Stellungnahme

zum Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität (StrÄndG)
11. Oktober 2006

Der BITKOM vertritt mehr als 1.000 Unternehmen, davon 800 Direktmitglieder mit 120 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Geräte-Hersteller, Anbieter von Software, IT- und Telekommunikationsdiensten sowie Content.

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10
10117 Berlin
+49. 30. 27576-0
Fax +49. 30. 27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Dr. Volker Kitz LL.M. (NYU)
Rechtsanwalt
Bereichsleiter
Telekommunikations- und
Medienpolitik
+49. 30. 27576-221
Fax +49. 30. 27576-222
v.kitz@bitkom.org

Präsident
Willi Berchtold

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Zusammenfassung

Die Bundesregierung hat am 20. September 2006 den Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität (StrÄndG) beschlossen. Der Entwurf soll das Übereinkommen des Europarates über Computerkriminalität vom 23. November 2003 sowie den Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme umsetzen. Er schafft neue Straftatbestände für das Ausspähen und Abfangen von Daten und für diesbezügliche Vorbereitungshandlungen.

Der BITKOM begrüßt im Grundsatz die Initiative und bittet um zügige Umsetzung der internationalen Vorgaben. Die wirtschaftlichen Werte, welche die ITK-Branche in den letzten Jahren aufgebaut hat, haben einen so signifikanten Stellenwert in der Gesamtwirtschaft eingenommen, dass Zerstörungen und Vertrauensmissbrauch hier massive Schäden hervorrufen können.

Im Einzelnen sind allerdings noch offene Fragen zu klären. Insbesondere dürfen die geplanten neuen Vorschriften nicht notwendige sicherheitsrelevante Aktivitäten der Unternehmen selbst in Frage stellen.

§ 202b StGB-E (Abfangen von Daten)

Wir regen an, Überschrift und Einordnung der Vorschrift zu überdenken. Der Begriff des Abfangens taucht im Tatbestand gar nicht auf und ist in der Überschrift missverständlich: Er könnte eher in Richtung eines Festhaltens oder Unterdrückens von Nachrichten deuten, um das es in der Vorschrift aber nicht geht. Da gerade im Strafrecht die Deliktsbezeichnungen sehr wichtig sind, können missverständliche Überschriften zu Missverständnissen bei der Anwendung führen.

§ 202b StGB-E regelt die Kenntnisnahme des Inhalts einer Datenvermittlung. Die Vorschrift steht insoweit im sachlichen Zusammenhang mit dem „Ausspähen von Daten“ in § 202a StGB, denn sie beschreibt eine weitere technische Form des Ausspähens. Beide Vorschriften nennen als Tathandlung das Sichverschaffen von Daten. § 202b StGB-E sollte daher eher als weiterer Absatz in § 202a StGB unter der gemeinsamen Überschrift „Ausspähen von Daten“ oder auch „Sichverschaffen von Daten“ verortet sein.

Offen ist zudem die Rechweite des Tatbestandsmerkmals der "nichtöffentlichen Datenübermittlung", das sich laut Begründung nach der „Art des Übertragungsvorgangs“ richten soll. Es ist allgemein bekannt, dass unverschlüsselte Nachrichten so gut wie öffentlich zugänglich sind. Ob sich das Tatbestandsmerkmal in diesem Zusammenhang – wie die Entwurfsbegründung vorschlägt – mit einem Rückgriff auf die Auslegungsgrundsätze des „nicht öffentlich gesprochenen Wortes“ in § 201 Abs. 2 Nr. 2 StGB hinreichend sicher klären lässt, ist fraglich, denn dort geht es nicht um Übertragungsvorgänge.

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

§ 202c Abs. 1. StGB-E ist nach Ansicht der Branche einerseits zu weit, andererseits zu eng gefasst:

Keine Kriminalisierung sicherheitsrelevanter Handlungen

Ausweislich der Begründung sollen „nur Hacker-Tools“, nicht aber „allgemeine Programmier-Tools, -sprachen oder sonstige Anwendungsprogramme“ unter den objektiven Tatbestand der Vorschrift fallen. Damit dürften etwa Antivirensoftware und andere Sicherheitsprogramme ausgenommen sein.

