Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Fachbereich Rechtspflege

Einblick in die Cybercrime am Beispiel des Phishing

Christoph Stammer
Dr. Anastasia Baetge [Hrsg.]

Beiträge aus dem Fachbereich Rechtspflege
Nr. 01/2014
Herausgeber der Reihe: Dekan Fachbereich Rechtspflege

Einblick in die Cybercrime am Beispiel des Phishing

Diplomarbeit

An der Hochschule für Wirtschaft und Recht in Berlin
Fachbereich Rechtspflege
Im Lehrgebiet Strafrecht

Vorgelegt von Christoph Stammer

Einstellungsjahrgang 2009
Prüfungsjahrgang 2012

Erstprüferin:	Prof. Dr. Anastasia Baetge
Zweitprüfer:	Prof. Roland Böttcher
Vorgelegt am:	27.03.2014

Inhaltsverzeichnis

A. Einleitung 1

B. Phänomen Internetkriminalität 2

I. Begriff und Funktionsweise – Medium Internet 2

II. Computerkriminalität / Internetkriminalität 2

III. Auslegung in die eng- bzw. weitgefasste Cybercrime 2

1. Cybercrime im engeren Sinne 3

2. Cybercrime im weiteren Sinne 3

C. Phishing 3

I. Herkunft 4

II. Klassisches Phishing (seit 2004) 4

III. Technischer Ablauf des Pharming 5

IV. Phishing per Malware 6

1. Eingriff durch Schadsoftware/Malware 6

2. Malwarephishing 6

a) Keylogger 7

b) Man-in-the-Middle-Angriff 7

c) DNS-Spoofing 7

d) Spear-Phishing 8

V. Entwicklung der Phishing-Formen 8

VI. Zwischenergebnis 9

D. Täter / Opfer 9

I. Täter 9

1. Underground Economy 10

2. Interessenlage 10

II. Opfer 11

E. Statistik 12

I. Internetnutzung 12

II. Schäden durch Cybercrime 13

III. Kriminalstatistik 14

IV. Zweckmäßigkeit der Untersuchung 14
V. Cybercrime im engeren Sinne 14
VI. Computerbetrug / Ausspähen und Abfangen von Daten 16
VII. Phishing 16
VIII. Nutzbarkeit der Kriminalstatistik 17
IX. Trends 18
X. Vergleich mit der Gesamtstatistik der erfassten Straftaten 19
F. Strafverfolgung durch Behörden 19
I. Ausgangssituation 19
II. Aufbau der Polizei bei Internetstraftaten 20
III. Polizeiliche Maßnahmen bei einem Phishing-Vorfall 20
IV. Hauptprobleme bei den Ermittlungen 21
G. Prävention 22
H. Strafbarkeit des Phishing 23
I. Auslandsbezug / Tatortprinzip 24
II. Strafbarkeit der Datenbeschaffung 25
1. § 202 a StGB - Ausspähen von Daten 25
2. § 202 b StGB - Abfangen von Daten 26
3. § 263 StGB - Betrug 26
4. § 240 StGB - Nötigung 27
5. § 263 a StGB - Computerbetrug 27
6. §§ 143, 143 a MarkenG und § 106 UrhG - Kennzeichenverletzung 27
7. § 44 Abs. 1, 43 Abs. 2 Nr. 1 und 4 BDSG - Datenverarbeitung und Erhebung 28
8. §§ 303 a, b StGB - Datenveränderung und Computersabotage 28
9. § 269 StGB - Fälschung beweiserheblicher Daten 28
a) Phishing-Mail 28
b) Die Phishing-Website 29
III. Strafbarkeit der Datenverwendung 30
1. § 202 a StGB - Ausspähen von Daten 30
2. § 202 b StGB - Abfangen von Daten 31

3. § 202 c StGB - Vorbereiten des Ausspähens und Abfangens von Daten 31
4. § 263 a StGB - Computerbetrug 32
5. § 269 StGB - Fälschung beweiserheblicher Daten
§ 270 StGB - Täuschung im Rechtsverkehr bei Datenverarbeitung 33
6. § 303 a StGB - Datenveränderung 34
7. § 303 b StGB - Computersabotage 34
8. Anwerben des Finanzagenten 34

IV. Besonderheiten bei der Datenbeschaffung durch Malware 35
1. § 263 a Abs. 3 StGB - Computerbetrug 35
2. § 303 a StGB - Datenveränderung 36

I. Zuviel des Guten - Beeinträchtigung der Softwareentwicklung 36
I. Beispiele für Dual-Use-Tools/objektiver Tatbestand des § 202 c StGB 37
II. Subjektiver Tatbestand des § 202 c StGB 37
III. Zwischenergebnis 38

J. Finanzagent / Finanzkurier 38
I. Anwerben des Finanzagenten / Finanzkurier 39
II. Strafbarkeit des Finanzagenten 39
III. §§ 263 a, 25 StGB - Strafbarkeit wegen Mittäterschaft zum Computerbetrug 39
IV. §§ 263 a, 27 StGB - Strafbarkeit wegen Beihilfe zum Computerbetrug 40
V. § 261 StGB - Geldwäsche; Verschleierung unrechtmäßig erlangter Vermögenswerte ... 41
VI. Verstoß gegen das Kreditwesengeschäft 42
VII. Zusammenfassung Finanzagent 42

K. Zusammenfassung der Diplomarbeit 42

L. Resümee 43

Anhang 45

Literatur und Quellenverzeichnis

Arbeitsgruppe Identitätsschutz im Internet	„Phishing“ – Stand 2014.
ARD / ZDF – Onlinestudie	vom 04.09.2013 Mobile Internetnutzung steigt rasant – Boom bei Endgeräten führt zu hohem Anstieg der täglichen Nutzungsdauer.
Beck, Simon Markus Dornis, Tim W.	„Phishing“ im Marken(straf)recht, CR 2007, Seite 642.
Bolduan, Gordon	Digitaler Untergrund, Technology Review, Ausgabe 4 / 2008, S.26 ff.
Borges, Georg	Stellungnahme zum Gesetzesentwurf der Bundesregierung zum Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität vom 19.03.2007 Rechtsfragen des Phishing – Ein Überblick, NJW 2005, Seite 3313 ff.
Biallaß, Isabelle Desiree	Zur Frage der Geldwäsche durch Weitergebe eingehender Gelder, ZUM 2006, Seite 879-880.
Bitkom-Studie	vom 12.02.2014 Smartphone-Boom setzt sich 2014 ungebrochen fort.
Bitkom-Studie	vom 19.07.2012 Online-Handel mit ausgezeichneten Perspektiven.
Bundesamt für Sicherheit in der Informationstechnik	Phishing gefährliche Umleitung für Ihre Passwörter. -Sicherheitstest-.
Bundeskriminalamt	Bundeslagebilder 2009-2012.
Bundesministerium Für Justiz	Besserer Schutz vor Hackern, Datenklau und Computersabotage, MMR 2006 Heft 11 XIV, Pressemitteilung vom 20.09.2006.
Bundesministerium für Wirtschaft und Energie	Cloud Computing (Stand: 2014).
Ernst, Stefan	Das neue Computerstrafrecht, NJW 2007, Seite 2661-2666.
Ester, Marc Aurél Benzmüller, Ralf	Underground Economy, gData (Stand: 2009).
Fahl / Winkler	Definition und Schemata Strafrecht, 3. Auflage, München 2010.

Fox, Dirk	Phishing, DuD 2005, S. 365.
Gercke, Marco Brunst, Phillip	Praxishandbuch Internetstrafrecht, 1. Auflage, Stuttgart 2010.
Gercke, Marco	„Die Strafbarkeit von Phishing und Identitätsdiebstahl“, CR 2005, S. 606 ff.
Goeckenjan, Ingke	Phishing von Zugangsdaten für Online-Bankdienste und deren Verwertung, wistra 2008, Seite 128.
	Auswirkungen des 41. Strafrechtsänderungsgesetzes auf die Strafbarkeit des „Phishing“, wistra 2009, Seite 47.
Graf, Jürgen-Peter	Phishing derzeit nicht generell strafbar, NStZ 2007, Seite 129 ff.
Geschonneck, Alexander	Computerforensik – Computerstraftaten erkennen, ermitteln, aufklären, 5. Auflage, Heidelberg 2011.
Handelsblatt vom 20.03.2012	Smartphone-Nutzer fallen immer häufiger auf Phishing herein „China-Mobile verkauft jetzt I-Phones“, vom 17.01.2014
Heise Security	„Angriffe auf mit mTAN geschützten Konten“, vom 01.08.2013 „immer mehr mTAN-Betrugsfälle“, vom 31.10.2013
Kochheim, Dieter	Cyberfahnder IuK-Strafrecht – System, Begriffe, und Fallbeispiele (Stand: 01.05.2012).
	Cyberfahnder – Über das Verschwinden der Cybercrime; Automatisierte Malware (Stand: April 2012).
	Cyberfahnder – Malware, Social-Engeneering, Underground Economy (Stand: 24.05.2010).
Neuheuser, Stephan	Die Strafbarkeit des Bereithaltens und Weiterleitens des durch Phising erlangten Geldes, NStZ 2008, Seite 492.
Polizei	Polizeiliche Kriminalstatistik 2006-2012, Online-Dienst der Polizei
Popp, Andreas	Phishing, Pharming und das Strafrecht, MMR 2006, Seite 84 Von Datendieben und Betrügern – Zur Strafbarkeit des sogenannten Phishing, NJW 2004, S. 3517.
Reuters, Nachrichtenagentur vom 09.05.2013	Huge cyber bank theft spans 27 countries.

