.SIAK REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
SICHERHEITSAKADEMIE

.SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis

Reindl, Susanne (2007):

Das Phänomen „Phishing“. Aktuelles Computerstrafrecht

SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (1), 2-13.

doi: 10.7396/2007_1_A

Um auf diesen Artikel als Quelle zu verweisen, verwenden Sie bitte folgende Angaben:

Reindl, Susanne (2007). Das Phänomen „Phishing“. Aktuelles Computerstrafrecht, SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (1), 2-13, Online: http://dx.doi.org/10.7396/2007_1_A.

Online publiziert: 4/2014

Aktuelles Computerstrafrecht

DAS PHÄNOMEN "PHISHING"

SUSANNE REINDL, DR. , AO. UNIV.-PROF.
Institut für Strafrecht und Kriminologie der Universtiät Wien

61% der ca 3,9 Millionen Österreicher im Alter über vierzehn Jahre nutzen bereits das Internet, davon verwenden etwa 2,57 Millionen Online-Dienste auch zum Einkaufen im Netz.[1] Da verwundert es nicht, wenn es – sozusagen als Kehrseite dieser positiven Nutzungsmöglichkeiten – auch zu Missbrauchsfällen kommt. Der Strafgesetzgeber hat in den letzten Jahren auf neue Bedrohungen durch die Weiterentwicklung der Technologien im StRÄG 2002[2] und im StRÄG 2004[3] reagiert. Das Computerstrafrecht hat in den letzten Jahren einen unglaublichen Aufschwung genommen, was die Regelungsvielfalt und Dichte angeht. Dennoch stehen wohl schon in naher Zukunft weitere Novellen bevor. So hat beispielsweise der Rat der Europäischen Union am 24.02.2005 einen Rahmenbeschluss über Angriffe auf Informationssysteme verabschiedet[4], der bis 16.03.2007 umgesetzt werden soll. Der Rahmenbeschluss sieht zum einen die Verpflichtung zur Einführung bestimmter Straftaten vor, nämlich zur Sanktionierung des rechtswidrigen Zugriffs auf ein Informationssystem, des rechtswidrigen Systemeingriffs und des rechtswidrigen Eingriffs in Daten. Im Großen und Ganzen werden diese Handlungen auch derzeit schon vom österreichischen Strafrecht, insbesondere durch die Tatbestände der §§ 118a, 126a und 126b StGB erfasst. Allerdings sieht der Rahmenbeschluss für den System- und Dateneingriff ein Höchstmaß von mindestens einem bis zu drei Jahren vor (Art 6 RB). Darüber hinaus sollen schwerere Strafen vorgesehen werden, wenn die Taten des Rahmenbeschlusses im Rahmen einer kriminellen Organisation begangen werden. In diesem Zusammenhang wird man daher nicht bloß neue Qualifikationen einführen können, sondern sich etwa auch überlegen müssen, wie diese Mindesthöchststrafen ins Gesamtsystem der Vermögensdelikte eingepasst werden können, um auch die Gleichbehandlung und eine ausgewogene Schutzrelation zwischen Straftaten gegen körperliches Vermögen und gegen Daten und Informationssysteme zu wahren. Im ersten Teil des Beitrags soll eine allgemeine Übersicht über die derzeitige Systematik des Computerstrafrechts gegeben werden. Im zweiten Teil hingegen widmet sich der Beitrag der Anwendung des geltenden Computerstrafrechts auf das Phänomen des so genannten "Phishing".

1. ÜBERSICHT ÜBER DIE SYSTEMATIK

1.1. KERNBEREICH

1.1.1. BEREICHERUNGSDELIKTE

Das heutige Computerstrafrecht gliedert sich im Kernbereich in vier wesentliche Deliktsgruppen: Im Zentrum stehen die Bereicherungsdelikte, bei denen der Täter durch den Einsatz verschiedenster EDV-Instrumente eine Vermögensverschiebung weg vom Opfer erreicht und sich oder einen anderen dadurch bereichert. Das schon seiner Überschrift nach spezifische Delikt ist § 148a StGB, also betrügerischer Datenverarbeitungsmissbrauch. Die Rechtsprechung ist in der Anwendung zwar noch immer zurückhaltend, doch finden sich in den letzten Jahren immer wieder Verurteilungen nach diesem Delikt; so zB für das Überweisen von Geldbeträgen vom Konto des Opfers auf das Täterkonto am Überweisungsautomaten einer Bank[5], für das Aufladen einer Telefonwertkarte oder einer Quickgeldbörse am Bankomat unter Verwendung einer fremden Zahlungskarte[6], für missbräuchliches Telefonieren mit D-Netz-Telefonen[7] oder auch für das unbefugte Um- und Abbuchen von Sparbriefkonten[8].

Daneben werden aber verschiedene Malversationen auch von anderen Bereicherungsdelikten erfasst, wenn sich der Täter bei der Tatbegehung elektronischer Hilfsmittel bedient.

Nach der Judikatur wird etwa immer noch die missbräuchliche Behebung von Bargeld am Bankomat unter Verwendung einer fremden Karte als Diebstahl beurteilt.[9]

Aber auch andere Geschehen sind denkbar. Bisweilen erhalten Handy-Besitzer SMS[10], in denen ihnen mitgeteilt wird, sie hätten bei einem Spiel oder einem Preisausschreiben etwas gewonnen und sie mögen sich für die Auszahlung unter der im SMS angegebenen Telefonnummer melden. Gewonnen hat der Empfänger des SMS freilich in Wahrheit nichts. Die angegebene Nummer aber ist eine Mehrwertnummer, was allerdings für das Opfer nicht immer leicht bzw gar nicht zu erkennen ist. Ruft das Opfer die Nummer an, so laufen hohe Gebühren auf, ohne dass das Opfer irgendwie zu dem versprochenen Gewinn kommt.

