Phishing, Pharming und Identitätsdiebstahl – von Postbank bis Paypal

Seminararbeit zu Thema Nr. 2
des Seminars

Informationstechnische Grundlagen und strafrechtliche Beurteilung der Internetkriminalität

Vorgelegt von:
David Schneider
Mauermattenstraße 20
79183 Waldkirch
Matrikelnummer:1800408
SPB: 8
Studienjahr: 2006/2007

Angefertigt bei Prof. Dr. Ulrich Sieber
an der
Universität Freiburg

Inhaltsverzeichnis

Literaturverzeichnis

Borges, Georg	Rechtsfragen des Phishing – Ein Überblick, NJW 2005, S. 3313ff. (zit. Borges, NJW 2005)
Buggisch, Walter Kerling, Christoph	„Phishing“, „Pharming“ und ähnliche Delikte, Kriminalistik 2006, S. 531ff. (zit. Buggisch/Kerling, Kriminalistik 2006)
Buggisch, Walter	Fälschung beweiserheblicher Daten durch Verwendung einer falschen E-Mail-Adresse, NJW 2004, S. 3519ff (zit. Buggisch, NJW 2004)
Creifelds, Carl	Rechtswörterbuch, 17. Auflage, München 2002 (zit. Creifelds)
Ekey, Friedrich Klippel, Diethelm	Heidelberger Kommentar zum Markenrecht, Heidelberg 2003 (zit. Ekey/Klippel-Bearbeiter)
Fox, Dieter	Phishing, DuD 2005, S. 365 (zit. Fox, DuD 2005)
Gajek, Sebastian Schwenk, Jörg Wegener, Christoph	Identitätsmissbrauch im Onlinebanking, DuD 2005, S. 639ff. (zit. Gajek/Schwenk/Wegener, DuD 2005)
Gercke, Marco	Die Strafbarkeit von „Phishing“ und Identitätsdiebstahl, CR 2005, S. 606ff. (zit. Gercke, CR 2005)
Hilgendorf, Eric Frank, Thomas Valerius, Brian	Computer- und Internetstrafrecht, Berlin 2005 (zit. Hilgendorf/Frank/Valerius, Computer- u. Internetstrafrecht)
Hilgendorf, Eric	Grundfälle zum Computerstrafrecht, JuS 1997, S. 130ff. (zit. Hilgendorf, JuS 1996)

Joecks, Wolfgang	Studienkommentar StGB, 6. Auflage, München 2005 (zit. Joecks)
Kind, Michael Werner, Dennis	Rechte und Pflichten im Umgang mit PIN und TAN, CR 2006, S. 353ff. (zit. Kind/Werner, CR 2006)
Kindhäuser, Urs Nikolaus, Sonja	Der Tatbestand des Betrugs (§ 263 StGB), JuS 2006, S. 293ff. (zit. Kindhäuser/Nikolaus, JuS 2006)
Kloepfer, Mathias	Informationsrecht, München 2002 (zit. Kloepfer, Informationsrecht)
Knupfer, Jörg	Phishing for money, MMR 2004, S. 641ff. (zit. Knupfer, MMR 2004)
Küper, Wilfried	Strafrecht Besonderer Teil Definitionen mit Erläuterungen, 6. Auflage, Heidelberg 2005 (zit. Küper, BT)
Lackner, Karl Kühl, Kristian	Strafgesetzbuch Kommentar, 25. Auflage, München 2004 (zit. Lackner/Kühl)
Malek, Klaus	Strafsachen im Internet, Heidelberg 2005 (zit. Malek, Strafsachen im Internet)
Mankowski, Peter	Für einen Anscheinsbeweis hinsichtlich der Identität des Erklärenden bei E-Mails, CR 2003, S. 44ff. (zit. Mankowski, CR 2003)
Marberth-Kubicki, Annette	Computer- und Internetstrafrecht, München 2005 (zit. Marberth-Kubicki, Computer- und Internetstrafrecht)

Popp, Andreas	Von „Datendieben“ und „Betrügern“ – Zur Strafbarkeit des so genannten „phishing“, NJW 2004, S. 3517ff (zit. Popp, NJW 2004)
ders.	„Phishing“, „Pharming“ und das Strafrecht, MMR 2006, S. 84ff. (zit. Popp, MMR 2006)
Rengier, Rudolf	Strafrecht Besonderer Teil I Vermögensdelikte, 7. Auflage, München 2005 (zit. Rengier, BT I)
Roßnagel, Alexander Pfitzmann, Andreas	Der Beweiswert von E-Mail, MMR 2003, S. 1209ff. (zit. Roßnagel/Pfitzmann, MMR 2003)
Rudolphi, Hans Joachim Horn, Eckard Samson, Erich	Systematischer Kommentar zum Strafgesetzbuch: Band II Besonderer Teil, 7. Auflage, Neuwied 2005 (zit. SK-Bearbeiter)
Schönke, Adolf Schröder, Horst	Strafgesetzbuch Kommentar, 27. Auflage, München 2006 (zit. Sch/Sch-Bearbeiter)
Tröndle, Herbert Fischer, Thomas	Strafgesetzbuch und Nebengesetze - Kommentar, 53. Auflage, München 2006 (zit. Tröndle/Fischer)
Weber, Roman	Phishing: Brauchen wir einen Sondertatbestand zur Verfolgung des Internetphishings?, HRRS 2004 S. 406ff. (zit. Weber, HRRS 2004)
Wessels, Johannes Beulke, Werner	Strafrecht Allgemeiner Teil, 33. Auflage, Heidelberg 2003 (zit. Wessels/Beulke AT)

Anlagenverzeichnis

A. Einführung

Das Internet boomt nach wie vor. Verfügten im Jahre 1999 nur knapp 12 % der Bevölkerung über einen Internetzugang, sind es 2006 schon 66 %.[1] Mit steigenden Nutzerzahlen wächst auch der elektronische Geschäftsverkehr. 60 % der Internetnutzer kaufen regelmäßig Produkte und Dienstleistungen über das Internet, und 50 % verfügen über ein Bankkonto im Online-Banking.[2] Zwar vereinfacht die steigende Vernetzung viele alltägliche Geschäfte, doch führt sie auch zu einer enormen Bedrohung des Nutzers und seiner, oftmals sensiblen, Daten.[3] Konzentrierten sich Hacker anfänglich noch auf die Verbreitung destruktiver Viren, zielen die neuen Angriffe meist auf eine finanzielle Schädigung des Opfers, oder auf das Sammeln vertraulicher Daten, ab.[4] Hierbei tritt das so genannte Phishing verstärkt in Erscheinung. Ziel der Täter ist es hierbei den betroffenen Internetnutzer zur Preisgabe von Daten zu bewegen, mit deren Hilfe vermögensrelevante Verfügungen zu Lasten des Nutzers vorgenommen werden können.[5]

Die Täter versenden bspw. E-Mails unter einer dem Empfänger bekannten oder seriös erscheinenden Absenderadresse, und versuchen das Opfer auf diesem Wege zur gutgläubigen Preisgabe wichtiger Informationen, etwa Passwörtern, ID-Kennungen, oder der im elektronischen Zahlungsverkehr verwendeten PINS und TANS, zu bewegen. Der durch solche Phishing Attacken verursachte Schaden ist kaum abzusehen, offizielle Statistiken liegen derzeit noch nicht vor. Für den Zeitraum von Juni 2004 bis Mai 2005 wird der in den USA durch Phishing verursachte Schaden auf fast 1 Mrd. US-Dollar geschätzt.[6] Laut Nachrichtenmagazin Focus, belief sich der Schaden in Deutschland im Jahre 2005 auf schätzungsweise 4,5 Millionen Euro.[7] Es scheint also notwendig sich dem Phishing Phänomen auch auf juristischer Ebene zu nähern. Neben zivilrechtlichen Haftungsfragen ist vor allem die strafrechtliche Erfassung von Phishing in der Diskussion.[8] Vielfach wird kritisiert, dass das deutsche Strafrecht erst eingreife wenn es zu einer Verwendung der erlangten Daten gekommen ist, die vorbereitenden Handlungen jedoch nicht erfasst werden.[9]

---

[1] http://www.forschungsgruppe.de/Aktuelles/PM_Strukturdaten/ (alle Internetquellen zuletzt überprüft am 25.10.2006).
[2] http://www.forschungsgruppe.de/Aktuelles/PM_Strukturdaten/
[3] Kloepfer, Informationsrecht, S. 20 Rn. 42.
[4] http://www.zdnet.de/security/news/0,39029460,39140194,00.htm.
[5] Marberth-Kubicki, Computer- und Internetstrafrecht, Rn. 118.
[6] www.silicon.de/cpo/news-anitvirus/details.php?nr=2204; Borges, NJW 2005, S. 3313.
[7] http://focus.msn.de/finanzen/banken/phishing_nid_20621.html.
[8] Vgl. etwa Weber, HRRS 2004 , S. 406ff.
[9] So forderte die Bitkom die Einführung eines Phishing Tatbestandes: http://www.at-mix.de/news/713.html.

I. Gang der Untersuchung

Die Seminararbeit untersucht im Rahmen des Seminarthemas, „Informationstechnische Grundlagen und strafrechtliche Beurteilung der Internetkriminalität“, die strafrechtliche Beurteilung von Phishing, insbesondere die Reichweite des deutschen Strafrechts. Nach einigen einführenden Worten zur Begriffsdefinition des Phishing, wird zunächst der „klassische“ Phishing Ablauf dargestellt und sodann strafrechtlich bewertet. Neben dem „klassischen Phishing“ werden im Folgenden einige neue Phishing Varianten vorgestellt und diskutiert. Anschließend wird auf die Zukunft des Phishing und seine Weiterentwicklung, vor allem auf das immer stärker auftretende Pharming, eingegangen. Zuletzt wird dargestellt wie der Phisher an sein Geld kommt, und die Strafbarkeit etwaiger Gehilfen des Phishers untersucht.
Hauptaufgabe der Seminararbeit wird die Beantwortung der Frage sein inwieweit Phishing bereits nach geltendem Recht strafbar ist, und ob ggf. Reformierungsbedarf besteht.

II. Was ist Phishing?

1. Ursprung und Begriffsdefinition

Oftmals wird durch die Medien der Eindruck vermittelt Phishing sei eine komplett neue Form der Kriminalität. Ähnliche Betrugsversuche gab es jedoch schon lange Zeit bevor Internet und E-Mail zum alltäglichen Kommunikationsmittel wurden. In den 80er und 90er Jahren des 20. Jahrhunderts erlebte das sog. „social engineering“ seinen Durchbruch. Unter „social engineering“ versteht man das Erlangen vertraulicher Informationen durch Annäherung an den Geheimnisträger mittels gesellschaftlicher Kontakte.[10]
So gaben sich bspw. Hacker als Mitarbeiter eines Telefonkonzerns aus und erlangten auf diese Weise Passwörter, die es ihnen ermöglichten kostenlose Modemverbindungen herzustellen (Phreaking). Die Anfänge des Phishings reichen bis weit in die 90er Jahre zurück. So wurden anfänglich Nutzer von Instant Messengern, wie bspw. ICQ, aufgefordert ihrer Benutzerdaten in ein E-Mail Formular einzutragen. Auf diese Weise konnten die „Hacker“ den Chat Zugang ihrer Opfer unter deren Identität nutzen.
Die Etymologie des Wortes Phishing ist mindestens genauso umstritten wie seine rechtliche Beurteilung.

[10] Zum Begriff des „social engineering“: http://de.wikipedia.org/wiki/Social_Engineering_%28Sicherheit%29.

Oft wird darauf verwiesen es handle sich um eine Kombination der englischen Wörter „password“ und „fishing“.[11] Andere leiten es von dem englischen Wort „fishing“ (dt. abfischen) ab. Die Ersetzung des Buchstaben f durch Ph stelle lediglich eine Imitation des Wortes „Phreaking“ dar.[12] In Hackerkreisen sei es auch üblich den Buchstaben „f“ durch „ph“ zu ersetzen (sog. leet speak).[13] Was genau hinter der Wortschöpfung Phishing steckt wird nur schwer zu beantworten sein und ist im Rahmen der rechtlichen Beurteilung glücklicherweise irrelevant. Auch hinsichtlich der vom Phishing erfassten Fallgruppen besteht Uneinigkeit. Teile des Schrifttums bezeichnen Phishing als den massenhaften Versand von gefälschten E-Mails, mit deren Hilfe ihre Adressaten zur gutgläubigen Preisgabe von geheimen Zugangsdaten und Passwörtern veranlasst werden sollen.[14] Andere wiederum scheinen Phishing nur auf die täuschungsbedingte Herausgabe der im Onlinebanking verwendeten PINS und TANS zu beschränken.[15]

Zwar zielen ca. 90 % der Phishing Angriffe auf die Preisgabe von Bankdaten ab[16], betroffen sind jedoch auch Internetanbieter und Einzelhändler. Da es die Täter auch auf ebay-Konten, Providerzugangsdaten, usw. abgesehen haben und das Angriffsmuster in den meisten Fällen dem Phishing Angriff auf Zugangsdaten zu Onlinekonten gleicht, scheint es wenig sachgerecht Phishing in seiner Begrifflichkeit lediglich auf den Onlinebanking Fall zu beschränken. Am ehesten lässt sich Phishing als der Versand von E-Mails, der allein aus dem Grund erfolgt den Empfänger der E-Mail zu Preisgabe sensibler Daten zu bewegen[17], beschreiben. Ob die anschließende Verwendung der Daten auch noch unter dem Begriff des Phishing eingeordnet werden kann wird unterschiedlich beantwortet. Einige Autoren behandeln die Erlangung der Daten und die anschließende Nutzung ohne Abgrenzung unter dem Schlagwort Phishing.[18] Teilweise wird lediglich das „Abschwindeln“ der Daten als Phishing verstanden.[19] Die anschließende Verwendung der Daten wird dagegen als Identitätsdiebstahl oder Identitätsmissbrauch bezeichnet.[20] Unter Identitätsdiebstahl versteht man die missbräuchliche Nutzung personenbezogener Daten durch Dritte.