Seidel, Alexander	Die Strafbarkeit des Phishing nach Inkrafttreten des 41. Strafrechtsänderungsgesetzes , Online-Zeitschrift für Höchstrichterliche Rechtsprechung (hrr-Strafrecht.de) Heft 2/2010, Seite 85 ff.
Sparkasse Saarbrücken	Vishing.
Statistisches Bundesamt	Statistisches Jahrbuch, Deutschland und Internationales 2013 (Stand: 01.08.2013).
Stuckenberg, Friedrich	Zur Strafbarkeit von Phishing, ZStW 2006, Seite 879 ff.
Die Welt vom 16.01.2014	Telekom warnt vor falschen Rechnungen mit Viren.
Wernert, Manfred	Internetkriminalität - Grundlagenwissen, erste Maßnahmen und polizeiliche Ermittlungen, Stuttgart 2012.
Die Zeit vom 10.03.2014	Android wird zum Weltbetriebssystem.

Kommentare

Fischer, Thomas	Beck‘sche Kurz-Kommentare - Strafgesetzbuch, 61. Auflage, München 2014, StGB, § … Rnr.
Juris PraxisKommentar	Heckmann juris Praxiskommentar – Internetrecht, 2. Auflage Stand 2009, StGB,§ … Rnr.
Palandt	Beck‘sche Kurz-Kommentare – Bürgerliches Gesetzbuch, 73. Auflage, München 2014, BGB, § … Rnr.
Schönke / Schröder	Kommentar zum Strafgesetzbuch, 28. Auflage, München 2010, StGB, § … Rnr.

Rechtsprechung

Bundesgerichtshof	2. Strafsenat, Beschluss vom 26.04.2013 – 2 Ars 91/13 2. Strafsenat, Urteil vom 29.11.2006 - 2 StR 301/06 3. Strafsenat, Beschluss vom 28.02.2012 – 3 StR 453 / 11
Oberlandesgericht Koblenz	„Strafverfahren: Beschränkung der Berufung bei fehlerhafter Subsumtion des festgestellten Sachverhalts; Entscheidung im Revisionsverfahren“ 1. Strafsenat, Urteil vom 10.10.2007 – 1 Ss 267 / 07

Quellenverzeichnis

https://www.a-i3.org/content/view/932/203/ (recherchiert am 05.01.2014)

http://www.ard-zdf-onlinestudie.de/fileadmin/Onlinestudie/PDF/PM1_ARD-ZDF-Onlinestudie_2013.pdf (recherchiert am 03.01.2014)

http://www.bitkom.org/78651_78640.aspx (recherchiert am 12.02.2014)

http://www.bitkom.org/de/presse/74532_72867.aspx (recherchiert am 12.02.2014)

http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true (recherchiert am 15.11.2013)

https://www.bka.de/DE/Publikationen/PolizeilicheKriminalstatistik/pks__node.html?__nnn=true (recherchiert am 15.11.2013)

https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Phishing/phishing_node.html (recherchiert am 15.11.2013)

http://www.bmj.bund.de/media/archive/1317.pdf (recherchiert am 17.10.2013)

http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Navigation/Themen/cloud-computing.html (recherchiert am 15.02.2014)

https://www.sicherheitstest.bsi.de/ (recherchiert am 08.02.2014)

http://www.cyberfahnder.de/doc/Kochheim-IuK-Strafrecht.pdf (recherchiert am 15.11.2013)

http://www.cyberfahnder.de/doc/Kochheim-Cybercrime-Malware.pdf (recherchiert am 15.11.2013)

http://www.cyberfahnder.de/doc/Cybercrime-2010.pdf (recherchiert am 13.03.2014)

https://www.gdata.de/uploads/media/Whitepaper_Underground_Economy_9_2009_DE.pdf (recherchiert am 17.01.2014)

http://www.handelsblatt.com/technologie/it-tk/mobile-welt/it-sicherheit-smartphone-nutzer-fallen-haeufiger-auf-phishing-herein/6349776.html (recherchiert am 11.11.2013)

http://www.handelsblatt.com/unternehmen/it-medien/apple-expandiert-china-mobile-verkauft-jetzt-iphones/9349666.html (recherchiert am 17.01.2014)

http://www.heise.de/security/meldung/Angriffe-auf-mit-mTAN-geschuetzte-Konten-1928312.html (recherchiert am 08.10.2013)

http://www.heise.de/tp/news/Immer-mehr-mTan-Betrugsfaelle-2049308.html (recherchiert am 05.11.2013)

http://www.hrr-strafrecht.de/hrr/archiv/10-02/index.php?sz=7 (recherchiert am 13.09.2013)

http://www.pcwelt.de/ratgeber/Ist-der-PC-infiziert-Was-sind-Botnetze-und-was-hilft-dagegen-1084516.html (recherchiert am 11.11.2013)

http://www.kriminalpolizei.de/service/praevention-kompakt.html?tx_contagged[source]=default&tx_contagged[uid]=143&cHash=ed9d31b9681f238452038577ebbbc08f (recherchiert am 13.03.2014)

http://www.linksandlaw.de/linkingundframing6.htm (recherchiert am 22.02.2014)

http://www.abendzeitung-muenchen.de/inhalt.wie-sicher-ist-online-banking-bankkonto-leergeraeumt-trotz-mtans.6aa31670-0cfa-4fac-bb90-37e9dddd8f25.html (recherchiert am 22.03.2014)

http://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/phishing/tipps.html (recherchiert am 08.02.2014)

http://www.reuters.com/article/2013/05/09/net-us-usa-crime-cybercrime-idUSBRE9480PZ20130509 (recherchiert am 03.10.2013)

https://www.sparkasse-saarbruecken.de/onlinebanking/online_banking_angebot/vishing/beschreibung/index.php?n=%2Fonlinebanking%2Fonline_banking_angebot%2Fvishing%2Fbeschreibung%2F (recherchiert am 03.10.2013)

http://de.statista.com/statistik/daten/studie/186370/umfrage/anzahl-der-internetnutzer-weltweit-zeitreihe/ (recherchiert am 03.01.2014)

http://de.statista.com/statistik/daten/studie/3979/umfrage/e-commerce-umsatz-in-deutschland-seit-1999/ (recherchiert am 12.02.2014)

https://www.destatis.de/DE/Publikationen/StatistischesJahrbuch/StatistischesJahrbuch2013.pdf?__blob=publicationFile (recherchiert am 19.11.2013)

http://www.verbraucher-sicher-online.de/artikel/etan-itan-mtan-welche-denn-nun?page=0,6 (recherchiert am 11.11.2013)

http://www.welt.de/wirtschaft/webwelt/article123928616/Telekom-warnt-vor-falschen-Rechnungen-mit-Viren.html (recherchiert am 16.01.2014)

http://wirtschaftslexikon.gabler.de/Archiv/2682/dialer-v9.html (recherchiert am 15.11.2013)

http://www.zeit.de/digital/mobil/2014-03/google-bringt-entwickler-umgebung-fuer-wearables-android/seite-2 (recherchiert am 10.03.2014)

Abkürzungsverzeichnis

Abs.	Absatz
Aktz.	Aktenzeichen
a.a.O.	am angegebenen Ort
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BDSG	Bundesdatenschutzgesetz
BKA	Bundeskriminalamt
bzgl.	bezüglich
CR	Computer und Recht
dt.	deutsch
d.h.	das heißt
DuD	Datenschutz und Datensicherheit
ff.	fortfolgende
grds.	Grundsätzlich
HRRS	Höchstrichterliche Rechtsprechung im Strafrecht
iTAN	indizierte Transaktionsnummer
KWG	Kreditwesengesetz
LKA	Landeskriminalamt
MarkG	Markengesetz
MMR	MultiMedia und Recht
NJW	Neue Juristische Wochenzeitschrift
mTAN	mobile Transaktionsnummer
NStZ	Neue Zeitschrift für Strafrecht
OLG	Oberlandesgericht
PIN	Persönliche Identifikationsnummer
PKS	Polizeiliche Kriminalstatistik
Rnr.	Randnummer
S.	Satz
StGB	Strafgesetzbuch
TAN	Transaktionsnummer
u.	und
UrhG.	Urheberrechtsgesetz
v.	vom
vgl.	Vergleich
wistra	Zeitschrift für Wirtschaft und Steuerrecht

z.B.	zum Beispiel
ZUM	Zeitschrift für Urheber und Medienrecht

A. Einleitung

Vorgelegt wird die Diplomarbeit mit dem Titel „Einblick in die Cybercrime am Beispiel des Phishing“. Sie soll einen Überblick über die Entwicklung, die aktuellen Formen und die rechtliche Bewertung dieser Art der Kriminalität geben. Unter dem Begriff des Phishing versteht man das Entwenden persönlicher Daten, um einen finanziellen Vorteil zu erlangen. Bekannt ist die Straftat daher durch das „Abphishen“ von Kontozugangsdaten und Passwörtern.

