Kritische Würdigung des „Hackerparagrafen“ 202c Abs. 1 Nr. 2 deutsches Strafgesetzbuch

Heidi Schuster

Max-Planck-Gesellschaft
Hofgartenstr. 8, D-80539 München
heidi.schuster@gv.mpg.de

Schlagworte: Strafrecht, Computerkriminalität, Hackerparagraf
Abstract: Im Rahmen der Umsetzung von zwei europäischen Vorgaben zum Schutz der informationstechnischen Systeme vor Computerkriminalität hat der deutsche Gesetzgeber u. a. einen neuen Straftatbestand eingeführt, der kontrovers diskutiert wird. § 202c dStGB verlagert die Strafbarkeit in den Bereich der Vorbereitung und bestraft bestimmte Handlungen, die als Vorbereitung zu anderen Straftatbeständen aus dem Bereich der Computerkriminalität angesehen werden. Diese Abhandlung beschäftigt sich mit der Strafbarkeitsvariante des § 202 c Abs. 1 Nr. 2 deutsches Strafgesetzbuch (dStGB).[1]

1. Strafbarkeitssystematik

Vorbereitungshandlungen sind nur in Ausnahmefällen strafbar, da sie zeitlich vor dem Versuchsstadium liegen. Bei der Vorbereitung einer Straftat befindet sich der Täter in der Planungsphase, er ist von der „Jetzt geht es los“-Schwelle des Versuchs noch entfernt. Die Schwierigkeit der Strafbarkeit von Vorbereitungshandlungen liegt darin, dass auch an sich wertneutrale Handlungen, die jedoch nach der Vorstellung des Täters bereits die Haupttat fördern, von der Strafbarkeit erfasst sind. Dies führt in der Praxis zu Beweisproblemen, insbesondere wenn keine Indizien sichtbar sind, die einen Rückschluss auf die subjektive Vorstellung des Täters zulassen.

Im Bereich des § 202c dStGB liegt eine zusätzliches Problem vor. § 202c bestraft Vorbereitungshandlungen zu den Haupttaten § 202a dStGB (Ausspähen von Daten) und § 202b dStGB (Abfangen von Daten) bzw. über

1 Diese Abhandlung ist eine überarbeitete Fassung der Beiträge *Schuster*, Auswirkungen des Hackerparagraphen in der Praxis, Datenschutz PRAXIS, Ausgabe 10/07, und *Schuster*, Neue Vorschriften zur Computerkriminalität in Ehmann (Hrsg.), Datenschutz kompakt, Stand 04/08.

einen Verweis auch bzgl. der Haupttaten § 303a dStGB (Datenveränderung) und § 303b dStGB (Computersabotage). Während bei § 202a und § 202b dStGB der Versuch strafbar ist, ist bei § 303a und § 303b dStGB nur die vollendete Tat mit Strafe bedroht. Damit liegt die rechtsdogmatisch kritische Situation vor, dass im zeitlichen Verlauf der Delikte Datenveränderung und Computersabotage eine Strafbarkeitslücke entstanden ist: Vorbereitungshandlungen sind strafbewehrt, der Versuch ist straflos, die vollendete Tat ist strafbewehrt.

2. Objektiver Tatbestand

Im objektiven Tatbestand verlangt § 202c Abs. 1 Nr. 2 dStGB, dass der Täter ein Computerprogramm, dessen Zweck die Begehung einer Straftat nach §§ 202a, 202b, 303a oder 303b dStGB ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht.

2.1 Zweckbestimmung

Fraglich ist die Einordnung des Tatbestandmerkmals „Zweckbestimmung“. In den Gesetzesmaterialien finden sich hierzu widersprüchliche Hinweise. Denkbar sind folgende Varianten:

– Ausschlaggebend ist der objektive Zweck eines Computerprogramms. Dies würde bedeuten, dass vom objektiven Tatbestand auch solche Computerprogramme erfasst sind, die sowohl zu legalen als auch zu illegalen Zwecken eingesetzt werden können. Solche sog. Dual-Use-Tools werden im Bereich der IT-Sicherheit häufig eingesetzt, um Unternehmensnetze auf Sicherheitslücken und Angriffe zu untersuchen.
– Vom objektiven Tatbestand werden nur solche Computerprogramme erfasst, deren Zweck „in erster Linie“ der Begehung von Straftaten dient. Diese Auffassung kommt dem Text der europäischen Cybercrime Convention[2] am nächsten („computer program, designed or adapted primarily for the purpose of committing any of the offences“).