---

[11] Bspw.: Popp, NJW 2004, S. 3517; Malek, Strafsachen im Internet, Rn. 213; Hilgendorf/Frank/Valerius, Computer- u. Internetstrafrecht, Rn. 760.
[12] Fox, DuD 2005, S. 365.
[13] Gercke, CR 2005, S. 606; http://de.wikipedia.org/wiki/Phishing.
[14] Popp, MMR 2006, S. 84; Gercke, CR 2005, S. 606.
[15] Gajek/Schwenk/Wegener, DuD 2005, S. 639; Malek, Strafsachen im Internet, Rn. 213ff.; Kind/Werner, CR 2006, S. 353.
[16] http://www.heise.de/newsticker/meldung/70547.
[17] Gercke, CR 2005, S. 606.
[18] Kind/Werner, CR 2006, S. 353; Borges, NJW 2005, S. 3313.
[19] Popp, NJW 2004, S. 3517;
[20] Gercke, CR 2005, S. 606, (607).

Da der Phisher jedoch meist schon gegenüber seinem Opfer, und nicht erst bei Verwendung dessen Daten, unter einer anderen Identität auftritt macht diese Abgrenzung wenig Sinn. Phishing und Identitätsdiebstahl weisen in ihrer Konzeption gewisse Parallelen auf. Deswegen wird im Folgenden Identitätsdiebstahl als Oberbegriff für alle Delikte, bei denen sich der Täter einer fremden Identität bedient, verstanden.
Gerade weil sich die Methoden und Vorgehensweise der Phisher rasant ändern und weiterentwickeln[21], wird es wohl noch schwerer werden genaue Grenzen und Begriffsdefinitionen zu entwickeln.
Bislang konzentrieren sich die Phishing Angriffe in Deutschland hauptsächlich auf das Versenden von gefälschten E-Mails, mit deren Hilfe der Empfänger auf eine Website geführt wird, die Formularfelder zur Eingabe geheimer Zugangsdaten enthält. Dies wird auch als das klassische Phishing bezeichnet.[22] Konnte man Phishing Mails in der Vergangenheit relativ leicht an zahlreichen Rechtschreibfehlern und schlechtem Deutsch erkennen, werden die Phisher heutzutage zunehmend professioneller. Oftmals werden die Mails sogar graphisch an das Corporate Design des betreffenden Unternehmens angepasst.

2. Der „klassische“ Phishing Ablauf

Der klassische Phishing Angriff besteht in der Regel aus zwei Phasen. Hat es der Phisher auf Zugangsdaten für Onlinekonten abgesehen, sendet er eine Spam E-Mail ungezielt an zahlreiche Empfänger und spekuliert darauf, dass unter den vielen Empfängern auch Kunden der entsprechenden Bank, auf die er es abgesehen hat, sind. Der Inhalt dieser Mails soll regelmäßig einen offiziellen Eindruck gegenüber ihrem Empfänger erwecken und ihn zur Preisgabe seiner Zugangsdaten veranlassen. So wird bspw. behauptet, dass die Bank neue Sicherheitssysteme einführe oder ihr Service-Angebot verbessere, wozu es nötig sei PIN und TAN anzugeben.[23] Diese Phase wird als Trägerangriff oder Trägerphase bezeichnet.[24]
Um das vermeintliche Opfer nun auch zur tatsächlichen Preisgabe seiner Daten zu veranlassen bedarf es eines weiteren Schrittes. Hier stehen dem Phisher nun verschiedene Möglichkeiten offen. In den meisten Fällen ist der E-Mail ein Link beigefügt, der zu einer gefälschten Seite führt die der originären Seite der Bank optisch entspricht.[25]

[21] Siehe bspw.: Der Datenschutz-Berater vom 15.3.2006, S. 7.
[22] Gajek/Schwenk/Wegener, DuD 2005, S. 639 (640).
[23] Ein Beispiel zeigt Abbildung Nr. 1 im Anhang.
[24] Gajek/Schwenk/Wegener, DuD 2005, S. 639 (640)
[25] Ein Beispiel zeigt Abbildung Nr. 2 im Anhang.

Diese Website enthält Formularfelder, in welche der Kunde nun seine Zugangsdaten eingeben soll, die dann an den Phisher weitergeleitet werden. Man bezeichnet diesen zweiten Schritt auch als Täuschungsangriff.[26] Wie schon angedeutet stehen dem Phisher hinsichtlich der Träger- und Täuschungsphase verschiedene Wege offen um an die gewünschten Zugangsdaten zu gelangen.
So kann bspw. die E-Mail selbst Formularfelder zur Eingabe der Daten beinhalten (einer Website bedarf es dann nicht mehr), oder mit einem Trojaner versehen sein, der einen Key Logger auf dem Rechner des Opfers installiert und so die Tastatureingaben protokolliert.
Es soll hier jedoch nicht näher auf andere Methoden eingegangen werden, da dies unter Punkt C der Arbeit besprochen wird.

B. Strafrechtliche Beurteilung des klassischen Phishing

Es stellt sich nun die Frage in wie weit das Versenden der E-Mails und die Erstellung der korrespondierenden Website, neben der sich dem erfolgreichen Phishing Angriff anschließenden Verwendung der Daten, nach geltendem Recht strafbar ist. Die nun folgende strafrechtliche Untersuchung erstreckt sich daher auf das Versenden der E-Mails (I.), die Erstellung der gefälschten Website (II.) und die Nutzung der erlangten Daten (III.).

I. Strafbarkeit des Versendens von Phishing Mails und der Datenerlangung

1. Betrug, § 263 StGB

Da es die Phisher im Regelfall darauf abgesehen haben ihren Opfern einen Vermögensschaden zuzufügen, könnte bereits mit dem Versand der Phishing E-Mail ein Betrug i.S.d. § 263 StGB vorliegen.

a. Tatsachentäuschung und Irrtumserregung

Vorraussetzung ist zunächst, dass der Phisher den Empfänger der E-Mail über Tatsachen täuscht.

[26] Gajek/Schwenk/Wegener, DuD 2005, S. 639 (640).

Unter einer Täuschung versteht man die intellektuelle Einwirkung auf das Vorstellungsbild eines anderen mit dem Ziel der Irreführung über Tatsachen.[27] Tatsachen sind dem Beweis zugängliche Ereignisse oder Zustände der Gegenwart oder Vergangenheit.[28]
Mit dem Erstellen der E-Mail wollen die Phisher den Eindruck erwecken zur Abfrage der betreffenden Daten berechtigt zu sein.
Falls geheime Zugangsdaten zu Onlinekonten gephisht werden sollen, wird dem Empfänger der Mail in den meisten Fällen vorgespiegelt die Bank benötige dessen Zugangsdaten um etwaige Sicherheitslöcher zu schließen, oder ihr Serviceangebot zu verbessern.
Dies stellt eine Täuschung über Tatsachen i.S.d. § 263 I StGB dar. Nimmt der Empfänger die E-Mail jedoch nicht zur Kenntnis, weil sie bspw. durch einen Spam-Filter ausgelesen wird, fehlt es an einer Einwirkung auf das Vorstellungsbild des Empfängers. Somit stellt das Versenden der E-Mail erst ab Kenntnisnahme durch den Adressaten eine Täuschungshandlung dar.[29]

Nimmt der Empfänger die Nachricht zur Kenntnis und erliegt er infolge der Täuschungshandlung einem Irrtum, muss es auf Grund des Irrtums auch zu einer Vermögensverfügung dessen kommen.

b. Vermögensverfügung

Unter einer Vermögensverfügung versteht man jedes Handeln, Dulden oder Unterlassen, das unmittelbar eine Vermögensminderung herbeiführt. [30]
Alleine das Lesen der E-Mail kann somit keine Vermögensverfügung begründen.

Eine solche könnte jedoch in der Herausgabe der Daten zu erblicken sein. Das Offenbaren der Zugangsdaten stellt dann eine Vermögensverfügung dar, wenn die Daten selbst einen Vermögenswert bilden. Unter dem Vermögen versteht man die Gesamtheit der geldwerten Güter einer natürlichen oder juristischen Person.[31] Daneben zählen zu dem Vermögen auch Immaterialgüter und sonstige Rechte, soweit sie einen geldwerten Vorteil darstellen und als solche einen Marktpreis erzielen können.[32]

[27] BGHSt 47, 1 (3); Sch/Sch-Cramer, § 263 Rn. 6.
[28] Rengier, BT I, § 13 Rn. 2.
[29] Gercke, CR 2005 S. 607.
[30] Sch/Sch-Cramer § 263 Rn. 66.
[31] Tröndle/Fischer, § 263 Rn. 55.
[32] Tröndle/Fischer, § 263 Rn. 59.

Der Kenntnis der Zugangsdaten könnte ein immaterieller Vorteil zu kommen. Vorraussetzung wäre jedoch, dass diese Daten einen Marktpreis erzielen könnten. Dies ist aber gerade nicht der Fall. Die Bankdaten sind grundsätzlich nur für den Berechtigten Kunden bestimmt. Ein Verkauf, oder eine sonstige rechtsgeschäftliche Weitergabe ist nicht vorgesehen und in den AGB der Bank auch regelmäßig untersagt.[33]
Die Bankdaten gehören somit nicht zu dem von § 263 StGB geschützten Vermögen.

Da es dem Phisher allerdings mit den erlangten Daten möglich ist auf das Konto des Bankkunden zuzugreifen und Transaktion zu veranlassen, könnte man im Hinblick auf die Preisgabe der Bankdaten vielleicht dennoch eine Vermögensverfügung erblicken, denn das auf der Bank befindliche Geld hat zweifellos einen Vermögenswert.
Problematisch ist jedoch, dass die Preisgabe der Daten nicht unmittelbar zu einem Vermögensschaden des Kontoinhabers führt. Vielmehr tritt der endgültige Vermögensverlust erst ein wenn der Täter tatsächlich auf das Konto zugreift und eine Überweisung veranlasst.

Große Teile des Schrifttums verneinen hier eine Betrugsstrafbarkeit mangels Unmittelbarkeit zwischen Vermögensverfügung und Vermögensschaden. [34] Allein in der Preisgabe von PIN und TAN läge keine Verfügung die sich unmittelbar vermögensmindernd auswirke. Der Eintritt eines Vermögensschadens hänge nämlich von weiteren (deliktischen) Handlungen des Täters ab.

Entgegen dieser Auffassung stellen andere Stimmen, und auch die Rechtssprechung, auf eine schadensgleiche konkrete Vermögensgefährdung ab, die einem Vermögensschaden gleich stehe.[35] Begründet wird dies damit, dass zwischen Gefährdung und tatsächlichem Verlust der Vermögensposition wirtschaftlich nur ein quantitativer Unterschied bestehe.[36]

Da mit dieser Ansicht die Betrugsstrafbarkeit vorverlagert wird, ein Schaden ist ja gerade noch nicht eingetreten, ist eine restriktive Auslegung geboten. Der Eintritt des endgültigen Vermögensverlustes muss nahe liegen bzw. hinreichend wahrscheinlich sein.[37]

---

[33] Buggisch/Kerling, Kriminalistik 2006, S. 531 (534).
[34] Weber, HRRS 2004, S. 406 (408); Gercke, CR 2005, S. 606 (607); Popp, NJW 2004, S. 3517 (3518); Marberth-Kubicki, Computer- und Internetstrafrecht, Rn. 120.
[35] BGHSt 47, 160 (167); Rengier, BT I, § 13 Rn. 232.
[36] BGHSt 34, 394 (395)..
[37] BGHSt 21, 113; BGHSt 34, 394 (395); Lackner/Kühl, § 263 Rn. 40.

