Prof. Dr. Georg Borges 19.3.2007

Lehrstuhl für Bürgerliches Recht, deutsches und internationales Handels- und Wirtschaftsrecht, insb. Recht der Medien und der Informationstechnologie
Ruhr-Universität Bochum

Sprecher des Vorstands der Arbeitsgruppe Identitätsschutz im Internet e.V. (a-i3)

Stellungnahme

zum Gesetzentwurf der Bundesregierung – Entwurf eines … Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität (...StrÄndG)

für die öffentliche Anhörung am 21. März 2007

Der Gesetzentwurf dient der Umsetzung des Übereinkommens des Europarats über Computerkriminalität vom 23.11.2001 (Cybercrime Convention, ETS No. 185) sowie des Rahmenbeschlusses des Rates der Europäischen Union vom 24.2.2005 über Angriffe auf Informationssysteme (Abl. EU Nr. L 69 S. 67). Diese Instrumente sollen den Missbrauch der Informationstechnologie bekämpfen. Daher sollte die Umsetzung der in diesen Rechtsakten enthaltenen europa- und völkerrechtlichen Vorgaben im Hinblick auf das Ziel erfolgen, den Missbrauch der Informationstechnik effektiv zu bekämpfen. Zugleich muss verhindert werden, dass die Entwicklung der Informationstechnologie durch eine überschießende Pönalisierung des erwünschten technischen Fortschritts beeinträchtigt wird.

Die nachfolgende Stellungnahme beschränkt sich auf zwei Aspekte der komplexen Materie: auf die Strafbarkeit des Phishing und ähnlicher Formen der Internetkriminalität, die derzeit und voraussichtlich auch in Zukunft eine ernstzunehmende Gefahr für den elektronischen Geschäftsverkehr darstellen, und auf die Gefahr einer Beeinträchtigung der Softwareentwicklung durch die geplante Gesetzgebung (unten II.). Wegen der Umsetzung der Cybercrime

Convention und der sonstigen strafrechtsdogmatischen Aspekte sei auf die Stellungnahme von PD Dr. Stuckenberg, LLM., verwiesen.[1]

I. Strafbarkeit von Phishing und ähnlichen Angriffen

1. Gefahren für den elektronischen Geschäftsverkehr durch Phishing

Phishing und ähnliche Formen des Identitätsmissbrauchs im Internet sind zu ernstzunehmenden Gefahren für den elektronischen Geschäftsverkehr geworden. Beim Phishing handelt es sich um eine seit 2004 massenhaft auftretende Form der Internetkriminalität, die vor allem darauf gerichtet ist, durch Missbrauch von Zugangs- und Kontodaten im Onlinebanking Überweisungen vorzunehmen. In der ersten Generation der Angriffe („klassisches Phishing“) wurden gefälschte Mails versandt, die über gefälschte Hyperlinks Kunden einer Bank auf Imitate der Originalseite der betreffenden Bank führten, um sie zur Preisgabe der Zugangs- und Kontodaten wie PIN und TAN zu bringen. Heute hingegen greift das Phishing auf ein umfangreiches Portfolio von Angriffsmethoden und Strategien zurück, die auch technisch anspruchsvolle Schutzmaßnahmen umgehen können.[2]

Aktuelle Studien bestätigen, dass Phishing ein ernstzunehmendes Problem ist. So verzeichnete die US-amerikanische Anti Phishing Working Group (APWG) im Oktober 2006 einen Höchststand an Phishing-Seiten, im Dezember 2006 lag die Zahl der Seiten rund viermal so hoch wie im Dezember 2005.[3] Laut APWG sind im Dezember 2006 2.200 Webseiten identifiziert worden, die Crimeware vertreiben.[4] Der Begriff Crimeware bezeichnet spezielle Malware-Angriffe, die einerseits sensible Nutzerdaten (z.B. durch Keylogger) abfangen, aber andererseits auch die korrumpierten Systeme fernsteuern lassen, um sie als Infrastruktur für einen Phishing-Angriff zu nutzen (z.B. Botnetze zum Versand

---

[1] Siehe dazu auch *Borges/Stuckenberg/Wegener*, in DuD Heft 4/2007.

[2] Siehe dazu auch *Biallaß/Borges/Dienstbach/Gajek/Meyer/Schwenk/Wegener/Werner*, Aktuelle Gefahren im Onlinebanking: Technische und juristische Hintergründe, 2007, angenommen zum 10. Deutschen IT-Sicherheitskongress des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Mai 2007.

[3] Der Bericht ist abrufbar unter http://www.antiphishing.org/reports/apwg_report_december_ 2006.pdf.