Auch wenn sich die Täter in solchen Fällen der EDV bedienen, bleibt es doch bei einem klassischen Delikt, nämlich Betrug (§ 146 StGB).

Der Täter hat das Opfer durch die SMS-Nachricht getäuscht und in einen Irrtum geführt, aufgrund dessen es die Mehrwertnummer anwählt und sich selbst schädigt. Der Vermögensschaden entspricht den "frustrierten" Gebühren. Auf der anderen Seite werden die Täter aber – sofern sie erfolgreich waren – unrechtmäßig bereichert.[11]

1.1.2. SCHADENSDELIKTE

Der zweite große Bereich des heutigen Computerstrafrechts sind die Schadensdelikte. Dazu zählen die Datenbeschädigung (§ 126a StGB) und – in gewisser Weise als Ergänzung – die Funktionsstörung eines Computersystems (§ 126b StGB). Während die Datenbeschädigung auf verschiedene Formen des Unbrauchbarmachens von Daten abstellt, soll § 126b StGB auch denjenigen Täter erfassen, der Computer durch die Sendung von Massen-E-Mails "lahm legt", ohne zwingend einen Schaden an den Daten selbst herbeizufüh-

ren. Diese Regelung lässt unweigerlich an die Problematik der rechtlichen Bekämpfung von Spam-Mails denken, also von unerwünschten Massenmails, die in aller Regel zu Werbezwecken verschickt werden. Obwohl sich der Gesetzgeber dieses Problems zum Zeitpunkt der Beschlussfassung über § 126b StGB bereits bewusst war, ist diese Norm in Anbetracht seiner Tatbestandsmerkmale nicht als strafrechtliches Spamverbot zu verstehen. Während §107 TKG 2003[12] das Zusenden unerbetener Nachrichten mehr oder weniger per se als unzulässig erklärt und die Übertretung dieser Regelung nach § 109 TKG 2003 als Verwaltungsübertretung strafbar ist, greift § 126b StGB erst ein, wenn durch die Massensendung die Funktionsfähigkeit des Systems erheblich gestört ist. Im Extremfall – nämlich dann, wenn die Spam-Mails wegen der großen Datenmenge zB zum "Absturz" des Systems führen – können auch solche Attacken die kriminalstrafrechtliche Sanktion des § 126b StGB nach sich ziehen. Für die übliche Menge an Werbemails, die Nutzer von E-Maildiensten nahezu schon selbstverständlich erhalten, trifft dies aber nicht zu. Sollte die Funktionsstörung des Computersystems aber sogar eine Datenbeschädigung bewirken, dann kommt sogar Datenbeschädigung nach § 126a StGB in Betracht. Wenn nämlich zB Daten durch die Attacke bewusst unzugänglich gemacht werden, werden sie in den Worten des Gesetzes "unterdrückt".

1.1.3. INHALTSDELIKTE

Der dritte Bereich des EDV-Strafrechts betrifft die Inhaltsdelikte, also Delikte, die den Umgang mit bestimmten Inhalten unter Strafe stellen. Der Gesetzgeber sanktionierte auch schon vor der Nutzung des Internet verschiedentlich die Herstellung und Verbreitung gewisser Inhalte, so zB durch das Pornographie- und das Verbotsgesetz. Von besonderer Bedeutung ist in den letzten Jahren § 207a StGB (Pornographische Darstellungen Minderjähriger), der durch das StRÄG 2004[14] novelliert wurde und neben der Herstellung und Verbreitung auch den Besitz kinderpornographischen Materials bei Strafe verbietet. Im Zuge dieser Novelle wurde der strafbare Bereich wesentlich ausgedehnt: Zum einen werden nunmehr auch mündig minderjährige Darsteller von § 207a StGB geschützt. Zum anderen wurde der Begriff der pornographischen Darstellung legal definiert und erfasst nunmehr neben der Darstellung sexuellen Geschehens mit Körperkontakt auch reißerisch verzerrte, auf sich selbst reduzierte und von anderen Lebensumständen losgelöste Abbildungen der Genitalien oder Schamgegend ohne Körperkontakt (§ 207a Abs 4 Z 3 StGB). Das abgebildete Geschehen muss nach einer Variante der Definition nicht einmal auf einem realen Hintergrund beruhen (§ 207a Abs 4 Z 4 StGB). So reichen etwa bloße Computeranimationen aus[15], sofern freilich der Eindruck vermittelt wird, es handle sich um eine von § 207a Abs 4 Z 1 – 3 StGB erfasste wirklichkeitsnahe Abbildung des verpönten Geschehens.

Im Grunde kann aber jedes Äußerungsdelikt auch im Internet begangen werden.

Die Inhaltsdelikte wurden vom Gesetzgeber durchwegs so technikneutral konzipiert, dass sie sowohl auf traditionelle wie moderne Begehungsmethoden anwendbar sind.

Denkbar sind daher insbesondere auch die Begehung der Verhetzung, der Verleumdung oder – freilich idR als Privatanklagedelikte – der Ehrbeleidigungsdelikte mit den Mitteln moderner Kommunikationstechnik.