Der Täter muss den fraglichen Vorteil also ohne ernsthaftes Hindernis realisieren können, während umgekehrt das Opfer seine Vermögensposition eingebüßt hat.[38] So lässt der BGH die Aushändigung eines Scheckbuchs, oder einer Kreditkarte, durch eine Bank an den zum Missbrauch entschlossenen Täter für die Bejahung einer konkreten Vermögensgefährdung genügen.[39] Da der Täter mit Erlangung der Zugangsdaten alle nötigen Informationen für einen Kontozugriff in der Hand hält, kann dieser Ansicht nach also auch in Bezug auf das Phishing eine Vermögensgefährdung bejaht werden.[40]
Dass es für den endgültigen Eintritt des Schadens noch weiterer Handlungen des Phishers bedarf ist dieser Meinung nach unerheblich.[41]
Diese Ansicht wirft jedoch einige Widersprüchlichkeiten auf. Mit der Ausweitung des Tatbestandes auf eine Vermögensgefährdung wird das Erfordernis der Unmittelbarkeit der Vermögensverfügung, die den Selbstschädigungscharakter des § 263 StGB, im Gegensatz zu den Fremdschädigungsdelikten bspw. § 242 StGB, unterstreicht, unterlaufen.
Weiterhin spricht der Wortlaut des § 263 StGB von einer „Vermögensbeschädigung“ und nicht von einer bloßen Vermögensgefährdung. Würde man jene aber ebenfalls dem Tatbestand unterstellen, führt dies zu einer Vorverlagerung der Strafbarkeit was mit Art. 103 II GG kaum vereinbar wäre. Somit wären auch die Rücktrittsmöglichkeiten des Täters nach § 24 StGB erheblich beschnitten. Der Lehre von der schadensgleichen Vermögensgefährdung ist somit nicht zu folgen.

Eine Strafbarkeit nach § 263 StGB ist nicht gegeben.

2. Strafbarkeit wegen versuchten Betruges §§ 263 II, 32 StGB

Um eine Strafbarkeit wegen versuchten Betruges annehmen zu können, müsste der Phisher zunächst mit Tatentschluss hinsichtlich aller Tatbestandsmerkmale des objektiven Tatbestandes gehandelt haben.[42] Hinsichtlich Täuschung und Irrtumserregung liegt unzweifelhaft ein Tatentschluss vor. Allerdings fehlt es nach der hier vertretenen Auffassung am Vorsatz hinsichtlich einer Vermögensverfügung.

[38] Kindhäuser/Nikolaus, JuS 2006, S. 294 (297).
[39] BGH 33, 246; BGH 47, 167.
[40] Im Ergebnis zustimmend: Weber, HRRS 2004, S. 406 (409); Hilgendorf/Frank/Valerius, Computer- u. Internetstrafrecht, Rn. 765.
[41] BGH 16, 327; 17, 259.
[42] Wessels/Beulke, AT, Rn. 598.

Da der Phisher noch selbst aktiv werden muss um einen endgültigen Vermögensschaden herbeizuführen, erstreckt sich sein Tatentschluss gerade nicht auf die Unmittelbarkeit zwischen Vermögensverfügung und Vermögensschaden.

Eine Strafbarkeit nach den §§ 263, 22 StGB scheidet ebenfalls aus.

3. § 267 StGB in Bezug auf die E-Mail

Ebenso scheidet eine Strafbarkeit wegen Urkundenfälschung nach § 267 StGB aus, da es sich bei einer E-Mail nicht um eine verkörperte Gedankenerklärung, die der Urkundsbegriff voraussetzt[43], handelt.

4. § 269 StGB in Bezug auf die E-Mail

In Betracht kommt jedoch eine Strafbarkeit nach § 269 StGB, der die Strafbarkeitslücke schließen soll die daraus resultiert, dass § 267 StGB eine Verkörperung der Gedankenerklärung voraussetzt, was bei Daten nicht der Fall ist. Der Täter muss dafür beweiserhebliche Daten so speichern oder verändern, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart veränderte oder gespeicherte Daten gebrauchen.

a. beweiserhebliche Daten

Der Datenbegriff ist gesetzlich nicht näher bestimmt. Gemeinhin versteht man unter Daten alle durch Zeichen oder kontinuierliche Funktionen dargestellte Informationen jeder Art, die sich zum Zwecke der Datenverarbeitung codieren lassen, oder das Ergebnis eines Datenverarbeitungsvorgangs sind.[44]
Dies trifft auf eine E-Mail unproblematisch zu. Ob, auf Grund der hypothetischen Gleichsetzung mit dem Urkundsbegriff im Rahmen des § 269 StGB, nur solche Daten dem Tatbestand unterfallen die sichtbar gemacht werden können ist umstritten.[45] Dies kann aber in vorliegendem Fall dahinstehen, da es ohne weiteres möglich ist eine E-Mail am Computerbildschirm, etwa per Outlook oder einem anderen E-Mail Programm, wahrnehmbar zu machen.

[43] Küper, BT S. 294.
[44] Marberth-Kubicki, Computer- und Internetstrafrecht, Rn. 56.
[45] BGH NStZ-RR 03, 265; Tröndle/Fischer, § 269 Rn. 4.

Teile der Literatur sehen weiterhin nur solche Daten als taugliches Tatobjekt an, die bereits gespeichert wurden. Daten die erst noch gespeichert werden sollen unterfallen dieser Ansicht nach nicht dem Tatbestand des § 269 StGB.[46] Da § 269 StGB jedoch nicht auf den Datenbegriff des § 202a II StGB verweist, anders als etwa § 303a StGB, ist nicht einzusehen warum Daten die sich noch in der Eingabe befinden vom Tatbestand ausgenommen sein sollen. Der Datenbegriff des § 269 StGB muss somit weiter verstanden werden als der des § 202a StGB und erfasst jede Art von Art Daten, unabhängig davon ob sie schon gespeichert sind, oder erst noch gespeichert werden.[47] Somit stellt die E-Mail ab dem Zeitpunkt ihrer Eingabe in den Computer ein taugliches Tatobjekt dar.
Problematisch ist allerdings die „Beweiserheblichkeit" einer E-Mail. In Anlehnung an § 267 StGB muss es sich um solche Daten handeln, die dazu bestimmt und geeignet sind für ein Rechtsverhältnis, bzw. im Rechtsverkehr, Beweis zu erbringen.[48] Das einzelne Datum braucht hierbei nicht beweiserheblich zu sein, vielmehr genügt es wenn die Daten in ihrer Gesamtschau einen eigenen Beweiswert haben.[49]
Das Amtsgericht Bonn lehnte im Jahre 2001 die Beweiskraft von E-Mails gänzlich ab.[50] Begründet wurde dies damit, dass die Manipulierbarkeit von E-Mails allgemein bekannt sei. Dieser Auffassung folgte u.a. auch das Oberlandesgericht Köln.[51]
Auch Teile der Literatur messen einer E-Mail keinen eigenständigen Beweiswert zu, da dies, auf Grund der leichten Manipulierbarkeit, zu einem nicht tragbaren Verlust an Rechtssicherheit führen würde.[52]

Eine im Vordringen befindliche Ansicht spricht E-Mails im Gegensatz dazu eine Beweisgeeignetheit, im Wege des Anscheinsbeweises bzw. Beweises durch Augenschein, zu.[53]
Es mag zwar zutreffen, dass die Manipulationsmöglichkeiten bei E-Mails immens sind, jedoch ist es im Rahmen des § 267 StGB nicht erforderlich hinsichtlich der Gedankenerklärung einen Vollbeweis zu erbringen.[54] Auf Grund der Parallelität zu § 267, kann bei § 269 nichts anderes gelten.

[46] Malek, Strafsachen im Internet, Rn. 197.
[47] So auch: Sch/Sch-Cramer/Heine, § 269 Rn. 7; Tröndle/Fischer, § 269 Rn. 3.
[48] Buggisch, NJW 2004, S. 3519 (3520); Sch/Sch-Cramer/Heine, § 269 Rn. 9f.
[49] Sch/Sch-Cramer/Heine, § 269 Rn. 10.
[50] AG Bonn: Urteil vom 25.10.2001 – 3 C 193/01; abgedruckt in: CR 2002, S. 301.
[51] OLG Köln: Urteil vom 6.9.2002 – 19 U 16/02; abgedruckt in: CR 2003, S. 55.
[52] Rossnagel/Pfitzmann, NJW 2003, S. 1209.
[53] Mankowski, CR 2003, S. 44; Buggisch, NJW 2004, S. 3519 (3520); Knupfer, MMR 2004, S. 641 (642); Gercke, CR 2005, S. 606 (609); Buggisch/Kerling, Kriminalistik 2006, S 531 (533).
[54] Sch/Sch-Cramer/Heine, § 267 Rn. 11; RGSt 16, 264ff.

Fraglich ist zunächst, ob in der, unter einer bestimmten Adresse, versandten Erklärung ein Anscheinsbeweis dafür zu erblicken ist, dass diese Erklärung tatsächlich von der in der E-Mail als Absender bezeichneten Stelle stammt. Ein Anscheinsbeweis (prima-facie-Beweis) liegt vor, wenn ein Sachverhalt nach der Lebenserfahrung auf einen bestimmten (typischen) Verlauf hinweist.[55] Im Regelfall stammt die E-Mail tatsächlich von demjenigen, der aus ihr als Absender hervorgeht. Zwar mag es auch vereinzelt zu Manipulationen und Fälschungen von Absenderadressen, beim Phishing ist dies der Regelfall, kommen, diese Missbräuche stehen jedoch in keinerlei Relation zu der Anzahl der täglich versandten E-Mails, die nicht manipuliert wurden. Allein die bloße Möglichkeit, dass die E-Mail manipuliert wurde, vermag den Anscheinsbeweis nicht zu erschüttern. Vielmehr steht erst die ernsthafte Möglichkeit eines anderen Ablaufs der Annahme eines Anscheinsbeweises entgegen.[56]
Dass § 292a (a.F.) ZPO einen Anscheinsbeweis nur hinsichtlich elektronischer Dokumente mit einer qualifizierten elektronischen Signatur zu lies, lässt sich neuerdings nicht mehr als Argument gegen eine Beweisgeeignetheit von einfachen E-Mails ins Feld führen. Der Gesetzgeber hat diese Vorschrift durch Art. 1 JKomG vom 22.3.2005 aufgehoben. Teilweise wird argumentiert, die Annahme eines Anscheinsbeweises werfe eine ungerechtfertigte Risikoverteilung auf, bspw. in Fällen in denen jemand anderes die elektronische Identität des angeblich Erklärenden gestohlen und in dessen Namen Bestellungen getätigt hat.
Als plakative Beispiele werden die Damenunterwäsche für einen Lehrer oder die Pornohefte für einen Politiker genannt.[57] Da die Manipulationen in der Regel spurenlos erfolgten, bestünde keine Möglichkeit den Anscheinsbeweis zu erschüttern.
Dies mag zwar in bestimmten Fällen durchaus zutreffen, jedoch erreicht der Angreifer sein ursprüngliches Ziel, nämlich die betreffende Person in Misskredit zu bringen und ihren Ruf zu schädigen, unabhängig davon ob der E-Mail eine Beweiskraft zu kommt oder nicht. Bei einer lebensnahen Betrachtungsweise werden die „Geschädigten“ in den meisten Fällen die Bestellungen stillschweigend bezahlen und hinnehmen, um einen etwaigen Prozess und dem sich anschließenden Presserummel aus dem Weg zu gehen. Im Übrigen ist die Erschütterung des Anscheinsbeweises keinesfalls ausweglos.
Auch die Argumentation, dass elektronische Dokumente als Augenscheinsobjekte, § 371 ZPO, der freien richterlichen Beweiswürdigung nach § 286 ZPO unterfallen und somit keinen Anscheinsbeweis darstellen können[58], vermag nicht zu überzeugen.

[55] Creifelds, S. 70.
[56] OLG Düsseldorf, NJW-RR 2001, S. 101 (102).
[57] Rossnagel/Pfitzmann, NJW 2003, S. 1209 (1213).
[58] OLG Köln: Urteil vom 6.9.2002 – 19 U 16/02; abgedruckt in: CR 2003, S. 55.

Ein Augenscheinsobjekt ist eine Beweiskategorie und betrifft die Beweismittel, der Anscheinsbeweis Beweismaß und Beweiswürdigung.[59] Es handelt sich hier also um verschiedene Ebenen, eine Kollision liegt mithin nicht vor. Ferner werden die richterrechtlichen Anscheinsbeweise unter Berücksichtigung von § 286 ZPO entwickelt.[60] Da § 371 I S. 2 ZPO einer E-Mail ausdrücklich eine gewisse Beweiskraft zuspricht, scheint es, selbst wenn man die Möglichkeit eines Anscheinsbeweises ablehnt, kaum vertretbar E-Mails eine Beweisgeeignetheit abzusprechen.

