Hacker-Paragraph: Reale Bedrohung oder „Luftnummer“

Die am 17.09.2007 veröffentlichte Nachricht, dass eine Strafanzeige gegen das Bundesamt für Sicherheit in der Informationstechnologie (BSI) gestellt wurde, markiert einen weiteren Höhepunkt in der langen Diskussion um den so genannten Hacker-Paragraphen, § 202 c StGB. Hintergrund der Strafanzeige war die Bewerbung eines Tools durch das BSI, das potenziell unter den Hacker-Paragraphen fallen könnte. Es handelt sich dabei um den Password-Cracker „John the Ripper“. Die Strafanzeige wurde von dem Magazin „TecChannel“ erstattet. Zielrichtung des Magazins: Mit einem Urteil soll mehr Rechtssicherheit im Umgang mit Sicherheits-Tools gegeben sein.

Die Diskussion um den Hacker-Paragraphen wurde nicht nur während des Gesetzgebungsverfahrens intensiv geführt. Auch noch jetzt verunsichert die gesetzliche Neuregelung die Hersteller von Schutzsoftware. Dabei sind sich in den Grundaussagen eigentlich alle einig. Beispielsweise verweist das Bundesjustizministerium durch den Ministeriumssprecher darauf, dass das Gesetz nur denjenigen betrifft, der wirklich eine Computerstraftat vorbereitet. Nach Auffassung des Justizministeriums muss sich derjenige keine Sorgen machen, der sich nur um die Sicherheit seines eigenen Systems oder eines fremden Systems in dessen Auftrag kümmert. Allerdings lässt sich diese Auffassung des Justizministeriums nicht so ohne weiteres aus dem gesetzlichen Wortlaut herauslesen. Der Wortlaut lässt unterschiedliche Interpretationen zu, so dass vor diesem Hintergrund viele Sicherheitsexperten rechtliche Schwierigkeiten befürchten. Grundaussagen finden sich in der Gesetzesbegründung, die im Zweifel aber nicht die alleinige Basis einer rechtlichen Bewertung in einem eventuellen gerichtlichen Verfahren ist.

Alles in allem ist die gesetzliche Regelung für die Sicherheit in der Informationstechnologie eher ein Hindernis.

1. Europäische Grundlagen

Der Auslöser für die Aktivitäten des Gesetzgebers befindet sich auf europäischer Ebene. Der Europarat hat ein Übereinkommen über die Computerkriminalität am 23.11.2001 erzielt, das u.a. einen Mindeststandard bei den Strafvorschriften über be-

Ihre Ansprechpartner für rechtliche Beratungen:
Feil Rechtsanwälte, Georgsplatz 9, 30159 Hannover, Telefon: 0511 / 473906-01, eMail: feil@recht-freundlich.de

stimmte schwere Formen der Computerkriminalität fordert. Weiterhin verpflichtet der Rahmenbeschluss 2005/222/JI des Rates vom 24.02.2005 über Angriffe auf Informationssysteme die Mitgliedsstaaten. Danach sollen schwere Formen dieser Kriminalität unter Strafe gestellt werden.

Im Übereinkommen über Computerkriminalität vom 23.11.2001 verlangt Artikel 6 die Strafbarkeit von bestimmten Vorbereitungshandlungen für Computerstraftaten. Unter der Überschrift „Missbrauch von Vorrichtungen“ wird Folgendes vereinbart (bereinigte Übersetzung zwischen Deutschland, Österreich und Schweiz abgestimmte Fassung):

„1 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um folgende Handlungen, wenn vorsätzlich und unbefugt begangen, nach ihrem innerstaatlichen Recht als Straftaten zu umschreiben:

a Das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen

i einer Vorrichtung einschließlich eines Computerprogramms, die in erster Linie dafür ausgelegt oder hergerichtet worden ist, eine nach den Artikeln 2 bis 5 umschriebene Straftat zu begehen;

ii eines Computerpasswords, eines Zugangscodes oder ähnlicher Daten, den Zugang zu einem Computersystem als Ganzem oder zu einem Teil davon ermöglichen,

mit dem Vorsatz, sie zur Begehung einer nach den Artikel 2 bis 5 umschriebenen Straftat zu verwenden, und

b den Besitz eines unter Buchstabe a Ziffern i oder ii bezeichneten Mittels mit dem Vorsatz, es zur Begehung einer nach den Artikel 2 bis 5 umschriebenen Straftat zu verwenden. Eine Vertragspartei kann als gesetzliche Voraussetzung vorsehen, dass die strafrechtliche Verantwortlichkeit erst mit Besitz einer bestimmten Anzahl dieser Mittel eintritt.

2 Dieser Artikel darf nicht so ausgelegt werden, als begründe er die strafrechtliche Verantwortlichkeit in Fällen, in denen das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen oder wenn Besitz nach Absatz 1 nicht zum Zweck der Begehung einer nach den Artikeln 2 bis 5 umschriebenen Straftat, son-

Ihre Ansprechpartner für rechtliche Beratungen:
Feil Rechtsanwälte, Georgsplatz 9, 30159 Hannover, Telefon: 0511 / 473906-01, eMail: feil@recht-freundlich.de

dern beispielsweise zum genehmigten Testen oder zum Schutz eines Computersystems erfolgt.

3 Jede Vertragspartei kann sich das Recht vorbehalten, Absatz 1 nicht anzuwenden, sofern der Vorbehalt nicht das Verkaufen, Verbreiten oder anderweitige Verfügbarmachen der in Absatz 1 Buchstabe a Ziffer ii bezeichneten Mittel betrifft."