1.1.4. HANDLUNGEN GEGEN DIE ZUVERLÄSSIGKEIT VON URKUNDEN UND BEWEISZEICHEN

Der vierte Bereich ist vereinfacht formuliert das Urkundenstrafrecht: Bis zum StRÄG 2002 bereitete die strafrechtliche Erfassung von elektronischen Texten und deren Verfälschung größere Schwierigkeiten. Zwar war an Urkundendelikte zu denken, doch setzt der strafrechtliche Urkundenbegriff (§ 74 Abs 1 Z 7 StGB) das Vorliegen einer Schrift voraus. Die strafrechtliche Tradition geht zu Recht bis heute davon aus, dass eine solche Schrift nur dann vorliegt, wenn sie mit freiem Auge, also ohne den Einsatz computertechnischer Hilfsmittel lesbar ist.[16] Wurde damals ein klassischer Geschäftsbrief auf Papier unbefugt verändert, so konnte Urkundenfälschung nach § 223 StGB vorliegen. Verfälschte der Täter hingegen denselben Gedankeninhalt in einem E-Mail, so war die Verfälschung bestenfalls noch als Datenbeschädigung in Form der Veränderung der Daten denkbar. In aller Regel wird es aber am unmittelbaren Vermögensschaden gefehlt haben. Eine Strafbarkeit wegen der Urkundenfälschung kam jedenfalls nicht in Betracht.[17]

Diese Schutzlücke im Vergleich zu klassischen Schriftstücken hat der Gesetzgeber mit dem StRÄG 2002 geschlossen: Wer heute falsche Daten herstellt oder Daten mit dem Vorsatz verfälscht, dass sie im Rechtsverkehr zum Beweis eines Rechtes, eines Rechtsverhältnisses oder einer Tatsache gebraucht werden, kann sich nach § 225a StGB (Datenfälschung) strafbar machen. Die Datenfälschung wurde als Paralleltatbestand zur Urkundenfälschung nach § 223 StGB konzipiert. Dennoch gibt es einen wesentlichen Unterschied. Während § 223 Abs 2 StGB die Verwendung einer falschen oder verfälschten Urkunde eigenständig unter Strafe stellt, fehlt eine entsprechende Regelung in § 225a StGB für die Verwendung falscher oder verfälschter Daten. Für ihre Verwendung gilt daher nach wie vor, dass sie grundsätzlich straflos bleibt, sofern nicht durch die Verwendung überhaupt ein anderer Tatbestand erfüllt wird. Wer falsche oder verfälschte Daten iSd § 225a StGB für einen Betrug verwendet, der macht sich allerdings sogar wegen der Qualifikation des § 147 Abs 1 Z 1 StGB strafbar.

1.2. DELIKTE IM VORFELDBEREICH

1.2.1. Die bisher genannten Delikte werden insbesondere seit dem StRÄG 2002 durch Tatbestände im Vorbereitungsbereich ergänzt: Zum einen geht es um das Eindringen in fremde Computersysteme und das Auskundschaften von Daten, die für irgendwelche Taten in den bislang genannten Bereichen verwendet werden können. Diese Vorbereitungsdelikte sind va der widerrechtliche Zugriff auf ein Computersystem (§ 118a StGB) und das missbräuchliche Abfangen von Daten (§ 119a StGB). § 118a StGB ist als spezifisches Delikt für das Eindringen in fremde Computer gedacht. Dennoch sei aber darauf hingewiesen, dass auch nach diesem speziellen Tatbestand das bloße Eindringen nicht generell mit strafrechtlicher Sanktion belegt wird. Vielmehr macht sich nach § 118a StGB nur strafbar, wer folgende "Checkliste" erfüllt:

- Der Täter dringt in ein Computersystem oder einen Teil eines Systems ein, über das er nicht allein verfügen darf.
- Er dringt ein und verletzt dabei Sicherheitsvorkehrungen, die
  - im Computersystem angebracht und
  - spezifische Sicherungen sind.
- Der Täter handelt mit dem Vorsatz auf die eben beschriebene Tathandlung.
- Der Täter hat darüber hinaus die Absicht, sich von Daten Kenntnis zu verschaffen, die

- im System abgespeichert sind und
- nicht für ihn bestimmt sind.

- Der Täter beabsichtigt außerdem, diese Daten selbst zu verwenden, sie einem anderen Unbefugten zugänglich zu machen oder zu veröffentlichen.
- Und schließlich: Dem Täter kommt es darüber hinaus darauf an, durch diese Datenverwendung sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einen anderen zu schädigen.

Der Gesetzgeber hat aber im Jahr 2002 auch noch andere spezifische Vorbereitungsdelikte eingeführt. Noch eine Stufe weiter im Vorfeld ist § 126c StGB (Missbrauch von Computerprogrammen und Zugangsdaten) einzuordnen. § 126c StGB erfasst, vereinfacht gesagt, das Herstellen und Vertreiben von schädlichen Computerprogrammen wie zB von Computerviren oder Programmen zum Knacken von Passwörtern.[18]

1.2.2. Ein ähnliches Delikt findet sich auch im Nebenstrafrecht im § 10 ZuKG.[19] Danach macht sich strafbar, wer gewerbsmäßig so genannte Umgehungsvorrichtungen ua vertreibt, herstellt und einführt. Als Umgehungsvorrichtung gelten Mechanismen, die einen unentgeltlichen Zugang zu einem vom ZuKG geschützten Dienst, zB entgeltliche passwortgeschützte Datenbanken oder Zeitungsabonnements, ermöglichen, wobei freilich keine Zustimmung des Diensteanbieters vorliegt (§ 2 Z 8 ZuKG).

Ein typischer Strafbarkeitsfall ist der missbräuchliche Zugang zu Pay-TV-Diensten.