Gerade weil sich der elektronische Geschäftsverkehr immer rasanter weiterentwickelt, es heutzutage möglich ist nahezu alle alltäglichen Geschäfte über das Internet abzuwickeln und auch Justiz und Verwaltung mittlerweile vom elektronischen Postweg gebrauch machen, so ist es bspw. möglich einen Widerspruch per E-Mail einzulegen, ist es untragbar die Beweiskraft von E-Mails zu verneinen. Der elektronische Geschäfts- und Rechtsverkehr wäre bei einer solchen Betrachtungsweise erheblich gefährdet. So könnten sich Vertragsparteien von ihren per E-Mail abgegebenen Erklärungen mit der Behauptung lösen, die E-Mail stamme ja überhaupt nicht von ihnen. Das Gegenteil zu beweisen wird der Gegenpartei nur schwerlich gelingen. Mankowski bezeichnet dies als „Widerrufsrecht kraft Beweislastverteilung“.[61] Die erst genannte Ansicht ist somit abzulehnen.
Folglich sind E-Mails generell dazu geeignet für ein Rechtsverhältnis Beweis zu erbringen, sei es im Wege eines Anscheinsbeweises oder der freien richterlichen Beweiswürdigung. Die angeblichen Sicherheitsprobleme und die Beziehung zur Bank, von denen oftmals in Phishing Mails gesprochen wird, können zum Gegenstand eines Rechtsverfahrens gemacht werden. Somit handelt es sich auch bei Phishing Mails um beweisgeeignete Daten.

Die Phishing Mail ist auch unzweifelhaft zum Beweis im Rechtsverkehr bestimmt. Zwar wird der Urheber der Phishing Mail diese gerade nicht zum Gegenstand eines Rechtsverfahrens machen wollen, die Beweisbestimmung kann jedoch auch nachträglich durch Dritte, etwa den Adressaten der E-Mail, erfolgen.[62]

[59] BGH, NJW 1998, S. 79 (81).
[60] BGH, NJW 1998, S. 79 (81).
[61] Mankowski, CR 2003, S. 44.
[62] BGHSt 13, 235 (238); Joecks, § 267 Rn. 24ff.

b. Parallelität zum Urkundsbegriff des § 267 StGB

Laut § 269 StGB ist es erforderlich, dass die Daten bei ihrer Wahrnehmung einer unechten oder verfälschten Urkunde gleichstehen. Somit müssen Perpetuierungsfunktion, Beweisfunktion und Garantiefunktion hypothetisch vorliegen.

aa. Gedankenerklärung

Als erste Vorraussetzung müsste in der E-Mail eine Gedankenerklärung zu erblicken sein. Darunter versteht man die willentliche Entäußerung zur Nachrichtenübermittlung geeigneter und bestimmter Zeichen durch einen Menschen.[63] Der Phisher will seine Opfer mithilfe verschiedener Behauptungen willentliche zur Preisgabe von Zugangsdaten veranlassen, eine Gedankenerklärung liegt mithin vor.

bb. Beweiseignung und Beweisbestimmung

Wie bereits unter a festgestellt, ist die E-Mail auch zum Beweis im Rechtsverkehr geeignet und bestimmt.

cc. Erkennbarkeit des Ausstellers

Die E-Mail müsste nun auch ferner ihren (vermeintlichen) Aussteller erkennen lassen. Aussteller ist derjenige, dem das im Rechtsverkehr erklärte als eigene Erklärung zugerechnet wird, und von dem die Erklärung herrührt.[64] Der Täter gibt mit Erstellung der E-Mail vor, diese stamme von einer zur Abfrage der Daten legitimierten Stelle, bspw. von einer Bank oder einem Auktionshaus. Die Erkennbarkeit des Ausstellers ist somit gegeben.

dd. verfälschte oder unechte Urkunde

Die Daten müssen bei ihrer Wahrnehmung einer verfälschten oder unechten Urkunde entsprechen.

[63] SK-Hoyer, § 267 Rn. 1.
[64] BGHSt 13, 382; Sch/Sch-Cramer, § 267 Rn. 16ff.

Regelmäßig wird nur die Alternative der unechten Urkunde einschlägig sein, da die Täter im Normalfall eine Totalfälschung der E-Mail vornehmen und keine nachträgliche Manipulation einer original E-Mail erfolgt.
Unecht ist eine Urkunde immer dann, wenn sie nicht von demjenigen stammt, der in ihr als Aussteller bezeichnet ist, wenn also über die Identität des Ausstellers getäuscht wird.[65] Dies ist bei Phishing Mails unzweifelhaft der Fall.

ee. speichern bzw. verwenden der Daten

Als Tathandlungen kommen im Rahmen des § 269 StGB sowohl das Speichern als auch das Verwenden der Daten in Betracht. Daten werden gespeichert, wenn der Täter sie auf einem Datenträger zum Zwecke ihrer weiteren Verwendung erfasst, aufnimmt oder aufbewahrt.[66]
Hat der Phisher schon bei der Erstellung der E-Mail den entsprechenden Vorsatz diese später auch zu verwenden, ist die Tatvariante des Speicherns bereits erfüllt, wenn der Phisher die E-Mail erstmals auf seinem Rechner ablegt. Hat er die E-Mail bereits versandt, wird diese zunächst auf dem Server des Mailproviders gespeichert und nach Abruf durch den Benutzer auf dessen Rechner. Auch die Tatvariante des Gebrauchens ist mit dem Absenden der E-Mail erfüllt. Gebraucht werden Daten, wenn sie einem anderen zugänglich gemacht werden, eine tatsächliche Kenntnisnahme ist jedoch nicht erforderlich.[67]
Da jedoch auch gleichzeitig die Tatvariante des Speicherns erfüllt ist, kommt dem Gebrauchen im Fall des Phishing keine eigenständige Bedeutung zu.[68]

c. subjektiver Tatbestand

Der Täter muss zunächst bedingten Vorsatz hinsichtlich aller objektiven Tatbestandsmerkmale aufweisen. Darüber hinaus muss er auch mit der Absicht zur Täuschung im Rechtsverkehr handeln. Dies liegt vor, wenn der Täter einen anderen über die Echtheit der Erklärung täuschen und ihn dadurch zu einem rechtserheblichen Verhalten veranlassen will.[69]

[65] Joecks, § 267 Rn. 51.
[66] Tröndle/Fischer, § 269 Rn. 5.
[67] Sch/Sch-Cramer/Heine, § 269 Rn. 21.
[68] Gercke, CR 2005, S. 606 (609).
[69] Sch/Sch-Cramer, § 267 Rn. 48; Buggisch, NJW 2004, S. 3519.

Mit der Absendung der E-Mail kommt es dem Phisher gerade darauf an seine Opfer über die Echtheit der Erklärung zu täuschen und sie hierdurch zu einem rechtserheblichen Verhalten, nämlich der Preisgabe von sensiblen Daten, zu bewegen. Eine Täuschungsabsicht ist also im Regelfall gegeben.

Es bleibt somit festzuhalten, dass bereits das Versenden einer Phishing Mail im Regelfall nach § 269 StGB strafbar ist.

5. Strafbarkeit gem. § 143 MarkenG

Da die Phisher in ihren E-Mails oftmals das Corporate Design einer Bank, eines Internetauktionshauses, etc. übernehmen um ihre Erklärungen noch glaubhafter machen, könnte ein Verstoß gegen das Markengesetz und damit eine Strafbarkeit nach § 143 MarkenG vorliegen. Genießt eine Marke, nach § 4 MarkenG, markenrechtlichen Schutz[70], wird dem Inhaber der Marke, nach § 14 MarkenG, ein Ausschließlichkeitsrecht gewährt, das es ihm ermöglicht anderen die Nutzung seiner Marke zu untersagen. Voraussetzung nach § 14 II MarkenG ist, dass die Marke im geschäftlichen Verkehr verwendet wird. Der Begriff des geschäftlichen Verkehrs ist weit auszulegen. Hierunter fällt jede selbstständige, wirtschaftlichen Zwecken, dienende Tätigkeit, die nicht rein privates, amtliches oder geschäftsinternes Verhalten ist.[71]
Mag man das Versenden von Phishing Mails noch als Handeln im geschäftlichen Verkehr qualifizieren[72], scheint es doch überaus fraglich ob die weiteren Vorraussetzungen des § 14 MarkenG vorliegen.
Der Phisher benutzt die Marke weder für Waren, noch für Dienstleistungen. Vielmehr soll die Verwendung der Marke lediglich den Anschein erwecken, dass die E-Mail tatsächlich vom Berechtigten erstellt wurde. Somit sind schon die Voraussetzungen des § 14 MarkenG nicht erfüllt, weshalb eine Strafbarkeit nach § 143 MarkenG ausscheidet. Eine Ansicht in der Literatur sieht gleichwohl eine Strafbarkeit nach dem MarkenG als gegeben an. [73] Jedoch vermag sie nicht zu erklären, wo genau der Phisher die Marke zur Kennzeichnung von Waren oder Dienstleistungen verwendet, obwohl auch sie selbst ausdrücklich darauf hinweist, dass eine Markenrechtliche Verletzung nur in Betracht kommt, wenn die Marke als Kennzeichnung von Waren oder Dienstleistungen genutzt wird.

[70] so sind bspw. die Bezeichnungen „ebay“ und „Volksbank“ markenrechtlich geschützt.
[71] Ekey/Klippel-Fuchs-Wissemann ,§ 14 Rn. 50.
[72] Buggisch/Kerling, Kriminalistik 2006, S. 531 (532).
[73] Buggisch/Kerling, Kriminalistik 2006, S. 531 (532).

6. § 202a StGB hinsichtlich der erlangten Zugangsdaten

Eine Strafbarkeit nach § 202a StGB liegt nicht vor, da die Zugangsdaten nicht besonders gegen unberechtigten Zugriff gesichert sind.

7. Strafbarkeit nach § 44 1 Bundesdatenschutzgesetz (BDSG)

In Betracht kommt jedoch eine Strafbarkeit nach § 44 I BDSG. Erste Vorraussetzung ist, dass eine der in § 43 II BDSG bezeichneten Handlungen vorliegt. Vorliegend könnte man ein Erschleichen der Übermittlung von personenbezogenen Daten durch unrichtige Angaben in Erwägung ziehen, § 43 II Nr. 4 BDSG. § 3 I BDSG definiert „personenbezogene Daten“ als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten natürlichen Person. Diese Definition trifft neben Krankenakten, Kreditkartennummern, Geburtsdaten etc. auch auf die PIN und TAN Nummer eines Bankkunden, oder ein sonstiges Passwort, zu. Gibt der Bankkunde diese Daten, auf Grund der Täuschung durch den Phisher, auf der bereitgestellten Webseite ein, ist der Tatbestand des § 44 I i.V.m. § 43 II Nr. 4 erfüllt.

Eine Strafbarkeit nach § 44 I BDSG liegt somit vor.

II. Strafbarkeit hinsichtlich des Erstellens der nachgeahmten Website

Mit dem Erstellen der korrespondierenden Website könnte ebenfalls eine Strafbarkeit nach § 269 StGB gegeben sein.

1. Strafbarkeit gem. § 269 StGB

Beim klassischen Phishing erfolgt die Abfrage der Daten über vom Täter erstellte Internetseiten. Ebenso wie bei der zuvor versandten E-Mail soll beim Opfer der Eindruck erweckt werden, die Internetseite stamme von einer zu Datenabfrage legitimierten Stelle. Die auf der Internetseite bereitgestellten Informationen unterfallen ebenso wie die E-Mail dem Datenbegriff. Diese können auch zum Gegenstand eines Rechtsverfahrens gemacht werden und sind somit beweiserheblich.
Die funktionelle Parallelität zu einer Urkunde scheint also auf den ersten Blick gegeben.

Einige Stimmen im Schrifttum verneinen jedoch eine Strafbarkeit nach § 269, da es an einer Täuschung über den Aussteller fehle.[74] Begründet wird dies damit, dass nur die jeweilige IP Adresse einer Internetseite für ihren Aussteller stehe, jedoch nicht die in der Adresszeile angegebene URL. Da in den meisten Fällen die IP Adresse aber richtig ist, sofern kein IP Spoofingvorliegt, und der Phisher lediglich den Domainnamen (bspw. www.xy-bank.de) verändert, fehle es an einer Beeinträchtigung der Garantiefunktion womit eine Strafbarkeit nach § 269 ausscheide.
Dies mag zwar auf den ersten Blick richtig sein, diese Ansicht übersieht jedoch dass es nicht nur an Hand der IP Adresse möglich ist auf einen bestimmten Aussteller zu schließen. So gibt bspw. das Impressum einer Website schriftlich Auskunft über ihren Aussteller. Weiterhin informiert die IP Adresse nur darüber auf welchem Server sich die betreffende Website befindet, nicht jedoch wer sie tatsächlich programmiert hat, oder als ihr geistiger Urheber gilt. Die Phisher spiegeln ihren potentiellen Opfern vor die Website stamme von einem Kreditinstitut bzw. einem Auktionshaus oder einer ähnlichen Einrichtung, die zur Abfrage der betreffenden Daten berechtigt sei. Eine Täuschung über den wahren Urheber der Daten liegt somit vor.