Es wird in der Arbeit zuerst auf die unterschiedlichen Erscheinungsformen der Tathandlung „Phishing“ eingegangen, um zu erfahren, wie komplex und intelligent die Straftat mittlerweile ausgeführt wird.
Im Anschluss soll anhand der Fallzahlen der polizeilichen Kriminalstatistik und den Bundeslagebildern des Bundeskriminalamtes der Jahre 2006 bis 2012 ein Vergleich gezogen werden. Es wird dabei versucht, mögliche erkennbare Trends abzuleiten. Um ein besseres Verständnis für die Präventions- und Bekämpfungsmethoden des Phishing zu erlangen, wird anschließend das Verhältnis zwischen Cyberkriminellen und Opfern näher beleuchtet.

Ziel der Arbeit ist es, einen Gesamtüberblick hinsichtlich eines der bekanntesten und facettenreichsten Themen der Internetkriminalität zu erlangen. Auf rechtlicher Ebene soll dabei geprüft werden, ob es eines eigenen Straftatbestandes hinsichtlich des Phishing bedarf. Des Weiteren werden die unmittelbar Beteiligten näher beleuchtet. Dabei wird der „Helfer“ des Cyberkriminellen, der sogenannte Finanzagent auf seine Strafbarkeit und die IT-Branche hinsichtlich ihrer Betroffenheit geprüft.

B. Phänomen Internetkriminalität

Längst haben Kriminelle das Internet für Straftaten aller Art als Tatmittel für sich entdeckt. Der rasante Fortschritt in der Technologie beeinflusst die Erscheinungsformen dieser Kriminalität sowie Tat- und Tätertypologien nachhaltig. [1]

I. Begriff und Funktionsweise – Medium Internet

Als Internet wird ein elektronisches, weltweit erreichbares Netzwerk bezeichnet, in dem Datenpakete versandt werden. [2] In Deutschland nutzen 77,2 % der Gesamtbevölkerung das Internet täglich, dies entspricht 54,2 Millionen Menschen. Die durchschnittliche tägliche Nutzungsdauer des Internets liegt bei den Deutschen bei 169 Minuten. [3] Weltweit nutzen mehr als 2.5 Milliarden Menschen das Internet. [4] Aufgrund der immensen Geldbewegungen, welche im Internet stattfinden, ist es nicht verwunderlich, dass es auch zu kriminellen Zwecken genutzt wird.

II. Computerkriminalität / Internetkriminalität

„IuK" – Kriminalität, ist die Kriminalität, die im Zusammenhang mit der Informations- und Kommunikationstechnik steht. Sie umfasst alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik, oder gegen diese begangen werden.[5] In Deutschland ist sowohl der Begriff IuK – Kriminalität wie auch der Begriff Cybercrime gebräuchlich.[6] Die Internetkriminalität stellt dabei einen enger gefassten Bereich der Computerkriminalität dar.[7]

III. Auslegung in die eng- bzw. weitgefasste [8] Cybercrime

Um eine sinnvolle Abgrenzung zu schaffen, ist es nicht hilfreich zu versuchen die Internetkriminalität von der Computerkriminalität zu differenzieren. Da diese in den meisten Fällen einen fließenden Übergang hat, wird zwischen der engeren und der weiteren Auslegung der IuK-Kriminalität unterschieden.[9]

---

[1] Vgl. Wernert S. 10.
[2] Vgl. Wernert S. 9.
[3] ARD / ZDF Onlinestudie 2013 - http://www.ard-zdf-onlinestudie.de/fileadmin/Onlinestudie/PDF/PM1_ARD-ZDF-Onlinestudie_2013.pdf (recherchiert am 03.01.2014).
[4] Das Statistikportal - Statista http://de.statista.com/statistik/daten/studie/186370/umfrage/anzahl-der-internetnutzer-weltweit-zeitreihe/ (recherchiert am 03.01.2014).
[5] Allgemeingültige Definition des Bundeskriminalamtes.
[6] Vgl. Bundeslagebild und polizeiliche Kriminalstatistik im Zuge der Europäisierung.
[7] Vgl. Kochheim – Cyberfahnder IuK-Strafrecht S. 9.
[8] Vgl. Kochheim – Cyberfahnder IuK-Strafrecht S. 9.
[9] Vgl. Wernert S. 13 ff.

1. Cybercrime im engeren Sinne

Der enger gefasste Begriff des Cybercrime beschreibt die Erscheinungsformen, bei denen eine unmittelbare Nutzung und Missbrauch der Informations- und Kommunikationstechnik erfolgt.[10] Sie umfasst den betrügerischen Einsatz von Dialern [11] der Manipulation und missbräuchlichen Verwendung von Schadprogrammen / Malware (Keylogger; Trojaner) sowie der Nutzung von Botnetzen[12] um die wahren Täterkreise zu anonymisieren.[13] Dieser Bereich wurde zeitweise mit bis zu 90 % durch das Phishing dominiert. [14] Diese Vorbereitungshandlung dient dann im Nachhinein für weitere Straftaten oder den Verkauf der unzulässig abgegriffenen Daten in der „Underground Economy“[15]. Das Problem des Phishings und die mit dem Phishing abgedeckten Strafnormen lassen sich unter die Cybercrime im engeren Sinne subsumieren.[16]

2. Cybercrime im weiteren Sinne

Der weiter gefasste Begriff beinhaltet alle Straftaten, bei denen mithilfe von Informations- und Kommunikationsmedien (dem Internet, Telefon usw.) Straftaten geplant, vorbereitet und ausgeführt werden.[17] Die Straftaten stellen für sich betrachtet keine IuK – Straftaten dar (z. B. die Beleidigung § 185 StGB; Erpressung § 253 StGB). Es ist möglich fast jede Straftat über die IuK zumindest zu effektiveren.

C. Phishing

Der Begriff Phishing ist ein englisches zusammengefügtes Kunstwort aus „P“ für „Password“ und „fishing“ für Fischen. Es beschreibt die Erlangung von Daten über gefälschte Webseiten, betrügerische E-Mails und Schadsoftware/Malware (Trojaner;

[10] Vgl. Kochheim - Cyberfahnder IuK-Strafrecht S.9.
[11] Kostenpflichtige Einwahlprogramme ins Internet – Vgl. (Wirtschaftslexikon Gabler) http://wirtschaftslexikon.gabler.de/Archiv/2682/dialer-v9.html (recherchiert am 15.11.2013).
[12] Vgl. Wernert S. 15 - Botnetze: Zusammenschluss von fremdgesteuerten Rechnern; Vgl. http://www.pcwelt.de/ratgeber/Ist-der-PC-infiziert-Was-sind-Botnetze-und-was-hilft-dagegen-1084516.html (recherchiert am 11.11.2013).
[13] Vgl. Kochheim a.a.O.
[14] Vgl. Wernert S. 14.
[15] Illegales Wirtschaftsforum der Cyberkriminellen.
[16] Vgl. Kochheim - Cyberfahnder IuK-Strafrecht S. 9, 28.
[17] Vgl. Wernert S. 17, Vgl. Kochheim a.a.O.

Keylogger) durch Kriminelle. [18] Wobei nicht nur Passwörter für Konten abgefangen werden, sondern auch alle anderen zur digitalen Identität[19] gehörenden Daten.

I. Herkunft

Der massenhafte Abgriff von geheimen Daten, insbesondere Zugangsdaten wie PIN und TAN für das Online-Banking erfolgt verstärkt seit 2004 [20] und hat seinen Ursprung in den USA.[21] Dort wurde das Phänomen erstmals 1996 beschrieben. Die damaligen ausgespähten Zugangscodes „Phishes" nutzten die Hacker, um einen kostenlosen Zugang zum Internet zu erlangen. [22] In der heutigen Zeit ist eine Internetverbindung eine kostengünstige Angelegenheit und die damalige Art des phishen existiert nicht mehr. Da das Phänomen des Phishings einem ständigen Wandel unterzogen ist, werden nachfolgend die aktuellen Erscheinungsformen vorgestellt.

II. Klassisches Phishing (seit 2004)

Das klassische Phishing ist heute vielfach bekannt unter dem Versenden unzähliger Massenmails (Spam-Mails). Diese werden an unwissende Home-Banking-Kunden und beliebige Nutzer verschiedener Internetdienste versandt, bei denen finanzielle Transaktionen über das Internet abgefertigt werden. [23] Die erforderlichen E-Mailadressen werden in Internetforen zuvor käuflich erworben.[24] In dieser Form war Phishing jahrelang in seiner häufigsten Form anzutreffen. Das Opfer wurde aufgefordert, seine vertraulichen Zugangsdaten an den jeweiligen Vertragspartner zu übermitteln.[25] Es kann sich hierbei ganz klassisch und in der häufigsten Form um die PIN und TAN [26] - Nummern handeln, aber auch um Kreditkartennummern;

---

[18] Vgl. Die Kriminalpolizei – Zeitschrift der Gewerkschaft der Polizei http://www.kriminalpolizei.de/service/praevention-kompakt.html?tx_contagged[source]=default&tx_contagged[uid]=143&cHash=ed9d31b9681f238452038577ebbbc08f (recherchiert am 13.03.2013).

[19] „Die digitale Identität definiert die persönlichen Möglichkeiten und Rechte Einzelner im Internet und ermöglicht auf diese Weise Aktivitäten im Netz. Konkret handelt es sich um alle Nutzer-Accounts also z.B. Zugangsdaten zu Online Vertriebsportalen (Amazon, Ebay) ; Social-Networking-Plattformen (Facebook, Twitter) ; berufsspezifische Informationen bei Heimarbeitsplätzen; E-Mail-Accounts; Bankkonten und Aktiendepots; alle zahlungsrelevanten Informationen" – Wernert S. 14 ff.