Bemerkenswert ist, dass zum einen auf den Vorsatz abgestellt wird, eine entsprechende Straftat zu begehen. Weiterhin wird bei einem Computerprogramm, das strafrechtliche Relevanz haben soll, verlangt, dass dies in erster Linie dafür ausgelegt ist, rechtswidrig eingesetzt zu werden.

Der Rahmenbeschluss vom 24.02.2005 fordert in Artikel 2, dass ein rechtswidriger Zugang zu Informationssystemen unter Strafe gestellt wird. Gleiches gilt für den rechtswidrigen Systemeingriff und den rechtswidrigen Eingriff in Daten. Artikel 5 fordert in Absatz 1, dass jeder Mitgliedsstaat sicherstellt, dass die Anstiftung oder Beihilfe zur Begehung dieser oben genannten Straftaten unter Strafe gestellt ist. Dabei wird gem. Artikel 6 erwartet, dass eine wirksame, verhältnismäßige und abschreckende strafrechtlich Sanktion festgelegt ist.

2. Deutsches Gesetzgebungsverfahren

Auf Basis eines Gesetzesentwurfes der Bundesregierung vom 22.09.2006 wurde das Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität auf den Weg gebracht. Mit diesem Gesetzesvorschlag sollten die Vorgaben des europäischen Rechts zur Computerkriminalität in nationales Recht umgesetzt werden. Änderungen und Ergänzungen des Strafgesetzbuches sowie eine Änderung des § 130 des Gesetzes über Ordnungswidrigkeiten waren dazu notwendig.

Bereits der mit Drucksache 16/3656 des Deutschen Bundestages veröffentlichte Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität enthält den später in Kraft gesetzten § 202 c StGB im Wortlaut. Unter der Überschrift „Vorbereiten des Ausspähens und Abfangens von Daten" wurde seitens der Bundesregierung folgender Textvorschlag an den Deutschen Bundestag übermittelt:

Ihre Ansprechpartner für rechtliche Beratungen:
Feil Rechtsanwälte, Georgsplatz 9, 30159 Hannover, Telefon: 0511 / 473906-01, eMail: feil@recht-freundlich.de

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

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202 a 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."

Nach Auffassung des Gesetzgebers, die er in der Gesetzesbegründung wiedergibt, entspricht das deutsche Strafrecht den Vorgaben zum materiellen Strafrecht des Europarat-Übereinkommens und den Vorgaben des EU-Rahmenbeschlusses bereits weitgehend. Daher sollte es nur zu Änderungen in Teilbereichen kommen.

Zu § 202 c StGB führt der Gesetzgeber u.a. wie folgt aus:

> „Erfasst werden insbesondere die so genannten Hacker-Tools, die bereits nach der Art und Weise ihres Aufbaus darauf angelegt sind, illegalen Zwecken zu dienen, und die aus dem Internet weitgehend anonym geladen werden können. Insbesondere die durch das Internet mögliche Weiterverbreitung und leichte Verfügbarkeit der Hacker-Tools sowie ihre einfache Anwendung stellen eine erhebliche Gefahr dar, die nur dadurch effektiv bekämpft werden kann, dass bereits die Verbreitung solcher an sich gefährlichen Mittel unter Strafe gestellt wird."

Der Gesetzgeber sieht allerdings auch das Risiko einer Überkriminalisierung. Er verweist dabei auf den objektiven Tatbestand, der auf die Bestimmung des Computerprogramms als Mittel zur Begehung einer Straftat zum Abfangen und Ausspähen von Daten abstellt. Dabei kommt es nach Auffassung des Gesetzgebers auf die objektivierte Selbstbestimmung des Programms an. Wörtlich wird in der Gesetzesbegründung wie folgt ausgeführt:

> „Somit ist sichergestellt, dass nur Hacker-Tools erfasst werden und die allgemeinen Programmier-Tools, -Sprachen oder sonstigen Anwendungsprogramme bereits nicht unter den objektiven Tatbestand der Strafvorschrift

Ihre Ansprechpartner für rechtliche Beratungen:
Feil Rechtsanwälte, Georgsplatz 9, 30159 Hannover, Telefon: 0511 / 473906-01, eMail: feil@recht-freundlich.de

> fallen. 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."

Um dies an dieser Stelle noch einmal zu wiederholen, für den Gesetzgeber reicht nach den Ausführungen in der Drucksache 16/3656 vom 30.11.2006, dass das Tool auch die Begehung einer Straftat (Ausspähen oder Abfangen von Daten) als Zweck verfolgt. Zur Problematik der so genannten dual-use-Programme wird später noch Stellung zu nehmen sein. Offensichtlich ist der Gesetzgeber zu diesem Zeitpunkt aber noch davon ausgegangen, dass solche dual-use-Pogramme ebenfalls strafrechtlich zu belangen sind.