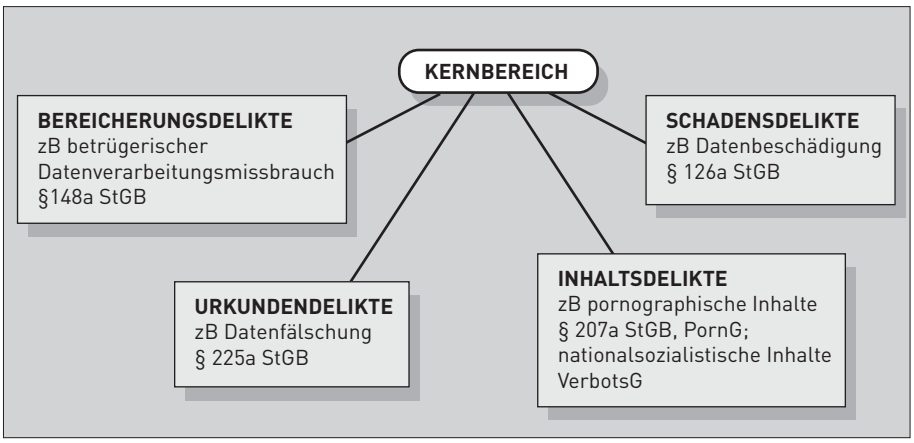
Der rechtmäßige Nutzer schließt mit dem Anbieter einen Vertrag über den Bezug von Programmen ab und erhält daraufhin die Berechtigung, mittels der erforderlichen technischen Einrichtungen (Decoder, Smartcard) die an sich verschlüsselt ausgesendeten Programme zu entschlüsseln und auf diese Weise zu konsumieren. Der Straftäter im Sinne des ZuKG stellt nun beispielsweise ohne Zustimmung des Fernsehanbieters gewerbsmäßig solche Berechtigungskarten (Smartcards) her oder vertreibt sie. Sogar die gewerbsmäßige Innehabung von Umgehungsvorrichtungen wird mit gerichtlicher Strafe bedroht (§ 10 Abs 2 ZuKG). Damit ist etwa gemeint, dass jemand eine illegale Smartcard verwendet und die mit ihrer Hilfe entschlüsselten Signale gegen Gebühren anderen Nutzern zur Verfügung stellt.[20] Lediglich derjenige, der bloß zum privaten Gebrauch eine solche Umgehungsvorrichtung einführt, erwirbt oder sich sonst verschafft (damit freilich auch besitzt), bleibt aufgrund der ausdrücklichen Anordnung in § 10 Abs 3 ZuKG straflos.[21]

1.2.3. Die neueste Schicht des Computerstrafrechts betrifft die Entfremdung und Fälschung von unbaren Zahlungsmitteln. Zwar sind diese Tatbestände nicht unmittelbar EDV-spezifisch, doch spielt der Einsatz von EDV-Mitteln gerade bei der Fälschung unbarer Zahlungsmittel eine große Rolle, weshalb die neuen Bestimmungen auch als Teil des EDV-Strafrechts angesehen werden sollten. Mit dem StRÄG 2004 wurden eigene Bestimmungen gegen die Fälschung und Entfremdung von unbaren Zahlungsmitteln als Vorbereitungshandlungen für spätere missbräuchliche Vermögensverschiebungen in Umsetzung europarechtlicher Vorgaben[22] geschaffen.[23]

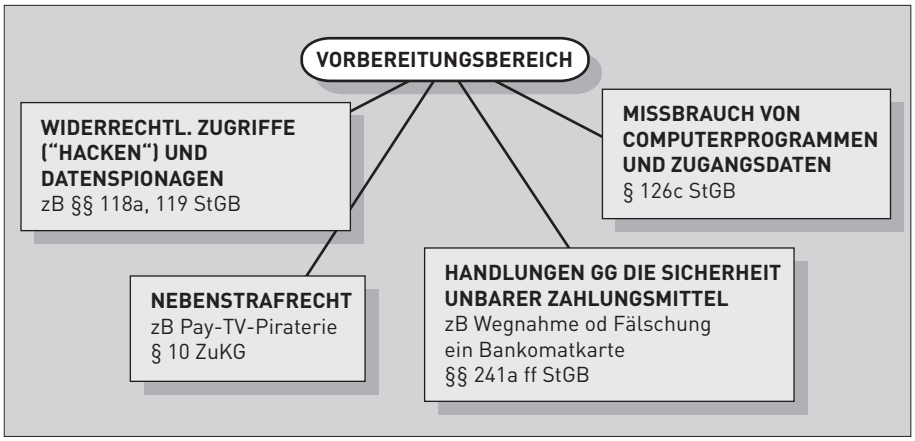
1.3. ABSCHLIESSENDE DARSTELLUNG

In der folgenden Darstellung wird das beschriebene System noch einmal abgebildet.

Grafik: Reindl



Grafik: Reindl



2. DIE ANWENDUNG DES COMPUTERSTRAFRECHTS AUF DAS PHÄNOMEN "PHISHING"

2.1. FAKTISCHER ABLAUF

In letzter Zeit tritt dieses Phänomen Berichten zufolge verstärkt auf. Bei Phishing-Attacken in ihrer ursprünglichen Form wurden E-Mails an die potentiellen Opfer verschickt, die scheinbar von Bankinstituten stammten. Dem Empfänger wurde in den Mails erklärt, es gäbe ein Sicherheitsproblem bei seiner Bank. Um dieses Problem zu beheben, sei es nötig, dass er seinen Pin-Code und allfällige weitere Daten für Telebankingvorgänge, zB Transaktionsnummern, auf der Homepage der Bank eingebe. Die Adresse der Homepage wurde im Mail ebenfalls angegeben. Rief der Empfänger nun tatsächlich die angegebene Internetadresse auf und gab die gewünschten Bankdaten ein, so wurden diese Daten abgefangen und im Anschluss dafür verwendet, das betreffende Konto – idR mittels Überweisung – zu plündern.