2 Übereinkommen des Europarates über Computerkriminalität vom 23. 11. 2001, in Kraft seit 01. 07. 2004.

– Die Strafbarkeit bezieht sich nur auf solche Computerprogramme, denen die illegale Verwendung immanent ist. Dies sind Programme, die aufgrund ihres Aufbaus oder ihrer Beschaffenheit auf die Begehung von Computerstraftaten angelegt sind.

In der Gesetzesbegründung äußert sich die Bundesregierung dahingehend, dass es allein auf den objektiven Zweck eines Programms ankommt. Dies würde bedeuten, dass Dual-Use-Tools vom objektiven Tatbestand umfasst wären. In einer späteren Gegenäußerung zur Stellungnahme des Bundesrates nimmt die Bundesregierung hingegen eine völlig entgegengesetzte Position ein: Dual-Use-Tools werden nun explizit vom Anwendungsbereich des § 202c dStGB ausgenommen, stattdessen stellt die Bundesregierung nun darauf ab, dass die illegale Verwendung den fraglichen Computerprogrammen immanent sein müsse. Welche Richtung die Gerichte einschlagen werden, bleibt abzuwarten.

2.2 Strafbare Handlungen

Der bloße Einsatz der kritischen Computerprogramme ist nicht unter Strafe gestellt. Strafbar sind Handlungen, die auf den eigenen Erwerb – herstellen, verschaffen, kaufen – oder auf die die Verbreitung an andere – anderen verschaffen, überlassen, verbreiten oder sonst zugänglich machen – abzielen. Da ein Einsatz in der Regel jedoch mit einem vorherigen Erwerb bzw. in etlichen Fällen auch mit einer Weiterverbreitung verbunden ist, ist das Risiko einer Strafbarkeit in den meisten Fällen in der Praxis vorhanden.

3. Subjektiver Tatbestand

Welche Voraussetzungen auf subjektiver Ebene erfüllt sein müssen, ist ebenso unklar. Der Vorsatz des Täters muss sich auf alle objektiven Merkmale beziehen. Welche darüber hinaus gehenden Elemente in der subjektiven Vorstellung des Täters vorliegen müssen, hängt davon ab, welche Deliktsnatur für § 202c dStGB angenommen wird.

3.1 Deliktsnatur

In der Gesetzesbegründung behandelt die Bundesregierung die Vorschrift als abstraktes Gefährdungsdelikt. Dies würde bedeuten, dass keine konkrete

Gefährdung vorliegen müsste. Der Vorsatz des Täters müsste sich nicht auf eine konkretisierte zukünftige Haupttat beziehen. Der Wortlaut der Vorschrift „wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er . . .“ legt hingegen eine Einordnung als konkretes Gefährdungsdelikt nahe. Der Täter muss zumindest eine Vorstellung von der in ihren wesentlichen Umrissen konkretisierten eigenen oder fremden Haupttat haben. Aus der Gegenäußerung der Bundesregierung zur Stellungnahme des Bundesrates lässt sich diese Sichtweise herauslesen.

Die Annahme eines konkreten Gefährdungsdelikts würde auch die Problematik entschärfen, dass zur Tatbestandverwirklichung bereits das Vorliegen von Eventualvorsatz ausreichend ist.

3.2 Eventualvorsatz

Eventualvorsatz liegt dann vor, wenn der Täter das Risiko einer Straftat als mögliche Folge hinnimmt. Hier ergeben sich die klassischen Probleme der Abgrenzung zur bewussten Fahrlässigkeit: Hier vertraut der Täter darauf, dass die mögliche strafbare Folge nicht eintritt.