Im Rechtsausschuss kam es dann zu einer sehr ausführlichen rechtlichen Diskussion, auf die dann in der Drucksache 16/5449, der Beschlussempfehlung und dem Bericht des Rechtsausschusses vom 23.05.2007, Bezug genommen wird. Nach Auffassung des Rechtsausschusses kriminalisiere der Gesetzentwurf nicht den branchenüblichen Einsatz von Hacker-Tools durch Netzwerkadministratoren, insbesondere wenn diese nur die Sicherheit des eigenen Datennetzes prüfen wollten. Der Rechtsausschuss stellt klar, dass § 202 c StGB hinsichtlich der Zweckbestimmung im Sinne des Artikels 6 des Europarats-Übereinkommens auszulegen ist. Dabei sollen nur Computerprogramme von der Strafvorschrift betroffen sein, die in erster Linie dafür ausgelegt oder hergestellt würden, um damit Straftaten nach den §§ 202 a, 202 b StGB zu begehen. Die bloße Geeignetheit zur Begehung solche Straftaten begründet keine Strafbarkeit, wie der Rechtsausschuss ausführt. Weiter heißt es:

> „Die Strafvorschrift habe in erster Linie professionelle Anbieter im Blick, die durch die Bereitstellung von Computerprogrammen, die für die Begehung von Straftaten geschrieben würden, ein vom Gesetzgeber als unerwünscht und strafbar angesehenes Verhalten unterstützen und damit Gewinn erzielten."

So sicher ist sich der Gesetzgeber allerdings in Gestalt seines Rechtsausschusses nicht. Es wird im Weiteren nämlich darauf hingewiesen, dass die Auswirkungen der neuen Strafvorschriften genau zu beobachten sind. Sollten Programmentwickler und Firmen, die nicht aus krimineller Energie heraus handelten, in Ermittlungsverfahren

Ihre Ansprechpartner für rechtliche Beratungen:
Feil Rechtsanwälte, Georgsplatz 9, 30159 Hannover, Telefon: 0511 / 473906-01, eMail: feil@recht-freundlich.de

durch die neuen Strafvorschriften einbezogen werden, soll nach Auffassung des Rechtsausschusses zeitnah reagiert werden.

3. Neues Gesetz und Kritik

Der neue § 202 c StGB, der das Vorbereiten des Ausspähens und Abfangens von Daten unter Strafe stellt, ist ab dem 11.08.2007 gültig und in Kraft. Bei der rechtlichen Bewertung und bei der Frage der Anwendung dieser gesetzlichen Neuregelungen auf Hacker-Tools wird eine große Bandbreite von Rechtsauffassungen vertreten. Die Stellungnahmen reichen von „man muss sich keine Sorge machen“ bis hin zu dramatischen Schilderungen drohender Gefahren für die IT-Sicherheit. Die eingangs geschilderte Strafanzeige gegen das Bundesamt für Sicherheit in der Informationstechnologie macht aber deutlich, dass die rechtlichen Bewertungen noch nicht abschließend geklärt sind.

In der Diskussion wird immer wieder zu Recht darauf verwiesen, dass Systemadministratoren und IT-Dienstleister häufig damit beauftragt werden, Angriffe auf Systeme zu simulieren, um Schwachstellen zu überprüfen. Dies soll nach Auffassung der Bundesregierung auch so bleiben. In der Gegenäußerung der Bundesregierung (Drucksache 16/3656 Anlage 3) nimmt die Bundesregierung zu der geäußerten Kritik Stellung und verweist darauf, dass die verschiedenen Gesichtspunkte bereits beim Regierungsentwurf einer eingehenden Überprüfung unterzogen worden sind. Weiter führt die Bundesregierung aus:

> „Die Befürchtung, dass auch der gutwillige Umgang mit Softwareprogrammen zur Sicherheitsüberprüfung von IT-Systemen von § 202 c StGB-E erfasst werden könnte, ist nicht begründet. Die Nichterfassung des gutwilligen Umgangs mit Softwareprogrammen zur Sicherheitsüberprüfung von IT-Systemen wird bereits auf Tatbestandsebene durch zwei gesetzliche Tatbestandsmerkmale abgesichert. Einerseits muss es sich objektiv um ein Computerprogramm handeln, dessen Zweck die Begehung einer Computerstraftat ist, und andererseits muss die Tathandlung – also das Herstellen, Verschaffen, Verkaufen, Überlassen, Verbreiten oder sonst Zugänglichmachen – zur Vorbereitung einer Computerstraftat erfolgen.“

Ihre Ansprechpartner für rechtliche Beratungen:
Feil Rechtsanwälte, Georgsplatz 9, 30159 Hannover, Telefon: 0511 / 473906-01, eMail: feil@recht-freundlich.de

Weiter führt die Bundesregierung aus, dass durch die objektive Beschränkung keine Computerprogramme strafrechtlich erfasst werden, die beispielsweise der Überprüfung, der Sicherheit oder Forschung in diesem Bereich dienen. Bei Programmen, deren funktionaler Zweck nicht eindeutig ein krimineller ist (dual-use-Programme), ist der objektive Tatbestand nicht erfüllt. Die bloße Eignung von Software zur Begehung von Computerstraftaten ist nicht ausreichend. Solche Programme fallen nach Auffassung der Bundesregierung aus dem Tatbestand heraus, die lediglich zur Begehung von Computerstraftaten missbraucht werden können.

Weiterhin wird darauf verwiesen, dass die Tathandlung zur Vorbereitung einer Computerstraftat erfolgen muss. Der Täter muss beispielsweise das Abfangen oder Ausspähen von Daten in Aussicht genommen haben. Das ist beispielsweise bei einer Sicherheitsüberprüfung, bei der Entwicklung von Sicherheitssoftware oder zu Ausbildungszwecken im Bereich der IT-Sicherheitsbranche nicht der Fall. Dies geht nach der in der Drucksache 16/3656 wiedergegebenen Auffassung der Bundesregierung sogar so weit, dass bei ursprünglich kriminellen Zwecken dienenden Computerprogrammen, wenn diese ausschließlich zu nicht kriminellen Zwecken eingesetzt werden, keine Anhaltspunkte für eine eigene oder fremde Computerstraftat bestehen. Es wird dann keine Computerstraftat in Aussicht genommen. Wer also beispielsweise für das Entwickeln von Sicherheitssoftware sich Schadprogramme verschafft, der handelt nicht zur Vorbereitung einer Computerstraftat.