Die oben entwickelten Grundsätze[75] lassen sich also ohne Probleme auf die Erstellung der Website übertragen.

Eine Strafbarkeit nach § 269 StGB liegt mithin vor.

III. Strafbarkeit bezüglich des Verwendens der gephishten Daten

Da dem Täter zahlreiche Möglichkeiten offen stehen, die erlangten Daten missbräuchlich zu verwenden, etwa um sein Opfer in Misskredit zu bringen oder ihm Unannehmlichkeiten zu bereiten (zum Bsp. durch ändern des Passwortes eines Ebay Accounts), beschränkt sich die folgende Darstellung auf vermögensrelevante Schädigungen, die durch die Verwendung von PIN und TAN im Rahmen des Bankdaten Phishens entstehen.

[74] Popp, MMR 2006, S. 84 (85); Hilgendorf/Frank/Valerius, Computer- u. Internetstrafrecht, Rn. 183.
[75] Siehe: B, I, 4.

1. Strafbarkeit gem. § 202a StGB

Da es dem Täter möglich ist mit den erbeuteten PIN und TAN Nummern persönliche Daten des Opfers, wie etwa seine Stammdaten oder den Kontostand, abzufragen, könnte zunächst eine Strafbarkeit nach § 202a StGB gegeben sein.

a. Tatobjekt: Nicht für den Täter bestimmte Daten, die gespeichert und besonders gesichert sind

Unter Daten i.S.d. § 202a StGB versteht man alle durch Zeichen oder kontinuierliche Funktionen dargestellte Informationen, die sich codieren lassen, oder das Ergebnis eines Datenverarbeitungsvorgangs sind.[76]
Einschränkend unterfallen § 202a StGB nur solche Daten, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden,
§ 202a II StGB.
Gespeichert sind Daten, wenn sie zum Zweck ihrer Weiterverwendung erfasst, aufgenommen oder aufbewahrt sind.[77] Da die Kontoinformationen auf einem Computer der Bank fixiert sind, ist auch dieses Tatbestandsmerkmal erfüllt.
Ferner müssten diese Daten nun auch gegen unberechtigten Zugang besonders gesichert sein. Gegen unberechtigten Zugang besonders gesichert sind Daten, wenn Vorkehrungen, softwaretechnischer oder mechanischer Art, speziell zu dem Zweck getroffen sind den Zugang Unbefugter zu verhindern oder zu erschweren.[78]
Es kommt darauf an, ob die Sicherung geeignet erscheint einen wirksamen, wenn auch nicht absoluten, Schutz zu erreichen und namentlich auch das Interesse des Berechtigten an der Geheimhaltung zu dokumentieren.[79]
Da der Zugriff auf die Daten nur nach Eingabe von PIN und TAN Nummer freigegeben wird, liegt eine solche abstrakte Sicherung vor. Fraglich ist, ob in der willentliche Preisgabe der Zugangsdaten durch den Kontoinhaber eine Aufgabe des Geheimhaltungsinteresses zu erblicken ist. Dies wird wohl kaum der Fall sein, bedenkt man dass die Sicherungsmaßnahmen durch die Bank selbst eingeführt wurden. Somit wird ihr eigenes Geheimhaltungsinteresse ausgedrückt, welches nicht zur Disposition des Benutzers steht.

[76] Sch/Sch-Lenckner, § 202a Rn. 3.
[77] Tröndle/Fischer, § 202a Rn. 5.
[78] Lackner/Kühl, § 202a Rn. 4; Tröndle/Fischer, § 202a Rn. 8.
[79] Lackner/Kühl, § 202a Rn. 4.

Auch wird der Benutzer täuschungsbedingt davon ausgehen, dass seine Daten nicht in die Hände Dritter fallen und lediglich, ähnlich wie bei einer Transaktion, dem Beweis seiner Identität dienen.

Weiterhin dürfen die Daten auch nicht für den Täter bestimmt sein. Dies ist der Fall, wenn die Daten nach dem Willen des Berechtigten nicht in den Herrschaftsbereich des Täters gelangen sollen.[80] Der Kontoinhaber geht davon aus, dass seine Daten nur von der Bank verwendet werden, etwa um die Sicherheitsstandards zu erhöhen. Sein Einverständnis erstreckt sich jedoch nicht auf weitergehende Handlungen, wie etwa die Abfrage seines Kontostands. Die Daten sind nach dem Willen des Berechtigten also gerade nicht für den Phisher bestimmt.

b. Tathandlung: sich verschaffen von Daten

Der Täter muss sich diese Daten verschaffen. Verschaffen bedeutet das Herstellen der eigenen Herrschaft, oder derjenigen eines anderen, über die Daten und zwar unter Überwindung der besonderen Zugangsicherung.[81] Verschafft sind die Daten demnach, wenn der Täter durch optische Wahrnehmung von ihnen Kenntnis erlangt hat. Sobald der Phisher den Kontostand oder die betreffenden Stammdaten abruft und diese auch positiv zur Kenntnis nimmt, hat er sich die Daten i.S.d. § 202a verschafft.

c. subjektiver Tatbestand

Bedingter Vorsatz (dolus eventualis) ist zu Verwirklichung des § 202a StGB ausreichend.

Diesen wird der Phisher auch regelmäßig aufweisen, so dass er sich mit dem Abruf der Daten gem. § 202a StGB strafbar macht.

2. Strafbarkeit gem. § 263a StGB

Sollte der Täter nun auch eine Überweisung mithilfe der erlangten Daten vornehmen, könnte er sich eines Computerbetrugs gem. § 263a StGB strafbar gemacht haben.

[80] Lackner/Kühl, § 202a Rn. 3.
[81] Lackner/Kühl, § 202a Rn. 5; Sch/Sch-Lenckner, § 202a Rn. 10.

Vorraussetzung ist, dass der Täter das Vermögen eines anderen dadurch beschädigt, indem er das Ergebnis eines Datenverarbeitungsvorgangs durch eine unrichtige Programmgestaltung, durch die Verwendung unrichtiger oder unvollständiger Daten, durch die unbefugte Verwendung von Daten oder durch sonstige unbefugte Einwirkungen auf den Ablauf, beeinflusst.

a. unbefugte Verwendung von Daten

Beim Phishing scheiden die Alternativen der Verwendung unrichtiger Daten und die unrichtige Programmgestaltung aus. In Betracht kommt jedoch die unbefugte Verwendung von Daten. Daten werden verwendet, wenn sie in einen Datenverarbeitungsprozess eingegeben werden.[82]
Hinsichtlich der Auslegung des Merkmals „unbefugt“ bestehen einige Schwierigkeiten.
Einer Ansicht nach ist jedes Verhalten unbefugt, das dem (mutmaßlichen) Willen des über die Datenverarbeitungsanlage Verfügungsberechtigten widerspricht.[83] Einer anderen Auffassung nach muss sich die Auslegung an § 263 StGB orientieren. Insoweit ist zu fragen, ob die Verwendung der Daten gegenüber einem Menschen als zumindest schlüssige Vorspiegelung der Befugnis zu deuten wäre, sog. Betrugsspezifische Interpretation.[84] Sobald sich der Phisher mit den Zugangsdaten Zugriff zu einem Onlinekonto verschafft, liegt unproblematisch die Eingabe in eine Datenverarbeitungsanlage vor. Auch dürfte sein Verhalten kaum dem Willen des Verfügungsberechtigten, der Bank, entsprechen. Würde er die Daten gegenüber einem Menschen, bspw. einem Bankangestellten, verwenden, hätte sein Verhalten auch Täuschungswert. Somit führen beide Ansichten zum selben Ergebnis, eine unbefugte Verwendung von Daten liegt vor, ein Streitentscheid ist somit entbehrlich.

b. Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs

Die Eingabe der Daten müsste nun auch das Ergebnis eines Datenverarbeitungsvorgangs beeinflusst haben. Dies entspricht dem Irrtum und der Verfügung beim Betrug nach § 263. Das Ergebnis eines Datenverarbeitungsvorgangs ist dann beeinflusst, wenn es von dem Arbeitsergebnis abweicht das ohne die Tathandlung erzielt worden wäre.[85] Veranlasst der Phisher eine Geldtransaktion, liegt eine solche Beeinflussung vor.

[82] Rengier, BT I, § 14 Rn. 7; Tröndle/Fischer, § 263a Rn. 8.
[83] BGHSt 40, 331 (334); Hilgendorf, JuS 1997, S. 130 (131).
[84] Tröndle/Fischer, § 263a Rn. 11ff.
[85] Tröndle/Fischer, § 263a Rn. 22.

c. unmittelbarer Vermögensschaden

Wird die Transaktion erfolgreich abgeschlossen und befindet sich das Geld nun auf dem Konto des Phishers, oder eines Mittelsmanns, liegt auch ein Vermögensschaden vor.

d. subjektiver Tatbestand

Auch der subjektive Tatbestand ist zu bejahen. Der Phisher handelt hinsichtlich der objektiven Tatbestandsmerkmale mit Vorsatz und in der Absicht der rechtswidrigen, stoffgleichen Bereicherung.

Eine Strafbarkeit gem. § 263a StGB ist gegeben.

3. Ergebnis

Wie die vorausgegangene Untersuchung gezeigt hat, ist bereits das Versenden von Phishing Mails und die Erstellung der korrespondierenden Website, zumindest was das klassische Phishing anbelangt, nach geltendem Recht strafbar. Zwar mag man je nach juristischer Würdigung, besonders hinsichtlich der Strafbarkeit nach § 269, zu einem abweichenden Ergebnis gelangen, jedoch vermögen die Ansichten die eine Strafbarkeit nach § 269 verneinen kaum zu überzeugen. § 269 StGB gibt der Justiz ein adäquates Mittel an die Hand um das Phishing bereits im Vorfeld eines Vermögensschadens zu bekämpfen. Was die Strafbarkeit hinsichtlich der Verwendung der gephishten Daten anbelangt tun sich kaum juristische Probleme auf. Auch sind hier bereits erste justizielle Aufarbeitungen erfolgt.
So sah das Amtsgericht Hamm bei Verwendung der erlangten Daten für eine Geldtransaktion den Tatbestand des Computerbetrugs als verwirklicht an.[86] Ob das deutsche Strafrecht auch gegenüber neueren Varianten des Phishing gewappnet ist, wird das folgende Kapitel zeigen.

C. Neue Phishing Varianten

Da das Phishing Phänomen inzwischen weitgehend bekannt ist, und sich auch die Banken mittels Informationsbroschüren und Warnhinweisen um eine Sensibilisierung ihrer Kunden bemühen, fällt es den Phishern zunehmend schwerer die gewünschten Erfolge zu verbuchen.

[86] AG Hamm, Urteil vom 5.9.2005 – 10 Ds 101 Js 244/05-1324/05. Abgedruckt in: CR, 2006 S. 70.

So ist es nicht verwunderlich, dass die klassische Phishing Welle mittlerweile abebbt und sich die Phisher neurer Methoden bedienen um an die gewünschten Informationen zu gelangen. So tritt das so genannte „Pharming“ verstärkt in Erscheinung. Was sich genau hinter diesem Wort verbirgt soll jedoch in einem eigenen Kapitel besprochen werden.[87] Im Folgenden werden nun einige neue ausgewählte Angriffsmethoden abseits vom klassischen Phishing vorgestellt und strafrechtlich bewertet.

I. Trojaner Angriffe

Immer öfter versuchen die Phisher Trojaner auf den Systemen ihrer Opfer einzuschleusen. Diese Schädlinge installieren dann meist einen so genannten Keylogger auf dem Opferrechner mit dem die Tastatureingaben, und somit auch die Eingabe von PIN und TAN, belauscht werden.
Derartige Trojaner beschränken sich jedoch nicht nur auf das Protokollieren von Tatstatureingaben, sie verhindern auch dass Informationen, wie etwa die TAN, die nur einmalig verwendet werden kann, versandt werden. Somit steht dem Phisher im Falle eines erfolgreichen Angriffs eine noch unbenutzte TAN zu Verfügung.
Um die Trojaner auf den Rechnern der Opfer einzuschleusen bedienen sich die Phisher unterschiedlicher Methoden. Teilweise werden die Trojaner mit einer E-Mail verschickt, die, ähnlich wie beim klassischen Phishing, vorgibt vom betreffenden Kreditinstitut zu stammen. Um den Nutzer nun auch zur Installation des Trojaners zu bewegen wird vorgegeben die angehängte Datei sei eine neue Software, die das Onlinebanking Angebot der Bank noch verbessere oder sicherer mache.
Eine andere, noch gefährlicherer, Methode ist es den Trojaner auf eine CD-Rom aufzuspielen und diese per Post an das vermeintliche Opfer zu schicken. Auch hier wird behauptet die CD enthalte neue Homebanking Software.
Diese neue Angriffsart ist strafrechtlich ähnlich wie das klassische Phishing zu bewerten. Das Erstellen der Email, oder der CD-Rom ist nach § 269 StGB strafbar und auch hinsichtlich der anschließenden Verwendung der Daten ergeben sich keine Besonderheiten, hier liegt in den meisten Fällen eine Strafbarkeit nach den §§ 263a, 202a vor. Hinsichtlich der Verwendung eines Trojaners, könnte zusätzlich noch eine Strafbarkeit nach § 263a II und § 303a StGB gegeben sein.