In Wahrheit stammten die Mails nicht von Bankinstituten, sondern von Phishing-Tätern.

Der etwas sensibilisierte Mailempfänger kann bei dieser Vorgehensweise in aller Regel noch relativ leicht erkennen, dass es sich um eine Fälschung handelt. Zum einen deuten nämlich trotz relativ guter formaler Gestaltung der meisten Mails vielfach Fehler in der Orthographie auf die Fälschung hin. Zum anderen haben österreichische Institute ihre Kunden bereits

mehrfach darauf hingewiesen, dass sie derart sensible Kundendaten nicht per E-Mail anfragen würden.

In letzter Zeit wurden aber auch Mails verschickt, die den Zusammenhang mit geplanten Finanztransaktionen nicht so leicht erkennen lassen. So war etwa einer Meldung in der Wiener Zeitung zu entnehmen, dass Mails verschickt wurden, in denen angebliche BBC-Berichte angekündigt wurden.[24] Wer den ganzen Artikel lesen wollte, musste die BBC-Homepage aufrufen, deren (vermeintliche) Adresse im Mail angegeben war. Die Opfer, die diese Adresse anklickten, gelangten auf eine sehr gut gefälschte Homepage, die tatsächlich auch den entsprechenden Artikel in voller Länge enthielt. Während der User diesen Artikel las, installierte sich aber ein bösartiges Computerprogramm auf seinem PC.

Dieses Programm wurde aktiviert, sobald der User die Internetseite eines Finanzinstitutes aufrief und Transaktionen tätigen wollte.

PIN und TAN wurden mitprotokolliert und die Verbindung zum Institut unterbrochen, so dass die vom User gewünschte Transaktion nicht mehr durchgeführt wurde. Während sich das Opfer noch über die Probleme im Aufbau der Internetverbindung wunderte, wurden die entsprechenden Berechtigungsdaten für kriminelle Vermögensverschiebungen verwendet. Im Ergebnis wurden auch hier die Konten mittels Online-Überweisung geplündert.

2.2. RECHTLICHE BEURTEILUNG

2.2.1. PHISHING IN KLASSISCHER FORM

Bei diesen Vorgängen stellt sich nun die Frage, ob und gegebenenfalls ab wann strafrechtliche Sanktionen zum Tragen kommen. Zunächst soll dabei die klassische Variante beurteilt werden, bei der der Täter sein Opfer ohne Hilfe eines Trojaners dazu bringt, die gewünschten Daten selbst auf der gefälschten Homepage bekannt zu geben.

Der faktische Ablauf zerfällt in mehrere Stadien: Zuerst werden Mails verschickt mit der Aufforderung, die Daten auf der Homepage einzugeben. Erst im zweiten Handlungskomplex werden diese Daten auch tatsächlich für Vermögensverschiebungen genutzt.

Die eigentliche unbefugte Vermögenstransaktion ist strafrechtlich leicht einzuordnen. Unter Verwendung der Zahlungsdaten wird sie typischerweise als Online-Überweisung durchgeführt. Die Umbuchung erfolgt in diesem System bargeldlos und voll automatisch.

Es handelt sich somit um keine Entfremdung körperlicher Sachen, weshalb Diebstahl (§ 127 StGB) ausscheidet.

Da der Täter seine Berechtigung zur Überweisung zwar fälschlich vorgibt, er aber bei einem solchen automatischen Ablauf keinen Menschen täuscht, ist auch nicht vom Vorliegen eines Betrugs auszugehen. Denn dieser kann nach hM nur angenommen werden, wenn der Täter einen Menschen durch Täuschung über Tatsachen in die Irre führt.[25]

Nichtsdestotrotz ist das vorliegende Geschehen täuschungs- und betrugsähnlich: Der Täter gibt durch die Eingabe der Daten dem System gegenüber vor, der verfügungsbefugte Kontoinhaber oder zumindest ein von diesem Ermächtigter zu sein, was freilich nicht stimmt. Weil aber die Daten tatsächlich dem Konto zugewiesen sind und sich keine gegenteiligen Angaben

im System finden, die gegen die Verfügungsberechtigung sprechen, sind im System aufgrund der täuschungsgleichen Dateneingabe alle Voraussetzungen für die Überweisung gegeben. Dieser Programmschritt wird sozusagen aufgrund irrtumsgleicher Motivation gesetzt. Darin liegt auch die Parallele zur Selbstschädigung des Opfers beim klassischen Betrug. Aufgrund dieser Betrugsähnlichkeit sind solche Fälle daher unter den betrügerischen Datenverarbeitungsmissbrauch nach § 148a StGB zu subsumieren.[26] Überdies wird der Täter typischerweise auch mit dem erforderlichen Vorsatz handeln.

Es stellt sich allerdings die Frage, ob nicht bereits auch der erste Handlungskomplex, also die Datenspionage, eine eigenständige Strafbarkeit begründen kann.

Das Herauslocken der Daten lässt zunächst vielleicht sogar an Betrug nach § 146 StGB denken, immerhin wird das Opfer anfangs getäuscht und am Ende steht der Vermögensschaden.

Betrug setzt aber eine Täuschung des Opfers voraus, die unmittelbar zu einer selbstschädigenden Vermögensverschiebung führt.[27] Muss der Täter hingegen nach der Täuschung noch selbst weitere Handlungen setzen, um letztlich einen Vermögensschaden herbei zu führen, fehlt es an der für den Betrug charakteristischen unmittelbaren Selbstschädigung. Im vorliegenden Fall verändert sich die Vermögenssituation des Opfers durch die Bekanntgabe der Daten noch nicht. Erst durch die nachfolgende Verwendung der Daten bei der Überweisung vom Konto des Opfers auf ein vom Täter ausgewähltes anderes Konto tritt ein effektiver Vermögensschaden ein. Mangels selbstschädigender Vermögensverfügung scheidet eine Betrugsstrafbarkeit für das Herauslocken der Daten aus.