Ein Teil der juristischen Literatur folgt zwar dem Bewertungsergebnis der Bundesregierung, setzt aber auf eine andere Argumentation. In der Kritik an der Argumentation der Bundesregierung wird darauf verwiesen, dass bei realitätsnahen Tests Angriffe simuliert werden und dabei Programme verwendet werden, die auch bei wirklichen Angriffen eingesetzt werden. Diese Programme dienen regelmäßig auch dem objektiven Zweck der Begehung von Straftaten. Insoweit wird dann der objektive Tatbestand nicht ausgeschlossen. In der weitergehenden rechtlichen Argumentation wird aber darauf verwiesen, dass die Vorbereitung einer Computerstraftat nach § 202 a StGB und § 202 b StGB erfolgen muss. Wenn ein Einverständnis eines Berechtigten vorliegt, sind entsprechende Sicherheitstests, die auch das Ausspähen oder Abfangen von Daten zum Inhalt haben, nicht mehr unbefugt.

Ihre Ansprechpartner für rechtliche Beratungen:
Feil Rechtsanwälte, Georgsplatz 9, 30159 Hannover, Telefon: 0511 / 473906-01, eMail: feil@recht-freundlich.de

Zum Teil wird auch die Argumentation vertreten, dass die Gerichte bei der strafrechtlichen Bewertung auch die Gesetzesbegründung und beispielsweise die oben zitierten Äußerungen der Bundesregierung mit berücksichtigen. Weiterhin wird auf die einschränkenden Formulierungen der europäischen Vorgaben hingewiesen, die ebenfalls als Auslegungshilfe bei der rechtlichen Betrachtung mit hinzuzuziehen sind. An dieser Stelle soll zunächst das Grundgesetz zu Wort kommen. Gemäß Art. 103 Abs. 2 GG ist der Gesetzgeber verpflichtet, die Voraussetzungen der Strafbarkeit so genau zu umschreiben, dass Tragweite und Anwendungsbereich der Straftatbestände schon aus dem Gesetz selbst zu erkennen sind und sich durch Auslegungen ermitteln und konkretisieren lassen. Dies ist der Maßstab, an der sich der Gesetzgeber auch hinsichtlich des Hacker-Paragraphen messen lassen muss. In Anbetracht der umfangreichen Diskussion ist bereits ohne weitergehende Betrachtung der juristischen Auseinandersetzung festzustellen, dass die Anforderungen nicht erfüllt sind. Offensichtlich ist aus dem Gesetz heraus selbst nicht zu erkennen, für welche Tragweite und Anwendungsbereich der Straftatbestand gelten soll.

Es ist davon auszugehen, dass es sich bei dem neuen § 202 c StGB um ein so genanntes abstraktes Gefährdungsdelikt handelt. Ähnliche Formulierungen finden sich beispielsweise in § 149 Abs. 1 StGB, der sich mit dem Thema Geldfälschung beschäftigt. Da der Gesetzgeber eine generelle Kriminalisierung von Hacker-Tools anstrebt, ist ein solches abstraktes Gefährdungsdelikt anzunehmen. Die österreichische Norm, die den gleichen Tatbestand regeln will, verweist beispielsweise nicht auf Vorbereitungshandlungen. In § 126 c österreichisches StGB wird auf das Wissen oder die Absicht, eine Computerstraftat zu begehen, abgestellt. Bei abstrakten Gefährdungsdelikten ist nicht ein wie auch immer gearteter Erfolg notwendig. Der Tatbestand verlangt nicht den Eintritt einer Gefahr, sondern beschreibt ein bloßes Tun, das deshalb bestraft wird, weil es leicht eine konkrete Gefahr auslösen kann. Der Bundesgerichtshof verweist darauf, dass die Gefährlichkeit also nicht Merkmal des Tatbestandes, sondern ein gesetzgeberischer Grund der Strafandrohung ist. Bei der Vorbereitung der Fälschung von Geld- und Wertzeichen in § 149 StGB, der ähnlich formuliert ist, werden die Vorbereitungshandlungen zur Fälschung selbständig unter Strafe gestellt. Unerheblich ist dabei, ob die Tat zur Förderung objektiv geeignet ist. Weiterhin ist unerheblich, ob die vorbereitete Tat später ausgeführt wird.

Ihre Ansprechpartner für rechtliche Beratungen:
Feil Rechtsanwälte, Georgsplatz 9, 30159 Hannover, Telefon: 0511 / 473906-01, eMail: feil@recht-freundlich.de

Auf der Ebene des Vorsatzes genügt ein so genannter „bedingter Vorsatz“. Dieser muss auch die Tathandlung als „Vorbereitung“ erfassen. Ein Täter muss zumindest billigend in Kauf nehmen, durch die Handlung eine Computerstraftat zu ermöglichen oder zu fördern. Umstritten ist, ob eine Konkretisierung dieser Tat zum Zeitpunkt der Handlung erforderlich ist.