Beim eigenen Erwerb eines kritischen Computerprogramms lässt sich der Eventualvorsatz verhältnismäßig einfach bestätigen bzw. entkräften, z. B. durch die schlüssige Darstellung, dass ein bestimmtes Computerprogramm erworben wurde, um einen erforderlichen Sicherheitsscan durchzuführen.

Problematischer ist die Entkräftung des Eventualvorsatzes, wenn es um die Vorbereitung einer fremden Haupttat geht, der Täter also ein kritisches Computerprogramm Dritten zur Verfügung stellt. Wird ein Dual-Use-Tool in einem Kreis von untereinander bekannten IT-Sicherheitsspezialisten zu Testzwecken verbreitet, so wird der hierfür Verantwortliche noch in der Lage sein, darzulegen, dass er bei der Verbreitung davon ausgegangen ist, dass die ihm bekannten Personen das Tool nur für legale Zwecke nutzen werden.

Wird aber dasselbe Dual-Use-Tool an einen unbekannten Nutzerkreis verbreitet, z. B. per Download von einer Website, so wird der hierfür Verantwortliche Schwierigkeiten haben, schlüssig darzulegen, dass er darauf vertraut hat, dass die ihm unbekannten Nutzer das Tool nur für legale Zwecke einsetzen werden. Sollte die Rechtsprechung § 202c dStGB als abstraktes Gefährdungsdelikt ansehen, besteht eine nur geringe Chance für die Entkräftung des Vorwurfs, dass der Verantwortliche das Risiko, dass das Tool für illegale Zwecke benutzt werden wird, in Kauf genommen hat.

4. Folgen für die Praxis

Die arbeitsvertragliche Tätigkeit von EDV-Mitarbeitern in Unternehmen wird von § 202c dStGB nicht erfasst. Entweder liegt ein tatbestandsausschließendes Einverständnis bzw. eine rechtfertigende Einwilligung des Berechtigten vor oder die Strafbarkeit scheidet – wie bei 3.2 dargelegt – im subjektiven Tatbestand aus.

Installieren EDV-Mitarbeiter Programme auf den Rechnern anderer Nutzer, so ist darauf zu achten, dass jeder Nutzer nur diejenigen Programme erhält, die er für seine Tätigkeit benötigt. Andernfalls könnte dies zu Problemen bzgl. des Eventualvorsatzes der EDV-Mitarbeiter im Hinblick auf eine Straftat durch andere Nutzer führen.

Am problematischsten ist die Bereitstellung von Software-Sammlungen zum Download. Etliche Unternehmen bieten entweder eigene Software-Sammlungen zum Download für externe Dritte an oder spiegeln solche Sammlungen von Original-Servern, die sich typischerweise außerhalb der EU befinden. Um das Risiko einer potentiellen Strafbarkeit zu minimieren, sollten kritische Komponenten nicht angeboten bzw. entfernt werden, sofern dies aus rechtlicher und/oder praktischer Sicht möglich ist.[3] Sollen kritische Komponenten angeboten werden, so sind zusammen mit dem Angebot deutliche und detaillierte Hinweise auf die Rechtslage aufzunehmen.[4] Eine allgemeine Distanzierung von einer eventuellen illegalen Anwendung durch Dritte ist nicht ausreichend, die Hinweise müssen für jede kritische Komponente den entsprechenden Warnhinweis enthalten, z. B. „Denial-of-Service-Angriffe dürfen nur an eigenen Systemen und mit vorheriger Zustimmung des Systembetreibers durchgeführt werden".

Insgesamt bleibt abzuwarten, wie die Rechtsprechung mit den bestehenden Unsicherheiten umgehen wird.

---

3 Eine Entfernung von kritischen Komponenten aus Software-Sammlungen ist oft mit unverhältnismäßigem Aufwand an Zeit und Manpower verbunden. Wird von Original-Servern gespiegelt, dann müssen die Komponenten nach jeder neuen Spiegelung entfernt werden. Zusätzlich besteht die Gefahr, dass hierdurch gegen zivilrechtliche „Spiegel-Vereinbarungen" verstoßen wird.

4 Diese Hinweise sind bei Web-Servern unmittelbar vor dem Download-Link, bei FTP-Servern bei der Verzeichnisübersicht zu platzieren.