Zu denken wäre an ein weiteres Delikt, das an eine Täuschung über Tatsachen anknüpft, nämlich die Täuschung nach § 108 StGB. Allerdings muss der Täter das Opfer auch hier durch die Täuschung zu einer Selbstschädigung bringen, nämlich dazu, sich in einem Recht zu schädigen. Als Recht, das bereits durch die Datenherausgabe beeinträchtigt wird, kommt allenfalls ein Recht auf Wahrung des Geheimnisses an PIN und TAN in Frage. Schon die Existenz eines solchen eigenständigen (strafrechtlich geschützten) Rechtes erscheint allerdings zweifelhaft. Selbst jene Delikte, die ausdrücklich die Verletzungen der Privat- und Geheimnissphäre unter Strafe stellen (§§ 118 ff StGB; § 51 DSG), lassen nämlich die bloße Verletzung des Rechts auf Wahrung der Geheimnissphäre für die Strafbarkeit nicht ausreichen, sondern verlangen durchwegs zusätzliche (zumindest beabsichtigte) Beeinträchtigungen.[28]

Darüber hinaus muss es dem Täter aber nach § 108 StGB gerade darauf ankommen, das Opfer in diesem Recht zu schädigen. Im Vordergrund steht aber nicht die absichtliche Verletzung der Geheimsphäre des Opfers. Vielmehr beabsichtigt der Täter die spätere Vermögenstransaktion und somit die Vermögensschädigung des Opfers. Daher ist § 108 StGB für die Datenspionage als solche idR keine geeignete Strafnorm.

Da die PIN ein zumindest indirekt personenbezogenes Datum ist, könnte man auch an die Strafnorm des Datenschutzgesetzes denken. § 51 DSG (Datenverwendung in Gewinn- oder Schädigungsabsicht) normiert als Tathandlung allerdings erst die Verwendung der personenbezogenen Daten, nicht schon deren widerrechtliche Erlangung. Diese bildet grundsätzlich bloß eine Vorbereitungshandlung in Bezug auf § 51 DSG. Soll die Verwendung dem Ver-

schaffen unmittelbar folgen, könnte je nach Fallkonstellation möglicherweise bereits ein Versuch des § 51 DSG gegeben sein. Dennoch kann § 51 DSG nicht als passende Strafnorm für den Regelfall des "bloßen" Ausspionierens der Daten angesehen werden, weil im Ausspionieren selbst eben noch keine Verwendung der Daten liegt. Diese erfolgt vielmehr erst später, nämlich bei der Vermögenstransaktion.

Schließlich könnte man noch eine Strafbarkeit des Auskundschaftens nach § 126c StGB (Missbrauch von Computerprogrammen und Zugangsdaten) erwägen. § 126c Abs 1 Z 2 StGB stellt nämlich ua denjenigen unter Strafe, der sich ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen, mit dem Vorsatz verschafft, dass eine der im § 126c Abs 1 Z 1 StGB aufgezählten Straftaten begangen werde. Von den in § 126c aufgezählten Taten kommt als Delikt dafür nur § 148a StGB in Frage. In aller Regel wird – wie schon oben dargestellt – die nachfolgende Vermögensverschiebung ohnedies als betrügerischer Datenverarbeitungsmissbrauch nach § 148a StGB zu beurteilen sein. Diese Voraussetzung des § 126c StGB wäre also erfüllt.[29]

Bei den von den Tätern ausspionierten PIN- und TAN-Daten handelt es sich jedenfalls auch um Passwörter. Problematisch ist allerdings, ob es solche Daten sind, die einen Zugang zu einem Computersystem oder einen Teil davon ermöglichen. Der klassische Zugangscode ermöglicht es dem Nutzer ein System in Betrieb zu nehmen und etwa Daten hinzuzufügen, zu löschen, kurz die Funktionalitäten eines Computersystems umfassend zu nutzen.

Das typische Beispiel für diese Art Zugangscode ist das individuelle Passwort, das es dem Einzelnen ermöglicht, seinen PC vor Unbefugten zu schützen.

Bei Eingabe des Passwortes wird das System aktiviert und der PC kann genützt werden. Dabei kann der Nutzer umfassenden Zugriff auf das System erhalten, zB weil es sich um seinen privaten Laptop handelt und er Alleineigentümer und alleiniger Nutzer dieses Geräts ist. Der Nutzer kann aber auch bloß teilweisen Zugriff erhalten. Das wäre etwa der Fall, wenn sich mehrere Arbeitnehmer ein Gerät teilen, auf dem verschiedene Benutzerkonten eingerichtet sind. Die persönlichen Kennungen könnten in einem solchen Fall so eingerichtet werden, dass der Zugangscode nur den Zugang zu einem Teil des Systems eröffnet, indem beispielsweise nur die eigenen Dateien der angemeldeten Person anzeigt werden, nicht aber jene des zweiten Gerätenutzers.

In diesem Zugang zu bloßer Teilnutzung könnte ein Ansatz für die Strafbarkeit der gegenständlichen Datenspionage nach § 126c StGB gefunden werden.