[87] Siehe: D.

1. Strafbarkeit nach § 263a III

Um eine Strafbarkeit nach § 263a III zu begründen müsste es sich bei dem Trojaner um ein Computerprogramm handeln, dessen Zweck die Begehung eines Computerbetruges ist. Unter einem Programm versteht man eine durch Daten fixierte Arbeitsanweisung an den Computer.[88] Diese Definition trifft unstreitig auf einen Trojaner bzw. einen Keylogger zu. Fraglich ist allerdings ob der Zweck des Trojaners tatsächlich die Begehung eins Computerbetrugs ist. Nach der Regierungsbegründung ist nur auf den objektiven Zweck des betreffenden Programms abzustellen.[89] Somit kann grds. nur auf den Inhalt des Programms und nicht auf seine Verwendung abgestellt werden. Es kommen also vorliegend nur solche Programme in Betracht, die gerade im Hinblick auf eine Tatmodalität nach § 263 I StGB geschrieben wurden.[90] Es fehlt hier jedoch an der Bestimmung des Trojaners zur Begehung eines Computerbetrugs. Der Trojaner wird nur vorbereitend und nicht unmittelbar bei Begehung des Computerbetrugs eingesetzt.
Somit erscheint es sachgerecht das Herstellen oder sich Verschaffens eines Trojaners als straffreie Vorbereitungshandlung anzusehen. Würde man die Strafbarkeit auf Programme ausweiten, die ihrerseits nur eine spätere Betrugshandlung vorbereiten, würde man die Reichweite der Vorfeldkriminalisierung zu stark erweitern.[91]

Eine Strafbarkeit nach § 263a III StGB scheidet also aus.

2, Strafbarkeit nach § 303a StGB

Durch die Installation eines Trojaners bzw. Keyloggers kommt in erster Linie eine Strafbarkeit wegen des Veränderns von Daten in Betracht. Ob gleichzeitig auch Daten gelöscht, unterdrückt oder unbrauchbar gemacht werden, hängt vom Einzelfall und der Intention des Täters ab.
Verändert werden Daten, wenn sie einen anderen Informationsgehalt erhalten und dadurch der ursprüngliche Verwendungszweck beeinträchtigt wird.[92]

[88] Tröndle/Fischer, § 263a Rn. 6.
[89] BT-Drs. 15/1720, 11.
[90] Tröndle/Fischer, § 263a Rn. 32.
[91] Gercke, CR 2005, S. 606 (608).
[92] Sch/Sch- Stree, § 303a Rn. 4.

Da die Trojaner im Regelfall jedoch nichts an dem vorhandenen Datenbestand ändern, sondern nur leeren Speicherplatz beanspruchen, kann hier nicht von einem Verändern gesprochen werden.[93] Etwas anderes mag nur gelten wenn der Hacker mit Hilfe des Trojaners Veränderungen an den Dateien des Opfers vornimmt.

Allerdings blockieren die Trojaner, wenn es der Phisher auf Bankdaten abgesehen hat, die Eingabe der TAN Nummer durch den Benutzer. Eine TAN Nummer kann nämlich nur einmal verwendet werden. Hätte sie der Benutzer also bereits an die Bank übermittelt, wäre sie für den Phisher wertlos. Damit könnte die Alternative des Unterdrückens verwirklicht sein. Unterdrücken bedeutet, die Daten dauernd oder nur vorübergehend dem Zugriff des Berechtigten zu entziehen und dadurch ihre Verwendbarkeit auszuschließen.[94] In dem der Trojaner die Übermittlung der TAN Nummer durch den Benutzer verhindert, kann dieser, zumindest vorübergehend, nicht mehr auf seine Kontodaten zugreifen bzw. Transaktionen durchführen.

Eine Strafbarkeit nach § 303a ist somit bei entsprechendem eventual Vorsatz des Täters zu bejahen.

II. „Man in the middle“ Attacke

Eine besonders gefährliche Abwandlung des Phishing ist die so genannte Man in the middle Attacke. Der Angreifer steht hierbei zwischen den Kommunikationspartnern, bspw. der Bank und dem Kunden, und hat mit seinem System die komplette Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzteilnehmern. Auf diese Weise kann er die ausgetauschten Informationen nach Belieben einsehen und sogar manipulieren.
Dies kann auf verschiedene Arten erreicht werden und setzt fundierte technische Kenntnisse voraus. Nimmt der Angreifer eine man in the middle Position ein, so kann er bspw. eine vom Nutzer vorgenommene Überweisung ändern noch bevor diese bei der Bank eingeht. In einem solchen Fall kommt vor allem eine Strafbarkeit nach den §§ 269 und 303a in Betracht.

[93] Tröndle/Fischer, § 303a Rn. 12.
[94] Lackner/Kühl, § 303a Rn. 3.

1. Strafbarkeit nach § 269 StGB

Fängt der Täter eine Onlinetransaktion ab und ändert diese zu seinem Vorteil, könnte der Tatbestand des Fälschens beweiserheblicher Daten, § 269, verwirklicht sein. In Betracht kommt hier vor allem die Alternative des Veränderns von beweiserheblichen Daten.

a. Verändern von beweiserheblichen Daten

Eine Online Transaktion fällt unproblematisch unter den Begriff der beweiserheblichen Daten. Die Tathandlung des Veränderns, beschreibt die inhaltliche Umgestaltung der Daten.[95] Dies entspricht dem Verfälschen einer echten Urkunde, also dem Verändern der gedanklichen Erklärung in eine andere.[96] Ändert der Täter die Überweisung hinsichtlich des Begünstigten und ggf. der Höhe des zu überweisenden Betrages zu seinen Gunsten ab, erfüllt dies die Variante des Veränderns von Daten.

b. Parallelität zum Urkundsbegriff des § 267 StGB

Im Falle der visuellen Wahrnehmbarkeit der veränderten Daten, würde auch unproblematisch eine verfälschte Urkunde i.S.d. § 267 StGB vorliegen.[97]

Eine Strafbarkeit nach § 269 StGB liegt demnach vor.

2. Strafbarkeit gem. § 303a StGB

Da § 303a StGB auf den Datenbegriff des § 202a II StGB verweist, können nur Daten die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden ein taugliches Tatobjekt darstellen.
In vorliegendem Fall kommen vor allem Daten die sich in der Übermittlung befinden in Betracht. Übermittlung ist jede Weiterleitung von Daten, insbesondere im Online Verkehr.[98] Fängt der Täter die Online Transaktion auf dem Weg zu Bank ab und ändert ihren Inhalt, bevor er sie an die Bank weiterleitet, könnte darin ein Verändern von Daten zu erblicken sein.

[95] Tröndle/Fischer, § 269 Rn. 5.
[96] Tröndle/Fischer, § 267 Rn. 19.
[97] Zu den einzelnen Voraussetzungen siehe: B, I, 1, b.
[98] Tröndle/Fischer ,§ 202a Rn. 6.

Das Verändern von Daten erfordert das Herstellen eines neuen Dateninhalts, etwa durch inhaltliche Umgestaltung.[99] Dies trifft in vorliegendem Fall zu.

Demnach ist in den Fällen von Man in the middle Attacken neben einer Strafbarkeit aus § 269 StGB auch eine Strafbarkeit nach § 303a StGB gegeben. Zwischen den beiden Delikten besteht Tateinheit.[100]

III. „Vishing“

Vishing, VoIP-Phishing, ist eine neuartige Masche von Identitätsdieben an Kreditkartennummern, Passwörter oder Bankdaten zu gelangen. Diese Methode macht sich die niedrigen Kosten von VoIP (voice over IP) zu nutze. Die Täter richten einen IP-basierten Wardialer ein, der automatisiert regionale Telefonnummern anruft. Sobald eine angewählte Person das Telefon abnimmt beginnt eine Bandansage zu laufen, die bspw. folgendes mitteilt: „Ihre Kreditkarte wurde missbraucht. Bitte rufen Sie umgehend folgende Nummer an." Sobald das Opfer nun diese Nummer anruft, meldet sich ein Sprachportal, dass zur Verifizierung der Daten das Eintippen der Kreditkartennummer verlangt. Trat diese Art von Angriffen anfänglich nur in den USA auf, hat die Vishing Welle mittlerweile auch Deutschland erreicht.[101] Da die Täter, anders als beim Phishing, gerade keine Daten manipulieren, sondern ihre Opfer „nur“ belügen, kommt hinsichtlich dem Erschleichen der persönlichen Informationen, allenfalls eine Strafbarkeit nach § 44 I BDSG in Betracht.[102]

D. Pharming

Der Begriff Pharming wird für verschiedene Arten von Angriffen auf sog. Domain-Name-Server verwendet.
Angelehnt an das Wort Phishing, versucht das Kunstwort Pharming wohl auf den Umstand anzuspielen dass die Täter mitunter eine Vielzahl von Servern unterhalten, vergleichbar mit der Tierhaltung auf einer „farm“.[103]
Jede Seite im Internet ist einer bestimmten IP Adresse zugeordnet.

[99] Lackner/Kühl, § 303a Rn. 3.
[100] Lackner/Kühl, § 303a Rn. 6.
[101] http://www.at-mix.de/news/1698.html.
[102] Siehe: B, I, 4.
[103] Popp, MMR 2006, S. 84.; http://de.wikipedia.org/wiki/Pharming.

Da man sich solche IP Adressen relativ schlecht merken kann, wird die Nummernfolge der IP-Adressen in Domainnamen übersetzt, bspw. 192.176.230.00 = www.xy-bank.de. Wählt man also die Seite www.xy-bank.de über einen Browser an, kontaktiert man die dahinter stehende IP Adresse. An dieser Zuordnung von Domainname zu IP-Adresse setzen die Pharmer an und weisen einem bestimmten Domainnamen eine andere IP Adresse zu, die auf einen von ihnen unterhaltenen Server führt. Gibt ein Pharming Opfer den Domain Namen seiner Hausbank im Browser ein, wird es nun nicht auf die tatsächliche Seite seiner Bank mit ihrer festen IP-Adresse geführt, sondern landet bei einer IP Adresse, die die Pharmer für sich reserviert haben und dort ihre täuschend echte Bankseite eingestellt haben. Trägt das Opfer nun dort seine Zugangsdaten ein, werden diese direkt an den Pharmer weitergeleitet. Dies ähnelt dem Täuschungsangriff beim klassischen Phishing. Diese zielgerichteten Angriffe sind besonders gefährlich, da keine E-Mail vorausgeht die den Benutzer misstrauisch machen könnte. Ein Pharming Angriff läuft also auf rein technischer Ebene ab. Der Benutzer hat somit im Regelfall keine Möglichkeit den Angriff zu verhindern oder im Vorfeld zu bemerken.

I. Der technische Ablauf

Die Zuordnung eines Domain Namens zu einer bestimmten IP-Adresse erfolgt im Internet über sog. DNS-Server, vergleichbar mit einem Telefonbuch das einem Namen eine bestimmte Rufnummer zuordnet.
Will der Pharmer diese Zuordnung manipulieren, muss er also zunächst den DNS Server angreifen.
Um die Kontrolle über den DNS Server zu erlangen nutzen die Pharmer gezielt Schwachstellen in dessen Software aus. Oftmals werden hierfür sog. exploits verwendet.
Ein exploit ist ein Computerprogramm, oder Script, das spezifische Schwachstellen oder Fehlfunktionen eines anderen Computerprogramms ausnutzt.[104] Gelingt es dem Pharmer den DNS Server unter seine Kontrolle zu bringen, kann er verschiedenen Domainnamen andere IP-Adressen zu weisen. Dies wird auch als DNS-Spoofing (spoofing, engl.= Manipulation, Verschleierung) bezeichnet.
Muss ein Client nun einen bestimmten Domainnamen in eine IP-Adresse umwandeln, sendet das Betriebssystem eine entsprechende Anfrage an den nächstgelegen DNS-Server. Der kompromittierte Server liefert von nun an falsche DNS Antworten an alle Clients aus, die den Server zur Namensauflösung nutzen.

[104] http://de.wikipedia.org/wiki/Exploit.