[20] Vgl. Borges, Stellungnahme zum Gesetzesentwurf der Bundesregierung zum Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität vom 19.03.2007.

[21] Vgl. Stuckenberg (2006) S. 881.

[22] Vgl. Fox (2005) S. 365.

[23] Vgl. Fox (2005) S. 365; Kochheim - Cyberfahnder IuK-Strafrecht S. 28 ff; Wernert S. 99.

[24] Siehe Anhang, Abbildung Nr. 1, gData - Preisliste für Underground Artikel.

[25] Siehe Anhang, Abbildung Nr. 2 Arbeitsgruppe Identitätsschutz im Internet- Phishingmail.

[26] PIN: Personal Identification Number ; TAN: Transaktionsnummer.

Kennwörter oder die Zugangsdaten zu verschiedenen Internetdiensten wie PayPal oder Amazon.

Die Übermittlung der Daten an den „Phisher“ kann auf unterschiedlichste Arten erfolgen. Die „Ur-Form“, dass der Benutzer seine Kontaktdaten in die vorgefertigten Kästchen in der E-Mail einträgt und direkt an den Phisher weiterleitet, verliert mittlerweile durch Präventionsmaßnahmen und technische Entwicklungen an Bedeutung.[27]

Oftmals ist der E-Mail ein Link beigefügt, welchem der Nutzer folgen soll.[28] Das Opfer wird dann zu einer entsprechenden Seite weitergeleitet, welche seiner Bankwebsite verblüffend ähnlich nachgebildet ist.[29] Auch die Bedienung der Seite ist identisch. Diese Täuschungsmethoden und Überredungstechniken werden „Social Engineering“ genannt.[30] Der Nutzer soll keinen Verdacht schöpfen, dass er gerade nicht seiner Bank dabei hilft, ihren Service zu verbessern (oftmals Vorwand der „Phisher“ um an die Daten zu kommen), sondern einem Datenklau erliegt.[31] Da die gefälschten Webseiten sich oftmals auf mehreren unterschiedlichen Servern befinden und dies einer „Farm“ ähnelt, wenn der Täter im Nachhinein die Daten nur noch einsammelt, spricht man bei dieser Anwendungsform auch vom „Pharming“.[32]

III. Technischer Ablauf des Pharming

Um den Pharmingangriff zu verstehen, muss man wissen, dass jeder Seite im Internet eine bestimmte IP-Adresse zugeordnet ist. Diese IP-Adresse ist grundsätzlich nur einmal im Netz vergeben. Da man sich diese Zahlencodes (z. B. 85.151.52.87) eher schlecht merken kann, werden in der obigen Adressleiste diese Zahlen automatisch einem Domainnamen (Domainname zur obigen IP-Adresse http://www.polizei-bw.de/Seiten/default.aspx) zugeordnet, mittels dem „Domain Name System“ (DNS). [33] Gibt der Internetnutzer nun einen Domainnamen in seinen Browser[34] ein, so ordnet das DNS die entsprechende aufzurufende IP zu.

Der Pharmer ändert die Internetadresse / den Domainnamen nur minimal, um seine Glaubwürdigkeit zu erhalten. Auch die Fälschung einer vermeintlich sichereren https.// - Verbindung mit Sicherheitsschlüssel ist kein Problem und trägt zur Täuschung bei.

---

[27] Vgl. Kochheim, Automatisierte Malware S. 3.
[28] Siehe Anhang, Abbildung Nr. 3 Arbeitsgruppe Identitätsschutz im Internet – Pharming.
[29] Vgl. Geschonneck – Computerforensik, Seite 14; Vgl. Seidel HRRS (2010) S. 85 ff.; Goeckenjan wistra (2008) S. 128.
[30] Vgl. Kochheim a.a.O.
[31] Vgl. Fox (2005), Seite 365.
[32] Vgl. Kochheim - Cyberfahnder IuK-Strafrecht S. 28-30.
[33] Vgl. Wernert S. 49.
[34] Bsp. Firefox, Explorer, Google Crome

Am Ende steht immer die Weiterleitung der abgefangenen Daten an den Phisher / Pharmer oder eine Zwischenspeicherung auf einem sogenannten Drop-Zone-Server, um die Daten dann weiter zu veräußern.[35]

IV. Phishing per Malware

Malware stellt eine systemfremde Software dar, welche in die Systemintegrität einer anderen Software (z. B. Website der Bank; Einwahlprogramm ins Internet auf dem heimischen PC) eingreift. Der Zweck von Malware kann zerstörerisch sein (Dateien löschen; System unbrauchbar machen), ausforschend (Keylogger) oder missbräuchlich (modernes Phishing / Pharming). [36] Es handelt sich um eine bösartige Software, daher setzt sich das Wort Malware aus den englischen Wörtern „Malicious“ und „Software“ zusammen. [37] Weitere geläufige Begriffe für diese Schadsoftware sind Computerviren, Trojaner, Würmer oder Spyware.

1. Eingriff durch Schadsoftware/Malware

Ein Angriff mit einer Schadsoftware ist in immer gleiche Phasen unterteilbar. Über eine Außenverbindung erfolgt eine Injektion (Schritt Nr. 1) mit einem schädlichen Code (USB-Stick, Anhang einer E-Mail; oder Drive-By-Infection[38]). Dieser Code veranlasst die Software eine bestimmte Funktion auszuführen (Schritt Nr. 2 Infektion) unter Ausnutzung eines Exploits[39] in der Software. Befindet sich das Schadprogramm nun innerhalb der Software, kann es sich installieren und weitere Schadprogramme nachladen (Schritt Nr. 3). Je nach Funktion und Aufbau kann die Malware nun aktiv werden.[40]

2. Malwarephishing

Es gibt je nach Aufbau und Funktion der Malware verschiedene Möglichkeiten für den Phisher.

---

[35] eine Drop-Zone ist ein für den Kriminellen sicherer, anonymer, digitaler Speicherort von dem die erlangten Daten auch unproblematisch aus verschoben und verkauft werden können https://www.dsin-blog.de/drop-zone - siehe nachfolgend auch „Underground Economy“.
[36] Kochheim - Cyberfahnder IuK-Strafrecht S. 23.
[37] Vgl. BKA Cybercrime Bundeslagebild 2009.
[38] Drive-By-Infection : Schadsoftware wird beim Aufruf einer beliebigen Internetseite ohne Wissen des Opfers und ohne optische Anzeichen installiert – Vgl. Wernert S.99.
[39] Ist eine Schwachstelle im System der Software.
[40] Vgl. Kochheim - Cyberfahnder IuK-Strafrecht S. 24 ff.

a) Keylogger

Über einen Keylogger werden alle Tastatureingaben protokolliert und an den Täter weitergeleitet.[41]

b) Man-in-the-Middle-Angriff

Möglich ist auch ein Zwischenschalten der Malware als sogenannter Man-in-the-Middle-Angriff. Bei dieser Variante werden die Zugangsdaten normal von dem Benutzer eingegeben und das Onlinebanking-Konto freigeschaltet. Erst nachdem der Zutritt zum Konto erfolgt ist, schaltet sich die Schadsoftware zwischen Bank und Benutzer. Dies hat den Vorteil für den „Phisher", dass Sicherheitsfeatures wie es kleine Bilder sogenannte „Captchas"[42] oder das m-TAN Verfahren darstellen, durch das Opfer selbst umgangen werden. TAN und PIN werden dann automatisch von der Schadsoftware abgefragt bzw. das Geld wird direkt auf ein durch den Phisher vorab ausgesuchtes Konto überwiesen.[43] Rückmeldungen der Bank an den legitimen Online-Banking Benutzer werden unterdrückt.

c) DNS-Spoofing

Beim DNS-Spoofing wird durch die Malware die sogenannte Hostdatei des Betriebssystems geändert. Die Hostdatei ist eine lokale Textdatei und hat die Aufgabe eine schnellere Verbindung zu Webseiten aufzubauen, welche häufig aufgerufen werden.[44] Die aufgerufene IP-Adresse ist demnach vorgespeichert in der Hostdatei und es ist nicht mehr nötig einen externen DNS-Server zwischenzuschalten, dies spart in der Praxis Zeit.[45] Die Hostdatei leitet den Benutzer nun direkt auf die nachgeahmte Website des „Phishers". Diese Website ist für den Benutzer nicht mehr zu unterscheiden von der Originalwebsite.