Denn der PIN-Code, mit dem sich der Nutzer für die Durchführung von Online-Transaktionen anmeldet, eröffnet dem Nutzer das Online-Finanzsystem soweit, dass er zumindest einen Teil nutzen und darauf zugreifen kann, nämlich jenen Teil des Computersystems, der für die Durchführung von Transaktionen durch im System angemeldete Kunden vorgesehen ist. Mit anderen Worten ermöglicht der Code die Nutzung einer bestimmten Finanzfunktionalität des Online-Banking-Sys-

tems. Dass der Zugriff bloß auf einen Teil des Systems eröffnet wird, schadet nicht, sondern reicht nach dem Wortlaut des § 126c Abs 1 Z 2 StGB vielmehr ausdrücklich aus.[30]

Folgt man dieser Auffassung, so besteht eine eigenständige Strafbarkeit für das Ausspionieren der Daten für jenen Fall, in dem die geplante spätere Vermögenstransaktion das Tatbild des § 148a StGB verwirklichen würde. Andere Vermögensdelikte, wie etwa Betrug oder Diebstahl, sind hingegen nicht in § 126c StGB genannt. Werden Zahlungs- und Finanzdaten also ausspioniert, um solche Taten zu begehen, bleibt die Spionage für sich ohne eigene Strafbarkeit.[31] In solchen Fällen wird erst die vermögensschädigende Handlung strafrechtlich relevant.

2.2.2. PHISHING MIT HILFE EINES "BÖSARTIGEN" COMPUTERPROGRAMMS

Die obigen Ausführungen treffen auch auf den zweiten geschilderten Sachverhalt zu, also beim Phishing nach Einsatz eines Trojaners, der sich am PC des Opfers installiert und sodann gegebenenfalls Finanzdaten mitprotokolliert und an die Täter übermittelt. Allerdings könnte man zusätzlich eine Strafbarkeit wegen § 118a StGB oder §§ 119 oder 119a StGB überlegen.

§ 118a StGB bestraft den widerrechtlichen Zugriff auf ein Computersystem. Entsprechend der im ersten Abschnitt dieses Beitrags angeführten Checkliste müssen für die Strafbarkeit aber verschiedene Voraussetzungen gegeben sein: Dass der Täter in ein System oder einen Teil eines Systems eindringt, über das er nicht allein verfügen darf, wird in aller Regel gegeben sein. Aber schon die zweite Anforderung – Verletzen von spezifischen Sicherheitsvorkehrungen im Computersystem – wird in der Praxis aber oftmals dazu führen, dass die Strafbarkeit nach § 118a StGB zu verneinen ist: Zum einen setzt § 118a StGB voraus, dass eine spezifische Sicherung im Computersystem angebracht ist.

Bedauerlicherweise sind aber immer noch viele va private Geräte ohne jede Sicherung. Damit fallen sie aus dem Schutzbereich der Strafnorm hinaus.

Zum anderen muss der Täter die Sicherheitsvorkehrung verletzen. Nützt der Täter zur Installation seines bösartigen Programms aber bloß etwaige Sicherheitslücken aus, dann verletzt er keine Sicherheitsvorkehrung, weil diesbezüglich keine solche besteht. Er sucht dann bildlich gesprochen bloß nach unversperrten Eingängen und spaziert hindurch. Dieses bloße Ausnützen von Sicherheitslücken reicht nach der Entstehungsgeschichte[32] und dem Wortlaut für die Subsumtion nicht aus. Geübte Täter, von denen wohl bei groß angelegten Phishing-Attacken auszugehen ist, werden kaum eine Firewall oder ein Passwort tatsächlich umprogrammieren und knacken, was einem Verletzen gleichkommt. Solche Vorgehensweisen sind technisch zu aufwendig und in Anbetracht allfälliger "offener Zugänge" in die PCs aus Tätersicht auch gar nicht notwendig.

Sollte allerdings eine technische Variante gewählt werden, bei der tatsächlich eine spezifische Sicherung zerstört oder beschädigt wird[33], dann stellt sich noch die Frage, ob die relevanten Daten im attackierten System gespeichert sind. Werden sie nämlich erst bei der Transaktion selbst eingegeben und erfolgt der Zugriff auf diese Daten zeitgleich durch das bösartige Programm, so kann kaum von "im System gespeicherten Daten" gesprochen werden, wie dies der Wortlaut des § 118a StGB aber verlangt.

Aufgrund dieser Umstände erscheint eine Strafbarkeit nach § 118a StGB für die Datenspionage beim Phishing wenig wahrscheinlich.

Sollte aber ausnahmsweise eine Konstellation vorliegen, bei der der Zugriff auf bereits abgespeicherte Daten tatsächlich unter Verletzung einer spezifischen Sicherheitsvorkehrung erfolgt, dürfte der Rest der Checkliste bei Phishingtätern kaum mehr Schwierigkeiten bereiten. Denn die Daten sind nicht für die Täter bestimmt und sie beabsichtigen auch die gewinnbringende Verwendung der ausspionierten Daten.[34]

Zu überlegen bleibt noch eine allfällige Strafbarkeit nach §§ 119 oder 119a StGB für das Mitprotokollieren der Zahlungsdaten. So lange es nur um PINs und TANs geht, scheidet § 119 StGB (Verletzung des Telekommunikationsgeheimnisses) von vornherein aus, stellt er doch auf die Übertragung von Nachrichten ab, was bei der bloßen Abfolge von Berechtigungsdaten wohl nicht vorliegt.

§ 119a StGB (missbräuchliches Abfangen von Daten) hingegen sanktioniert das Abfangen von Daten unabhängig von deren gedanklichem Inhalt. Für eine Strafbarkeit nach § 119a StGB ist entscheidend, ob die Daten gleichsam auf ihrem Übertragungsweg ausgeforscht werden oder nicht. Denn § 119a StGB schützt – so wie auch § 119 StGB – nur das Übertragungsgeheimnis. Über die Strafbarkeit entscheidet somit der Zeitpunkt der Spionage. Nur der technische Zugriff auf die Daten am Übertragungsweg erfüllt den objektiven Tatbestand.