Teilweise erfolgt die Auflösung von Domainnamen in eine IP-Adresse jedoch nicht über einen Server, sondern über eine lokale Host-Datei auf dem Rechner des Benutzers. Diese Datei enthält eine Tabelle der häufig genutzten IP-Adressen, so dass die entsprechenden Adressen nicht immer von einem DNS-Server abgerufen werden müssen.
Gelingt es dem Pharmer auf die Host-Datei, etwa mittels eines Trojaners, zuzugreifen, kann er ebenfalls eine DNS-Spoofing Attacke ausführen. Diese Art von Pharming ist aber wenig effektiv, da sie nur lokal begrenzt ist und nicht alle Adressen des world wide web umfasst.

II. Pharming im Lichte des Strafrechts

Hinsichtlich der, sich einem Pharming Angriff anschließenden, Verwendung der erlangten Daten bestehen im Vergleich zum klassischen Phishing keine Besonderheiten. Im Regelfall liegt eine Strafbarkeit nach § 202a StGB und, je nach Intention des Täters, § 263a StGB vor. Das Erstellen der gefälschten Internetseite unterfällt wie oben ausgeführt[105] dem Tatbestand des § 269 StGB.

Sobald sich der Täter Zugang zu einem DNS Server verschafft und dessen gespeichterte IP-Adressen abruft liegt eine Strafbarkeit nach § 202a StGB vor, da die auf dem DNS Server gespeicherten Daten nicht für den Pharmer bestimmt und gegen unberechtigten Zugang besonders gesichert sind.

Das Verändern der Einträge im DNS-Server wird durch den Tatbestand der Datenveränderung, § 303a StGB, erfasst. Der Täter nimmt eine inhaltliche Umgestaltung der gespeicherten Daten vor und erfüllt somit die Tatbestandsalternative des Veränderns von Daten.

Attackiert der Pharmer die lokale Host-Datei eines Clients mittels eines Trojaners, ist auch hier der Tatbestand des § 303a erfüllt, sobald er die Einträge der Host-Datei verändert.

E. Phisherman's friend, oder: Wie kommt der Phisher eigentlich an sein Geld?

Hat der Phisher bzw. der Pharmer die gewünschten Zugangsdaten zu den Onlinekonten seiner Opfer erbeutet, steht er vor dem Problem das Geld auf sein Konto zu bekommen, ohne dass sich die Spur zu ihm zurückverfolgen lässt. Sein Geld muss also „gewaschen" werden.

[105] Siehe: B, II, 1.

Hierfür bedient er sich in der Regel inländischer Mittelsmänner, auf deren Konten das Geld überwiesen wird. Anschließend sollen diese dann das Geld über das Bargeldtransfersystem der Western Union Bank an die Phisher übersenden. Die Mittelsmänner werden von den Phishern per E-Mail[106] mit lukrativen Verdienstangeboten geködert. So geben die Phisher bspw. vor Personalabteilungsleiter eines aufstrebenden Unternehmens zu sein, das für seine Tätigkeiten im Finanzdienstleistungssektor zuverlässige Mitarbeiter sucht. Es wird ein gut bezahlter Nebenjob angeboten, der darin besteht Konten zur Verfügung zu stellen, eingezahltes Geld abzuheben und per Western Union nach Osteuropa zu überweisen. In letzter Zeit wurde auch eine neue Methode des Anwerbens publik. Die Anzeigen werden in Jobbörsen platziert, um sie auch für selbstständige und Unternehmen interessant zu machen.
Da diese so genannten „Finanzagenten" in der Regel gutgläubig handeln, stellt sich die Frage ob sie sich dennoch strafbar machen.

I. Strafbarkeit wegen Beihilfe zum Computerbetrug §§ 263a, 27 StGB

Das Amtsgericht Hamm verurteilte in seiner Entscheidung vom 5.9.2005 einen Finanzagenten wegen strafbarer Beihilfe zum Computerbetrug.[107] Diese rechtliche Würdigung wirft jedoch einige Fragen auf. Bedenkt man, dass der Computerbetrug mit dem Eintritt des Schadens vollendet ist[108], die Beendigung jedoch erst mit der Erlangung des angestrebten Vermögensvorteils eintritt[109], stellt sich das Problem, ob eine Beihilfe Handlung zwischen Vollendung und Beendigung überhaupt möglich ist. Der Schaden tritt ein sobald das Geld auf dem Konto des Finanzagenten eingeht. Den Vermögensvorteil erlangt der Phisher hingegen erst durch die Bar-Überweisung des Mittelsmannes. Die Rechtssprechung hält eine Beihilfe zwischen Beendigung und Vollendigung der Tat für möglich.[110]. Diese Ansicht stößt in der Literatur teilweise auf heftige Kritik.[111]
Dieser Streitstand könnte jedoch vorliegend nicht von Bedeutung sein, sollte der maßgebliche Gehilfenbeitrag schon vor Beendigung der Tat vorgelegen haben. Ein Hilfeleisten liegt in jedem Tatbeitrag, der die Haupttat ermöglicht oder erleichtert.[112] Es reicht aus, wenn der Gehilfenbeitrag mitwirksam für den Erfolg wurde. Er braucht nicht conditio sine qua non für den Erfolg zu sein.

---

[106] Ein Beispiel zeigt Abbildung Nr. 3 im Anhang.
[107] AG Hamm 10 Ds 101 Js 244/05-1324/05, abgedruckt in: CR, 2006 S. 70ff.
[108] Sch/Sch-Cramer, § 263a Rn. 38.
[109] Lackner/Kühl, § 263 Rn. 63; Rengier, BT I, § 13 Rn. 117.
[110] RGSt 71, 193 (194); BGHSt 3, 40 (43); 6, 248 (251).
[111] Etwa: Lackner/Kühl, § 27 Rn. 3.
[112] Wessels/Beulke, AT, Rn. 582.

Somit ist bereits in der Zuverfügung Stellung des eigenen Kontos, und nicht erst in der Bar-Überweisung an den Phisher, durch den Finanzagenten ein tauglicher Gehilfenbeitrag zusehen. Ein Streitentscheid ist somit nicht erforderlich.

Fraglich ist jedoch, ob auch von einem doppelten Gehilfen Vorsatz ausgegangen werden kann. Der Gehilfe muss den Willen und das Bewusstsein haben die Tat eines anderen zu fördern, wobei sein Vorstellungsbild den wesentlichen Unrechtsgehalt der Haupttat erfasst.[113] In den meisten Fällen handeln die Mittelsmänner gutgläubig und gehen nicht davon aus, dass sie gerade einem anderen bei einer rechtswidrigen Tat helfen. Dass sie auf Grund der Umstände davon hätten ausgehen müssen, dass etwas Rechtswidriges im Gange ist, mag allenfalls ein fahrlässiges Handeln begründen. Sofern berechtigte Zweifel am Vorsatz bestehen, ist eine Strafbarkeit nach den §§ 263a, 27 StGB in dubio pro reo abzulehnen.

II. Strafbarkeit wegen Geldwäsche, § 261 StGB

Das Geld, das sich auf dem Konto des Finanzagenten befindet ist taugliches Tatobjekt, da es aus einer der in § 261 I S. 2 Nr. 4 StGB genannten Taten stammt. Sobald der Finanzagent nun dieses Geld per Bar-Überweisung an den Phisher weiterleitet, könnte die Tathandlung des Verbergens/Verschleierns i.S.d § 261 I S. 1 StGB gegeben sein.
Verbergen ist jede Tätigkeit, die mittels einer nicht üblichen örtlichen Unterbringung oder einer den Gegenstand verdeckenden Handlung den Zugang zum Tatobjekt erschwert.[114] Darunter fällt auch die Geldüberweisung in andere Staaten.[115] Das Verschleiern der Herkunft umfasst alle irreführenden Machenschaften, die darauf abzielen, einem Tatobjekt den Anschein einer anderen (legalen) Herkunft zu verleihen oder zumindest die wahre Herkunft zu verbergen.[116]
Dies betrifft bspw. auch das Zurverfügungstellen eines Kontos zum Empfang illegaler Gelder.[117] Da sich die Tathandlung weitgehend überschneiden spielt es keine Rolle für welche Alternative man sich entscheidet. Beim Geldtransfer durch den Finanzagenten ist zumindest der objektive Tatbestand des § 261 StGB erfüllt.

[113] BGHSt 42, 135; Tröndle/Fischer, § 27 Rn. 8.
[114] Sch/Sch-Stree, § 261 Rn. 11.
[115] Tröndle/Fischer, § 261 Rn. 20.
[116] Sch/Sch-Stree, § 261 Rn. 11; Tröndle/Fischer, § 261 Rn. 21.
[117] AG Essen 12.1.1994 – 37 Ls 122/93 in ZIP 1994, S. 691.

Hinsichtlich des subjektiven Tatbestandes reicht es gem. § 261 V StGB aus, dass der Täter die tatsächliche Herkunft des Geldes leichtfertig nicht erkennt. Leichtfertigkeit liegt vor, wenn sich die kriminelle Herkunft des Gegenstandes nach Sachlage aufdrängt und der Täter dies aus besonderer Gleichgültigkeit oder grober Unachtsamkeit außer Acht lässt.[118] Ob der Finanzagent mit der Überweisung des Geldes leichtfertig handelt, ist nach den Umständen des Einzelfalls zu beurteilen. Wird ein hohes Entgelt für eine vergleichbare einfache und wenig aufwändige Tätigkeit, wie die Überweisung von Geld, versprochen liegt die Vermutung nahe dass hier etwas nicht stimmen kann. In einem solchen Fall trifft den Täter eine Erkundigungspflicht.[119]

III. Strafbarkeit wegen Verstoßes gegen das Kreditwesensgesetz (KWG)

Da es sich bei der Besorgung von Zahlungsaufträgen gegen Entgelt um eine Finanzdienstleistung handelt, macht sich ein Finanzagent regelmäßig auch nach den §§ 54 I Nr. 2, 32 I S. 1, 1 Abs. 1a Nr. 6 des KWG strafbar. [120]

IV. Ergebnis

Ob sich ein Finanzagent mit der Überweisung des Geldes dem Risiko einer Strafbarkeit aussetzt, hängt vom Einzelfall ab. Ignoriert er leichtfertig Tatsachen, die dafür sprechen, dass das Geld möglicherweise aus einer Straftat herrührt macht er sich der Geldwäsche nach § 261 StGB strafbar. Da ihm darüber hinaus nur in seltenen Fällen ein weitergehender Vorsatz zur Last gelegt werden kann, scheidet eine Strafbarkeit nach den §§ 263a, 27 StGB aus. Warum das Hammer Amtsgericht, in dem ihm vorliegenden Fall, den Angeklagten trotzdem nach §§ 263a, 27 und nicht nach § 261 StGB bzw. § 54 KWG verurteilte[121], ist nur schwerlich nachvollziehbar.

[118] BGH 33, 66; Tröndle/Fischer, § 261 Rn. 42.
[119] Tröndle/Fischer, § 261 Rn. 42.
[120] Vgl. Dazu die Pressemitteilung der Staatsanwaltschaft Konstanz vom 25.7.2006, abrufbar unter: http://www.jurpc.de/aufsatz/20060108.htm.
[121] AG Hamm 10 Ds 101 Js 244/05-1324/05, abgedruckt in: CR, 2006 S. 70ff.

F. Fazit

Die vorangegangene Darstellung hat gezeigt, dass bereits das geltende Recht eine strafrechtliche Erfassung des Phishing und dem Großteil seiner Abwandlungen ermöglicht.
Die Forderungen nach einem Einschreiten des Gesetzgebers und der Schaffung eines speziellen Phishing Tatbestandes sind somit unbegründet.
Schon die Aussage, dass Phishing straflos sei[122], ist nach den hier zu Grunde gelegten Auffassungen schlichtweg falsch. Zwar mag man bei einer abweichenden rechtlichen Würdigung zu dem Ergebnis kommen, dass zumindest die „vorbereitenden" Handlungen, wie das Versenden der E-Mail oder die Erstellung der Website, strafrechtlich nicht fassbar sind. Ob es deshalb jedoch der Einführung eines neuen Tatbestandes bedarf ist aus kriminalpolitischer Sicht äußerst fragwürdig. Die Kontaktaufnahme des Phishers zu seinem vermeintlichen Opfer ist für sich alleine genommen nichts weiter als eine (schriftliche) Lüge, bei der noch niemand zu Schaden kommt.
Falls es dem Phisher tatsächlich gelingt sein Opfer zu täuschen, macht er sich mit der Erlangung der Daten in den meisten Fällen nach dem Bundesdatenschutzgesetz strafbar.[123] Nutzt er danach diese Daten für vermögensschädigende Handlungen, greifen die §§ 263a und 202a StGB ein. Es besteht also ein umfassender strafrechtlicher Schutz.
Auch werden sich die „Phisher" durch einen neuen Tatbestand kaum abschrecken lassen, nehmen sie doch schon die drohende Strafbarkeit wegen Computerbetruges in Kauf.
Da sich gerade Banken und größere Unternehmen was die Phishing Attacken anbelangt sehr bedeckt halten, mit einer Strafanzeige würden ja Sicherheitslöcher in ihren Systemen bekannt, stellt sich darüberhinaus die Frage ob ein neuer Phishing Tatbestand auch wirklich „genutzt" würde.
Mit der steigenden technischen Versiertheit mit der Phishing Angriffe betrieben werden, man denke nur an Pharming oder Man in the middle Attacken, wird es auch immer schwerer werden die Täter tatsächlich zu fassen. Wer schon die notwendigen technischen Kenntnisse besitzt eine Pharming Attacke erfolgreich durchzuführen, dem wird es auch ein Leichtes sein seine Spuren, etwa mittels IP-Spoofing, so zu verwischen, dass eine Ergreifung durch die Strafverfolgungsbehörden nahezu aussichtslos erscheint. Es scheint mithin sinngerecht dem Phishing Phänomen auf technischer Ebene entgegen zu treten.

