfolgt die Datenerhebung im Offline-Modus. Erst bei einer bestehenden Datenverbindung werden die gewonnenen Informationen partiell an die Sicherheitsbehörde übermittelt, um das Entdeckungsrisiko deutlich zu minimieren.

6.4 Konflikt zwischen Online-Durchsuchung und § 202c StGB

Die Deutsche Bundesregierung verstößt mit der Entwicklung des so genannten Bundestrojaner (für die Online-Durchsuchung) gegen geltendes Recht. Im August diesen Jahres wurde der §202c StGB vom Bundestag verabschiedet, dass die Herstellung von Programmen zum Ausspähen und Abfangen von Daten unter Strafe stellt. Nach einem Bericht des Spiegels wurden die Arbeiten am Bundestrojaner im November dieses Jahres wieder aufgenommen.[1] Das BVerfGG beschäftigt sich nun mit der Frage, ob der Bundestrojaner als verfassungswidrig einzustufen ist.

Kritisch wird darüber hinaus bemerkt, dass mit dem Verbot der Beschaffung und Benutzung der Hacker-Tools auch der mögliche Widerstand gegen den Bundestrojaner unterbunden wird.[2]

7. Resümee

Die Untersuchung der Auswirkungen von § 202c StGB zeigt, dass der Paragraph statt für Sicherheit eher für Unsicherheit in der deutschen IT-Landschaft gesorgt hat.

Die Strafrechtsänderung hat die Vorgaben aus der Cybercrime-Convention des Europarates zwar umgesetzt, aber wie in Kapitel 5 gezeigt wurde, hat sie dabei viele Punkte im Unklaren gelassen, was nun zu einer Überkriminalisierung von Personen geführt hat, die im Bereich der IT-Sicherheit tätig sind. Die Einbeziehung einer gutartigen Nutzung der verbotenen Hacker-Tools wird in der Umsetzung der Bundesregierung nicht vorgesehen. Des Weiteren fehlen wichtige rechtliche Definitionen, wie beispielsweise die von Computerprogrammen.

Wie in den Kapitel 5.3 und 5.4 angeschnitten, wird der Paragraph daher scharf kritisiert und die Abschaffung oder Änderung des Gesetzestextes gefordert. Was genau jedoch passieren soll, ist unklar.

Eine Abschaffung des Gesetzes scheint sehr unwahrscheinlich. Auch wenn die Umsetzung vielleicht etwas misslungen ist, so ist der Bedarf für ein entsprechendes Gesetz zum besseren Schutz vor Computerstraftaten unbestritten. Außerdem hat sich die Bundesregierung durch die Unterzeichnung der Cybercrime-Convention zu einer Umsetzung dieser Vorlage verpflichtet.

---

1 Vgl. [SPIEGEL]

2 Vgl. [CCC-2007b]

Die European Expert Group for IT Security (EICAR) hat im Rahmen ihres diesjährigen Gipfels eine juristische Stellungnahme zur IT-Sicherheit mit § 202c StGB veröffentlicht[1]. Darin ergibt sich die Schlussfolgerung, dass zur Klärung der offenen Rechtsfragen eine Anhörung vor dem Bundesverfassungsgericht (BVerfG) angestrebt werden sollte.

Sollte die Anhörung Erfolg haben, würde die Untersuchung durch das BVerfG die Notwendigkeit der Überarbeitung des Gesetzes belegen.

In diesem Fall sollte die Überarbeitung die folgenden Punkte abdecken:

- Definition des Begriffs Computerprogramm: Was gilt als Computerprogramm und was nicht? Ist die Zweckbestimmung ein eindeutiges Kriterium zur Kategorisierung von Programmen?
- Eingrenzung der Vorbereitungshandlung: Wann gilt eine Handlung als Vorbereitung einer Straftat? Wie äußert sich der Wille bei diesem abstrakten Gefährdungsdelikt?
- Berücksichtigung des gutartigen Einsatzes der Sicherheits-Tools: Der Einsatz der betroffenen Tools zum Testen und Sichern von IT-Systemen muss eindeutig straffrei bleiben.

Bis diese Punkte geklärt sind, empfiehlt die juristische Stellungnahme im Umgang mit den Hacker-Tools auf 3 Sachverhalte zu achten:

- Sorgfalt im Umgang mit den Tools sowie auch mit der Verwahrung der Tools und den Schutz vor unerlaubtem Zugriff.
- Ausführliche Dokumentation der Beschaffung, der Benutzung und der Verwahrung der Tools.
- Bei der Benutzung der Tools, mit dem Ziel des Testens von IT-Systemen, von Unternehmen oder Privatpersonen immer die Einholung der Erlaubnis mit detaillierter Beschreibung des Umfangs der Tests.