Die Einführung des Mobile-TAN-Verfahrens (m-TAN oder auch sms-TAN) 2011/2012 sorgte zeitweise für einen starken Rückgang der Phishingzahlen und hebelte das DNS-Spoofing und andere Malware aus.[46] Durch die Nutzung eines zweiten Authentifizierungsgerätes (Handy, Smartphone) konnte eine weitere Sicherheitsstufe erschaffen werden. Die Tan wird erst generiert, wenn die Überweisung auf dem PC bestätigt werden muss. Der Benutzer erhält daraufhin

---

[41] Vgl. Kochheim - Cyberfahnder IuK-Strafrecht S. 24 ff.
[42] Siehe Anhang, Abbildung Nr. 4 - Sicherheitssoftware um Übergriffe mittels Malware zu verhindern.
[43] Vgl. Kochheim - Cyberfahnder IuK-Strafrecht S. 28.
[44] Vgl. Kochheim - Malware, Social-Engeneering, Underground Economy (2010) S. 105 ff.
[45] Siehe technischer Ablauf des Pharming.
[46] Vgl. Heise Security http://www.heise.de/security/meldung/Angriffe-auf-mit-mTAN-geschuetzte-Konten-1928312.html (recherchiert am 08.10.2013).

eine SMS-Nachricht, in der alle wichtigen Transaktionsdaten enthalten sind (Empfänger, Höhe des Geldbetrages und TAN-Nummer).[47]

Allerdings konnten auch diese Sicherheitsmaßnahmen bereits umgangen werden. Die Täter ließen sich eine weitere SIM-Karte für das Handy ausstellen und leiteten die TAN auf dieses Handy weiter.[48] Bei diesem Verfahren werden gezielt vermögende Benutzer ausgewählt mit hohem Überweisungslimit. Es wurden mehrere Fälle mit sechsstelligen Beträgen in Deutschland registriert.[49]

d) Spear-Phishing

Eine weitere Variante stellt das sogenannte „Spear-Phishing“ (engl. Speer) dar. Im Vergleich zu der massenhaften Verbreitung von Schadsoftware wird hier ein gezielter Angriff mittels Phishing-Mails auf ein bestimmtes Unternehmen oder eine bestimmte Bank geführt.[50] Die Mail ist dabei intelligent an den Web-Auftritt eines Geschäftspartners ausgerichtet. Der Erfolg ist bei diesen Attacken erheblich größer. Zum einen schöpfen Mitarbeiter seltener Verdacht, wenn sie in „gewohnter Umgebung“ getäuscht werden und zum Anderen werden die Phishing-Mails oftmals nicht als solche von den elektronischen Schutzprogrammen der Mail-Dienste wahrgenommen. Diese Malware-Abwehrmethoden funktionieren, in dem sie bereits bekannte Phishing-Mails abgleichen und löschen.[51] Völlig neue und individuell zugeschnittene Mails können nicht erkannt werden.

Den größten bisher durch eine Malware-Phishing-Attacke verursachten Schaden vermeldete die Bank of Muscat aus dem Oman am 19.02.2013. Es handelt sich hierbei auch um einen Spear-Phishing-Angriff, da nur Nutzer der Bank of Muscat betroffen waren. In 24 Ländern wurden innerhalb von 10 Stunden bei 36.000 Transaktionen insgesamt 40 Millionen US-Dollar erbeutet.[52]

V. Entwicklung der Phishing-Formen

Der neueste Trend der Phishing-Arten wird durch die ansteigende Benutzung sozialer Netzwerke wie Facebook und Twitter gefördert. Zum einen geben Benutzer schon eine Menge Informationen auf den Seiten öffentlich preis und zum anderen werden hier Spear-Phishing-Mails von „vermeintlichen Freunden“ versandt. Es wird darauf spekuliert, dass das Opfer weniger Argwohn hat, einen bestimmten Link

[47] Vgl. Heise Security a.a.O.
[48] Vgl. Heise Security http://www.heise.de/tp/news/Immer-mehr-mTan-Betrugsfaelle-2049308.html (recherchiert am 05.11.2013).
[49] Vgl. Heise Security a.a.O.
[50] Vgl. Geschonneck, S. 14.
[51] Vgl. Geschonneck, S. 15.
[52] Vgl. http://www.reuters.com/article/2013/05/09/net-us-usa-crime-cybercrime-idUSBRE9480PZ20130509 (recherchiert am 03.10.2013).

(Link enthält Malware) zu öffnen, wenn dieser von einer gut bekannten Person ohne erkennbare Schädigungsabsicht versendet wird.[53]

Eine weitere Entwicklung ist die Nutzung der Internettelefonie um Zugangsdaten abzugreifen. Es hat sich hier der Begriff des „Vishings“ etabliert.[54] Es werden dabei wahllos durch eine Software potentielle Opfer angerufen. Nimmt ein Benutzer das Gespräch an, wird er mit einer Bandansage einer größeren Bank konfrontiert. Es wird dem Opfer mitgeteilt, dass seine Zugangsdaten missbraucht wurden und er diese bei einem Rückruf bestätigen soll. Kommt es nun zu dem Fall, dass das Opfer auch bei dieser Bank ein Konto besitzt und keinen Verdacht schöpft, dass es sich um eine widerrechtliche Abfrage handelt, so erhält der „Phisher“ die Daten direkt vom Opfer, über die Tastatur seines Telefons.[55]

VI. Zwischenergebnis

Die vorgestellten wichtigsten Erscheinungsformen geben lediglich einen groben Überblick zur derzeitigen Phishing-Situation. Sie erheben auch keinen Anspruch auf Vollständigkeit, da dies bei der Vielzahl der Malware schlichtweg nicht möglich ist. Kombinierte Angriffe aus Malware und Spear-Phishing stellen für die Täter derzeitig die erfolgreichste Methode dar. Die Entwicklung des Phishings richtet sich stark an den Präventionsmaßnahmen der Banken aus.

D. Täter / Opfer

Nachfolgend sollen die Täterkreise und die Opfer des Phishings untersucht werden. Es wird dabei auf die Besonderheiten der Tatbegehung und des Umfeldes eingegangen.

I. Täter

Ein Ansatzpunkt für die präventive Bekämpfung ist das Verständnis hinsichtlich der Handlungsweisen des Täters und dessen Motivation. Bei Cyberkriminellen wird grundsätzlich zwischen einem Innentäter und einem Außentäter unterschieden.[56] Ein Innentäter ist bestens mit dem angegriffenen Netzwerk vertraut und muss sich

---

[53] Vgl. Geschonneck, S.15.

[54] „Voice Phishing“oder „ Voice over IP Phishing“ vgl. https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Phishing/phishing_node.html (recherchiert am 15.11.2013).

[55] Vgl. Sparkasse Saarbrücken https://www.sparkasse-saarbruecken.de/onlinebanking/online_banking_angebot/vishing/beschreibung/index.php?n=%2Fonlinebanking%2Fonline_banking_angebot%2Fvishing%2Fbeschreibung%2F (recherchiert am 03.10.2013).

[56] Vgl. Geschonneck S. 21.

nicht erst von außen Zugang verschaffen.[57] Beim Schwerpunkt dieser Arbeit, dem Phishing und seinen Erscheinungsformen ist allerdings fast immer von einem Außentäter auszugehen. Der einzige mögliche Fall eines Innentäters würde in der Infiltrierung eines Banksystems mittels Malware durch einen Angestellten bestehen.

1. Underground Economy

Es ist eine Entwicklung vom vormals männlichen heranwachsenden Einzeltäter, zu einer weltweit vernetzten und arbeitsteilenden Tätergemeinschaft erkennbar. Es gibt heute eine sogenannte „Underground Economy“, welche ein digitales und eigenes globales Wirtschaftssystem darstellt.[58] Von einzelnen Hackern kann man daher heute kaum noch reden.

Handelsplattformen für die Underground Economy sind die sogenannten „Boards“. Aufgebaut wie moderne Online-Verkaufsportale wie Amazon und Ebay ist es möglich, jegliche Information und Software zu erwerben. Der Preis für das Versenden von 1 Million Spam-Mails reicht von 300 € bis 800 €. Die Preise sind abhängig von der Qualität der Mails und auch von der Bonität der Empfänger.[59] Technisch nicht bewanderten Tätern ist es möglich sich die gesamte Straftat zu „erkaufen“. Auf den Boards können Sie sich sowohl die Technik als auch einen Ersteller der Malware mieten und beauftragen.[60] Die Bezahlung richtet sich nach der Komplexität der Malware und dem Empfängerkreis.

Mitglieder und Betreiber einzelner Boards führen untereinander auch eine Art Bandenkrieg, um die Vorherrschaft und Überlegenheit ihres Boards in der Szene zu demonstrieren und damit auch eine Art Werbung in eigener Sache zu betreiben.[61]

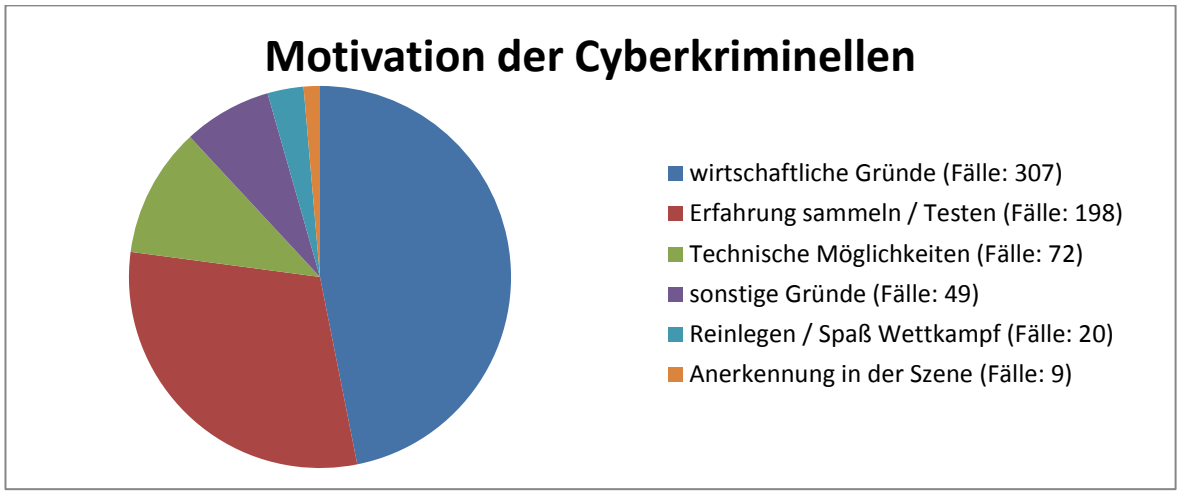
2. Interessenlage

Das Interesse eines Cyberkriminellen unterscheidet sich dabei nicht besonders von dem eines klassischen Kriminellen. Einziger Unterschied ist, dass im Vergleich häufig mehrere Motivationsbestände bei einer Tat zusammen auftreten. Nicht ausschließlich wirtschaftliche Gründe, sondern auch das Sammeln von Erfahrungen