Zu beachten ist auch bei § 119a StGB der extrem umfangreiche erweiterte Vorsatz, der der dreifachen Absichtlichkeit des § 118a StGB entspricht. Wählt ein Phishing-Täter allerdings eine technische Variante, die die Spionage am Übertragungsweg durchführt, sollte der erweiterte Vorsatz kaum je Probleme bereiten. Denn in aller Regel hat der Täter neben der Spionageabsicht auch die Absicht, die Daten bei einer späteren Überweisung für sich gewinnbringend und für andere schädigend zu nutzen.

[1] *Angaben aus dem Bericht über das zweite Quartal 2006 des Austrian Internet Monitor (www.integral.co.at; abgerufen am 26.09.2006).*

[2] *BGBl I 134/2002.*

[3] *BGBl I 15/2004.*

[4] *Rahmenbeschluss über Angriffe auf Informationssysteme vom 24.02.2005, ABl L 69 vom 16.03.2005.*

[5] *OGH 12 Os 45/06v vom 01.06.2006.*

[6] *OGH 15 Os 99/05f vom 13.10.2005.*

[7] *OGH EvBl 1998/35 = JBl 1998, 738 mAnm Bertel und Burgstaller.*

[8] *OGH 15 Os 131/95 vom 14.12.1995.*

[9] *Statt vieler OGH RZ 1997/50; dagegen ua S. Reindl, E-Commerce und Strafrecht, Wien/Graz (2003), 23 ff mit ausführlicher Begründung.*

[10] *Textnachrichten am Mobiltelefon.*

[11] *Dazu und zu weiteren Missbrauchsfällen im Telefonverkehr siehe S. Reindl, E-Commerce und Strafrecht, Wien/Graz (2003), 191-206.*

[12] *BGBl I 70/2003.*

[13] *Reindl, WK-StGB²(2005) § 126b Rz 18-20.*

[14] *BGBl I 2004/15.*

[15] *EBRV 294 BlgNR XXII.GP zu § 207a.*

[16] *Näher zur Schriftform Kienapfel/Schroll, WK-StGB2 (2006), § 223 Rz 28-36.*

[17] *Nur wenn der Täter das E-Mail weiter verwendete und zB als Täuschungsmittel bei einem Betrug einsetzte, war wiederum an Strafbarkeit zu denken.*

[18] *Näher dazu noch unten im Teil II.*

[19] *BGBl I 60/2000.*

[20] *EBRV 99 BlgNR XXI.GP zu § 10.*

[21] *Auch das unbefugte Konsumieren der Pay-TV-Sendung selbst ist nicht strafbar, auch nicht nach § 148a StGB (zur ausführlichen Begründung siehe S. Reindl, E-*

Commerce und Strafrecht, Wien/Graz (2003), 177-187, aA Engin-Deniz/Grünzweig, Pay-TV-Piraterie im Strafrecht, ecolex 2001, 587).

[22] *Rahmenbeschluss zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln vom 28.05.2001, ABl L 149 vom 02.06.2001.*

[23] *Dazu ausführlich bei Schroll, WK-StGB² § 74 Abs 1 Z 10 und §§ 241a ff.*

[24] *Regner/Hacker ködern mit BBC-Nachrichten, Artikel vom 31.03.2006, Wiener Zeitung Online (www.wienerzeitung.at; 26.09.2006).*

[25] *So schon F. Nowakowski, Das österreichische Strafrecht in seinen Grundzügen, (1955), 183. Freilich ist es nicht auszuschließen, dass ausnahmsweise die ausspionierten Daten einem Menschen gegenüber täuschend eingesetzt werden, um vermögenswerte Leistung zu erzielen. Dann käme Betrug nach §§ 146 ff StGB in Betracht.*

[26] *Zum Kriterium der Betrugsähnlichkeit siehe ausführlich S. Reindl, E-Commerce und Strafrecht, Wien/Graz (2003), 40 ff; zur Subsumtion von Online-Transaktionen unter § 148a StGB auch Kirchbacher/Presslauer, WK-StGB² (2006), § 148a Rz 28.*

[27] *Fuchs/Reindl, Strafrecht Besonderer Teil I, 145. Kienapfel/Schmoller, Studienbuch Strafrecht Besonderer Teil II § 146 Rz 6 ff.*

[28] *Vgl zB § 118a StGB, der im objektiven Tatbestand neben dem simplen Eindringen in die Privatsphäre die Verletzung spezifischer Sicherheitsvorkehrungen im Computersystem und im subjektiven Tatbestand Verwendungs- und Gewinn- bzw Schädigungsabsicht verlangt.*

[29] *Ist dieser Vorsatz nicht nachweisbar, sondern etwa ein Vorsatz im Sinne des § 146 StGB, scheidet § 126c StGB schon aus diesem Grund aus.*

[30] *Siehe dazu schon Reindl, WK-StGB² (2005) § 126c Rz 10.*

[31] *Zu denken ist freilich bei gegebenem örtlichen, zeitlichen und aktionsmäßigen Zusammenhang an die Strafbarkeit wegen des Versuchs des nachfolgenden Vermögensdelikts.*

[32] *EBRV 1166 BlgNR XXII.GP 24.*

[33] *Diesfalls wäre im Übrigen auch an Datenbeschädigung (§ 126a StGB) zu denken.*

[34] *Zu den einzelnen Tatbestandsmerkmalen des § 118a StGB siehe Reindl, WK-StGB² (2004) § 118a.*

[35] *Reindl, WK-StGB² (2004) § 119a Rz 1.*