[4] http://www.antiphishing.org/reports/apwg_report_december_ 2006.pdf.

von Phishing-Mails). Zugleich verschieben sich die Schwerpunkte der Angriffe vom klassischen Phishing auf raffiniertere Angriffsformen. So werden derzeit die meisten Schäden durch Trojaner-Angriffe verursacht.[5]

Über den Schaden, der durch den Missbrauch der gestohlenen Daten entsteht, und die Anzahl der Opfer ist nur wenig bekannt. In den USA geht man davon aus, dass in etwa bei 8 % der Onlinebanking-Kunden entsprechende Schäden durch Phishing aufgetreten sind.[6] Die Internetkriminalität erfasst nicht nur das Onlinebanking, sondern zahlreiche Bereiche des elektronischen Geschäftsverkehrs. So leidet etwa auch die Internetplattform von eBay unter einer hohen Zahl an Rechtsverletzungen, darunter auch Betrug infolge von Identitätsmissbrauch.

2. Strafbarkeit des Phishing nach geltendem Recht

Zur Strafbarkeit des Phishing nach geltendem Recht liegt bisher keine Rechtsprechung vor, da die Täter, die meist aus dem Ausland agieren, bisher regelmäßig nicht gefasst werden können. In der Literatur wird die strafrechtliche Beurteilung des Phishing kontrovers diskutiert.[7] Dabei besteht jedoch Einigkeit darin, dass jedenfalls ein erfolgreicher Angriff, der zu einer gefälschten Überweisung vom Konto des Bankkunden führt, als Computerbetrug nach § 263a StGB strafbar ist.[8] Auch die Entgegennahme von PIN und TAN auf einer

---

[5] Laut Bericht der APWG von Dezember 2006 ist die Anzahl von Phishing-Trojanern (Keyloggern) im Vergleich zum Dezember 2005 von 180 auf 340 gestiegen. Damit ist ein neuer Höchststand erreicht. Der Bericht ist abrufbar unter http://www.antiphishing.org/reports/apwg_report_december_2006.pdf.

[6] Consumerreports.org: US Consumers Lose More Than $8 Billion To Online Threats According To Consumer Reports Survey, September 2006. http://www.consumerreports.org/cro/cu-press-room/pressroom/2006/9/0609_eng0609son_ov.htm.

[7] *Gercke*, CR 2005, 606 ff.; *ders.*, ZUM 2005, 612, 617 f.; *Graf*, NStZ 2007, 129 ff.; *Hilgendorf*/*Frank*/*Valerius*, Computer- und Internetstrafrecht, 2005, Rz. 760 ff.; *Knupfer*, MMR 2004, 641 f.; *Marberth-Kubicki*, Computer- und Internetstrafrecht, 2005, Rz. 118 ff.; *Popp*, NJW 2004, 3517 f.; *ders.*, MMR 2006, 84 ff.; *Stuckenberg*, ZStW 118 (2006), 878 ff.; *Weber*, HRRS 2004, 406, 407 ff.; *Werner*, in: Borges (Hrsg.), Recht der Internet-Auktion, 2007, S. 190 ff.

[8] *Gercke*, CR 2005, 606, 611; *Knupfer*, MMR 2004, 641, 642; *Marberth-Kubicki* (Fn. 7), Rz. 119; *Popp*, NJW 2004, 3517, 3518; *ders.*, MMR 2006, 84 f.; *Stuckenberg*, ZStW 118 (2006), 878, 909 ff.; *Weber*, HRRS 2004, 406 f.

gefälschten Website ist strafbar.[9] Umstritten aber ist, ob das bloße Versenden einer Phishing-Mail einen Straftatbestand erfüllt. Die Strafverfolgungsbehörden haben vielfach keine Strafbarkeit gesehen. Dagegen wird in der Literatur zutreffend angenommen, dass eine E-Mail, die nach ihrer Gestaltung die E-Mail einer Bank darstellen soll, den Tatbestand der Fälschung beweiserheblicher Daten, § 269 StGB erfüllt.[10]

Ebenfalls umstritten ist die Strafbarkeit beim Abfangen von Passwörtern, PIN, TAN etc. durch Schadprogramme (z.B. Keylogger), das in der Praxis erhebliche Bedeutung hat. Hier wird teilweise ein Ausspähen von Daten nach § 202a StGB angenommen, andere Stimmen sehen hierin keine strafbare Handlung.[11] Damit besteht in einem wichtigen Punkt Unsicherheit über die Strafbarkeit des bloßen Verschaffens von Passwörtern.