---

[57] Vgl. Geschonneck S. 21.
[58] Vgl. Bolduan (2008) S. 31 ff ; Vgl. https://www.gdata.de/uploads/media/Whitepaper_Underground_Economy_9_2009_DE.pdf Siehe Anhang, Abbildung Nr. 1 - Preisliste(recherchiert am 17.01.2014).
[59] G data a.a.O.
[60] G data a.a.O.; Vgl. Geschonneck S. 16 ff.
[61] G data a.a.O.

und die Ausreizung der technischen Möglichkeiten stellt eine hohe Motivation für Phishing-Täter dar.[62]



[63]

Die Merkmale der Cybercrime-Verursacher sind fehlendes Unrechtsbewusstsein bei vermeintlicher oder oftmals auch tatsächlicher Anonymität auf Täterseite. Eine psychologische Hemmschwelle, wie sie vergleichbar bei einem Ladendiebstahl gegeben ist, entfällt zunehmend.[64] Gerade die Anonymität und die Einfachheit der Beschaffung der Tatmittel begünstigen die Entwicklung internationaler Strukturen.[65]

II. Opfer

Die allgemein bekannte Redewendung „Gelegenheit macht Diebe“ ist auch auf das Phishing anwendbar. Ein leichtsinniger und uninformierter Umgang erleichtert die Vorgehensweise der Täter erheblich. Eine Gefahr ist im Internet oftmals nicht unmittelbar wahrnehmbar. Obwohl es sehr viele Aufklärungsseiten und auch aktuelle Nachrichten zu dem Thema gibt, ist eine wachsende Risikobereitschaft der Mitglieder in der Informationsgesellschaft zu verzeichnen.[66]

Auffällig bei den immer häufiger genutzten mobilen Endgeräten ist, dass vor allem die Software von Google (Android) betroffen ist und die Software von Apple (Mac) vergleichsweise bisher größtenteils verschont bleibt von Cyberangriffen und Malware. [67]

---

[62] Vgl. G data https://www.gdata.de/uploads/media/Whitepaper_Underground_Economy_9_2009_DE.pdf (recherchiert am 14.01.2014).
[63] http://www.bka.de/informationen/account_missbrauch.pdf, Vgl. Geschonneck S. 20. - Darstellung und Informationen nochmal mit eigener Grafik zusammengefasst
[64] Vgl. Wernert S. 13.
[65] G data a.a.O.
[66] Gerke / Brunst, S. 9 Rnr. 4.
[67] http://www.handelsblatt.com/technologie/it-tk/mobile-welt/it-sicherheit-smartphone-nutzer-fallen-haeufiger-auf-phishing-herein/6349776.html (recherchiert am 11.11.2013).

Vermutlich hängt dies mit den Gegebenheiten für die Ersteller von Schadsoftwareprogrammen zusammen. Ein Trojaner für ein Apple Smartphone muss auf einem zu Apple gehörigen Betriebssystem dem Mac OS X geschrieben sein und zusätzlich noch in einer eigenen, für wenige Programmierer verständlichen Programmiersprache verfasst werden. Die Android-Software ist universal verwendbar und am weitesten verbreitet[68] (Windows, Linux oder auch Mac) und mit der geläufigsten einfacheren Programmiersprache „JAVA“ geschrieben. Zusätzlich muss berücksichtigt werden, dass die meisten Angriffe aus Russland, China und Osteuropa kommen, hier sind die Apple Geräte erst seit kurzer Zeit massentauglich erhältlich und noch kaum verbreitet.[69]

E. Statistik

Anhand der Statistik soll ein Überblick der derzeitigen Fallzahlen und die Entwicklung der Internetkriminalität aufgezeigt werden.

I. Internetnutzung

Eine Auswertung zur Internetnutzung des Statistischen Bundesamtes aus dem Jahr 2013 ergab, dass 83,5 % der Haushalte über einen stationären PC verfügten und 79,4 % der deutschen Bürger einen Internetzugang haben.[70] Seit einem Jahrzehnt stieg dieser Anteil kontinuierlich um das Doppelte auf die heutigen Werte.[71] Den größten Anteil an der Internetnutzung mit jeweils fast 90 % nehmen die Bereiche des Sendens und Empfangens von E-Mails ein und die Suche nach Informationen, Waren und Dienstleistungen.[72] Aber auch das für diese Arbeit entscheidende Feld des Online-Banking nutzen 50 % der Bürger. Schüler und Studenten nutzen mittlerweile zu 100 % das Internet als Lern- und Informationsquelle.[73]

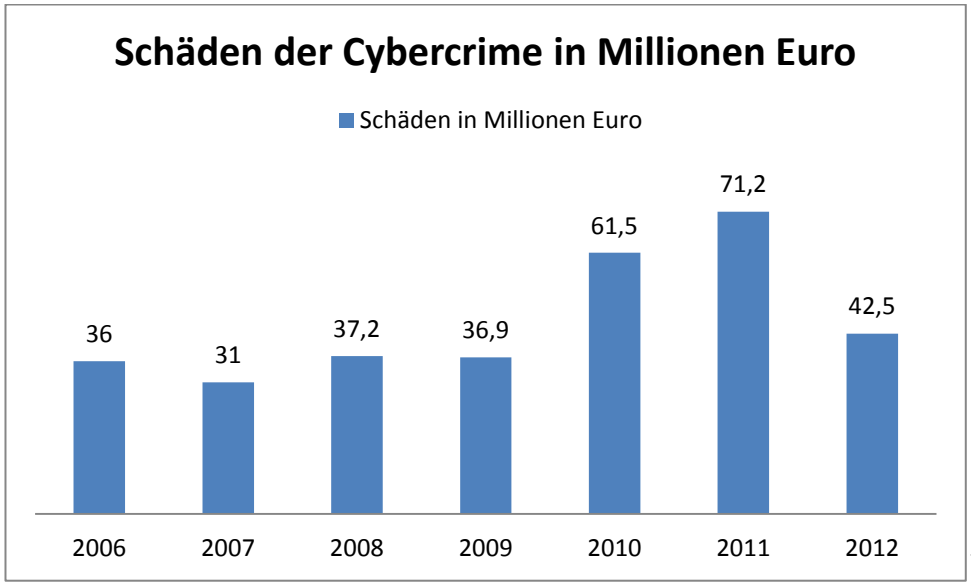
BITKOM-Studien verdeutlichten, dass der starke Trend zur allgegenwärtigen Erreichbarkeit und die Integration des Internets in den Alltag ungebrochen anhalten. Die Studien kamen zu dem Ergebnis, dass 9 von 10 der Internetnutzer auch Online-

---

[68] http://www.zeit.de/digital/mobil/2014-03/google-bringt-entwickler-umgebung-fuer-wearables-android/seite-2 (recherchiert am 10.03.2014).
[69] Vgl. Handelsblatt a.a.O. ; http://www.handelsblatt.com/unternehmen/it-medien/apple-expandiert-china-mobile-verkauft-jetzt-iphones/9349666.html (recherchiert am 17.01.2014).
[70] Vgl. Statistisches Bundesamt https://www.destatis.de/DE/Publikationen/StatistischesJahrbuch/StatistischesJahrbuch2013.pdf?__blob=publicationFile (recherchiert am 19.11.2013).
[71] Vgl. Statistisches Bundesamt https://www.destatis.de/DE/Publikationen/StatistischesJahrbuch/StatistischesJahrbuch2013.pdf?__blob=publicationFile (recherchiert am 19.11.2013).
[72] Statistisches Bundesamt a.a.O.
[73] Statistisches Bundesamt a.a.O.

Shopping betreiben und 97 % der verkauften Mobiltelefone heute internetfähige Smartphones (voraussichtlicher Verkauf von 40 Millionen Geräten 2014) sind.[74]
Das Statistische Bundesamt errechnete für das Jahr 2013 eine Rekordumsatzsumme im Netz von 33,1 Milliarden Euro. [75] Diese Zahlen verdeutlichen, dass über das Internet gewaltige Geldsummen fließen und es somit zwangsläufig auch ein interessantes Umfeld für Cyberkriminelle ist. Nachfolgend soll untersucht werden, welchen Einfluss Cyberkriminelle haben und welche Schlüsse daraus gezogen werden können.