Weitere Kritik wird dahin geübt, dass die Frage der Zweckbestimmung nicht klar geregelt ist. Nach Auffassung der Kritiker soll die bloße Eignung eines Programms für Computerstraftaten nicht ausreichen. Es muss der primäre, vorwiegende Zweck darin bestehen, entsprechende Straftaten begehen zu können. Dabei ist zu bedenken, dass Zwecke vom jeweiligen Verwender subjektiv bestimmt werden. Schwerpunktmäßig wird daher auf die Gestaltung des Designs des Programms abzustellen und dabei zu klären sein, ob das Programm hauptsächlich nur kriminellen Zwecken dienen soll. So wurde auch der § 126 c österreichisches StGB verfasst. Programme mit einem unspezifischen Anwendungsprofil sollen aus dem strafrechtlichen Anwendungsbereich herausgenommen werden. Auch der Verweis auf die Vorbereitung einer Computerstraftat wird als ungenau angesehen. Entsprechende rechtliche Diskussionen haben sich bereits bei anderen Straftatbeständen entfacht, da ein so genannter dolus eventualis für die Verwirklichung des subjektiven Tatbestandes ausreicht. Wer also eine illegale Verwendung für möglich hält, was beispielsweise bei der Verwendung dazu geeigneter Software bei einer ansonsten legalen Nutzung nicht auszuschließen ist, verwirklicht bereits den Straftatbestand. Die EU-rechtlichen Vorgaben verlangen dagegen ein wissentliches oder absichtliches Handeln.

Diese oben geschilderten Kritikpunkte wurden u.a. in der Sachverständigenanhörung des Rechtsausschusses in vielen Details vertieft.

Dennoch sah sich der Gesetzgeber nicht genötigt, mit wenigen Worten die nunmehr in Kraft gesetzte Strafrechtsvorschrift zu präzisieren und die Zweifelsfragen zu klären. Hier stellt sich die Frage, ob der Gesetzgeber vor dem Hintergrund der umfangreichen Diskussion und Kritik nicht ganz bewusst eine weite Anwendung des Gesetzes will. Wenn leicht mögliche Änderungen bewusst verweigert werden, kann im Gegenzug durchaus argumentiert werden, dass der Gesetzgeber entsprechende Auslegungs- und Anwendungsvarianten will oder – um mit den obigen Formulierungen zu sprechen -

Ihre Ansprechpartner für rechtliche Beratungen:
Feil Rechtsanwälte, Georgsplatz 9, 30159 Hannover, Telefon: 0511 / 473906-01, eMail: feil@recht-freundlich.de

zumindest billigend in Kauf nimmt. Böse Zungen behaupten in diesem Zusammenhang, dass vor dem Hintergrund des Bundestrojaners entsprechende gesetzliche Regelungen dem Interesse der Ermittlungsbehörden durchaus entgegenkommen. Bei strenger Anwendung des § 202 c StGB ist die Entwicklung und Anwendung einer Software, die vor dem Bundestrojaner warnt oder entsprechende Bundestrojaner auf den Rechnern entdeckt, auf jeden Fall ausgeschlossen.

4. Typische Situation in neuer rechtlicher Bewertung

Der neue § 202 c StGB führt für manche Situationen, die im Umfeld der IT-Sicherheitsfirmen Normalität sind, zu einer neuen rechtlichen Bewertung. Systemhäuser und IT-Dienstleister zeigen bei Kundenveranstaltungen immer wieder in Live-Demonstrationen, wie leicht es Hacker haben, auf fremde Rechner zuzugreifen. Dabei werden zumeist „echte“ Hacker-Tools eingesetzt. Hier stellt sich die Frage, ob die gesetzliche Neuregelung zu einem strafrechtlich relevanten Verhalten des „Hackers“, der die Live-Demonstration durchführt, führt. Auch die Frage, ob der Ausrichter der jeweiligen Kundenveranstaltung ebenfalls strafrechtlich belangt werden kann, soll kurz beleuchtet werden. Nach § 202 c StGB sind Vorbereitungshandlungen des Ausspähens und Abfangens von Daten strafbar. Dabei genügt bereits, dass jemand sich ein Computerprogramm, dessen Zweck die Begehung einer Computerstraftat ist, verschafft. Damit ist auch der bloße Besitz von Hacker-Tools strafbar, da diesem Besitz immer ein Sich-Verschaffen vorausgeht. Wenn also auf dem Notebook des „Hackers“ sich derartige Tools befinden, ist bereits eine Strafbarkeit gegeben. Der nahe liegende Hinweis, dass mit den Hacker-Tools doch kein unbefugtes Ausspähen oder Abfangen von Daten durchgeführt werden soll, ist für die rechtliche Bewertung ohne Belang. Bei dem Hacker-Tool handelt es sich um ein Computerprogramm, dessen Zweck die Begehung einer Computerstraftat ist, zumindest ist eine der vielleicht verschiedenen Zweckausrichtungen die Begehung einer Computerstraftat. Der „Hacker“ hat sich das entsprechende Programm verschafft und nimmt billigend in Kauf, dass mit dem Tool eine Computerstraftat vorbereitet wird. Hier zeigt sich, dass der weit gefasste Vorsatz, der bereits ein Billigend-in-Kauf-Nehmen unter Strafe stellt, in der Praxis jede Möglichkeit verhindert, entsprechende Hacker-Tools positiv einzusetzen. Zu einer ähnlichen Bewertung kommt man auch bei den dual-use-Programmen, die sowohl als Hacker-Tool missbraucht werden können, zum anderen aber auch für die Überprüfung von Sicherheits-

Ihre Ansprechpartner für rechtliche Beratungen:
Feil Rechtsanwälte, Georgsplatz 9, 30159 Hannover, Telefon: 0511 / 473906-01, eMail: feil@recht-freundlich.de

lücken genutzt werden. Auch hier handelt es sich um ein Computerprogramm, dessen Zweck – wenn auch nur als Teilzweck – die Begehung einer Computerstraftat ist. Auch hier wird wieder billigend in Kauf genommen, dass möglicherweise entsprechende Straftaten mit dem Programm begangen werden.