Die Bedeutung dieser umstrittenen Aspekte liegt vor allem in der Strafverfolgung und der effektiven Bekämpfung von Phishing. Hierfür ist es von Interesse, dass nicht erst in der Verwendung von Passwörtern, sondern bereits im Vorfeld, beim Verschaffen der Passwörter, unzweifelhaft eine strafbare Handlung vorliegt. Dies spricht dafür, die Strafbarkeit dieser Handlungen durch eine spezifische Norm im Rahmen des aktuellen Gesetzgebungsverfahrens zu sichern.

3. Die Bedeutung des § 202b und des § 202c E-StGB

Die Forderung verschiedener Stimmen der Literatur[12], von Wirtschaftsverbänden[13] und des Bundesrates[14], Phishing durch eine spezifische

---

[9] *Stuckenberg*, ZStW 118 (2006), 878, 890, 895.

[10] Dazu ausführlich *Stuckenberg*, ZStW 118 (2006), 878, 886 ff. Differenziert auch *Graf*, NStZ 2007, 129, 131.

[11] *Werner*, in Borges (Fn. 7), S. 190, 196 ff. (nur bei Vorhandensein eines aktuellen Virenschutzprogramms und einer Firewall), so wohl auch *Sieber*, in Hoeren/Sieber, Handbuch Mutimedia-Recht, Stand August 2006, Kap. 19 Rz. 420; a.A. *Eichelberger*, MMR 2004, 594; MünchKommStGB-*Graf*, 2003, § 202a Rz. 64.

[12] Siehe etwa *Graf*, NStZ 2007, 129, 132; *Osthaus*, in Borges (Hrsg.), Rechtsfragen der Internet-Auktion, 2007, S. 204 ff. mit einem Formulierungsvorschlag.

[13] Stellungnahme des BITKOM zum RegE v. 11.10.2006, S. 3.

Strafnorm zu erfassen, wird durch den RegE weitgehend erfüllt, da § 202b E-StGB und § 202c E-StGB Phishing und ähnliche Angriffe umfassend unter Strafe stellen.

a) Zahlreiche Varianten des Phishing, bei denen sich der Täter Passwörter verschafft, fallen unter § 202c Abs. 1 Nr. 1 E-StGB. Dies gilt insbesondere für klassisches Phishing durch E-Mail und gefälschte Website (dazu unten d), ebenso für Keylogging und Pharming jeglicher Form. Erfasst werden auch sog. Man-in-the-Middle-Angriffe, bei denen das Passwort, bzw. PIN und TAN, vom Täter sogleich, z.B. an die Website einer Bank, weitergeleitet werden.

Die Strafbarkeit nach § 202c Abs. 1 Nr. 1 E-StGB ist aber wohl bei solchen Angriffen zu verneinen, die innerhalb einer bestehenden Verbindung des Kunden zum Bankserver Daten, z.B. Betrag und Zielkonto, verfälschen. Diese Fälle werden aber durch § 202c Abs. 2 Nr. 2 E-StGB erfasst.

b) Bei Man-in-the-Middle-Angriffen, bei denen der Täter sich in die Kommunikation zwischen dem Nutzer und der Website, etwa einer Bank, einschaltet und Daten abfängt, ist der Tatbestand des § 202b StGB verwirklicht.

c) Alle Formen des Phishing, die mit Hilfe von Schadprogrammen, insbesondere Trojanern, durchgeführt werden, erfüllen § 202c Abs. 1 Nr. 2 E-StGB, da der Täter die entsprechenden Programme entweder herstellen oder beschaffen muss.[15] Dies gilt auch dann, wenn § 202c Abs. 1 Nr. 2 E-StGB mit dem nachfolgenden Vorschlag (unten II.) enger an die Europarats-Konvention angelehnt wird. Auch das klassische Phishing wird regelmäßig erfasst, da die Entgegennahme von PIN und TAN auf einer gefälschten Website eines entsprechenden Programms bedarf.

d) Strafbarkeitslücken werden vor allem in Bezug auf das klassische Phishing diskutiert. Hier greift § 202c Abs. 1 Nr. 1 E-StGB beim Onlinebanking ein, weil der beabsichtigte Zugriff auf das Konto den § 202a StGB im Hinblick auf die Kontodaten des Nutzers erfüllt.[16] Ob es dem Täter auf die Kontodaten ankommt, ist nach der Neufassung des § 202a E-StGB unerheblich, so dass

---

14 Vgl. Empfehlung der Ausschüsse zu § 202c E-StGB, BR-Drs. 676/01/06, S. 5 = BR-Drs. 676/06 (Beschluss vom 3.11.2006), S. 4, die insoweit nahezu wörtlich auf die Stellungnahme des BITKOM zurückgehen.