---

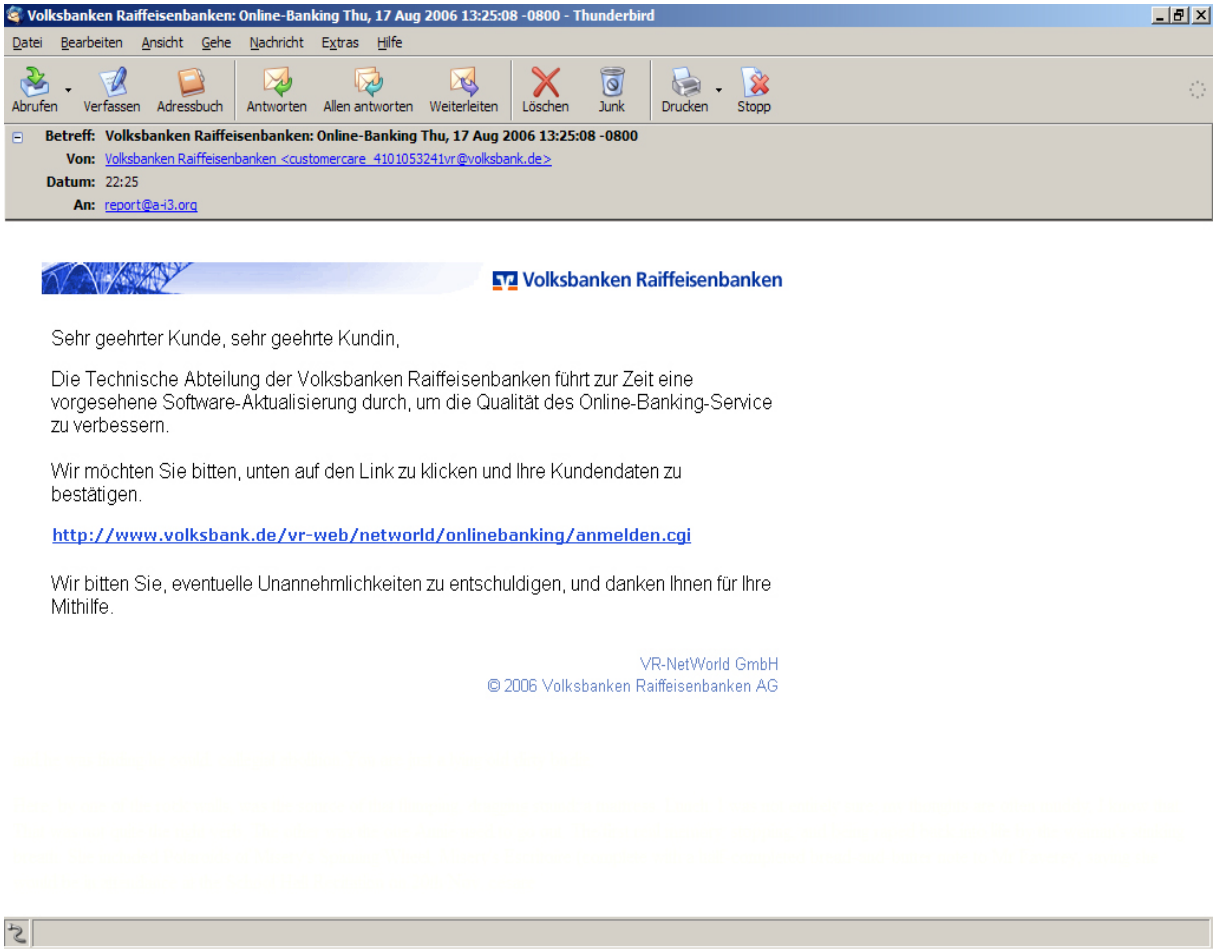
[122] vgl: Informationspapier der BITKOM, abrufbar unter: http://www.bitkom.org/files/documents/050426_BITKOMInformationspapier_zu_Phishing-V1.0f.pdf.
[123] siehe: B, I, 7.

Die Einführung neuer technischer Schutzmaßnahmen und die Aufklärung der Internetnutzer könnten dazu beitragen die Phishing Angriffe auf ein erträgliches Niveau zu senken.

G. Anhang

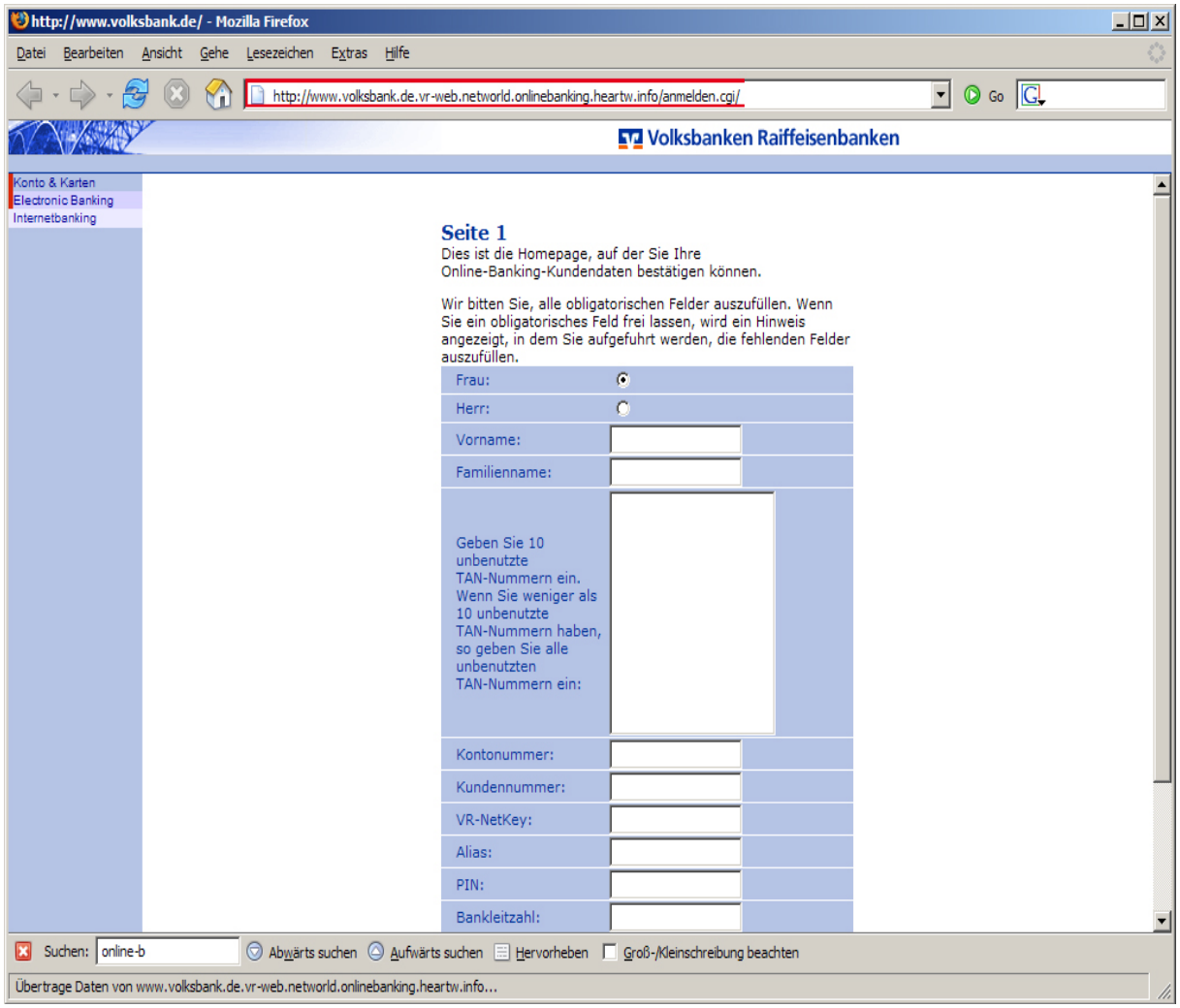
- **Abbildung 1: Phishing E-Mail**

(Quelle: https://www.a-i3.org/images/stories/Mails/17-08-06_volksbank.jpg)



- **Abbildung 2: Phishing Webseite**

(Quelle: https://www.a-i3.org/images/stories/Mails/17-08-06_volksbank2.jpg)



- **Abbildung 3: Geldwäsche Mail**

(Quelle: https://www.a-i3.org/content/view/908/138/)

Als Personalleiter unserer Gesellschaft bin ich seit Jahren für Rekrutierung zuständig und freue mich, Ihnen die vakante Position eines regionalen Managers für Zahlungsbearbeitung anzubieten. Da wir weltweit vertreten sind, kommen die Kunden aus vielen unterschiedlichen Ländern. Verwaltung der Geldtransfers, die von unseren deutschen Kunden beauftragt wurden , ist einer der Schwerpunkte, welche die zu jetzigen Zeitpunkt angebotene Tätigket ausmachen.

Zu den Aufgaben würden u.a folgende Tätigkeiten gehören

- Verwaltung und Weiterleitung der Kundengelder
- Hohe Erreichbarkeit und Verantwortungsbewusstsein

Ihre Vorteile:

- Sie werden zunächst unser Vertreter und Mittelsmann zwischen uns und unseren Kunden in Ihrem Land.
- Sie zahlen keine Gebühren und müssen nichts investieren (vergessen Sie betrügerische Stellenangebote, bei denen Sie erst zur Kasse gebeten werden).
- Sie haben eine flexible , interessante Arbeit , mit unterschiedlichen Tätigkeitsschwerpunkten und hohen Beförderungs-möglichkeiten
- Sie verdienen zuerst zwischen 500 und 1000 Euro pro Woche
- Sie können selbst Ihren Verdienst bestimmen. - da Sie auf einen Prozentsatz arbeiten - hängt Ihr Verdienst nur von Ihrer Arbeitsbereitschaft ab

Sie können Ihren Arbeitstag moglichst flexibel gestalten, um Ihrem Haupterwerb problemlos nachzugehen. Wichtig ist aber, daß unsere Kommunikation funktioniert und Sie für uns immer erreichbar sind. Es entstehen für Sie keine Ausgaben, d.h. Sie brauchen kein Startkapital, Investitionen oder eigene Auslagen.

An die Bewerber werden folgende Anforderungen gestellt

- Internet, E-Mail, Grundkenntnisse der Hauptzahlungssysteme.
- Es wäre wünschenswert, wenn Sie ein eigenes Konto in einem deutschen Geldinstitut mit Online Banking hätten.
- Für diese Beschäftigung brauchen Sie von 2 bis 8 Stunden freie Zeit in der Woche.
- Genauigkeit, Pünktlichkeit, Zuverlassigkeit und naturlich eine gesunde Arbeitseinstellung

Falls Sie für unser Angebot Interesse haben und bereit sind, eine gut bezahlte, aber auch verantwortungsvolle Arbeit auszuführen, so schreiben Sie uns bitte an: full-support@bk.ru

Eine kurzgefasste Bewerbung mit Foto ist besonders willkommen.

Nach der Bearbeitung Ihrer Bewerbung, wird Ihnen im Falle einer Zusage Ihre Tätigkeit genauestens erläutert, Sie werden mit unse-rer Gesellschaft bekannt gemacht und es folgt in kürze der Arbeitsvertrag

Wir hoffen auf eine gute und erfolgreiche Zusammenarbeit
Mit freundlichen Grüssen

Aleksej Kurilin

Ihre Email wurde uns von der B&W Werbegesellschaft zu Verfügung gestellt. Falls es zu einer Fehlinformation kam und Sie kein Interesse an den aufgeführten Tätigkeiten haben, betrachten Sie folgende Email als Gegenstandslos.

Diese Email wurde von einem unserer Email Roboter erstellt.
Antworten Sie bitte nicht an folgende Email mit der Option '' an Absender antworten''. , senden Sie keine Emails an die Absenderadresse, da Ihre Email automatisch gelöscht wird.

Ich versichere, dass ich diese Seminararbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe.

Freiburg, den 28.10.2006