Vor dem Hintergrund der obigen Ausführungen kann im Moment nur davon abgeraten werden, entsprechende Live-Demonstrationen durchzuführen. Zurzeit ist eine solche Live-Demonstration ein Verstoß gegen § 202 c StGB.

Auch im Alltag der EDV-Administratoren gibt es immer wieder Situationen, die unter dem neuen § 202 c StGB bewertet werden müssen. Insbesondere der Einsatz von dual-use-Programmen bereitet bei der rechtlichen Beurteilung Schwierigkeiten. Wenn beispielsweise ein Administrator in regelmäßigen Abständen die Sicherheit der Passworte durch ein Programm prüfen lässt, das alle möglichen Passworte testet und dann möglicherweise auf das Passwort eines Nutzers stößt, hat dies sicherlich im Rahmen der IT-Sicherheitsmaßnahmen seinen Sinn. Allerdings kann ein böswilliger Nutzer das gleiche Programm auch dazu nutzen, sich unberechtigt Zugang zu Daten und IT-Systemen zu verschaffen. Die Bundesregierung hat, wie oben skizziert, die Auffassung vertreten, dass solche dual-use-Programme nicht unter den objektiven Tatbestand fallen. Dies ist aber dem Gesetzeswortlaut so nicht zu entnehmen. Der Gesetzeswortlaut spricht nur von einem Zweck und nicht von einem überwiegend oder ausschließlichen illegalen Zweck. Die Gesetzesbegründung ist diesbezüglich ebenfalls nicht eindeutig positioniert. Zu § 202 c StGB wird in der Drucksache 16/3656 wie folgt ausgeführt:

> „Es reicht, wenn die objektive Zweckbestimmung des Tools auch die Begehung einer solchen Straftat ist."

Der Gesetzgeber stellt klar, dass nicht ausschließlich eine entsprechende Bestimmung vorliegen muss. Dies wird in der Gegenäußerung der Bundesregierung, die ebenfalls oben zitiert wurde, wieder relativiert. Aufgrund der widersprüchlichen Gesetzesbegründungen kann aber nicht von einer eindeutigen Positionierung des Gesetzgebers bei der Nutzung von dual-use-Programmen durch IT-Administratoren gesprochen werden. Es bleibt ein Strafbarkeitsrisiko.

Ihre Ansprechpartner für rechtliche Beratungen:
Feil Rechtsanwälte, Georgsplatz 9, 30159 Hannover, Telefon: 0511 / 473906-01, eMail: feil@recht-freundlich.de

In IT-Sicherheitskreisen ist es selbstverständlich, Schadsoftware, Viren und andere Software zu untersuchen, um entsprechende Abwehrstrategien entwickeln zu können. Dies geschieht in der Regel in offenen oder halb offenen Foren. Dies ist für die Weiterentwicklung der IT-Sicherheit als Methode unabdingbar. Wenn dieses Verhalten allerdings aus dem Blickwinkel des neuen § 202 c StGB betrachtet wird, so ist der objektive Tatbestand erfüllt. Es liegt ein Sich-Verschaffen oder auch eine Verbreitungshandlung vor. Die weitergehende Strafbarkeit hängt dann vom Vorliegen des Vorsatzes ab. Zwar wird bei solchen Foren angestrebt, Abwehrstrategien zu entwickeln, da solche Foren aber jedermann Zutritt gewähren, können Schadprogramme auch zu illegalen Zwecken heruntergeladen und eingesetzt werden. Dies wird auch von den Beteiligten billigend in Kauf genommen. Ohne dieses Risiko, das nicht völlig beseitigt werden kann, ist der derzeitige Standard der IT-Sicherheit nicht zu halten. Um es deutlich zu sagen: Bei dieser Art von Diskussionen oder auch bei einer entsprechenden Beteiligung an solchen Diskussionen liegt wegen des billigenden In-Kauf-Nehmens eine Straftat vor. Zum Teil wird in der juristischen Literatur und wurde auch im Gesetzgebungsverfahren die Hoffnung geäußert, dass die Rechtsprechung Wege finden wird, die Strafbarkeit zu verneinen. Ob sich diese Hoffnung erfüllen wird, bleibt aber abzuwarten.

Einig sind sich allerdings der Gesetzgeber und auch alle, die die entsprechende gesetzliche Regelung beurteilen. So weit sollte das Gesetz nicht gefasst sein und die beiden soeben geschilderten Situationen der IT-Administratoren und Maßnahmen zur Entwicklung von Abwehrstrategien gegen Schadprogramme sollten eigentlich straffrei bleiben. Hier muss sich der Gesetzgeber deutlich fragen lassen, warum er trotz verschiedener Warnungen und Hinweise von Sachverständigen die kleinen angeregten sprachlichen Korrekturen und Präzisierungen des Gesetzestextes nicht vorgenommen hat. Nur ein SPD-Abgeordneter und die Fraktion Die Linke stimmten gegen das Gesetz. Wenn das Parlament sich so über die Bedenken von Experten hinwegsetzt und es bei einer unklaren Gesetzeslage belässt, ist fast davon auszugehen, dass eine entsprechend scharfe Anwendung der gesetzlichen Regelungen gewünscht ist. Der oben skizzierte Verweis auf die österreichischen strafrechtlichen Regelungen macht aber deutlich, dass dies nicht gezwungenermaßen und schon gar nicht aufgrund der EU-Vorgaben unweigerlich der Fall sein musste.