15 *Borges/Stuckenberg/Wegener*, DuD Heft 4/2007.

16 *Stuckenberg*, ZStW 118 (2006), 878, 906.

Strafbarkeitslücken, die bei der bisherigen Fassung des § 202a StGB bestünden, ausgeräumt sind. Ob es gleichwohl Fälle gibt, in denen § 202a StGB nicht verwirklicht wird, ist schwer zu übersehen.

4. Ergebnis. Erweiterung des § 202c E-StGB statt eines speziellen Phishing-Tatbestands

Mit der geplanten Gesetzesänderung wird Phishing umfassend unter Strafe gestellt. Eine Lücke kann allenfalls beim folgenlosen Versenden einer Phishing-Mail entstehen, wenn diese ausnahmsweise nicht den Straftatbestand des § 269 StGB erfüllen sollte. Da die praktische Bedeutung des klassischen Phishing abnimmt, scheint es nicht notwenig, wegen der Ausnahmefälle eine spezielle Strafnorm zu schaffen.

Dagegen erscheint es sinnvoll, § 202c E-StGB dahin zu erweitern, dass nicht nur die §§ 202a, b StGB, sondern explizit auch § 263 StGB und § 263a StGB als die Normen genannt werden, die bei erfolgreichen Phishing-Angriffen verwirklicht werden und den Schwerpunkt des Unrechts ausmachen.

II. Unerwünschte Pönalisierung von Softwareentwicklung durch § 202c E-StGB?

Seitens der Praxis wurde vielfach die Befürchtung geäußert, § 202c Abs. 1 Nr. 2 E-StGB könne bei weiter Auslegung auch die Entwicklung oder den Vertrieb von Software erfassen, die für Entwicklungen im Bereich der IT-Sicherheit verwendet werden. Diese Sorge ist teilweise begründet, da § 202c Abs. 1 Nr. 2 E-StGB sowohl im objektiven als auch im subjektiven Tatbestand zu weit gefasst ist.

1. Objektive Zweckbestimmung und dual use tools

§ 202c Abs. 1 Nr. 2 E-StGB erfasst Programme, deren *Zweck* das Ausspähen oder Abfangen von Daten ist. Eine ausschließliche Bestimmung zu diesem Zweck ist demnach nicht erforderlich.[17] Dies wäre auch nicht sinnvoll, da diese Straftaten

---

[17] *Borges/Stuckenberg/Wegener*, DuD Heft 4/2007.

auch mit Programmen verwirklicht werden können, die sowohl zu legalen als auch zu illegalen Zwecken verwendet werden können.

a) Beispiele

Passwort-Scanner

Ein Beispiel für Dual-Use-Software sind Passwort-Scanner. Sie werden von Systemadministratoren und IT-Sicherheitsbeauftragten in Unternehmen dazu verwendet, die Sicherheit von Passwörtern zu testen. Sollte ein Passwort nicht dem Sicherheitsstandard entsprechen, wird dem Nutzer ein entsprechender Hinweis, mit der Aufforderung sein Passwort zu ändern, gegeben. Diese Programme können auch eingesetzt werden, um Passwörter Dritter herauszufinden und zu missbrauchen.

Netzwerksniffer

Netzwerksniffer überwachen den gesamten Datenverkehr an einer Netzwerkkarte und können ihn auch aufzeichnen. Ein bekanntes Beispiel ist das Programm Wireshark (etherreal). Netzwerksniffer dienen normalerweise zur Fehlerdiagnose und zur Netzwerkoptimierung. Wird beispielsweise eine hohe Bandbreitennutzung festgestellt, so ermöglichen Sniffer den Rückschluss auf das Programm, welches den Datenverkehr verursacht. Sniffer können auch eingesetzt werden, um sensible Daten wie z.B. Passwörter oder PINs aufzuzeichnen. Angriffe können auch aus dem Internet erfolgen, wenn sich der Angreifer Zugriff auf einen an das lokale Netzwerk angeschlossenen Rechner verschafft, etwa durch das Einschleusen von Schadsoftware.

Portscanner

Portscanner werden eingesetzt, um offene Ports in Netzwerken zu finden. Der Administrator hat dann die Möglichkeit, diese Ports zu schließen, wenn sie nicht benötigt werden. Allerdings ermöglichen sie es Angreifern auch, Schwachstellen aufzuspüren.