8. Literatur

[BGH2007]	Bundesverfassungsgericht http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg07-082.html; Abruf: 17. November 2007
[BINBLOG]	#!/bin/blog http://www.binblog.de/ Abruf: 03.12.2007
[BMI1-2007]	Bundesministerium des Innern „Fragenkatalog des Bundesfinanzministerium der Justiz“ Abruf: 22. August 2007
[BMI2-2007]	Bundesministerium des Innern „Fragenkatalog der SPD-Bundestagsfraktion“ Abruf: 22. August 2007
[BSI]	Bundesministerium für Sicherheit und Informationstechnik http://www.bsi.de/produkte/boss/index.htm Abruf: 01.12.2007
[BT]	Deutscher Bundestag – Petition „Wahlrecht: Stimmabgabe mit Wahlgeräten“ http://itc.napier.ac.uk/e-Petition/bundestag/view_petition.asp?PetitionID=294

1 Vgl. [EICAR]

	Abruf: 18. November 2007
[BZ]	Förster, Andreas: „Beamte unter Verdacht“, Berliner Zeitung Ausgabe: 31.08 2007 – Politik S. 2
[CCC-2007a]	Chaos Computer Club e.V. http://www.ccc.de/cybercrime/ Abruf: 26. November 2007
[CCC-2007b]	Chaos Computer Club e.V. http://www.ccc.de/updates/2007/paragraph-202c?language=de Abruf: 26. November 2007
[DeBuTa-2006]	Deutscher Bundestag: Drucksache 16/3656 – Entwurf eines Strafrechtsänderunggesetzes zu Bekämpfung der Computerkriminalität
[DeBuTa-2007]	Deutscher Bundestag: Drucksache 16/5449 - Beschlussempfehlung und Bericht des deutsche Bundestages zu dem Gesetzentwurf der Bundesregierung Drucksache 16/3656
[DS]	Die Datenschleuder – Das wissenschaftliche Fachmagazin für Datenreisende, ein Organ de Chaos Computer Club, Ausgabe 83, Juli 2004
[EICAR]	European Expert Group for IT Security http://www.eicar.org/press/infomaterial/JLUSSI_LEITFADEN_web.pdf Abruf: 03.12.2007
[eRecht-2007]	Otto, Philipp: „Recht der neuen Medien“, eRecht24.de, http://www.e-recht24.de/news/strafrecht/567.html, Abruf: 26. November 2007
[GI]	Gesellschaft für Informatik: „Entwurfsfassung des § 202c StGB droht Informatiker/innen z kriminalisieren“, http://www.gi-ev.de/aktuelles/meldungsdetails/meldung/159/ Abruf: 03.12.2007
[Heise-2007a]	Krempl, Stefan: „Bundesrat billigt verschärfte Hackerparagraphen“, www.heise.de, Heise Verla http://www.heise.de/security/news/meldung/92334 Abruf: 26. November 2007
[Heise-2007b]	Kuri, Jürgen: „Heimliche Online-Durchsuchungen sind unzulässig“, www.heise.de, Heise Verlag http://www.heise.de/newsticker/meldung/84776 Abruf: 17. November 2007
[JE]	Java Exploits http://www.javaexploits.de/ Abruf: 02.12.2007
[KISMAC]	KisMAC http://kismac.macpirate.ch/ Abruf: 02.12.2007
[PC WELT]	Ziemann, Frank: „Der Chaos Computer Club wird 25“, PC Welt http://www.pcwelt.de/start/sicherheit/archiv/57239/ Abruf: 30.11.2007
[PHPBUG]	Month of the PHP Bug http://www.php-security.org/ Abruf: 30.11.2007
[Spiegel]	www.spiegel.de: „Schäuble treibt Online-Durchsuchung weiter voran“, Spiegel # 47/2007 S. 20 http://www.spiegel.de/spiegel/vorab/0,1518,517946,00.html Abruf: 26.November 2007
[SPITBLOG]	Reineke, Lars: „Selbstanzeige wegen "Hackertools" (II)“, www.spitblog.de http://www.spitblog.de/2007/10/07/selbstanzeige-wegen-hackertools-ii/ Abruf: 28.11.2007
[STGB]	Strafgesetzbuch der Bundesrepublik Deutschland Letzte Änderung: 26.10.2007
[StrÄndG-2007]	Gesetzentwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität Bundesministerium für Justiz http://www.bmj.de/files/-/1317/RegE%20Computerkriminalit%E4t.pdf Abruf: 26. November 2007
[TECCHANNEL-a]	Eckert, Michael: „Das BSI und § 202c: Der Hackerparagraf und das Bundesamt“ www.tecchannel.de, http://www.tecchannel.de/sicherheit/grundlagen/1729025/ Abruf: 02.12.2007
[TECCHANNEL-b]	Hartmann, Mike: „Das BSI und der Hackerparagraf § 202c: TecChannel legt Beschwerde ein“ www.tecchannel.de, http://www.tecchannel.de/sicherheit/news/1737683/ Abruf: 02.12.2007
[TR]	Stieler, Wolfgang: „Unüberlegte Streuung - Sollte man Sicherheitslücken öffentlich machen?“, i Technology Review Deutsche Ausgabe 12/2007, Heise Verlag

[VISUKOM] Neudorfer, Nadja: „Hackerparagraf gibt Anlass zu Verfassungsbeschwerde“, www.visukom.de, http://www.visukom.de/deutsche_Version.1.0.html?&tx_ttnews[pointer]=1&cHash=06e0c0cd4 Abruf: 01.12.2007