II. Schäden durch Cybercrime



[76]

Aufgenommen in der Schadensstatistik sind lediglich der Computerbetrug nach § 263 a StGB (im Jahre 2012: 42,5 Mio. Euro) und der Betrug mit Zugangsdaten zu Kommunikationsdiensten. Bereiche wie das Phishing sind nur mit den einzelnen Fallzahlen unter Ihrem PKS-Schlüssel ersichtlich. Im Jahr 2012 ist ein Rückgang von ca. 40 % ersichtlich. Es ist allerdings nicht möglich, diesen Rückgang an eine bestimmte Ursache zu knüpfen. Vielmehr ist er wohl auf die Vielzahl der Präventionsmaßnahmen zurückzuführen. Im Bezug auf den entstandenen Schaden wird Phishing allerdings mit unter § 263 a StGB in der Schadensstatistik geführt.[77]

---

[74] Vgl. Bitkom-Studien, http://www.bitkom.org/78651_78640.aspx (recherchiert am 12.02.2014) ; http://www.bitkom.org/de/presse/74532_72867.aspx (recherchiert am 12.02.2014).
[75] http://de.statista.com/statistik/daten/studie/3979/umfrage/e-commerce-umsatz-in-deutschland-seit-1999/ (recherchiert am 12.02.2014).
[76] Vgl. eigene Darstellung mit Hilfe der Bundeslagebilder von 2006 – 2012 zusammengestellt für die gesamte Bundesrepublik Deutschland.
[77] BKA, Cybercrime Bundeslagebild 2012.

III. Kriminalstatistik

Mithilfe des Bundeslagebildes und der polizeilichen Kriminalstatistik, jeweils aus dem Jahr 2012 soll nachfolgend eine Bewertung der aktuellen Gefährdungslage dargestellt werden. Für die Bereiche des Phishings sind die Zahlen des Computerbetruges (§ 263 a StGB) und des Abfangens / Ausspähens von Daten (§§ 202 a, b StGB) relevant.

IV. Zweckmäßigkeit der Untersuchung

Ein wichtiger Ansatzpunkt für die Bekämpfung der Internetkriminalität ist das Wissen darüber, wie sie sich entwickelt, um so mögliche Trends früh zu erkennen und präventive Schritte einleiten zu können. Es bedeutet gezielt die Wirtschaft, Behörden und die Ersteller von Schadensabwehrprogrammen vorzubereiten, um dadurch Schaden vorzubeugen. Durch öffentliche Informationsprogramme können private Nutzer und auch Unternehmen zu einem überlegteren Internetverhalten überzeugt werden bzw. vor Schadsoftware gewarnt werden.[78]

In der Praxis stellt sich die Prävention oftmals so dar, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Bürgern über kostenlose Prüfprogramme die Möglichkeit bietet, den PC auf Schadsoftware zu prüfen bzw. den Abgriff der digitalen Identität festzustellen.[79] Im Nachfolgenden erklärt dann ein Informationsblatt wie sich der Bürger verhalten sollte.

V. Cybercrime im engeren Sinne

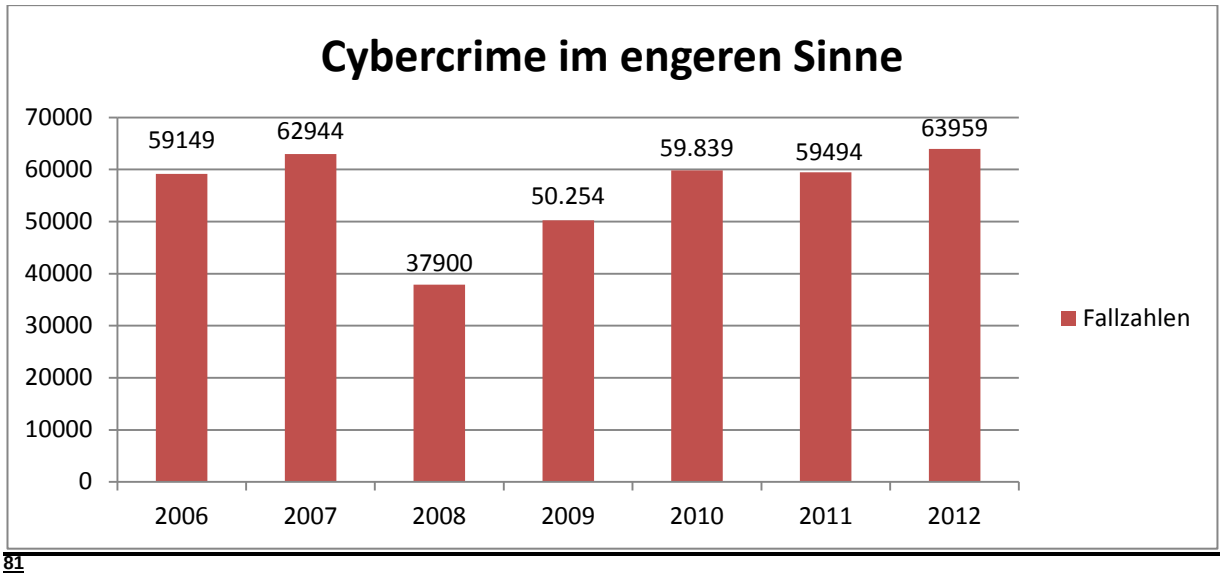
Die Cybercrime im engeren Sinne erfasst die Fallzahlen, welche unter Ausnutzung der modernen Informations- und Kommunikationstechnik oder gegen diese begangen werden.[80] Nicht erfasst sind die Fälle, in denen das Internet lediglich zur Hilfe genommen wird, um die Begehung einer Straftat zu vereinfachen, wie z. B. Stalking oder Bedrohung über soziale Netzwerke.

---

[78] Vgl. Welt, http://www.welt.de/wirtschaft/webwelt/article123928616/Telekom-warnt-vor-falschen-Rechnungen-mit-Viren.html (recherchiert am 16.01.2014).

[79] www.sicherheitstest.bsi.de (recherchiert am 08.02.2014).

[80] Vgl. Cybercrime Bundeslagebild 2012.



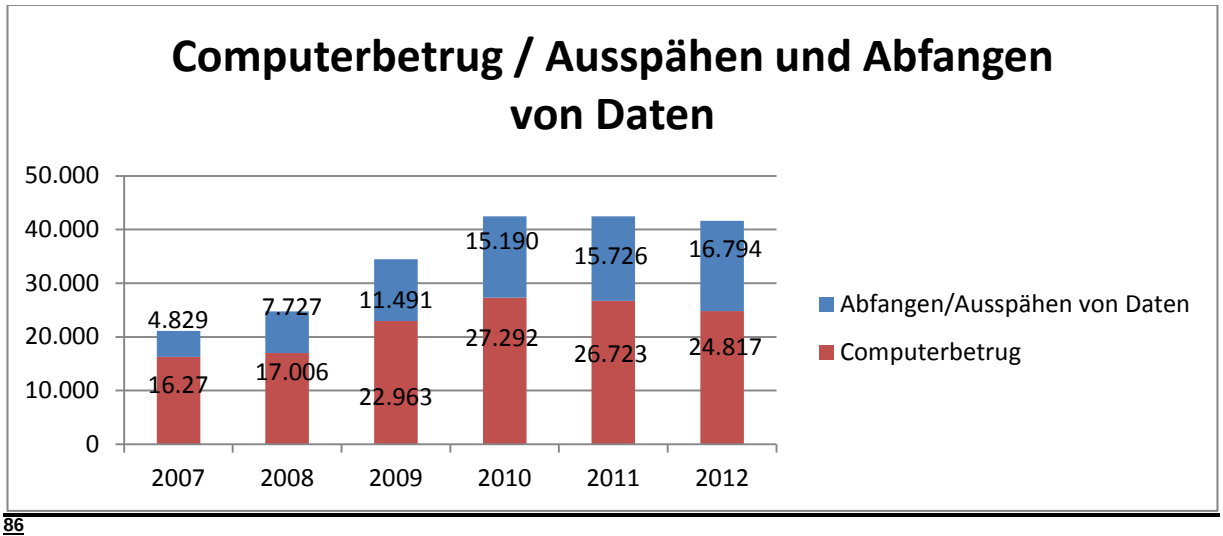
[81]

Erkennbar ist ein Einbruch der Fallzahlen im Jahre 2008. Eine wirklich befriedigende Begründung für diesen Abfall lässt sich aus der Kriminalstatistik (auch der Vorjahre) nicht entnehmen. Ein Grund für den Abfall kann allerdings in dem durch die Banken eingerichteten I-TAN Verfahren liegen.[82] Im Jahre 2012 erfolgte eine leichte Steigerung von 8 % gegenüber dem Vorjahr.[83]

Die wachsenden Fallzahlen nach 2009 lassen sich auf die gesteigerte Professionalität der Hacker und Virenautoren bei Ihrer Schadenssoftware, der lernenden Tätergemeinschaft im Zusammenhang mit dem „Social Engineering“[84] und vor allem dem steigenden Ausmaß an einem arbeitsteiligen Vorgehen durch Bootnetze und Chatforen zurückführen.[85] Des Weiteren steigt logischerweise mit der Vielfältigkeit des Internets auch die Möglichkeit mehr Straftaten zu begehen, bzw. neue Delikte zu entwickeln.

[81] Vgl. eigene Darstellung mit Hilfe der Bundeslagebilder 2006- 2012 vom BKA.
[82] Def.: I-Tan verfahren – indiziertes Tan-Verfahren, die Bank fordert eine bestimmte TAN für den Zahlungsvorgang und keine beliebige. Vgl.: Statistik nachfolgend Phishing im Onlinebanking; http://www.verbraucher-sicher-online.de/artikel/etan-itan-mtan-welche-denn-nun?page=0,6 (recherchiert am 11.11.2013).
[83] Vgl. Bundeslagebild 2012.
[84] Vgl. Bundeslagebild 2009.
[85] Vgl. Bundeslagebild 2009.