Da aber die Zweckbestimmung im Tatbestand objektiviert zu betrachten ist, beinhaltet die derzeitige Formulierung des Tatbestandes ein großes Risiko, dass Rechtsanwender auch die genannten Instrumente kriminalisieren. Die Ausführungen auf S.18 der Begründung, wonach die objektive Zweckbestimmung lediglich „auch“ die Begehung einer entsprechenden Straftat zu sein braucht, verstärken diese Bedenken. Gerade die Entwicklung der herrschenden Meinung zum Sichverschaffen im geltenden § 202a

StGB zeigt, wie schnell die Rechtsanwendung weit über die Intention des Gesetzgebers hinausgehen kann.

Zum anderen schaffen und benutzen etwa IT-Sicherheitsexperten und andere vorsorgliche Branchenteilnehmer Programme, die manche Rechtsanwender durchaus als „Hacker-Tools“ einordnen könnten.

In beiden Fällen ist für ein sachgerechtes Ergebnis der subjektive Tatbestand entscheidend; ankommen muss es auf einen auf die Begehung der bezeichneten Taten gerichteten Vorsatz. Die Formulierung „…vorbereitet, indem…“ deutet dies nur an. Wir verstehen, dass sich diese Formulierung an den bereits bestehenden Tatbeständen etwa in §§ 149 Abs. 2, 263a Abs. 3, 275 Abs. 1 StGB orientiert und man insoweit auf die dort gefundenen Auslegungsgrundsätze für Vorbereitungstaten zurückgreifen kann.

Es ist aber bedauerlich, dass die Begründung das Erfordernis des Vorsatzes nicht noch einmal deutlich für die gesamte Vorschrift heraushebt. Bisher tut sie dies nur zu Abs. 1 Nr. 1 (S. 19 oben), was einen für die Bekämpfung elektronischer Schädlinge kontraproduktiven und vom Gesetzgeber sicher nicht so gewollten Gegenschluss hinsichtlich Nr. 2 zulassen könnte. Notwendig wäre ein ausdrücklicher Hinweis darauf, dass das Vorsatzerfordernis gerade Handlungen der genannten vorsorglichen Branchenteilnehmer von der Strafbarkeit ausschließt.

Ausdrückliche Strafbarkeit von Phishing

Der BITKOM hat sich bereits wiederholt dafür ausgesprochen, Phishing ausdrücklich unter Strafe zu stellen. Die Diskussion über eine Strafbarkeit von Phishing de lege lata ist sehr kontrovers. Eine Fälschung beweiserheblicher Daten (§ 268 StGB) wird nur in besonderen Einzelfällen vorliegen. Soweit das Phänomen über die „schadensgleiche Vermögensgefährdung“ beim Betrug erfasst werden soll, ist dies bedenklich: Es handelt sich hierbei um eine richterliche Rechtsfortbildung, die ohnehin nahe an der Grenze zum Analogieverbot steht oder diese sogar überschreitet. Darauf zu „hoffen“, dass die höchstrichterliche Rechtsprechung dieses ohnehin neben dem Gesetzeswortlaut stehende Institut bei Gelegenheit noch weiter ausdehnt, scheint uns nicht der richtige Weg zu sein.

Tatsache ist jedenfalls, dass Staatsanwaltschaften Ermittlungsverfahren einstellen, weil sie derzeit keinen Straftatbestand erfüllt sehen. Damit bleibt ein massenhaftes Verhalten, das immensen wirtschaftlichen Schaden anrichtet und mit einem hohen Maß an krimineller Energie einhergeht, derzeit ungeahndet.

Da § 202c Abs. 1 Nr. 1 StGB-E bereits einen guten Ansatz für einen entsprechenden Phishing-Straftatbestand enthält, schlagen wir vor, die Gelegenheit zu ergreifen und den bisherigen Entwurf so zu erweitern, dass er auch Phishing erfasst. Dafür dürfte bereits eine auf Abs. 1 Nr. 1 beschränkte Versuchsstrafbarkeit ausreichen. Eine Phishing-Nachricht ist der Versuch, sich ein Passwort zu verschaffen, um sich mit diesem Passwort gemäß § 202a Abs. 1 StGB-E unbefugt Zugang zu besonders gesicherten

Daten zu verschaffen. Da diese Nachrichten wegen des damit einhergehenden Vertrauensverlustes in den elektronischen Geschäftverkehr einen enormen wirtschaftlichen Schaden anrichten, ist eine Strafbarkeit auch durchaus gerechtfertigt. Bei allen Kontroversen über die Beurteilung einer Strafbarkeit de lege lata besteht Einigkeit darüber, *dass* solche Handlungen im Ergebnis strafwürdiges Unrecht darstellen.