Ihre Ansprechpartner für rechtliche Beratungen:
Feil Rechtsanwälte, Georgsplatz 9, 30159 Hannover, Telefon: 0511 / 473906-01, eMail: feil@recht-freundlich.de

Ein weiterer Aspekt ist bei allen GmbHs und AGs zu bedenken. Wenn sich die weite Auslegung, die sich am Wortlaut des Gesetzes orientiert, durchsetzen sollte, ist damit zu rechnen, dass der bisherige Sicherheitsstandard oder die IT-Infrastruktur absacken wird. Dann ist allerdings im Rahmen des Risikomanagements eine Neubewertung der Risiken in Zusammenhang mit der EDV vorzunehmen. Diesbezüglich sollte jeder Vorstand oder Geschäftsführer zur Vermeidung einer persönlichen Haftung die weitere Entwicklung verfolgen und entsprechende Maßnahmen im Rahmen des Risikomanagements vornehmen.

5. Wege aus dem Dilemma

Die Varianten für Lösungswege sind, wenn man den Kopf nicht in den Sand stecken will, begrenzt. Bei einigen Unternehmen, auch größeren Unternehmen, drängt sich der Eindruck auf, dass durch bloße Nichtbeachtung der gesetzlichen Regelungen oder einer gewissen Ignoranz das Bedrohungsszenario sich nicht verwirklicht. Anhand eines Beispiels, das ein Sachverständiger im Rahmen der Anhörung zum Gesetzgebungsvorhaben brachte, wird allerdings schnell deutlich, wie trügerisch diese Hoffnung ist. Ein Sachverständiger verwies beispielsweise darauf, dass konkurrierende Unternehmen, die in einem harten Wettbewerb stehen, durchaus nach Erteilung eines Auftrages an den Konkurrenten, bei einem Unternehmen umfangreiche Prüfungen der IT-Sicherheit vorzunehmen, dem Gedanken an eine Strafanzeige näher treten könnte. So ließe sich ein entsprechender Mitbewerber durchaus PR-wirksam schädigen. Da die Prüfung der IT-Infrastruktur durch externe IT-Dienstleister insbesondere eine gute Vertrauensbasis erfordert, wären solche Maßnahmen, wie eine Strafanzeige gegen den Mitbewerber, in erheblichem Maße geschäftsschädigend. Im zunehmend harten Wettbewerb erscheint es nicht ausgeschlossen, dass solche Maßnahmen ergriffen werden. Die Strafanzeige gegen das Bundesamt für Sicherheit in der Informationstechnologie zeigt, dass von den strafrechtlichen Möglichkeiten durchaus Gebrauch gemacht wird. Die Variante, zunächst nur abzuwarten, erscheint daher nicht die richtige Lösungsstrategie zu sein.

Zum Teil wird insbesondere bei größeren Unternehmen diskutiert, durch anerkannte Strafrechtler eine Begutachtung der Rechtslage vornehmen zu lassen. Solche Gutachtenaufträge sind von der Hoffnung getragen, dass Strafrechtler dann auf die Gesetzes-

Ihre Ansprechpartner für rechtliche Beratungen:
Feil Rechtsanwälte, Georgsplatz 9, 30159 Hannover, Telefon: 0511 / 473906-01, eMail: feil@recht-freundlich.de

begründung verweisen und argumentieren werden, dass entsprechende strafrechtliche Bedrohungen nicht bestehen. Wenn dann dennoch eine Strafverfolgung stattfindet, könnte auf Ebene der Schuldfrage zweifelhaft sein, ob solche Unternehmen strafrechtlich verfolgt werden können. Auch dies ist ein eher defensiver Umgang mit diesem brisanten Thema. Die tägliche Lektüre der einschlägigen Fachpresse zeigt, dass Maßnahmen zur IT-Sicherheit dringend erforderlich sind und daher das Prinzip Hoffnung, das letzten Endes Basis auch für die Erstellung der Gutachten ist, nicht ausreichend ist.

Der Rechtsausschuss hatte in seiner 64. Sitzung am 23. Mai 2007 den Gesetzesentwurf beraten und bezüglich des § 202 c StGB angemerkt, dass der Gesetzgeber die Auswirkung der neuen Strafvorschriften genau zu beobachten hat. Wenn Programmentwickler und Firmen, die ohne kriminelle Energie im Markt für IT-Sicherheit agieren, in Ermittlungsverfahren einbezogen werden, muss nach Auffassung des Rechtsausschusses auf solche Entwicklungen zeitnah reagiert werden. Die Strafanzeige gegen das Bundesamt für Sicherheit in der Informationstechnologie ist sicherlich ein erstes Signal in diese Richtung. Hier sollte der Gesetzgeber mit seinen Äußerungen ernst genommen werden. Auch die bereits zum Teil erfolgten Selbstanzeigen sind ein guter Weg, Klarheit in Hinsicht der strafrechtlichen Bewertung bestimmter Handlungen zu erlangen. Allerdings ist wohl nicht zu erwarten, dass der Einsatz von Hacker-Tools zur Entwicklung von Abwehrstrategien bzw. die Beteiligung an entsprechenden Diskussionen straffrei bleiben wird. Allerdings hat sich aber in der Vergangenheit gezeigt, dass bestimmte rechtliche Entwicklungen durchaus überraschende Wendungen nehmen können. Daher bleibt zunächst nur abzuwarten, wie die Strafverfolgungsbehörden auf entsprechende Anzeigen reagieren. Es ist allerdings den Beteiligten anzuraten, bei einer Zurückweisung der Strafanzeige, aus welchen rechtlichen Gründen auch immer, die weitergehenden Rechtsmittel auszuschöpfen, um die Strafverfolgungsbehörden in die Ermittlungen und Verfolgung entsprechender Straftaten hineinzuzwingen. So wird die Branche Sicherheit im Umgang mit den neuen Gesetzen erlangen.