Fernwartungssysteme

Fernwartungssysteme ermöglichen die Fernsteuerung und Fernwartung von Computersystemen und erlauben häufig den nahezu vollständigen Zugriff

auf das entfernte Computersystem. Ein Beispiel für eine legale Nutzung sind etwa Helpdesk-Anwendungen. Solche Programme können jedoch auch genutzt werden, um Computer zu illegalen Zwecken fernzusteuern.

b) Risiken für Softwareentwicklung und Netzwerkverantwortliche

Die angesprochenen Typen von Software gehören zu den typischen Arbeitsmitteln von Netzwerkadministratoren und IT-Sicherheitsbeauftragten. So werden etwa Passwortscanner in Unternehmen verwendet, um zu testen, ob die von den Angestellten verwendeten Passwörter den Sicherheitsrichtlinien entsprechen. Hierbei handelt es sich um eine der zentralen Aufgaben von IT-Sicherheitsbeauftragten. Dies bedeutet, dass der objektive Tatbestand des § 202c Nr. 2 StGB-E in der Praxis der Softwareentwicklung vielfach verwirklicht wird.

2. Der subjektive Tatbestand des § 202c E-StGB und dual use tools

Auch der subjektive Tatbestand des § 202c E-StGB bietet nur geringes Eingrenzungspotential. Zwar wird mit der Bezugnahme auf die §§ 202a, 202b E-StGB wird die Verwendung der Testprogramme zu den dort genannten Straftaten in den subjektiven Tatbestand des § 202c E-StGB einbezogen. Jedoch genügt im Rahmen des § 202c E-StGB in subjektiver Hinsicht dolus eventualis. Die Möglichkeit einer illegalen Verwendung derartiger Software ist nicht auszuschließen. Dies ist Softwareentwicklern auch bekannt. Es ist daher möglich, ein Inkaufnehmen einer solchen Straftat auch in Fällen anzunehmen, in denen Softwareentwickler im Bereich der IT-Sicherheit Programme, die zu ihrem üblichen Arbeitswerkzeug gehören, weiterentwickeln oder verbreiten.

3. Notwendige Einschränkung des § 202c E-StGB

Zur Vermeidung dieser Risiken sollte § 202c Abs. 1 Nr.2 E-StGB im objektiven wie im subjektiven Tatbestand enger gefasst werden. Im objektiven Tatbestand sollte § 202c Abs. 1 Nr. 2 E-StGB auf die Programme beschränkt werden, deren

Zweck vorrangig die Begehung von Straftaten ist.[18] Die Konvention ermöglicht dies, da sie ihrerseits auf den vorrangigen Zweck verweist und Testsoftware ausdrücklich ausnimmt.

Außerdem sollte die Strafbarkeit nach § 202c Nr. 2 E-StGB hinsichtlich der subjektiven Anforderungen eingeschränkt werden. Im Rahmen des § 202c StGB sollte in subjektiver Hinsicht positive Kenntnis oder Absicht erforderlich sein Dies würde mit der Konvention übereinstimmen, die hier den Begriff des „intent“ verwendet, der Absicht und positive Kenntnis umfasst, nicht aber das Inkaufnehmen (*dolus eventualis*).

III. Fazit

1. Der Gesetzentwurf gewährleistet durch die §§ 202b, 202c E-StGB die umfassende Strafbarkeit des Phishing und ähnlicher Formen des Identitätsmissbrauchs und beseitigt etwaige Strafbarkeitslücken, soweit diese von praktischer Bedeutung sind. Eine darüber hinausgehende spezielle Strafnorm zum Phishing erscheint nicht notwendig. Dagegen erscheint es sinnvoll, § 263 StGB und § 263a StGB als die zentralen Delikte, die beim Phishing und ähnlichen Angriffen verwirklicht werden, in den Tatbestand des § 202c E-StGB aufzunehmen.

2. § 202c Abs. 1 Nr. 2 E-StGB ist zu weit gefasst und birgt das Risiko, dass legale Tätigkeiten der Softwareentwicklung und –verbreitung im Bereich der IT-Sicherheit pönalisiert wird. Daher sollte § 202c Abs. 1 Nr. 2 E-StGB dahin gefasst werden, dass die Programme ihrer Art nach vorrangig zur Begehung von Straftaten nach §§ 202a, 202b E-StGB geeignet sein müssen. In subjektiver Hinsicht sollte § 202c E-StGB auf Absicht und Kenntnis begrenzt werden.

---

[18] *Borges/Stuckenberg/Wegener*, DuD Heft 4/2007 mit einem Formulierungsvorschlag.