Ein weiterer rechtlicher Ansatzpunkt, der bisher noch nicht intensiv verfolgt wurde, ist unter dem Stichwort „Verfassungsbeschwerde“ zusammenzufassen. Die strafrechtlichen Regelungen führen faktisch für viele Unternehmen, die sich mit dem Thema IT-

Ihre Ansprechpartner für rechtliche Beratungen:
Feil Rechtsanwälte, Georgsplatz 9, 30159 Hannover, Telefon: 0511 / 473906-01, eMail: feil@recht-freundlich.de

Sicherheit beschäftigen, zu erheblichen Einschränkungen ihrer beruflichen Tätigkeit. Artikel 12 GG formuliert die Berufsfreiheit wie folgt:

> „Alle Deutschen haben das Recht, Beruf, Arbeitsplatz und Ausbildungsstätte frei zu wählen. Die Berufsausübung kann durch Gesetz oder aufgrund eines Gesetzes geregelt werden."

Die Strafbarkeit von dual-use-Programmen führt faktisch dazu, dass bestimmte Tätigkeiten im Umfeld der IT-Sicherheitsmaßnahmen nicht mehr möglich sind. Hierin liegt ein weiterer Weg, mit Hilfe der grundrechtlichen Vorschriften Einfluss auf die Strafgesetzgebung zu nehmen. Sicherlich ist auch dieser Weg steil und dornig. In Anbetracht der wenigen Lösungsstrategien sollte allerdings jegliche Möglichkeit genutzt werden, die gesetzliche Regelung in § 202 c StGB in ihrem Anwendungsbereich einzuschränken. Anderenfalls besteht doch die erhebliche Bedenken, dass die von vielen befürchteten Schreckensszenarien doch Wirklichkeit werden.

Der Zulässigkeit der Verfassungsbeschwerde könnte der Grundsatz der sog. Subsidiarität entgegenstehen. Danach ist zunächst der Rechtsweg vor den ordentlichen Gerichten auszuschöpfen. Der Grundsatz der Subsidiarität verlangt nach der Rechtsprechung des Bundesverfassungsgerichts allerdings nicht, dass ein Betroffener vor der Erhebung der Verfassungsbeschwerde gegen eine straf- oder bußgeldbewehrte Rechtsnorm zunächst eine Zuwiderhandlung begeht und dann im Straf- oder Bußgeldverfahren die Verfassungswidrigkeit der Norm geltend macht (Beschluss vom 14. November 1989, 1 BvL 14/85).

6. Zusammenfassung

Die Nutzung, das Beschaffen oder das sonst Zugänglichmachen von Schadprogrammen und Hacker-Tools muss unterbleiben. Die Beteiligung an Internetdiskussionen über Abwehrstrategien ist unter den neuen strafrechtlichen Gesichtspunkten durchaus kritisch.

Beim Einsatz von dual-use-Programmen, die sowohl zur Überprüfung der IT-Sicherheit als auch zum Missbrauch und dem Begehen von Computerstraftaten genutzt werden

Ihre Ansprechpartner für rechtliche Beratungen:
Feil Rechtsanwälte, Georgsplatz 9, 30159 Hannover, Telefon: 0511 / 473906-01, eMail: feil@recht-freundlich.de

können, besteht zurzeit insbesondere die Hoffnung, dass die Strafverfolgungsbehörden nicht umfassend tätig werden. Ob sich diese Hoffnung bestätigt, muss der weiteren rechtlichen Diskussion überlassen werden. Auch werden die bereits eingeleiteten Ermittlungsverfahren zeigen, wie ernst die Strafverfolgungsbehörden die gesetzlichen Strafvorschriften nehmen.

Jeder Weg, der den Parlamentariern auch vor dem Hintergrund der aktuellen innenpolitischen Diskussionen (Stichwort: Bundestrojaner und Online-Durchsuchungen) die Brisanz der Neuregelung in § 202 c StGB deutlich macht, ist recht. Hier ist vielleicht noch mehr Kreativität im Umgang mit dem deutschen Gesetzgeber notwendig.

Es ist zu wünschen, dass beteiligte Unternehmen Verfassungsbeschwerden einreichen, um auch dem höchsten deutschen Gericht die Möglichkeit zu geben, die Strafvorschrift auf ihre Grundrechtskonformität zu prüfen. Die Vorschrift entspricht bei genauer Betrachtung nicht den Anforderungen, die die Gründungsväter und Autoren des Grundgesetzes für Strafvorschriften formuliert haben. Daher scheint die Verfassungsbeschwerde durchaus eine realistische Möglichkeit, eine Änderung des Gesetzes herbeizuführen.

Ihre Ansprechpartner für rechtliche Beratungen:
Feil Rechtsanwälte, Georgsplatz 9, 30159 Hannover, Telefon: 0511 / 473906-01, eMail: feil@recht-freundlich.de