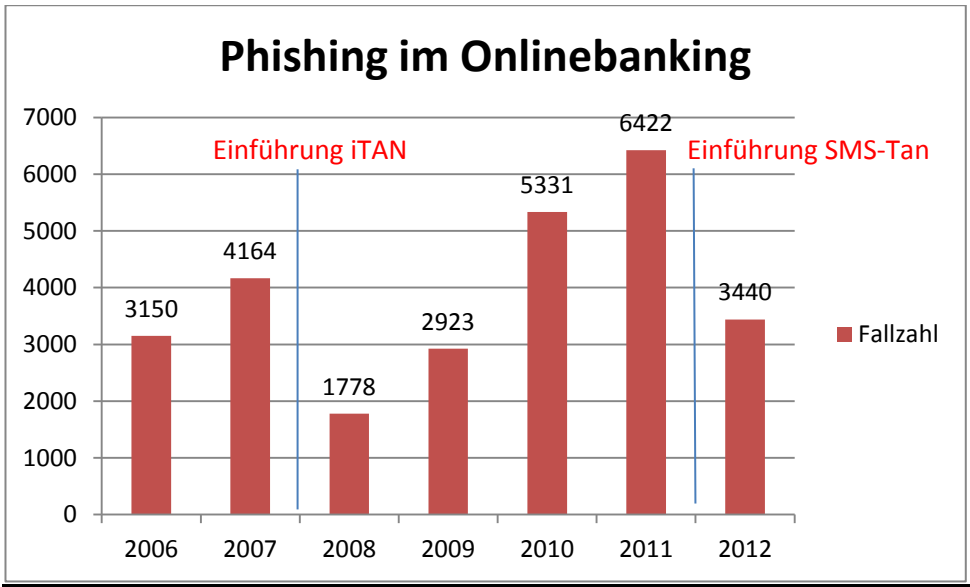
VI. Computerbetrug / Ausspähen und Abfangen von Daten



[86]

Mit einem Anteil von 39 % an allen erfassten Straftaten im Bereich der Internetkriminalität stellt der Computerbetrug nach § 263 a StGB immer noch den größten Anteil dar. Innerhalb von 5 Jahren erfolgte ein Anstieg von knapp 60 %. Die größte Steigerung mit über 375 % erfolgte allerdings beim Abfangen und Ausspähen von Daten innerhalb der letzten 5 Jahre.[87]

VII. Phishing



[88]

Obwohl vor allem beim Phishing durch die Täter intelligente Weiterentwicklungen zu betrachten sind, ist hier ein Einbruch der Fallzahlen von 2011-2012 ersichtlich. Mit einem Abfall von fast 50 % zum Vorjahr zeigen die unternommenen Maßnahmen

[86] Eigene Darstellung mit Hilfe der Polizeilichen Kriminalstatistik 2007 – 2012.
[87] Polizeiliche Kriminalstatistik 2007 – 2012 ; Cybercrime Bundeslagebild 2012; Informationen statistisches Bundesamt.
[88] Eigene Darstellung mit Hilfe der Bundeslagebilder 2006 - 2012.

Wirkung. Dieser Trend stützt sich maßgeblich auf das ständige Nachrüsten der Banken bei Ihren Sicherheitssystemen; der Sensibilisierung der Anwender und einem effektiven IT-Management der Behörden. Bei fast allen Banken wurde das im Vergleich sichere „SMS-Tan–Verfahren“ eingeführt, worin wohl der eigentliche Grund liegen dürfte.[89] Allerdings stellen sich Cyberkriminelle sehr schnell auf neue Gegebenheiten ein. Dies erkennt man am starken Anstieg der Fallzahlen in der Statistik nach der Einführung des iTAN – Verfahrens 2007 / 2008.[90] Es kann heute noch keine gesicherte Feststellung getroffen werden, wie sich die Einführung des SEPA-Verfahrens auswirkt.

Eine Führungsrolle unter den Banken für sicheres Online-Banking haben meines Erachtens die Sparkassen und die Postbank übernommen. Diese brachten die neuen technischen Möglichkeiten zur Verschlüsselung zeitnah zur Anwendung. Die DiBa-Bank, welche eine reine Onlinebank ist hat die Umstellung vom mittlerweile überholten iTan-Verfahren, auf das sichere SMS-TAN-Verfahren bisher verpasst.[91]

Der herbeigeführte Schaden durch Phishing ist für die Täter allerdings weiterhin höchst profitabel. 2012 konnten durchschnittlich 4.000 €[92] bei einem Übergriff erlangt werden, bei einer sehr geringen Aufklärungsquote von nur 15,2 %[93] (wobei sich diese Aufklärungsquote wohl allein auf den Finanzkurier bezieht – keine Auskunft dahingehend durch die Ermittlungsbehörden oder dem Statistischen Bundesamt möglich).

Der durch Phishing registrierte Schaden lag 2012 bei 13,8 Millionen Euro, wobei die Dunkelziffer um ein Vielfaches höher sein wird. Durch das Bundeskriminalamt wird geschätzt, dass der eigentliche Schaden um 60 % höher einzustufen ist.[94]

VIII. Nutzbarkeit der Kriminalstatistik

Es besteht ein extrem großes Dunkelfeld im Bereich der Cybercrime.[95] Dies ist darauf zurückzuführen, dass viele Straftaten über das Versuchsstadium nicht hinausgehen, da natürlich auch eine voranschreitende Entwicklung der Sicherungssoftware erfolgt und somit die vermeintlich Geschädigten den Angriff gar

[89] „SMS-TAN-Verfahren“ – allein der Befall mit Schadsoftware auf dem Rechner ist nicht mehr ausreichend, da ein weiteres Kommunikationsmedium gehackt werden muss, nämlich das Handy/Smartphone des Nutzers – die benötigte Schadsoftware ist allerdings schon vorhanden, nur noch nicht sehr weit verbreitet . http://www.abendzeitung-muenchen.de/inhalt.wie-sicher-ist-online-banking-bankkonto-leergeraeumt-trotz-mtans.6aa31670-0cfa-4fac-bb90-37e9dddd8f25.htm (recherchiert am 22.03.2014); Bundeslagebild 2012.

[90] Siehe Statistik „Phishing im Onlinebanking“.

[91] Eigene Nutzung der jeweiligen Systeme.

[92] Bundeslagebild Cybercrime 2012.

[93] PKS Grundtabelle zum Tatmittel „Internet“ vom 13.02.2013.

[94] Bundeslagebild Cybercrime 2010.

[95] Bundeslagebild Cybercrime 2012.

nicht erst anzeigen oder bemerken.[96] Unternehmen zeigen eine finanzielle Schädigung häufig nicht an, um ihre öffentliche Außendarstellung nicht zu gefährden.

Des Weiteren ist die Statistik leider nur bedingt nutzbar, da nur die Daten erhoben werden, bei denen sich der Täter im Bundesgebiet befindet.[97] Da man z. B. den Ort der Versender der Phishing-E-Mails oftmals nicht feststellen kann, bzw. dieser sich oftmals im Ausland befindet, werden diese gar nicht in der Statistik erfasst. Auch taucht eine immer gleich arbeitende Phishing-Mail nur einmal in der Statistik auf.

Eine reale Bewertung der Gefährdungslage auf der Grundlage statistischer Zahlen ist demnach nicht möglich, absehbare Trends hingegen schon.

IX. Trends

Die zeitliche Internetnutzung der Deutschen ist im Jahr 2013 erneut stark angestiegen. Vor allem bei mobilen Endgeräten hat sich die Nutzung im Vergleich zum Vorjahr fast verdoppelt (von 23 % auf 41 %).[98] Es ist sehr wahrscheinlich, dass Geräten wie der Google Glass[99], dem Smartphone und Tablets von Täterseite her noch höhere Aufmerksamkeit zukommen wird. Eine 2011 erstellte Studie besagt, dass Phishing-Angriffe auf Smartphone 3-mal erfolgreicher sind als ähnliche auf Computer.[100] Die Erklärung dafür ist denkbar einfach. Da die Adressleiste in der Mail oftmals nicht angezeigt wird und auch vergleichsweise viel kleiner ist als am Computer, wird ihr nicht die gleiche Beachtung geschenkt. Die durch Warnungen und Aufklärungsprogramme herausgegebenen Hinweise werden einfach nicht beachtet auf einem Smartphone, da diese für vermeintlich sicherer gehalten werden.[101]

Die Nutzer müssen Ihr Smartphone oder Tablet mehr als PC verstehen. Verhaltensweisen welche dort bereits greifen und zum Rückgang der Fälle geführt haben (Aufklärung, regelmäßige Aktualisierungen der Schadensabwehrsoftware, Erstellung eines Passwortes, nicht gedankenloses Herunterladen von Software/Apps) müssen auch auf den mobilen Endgeräten zur Anwendung kommen.

---

[96] Bundeslagebild Cybercrime 2012.
[97] Geschonneck, S. 24
[98] ARD / ZDF – Onlinestudie 2013, http://www.ard-zdf-onlinestudie.de/fileadmin/Onlinestudie/PDF/PM1_ARD-ZDF-Onlinestudie_2013.pdf (recherchiert am 03.01.2014).
[99] Elektronische Datenbrille ausgestattet mit ständigem Internetzugang und einer integrierten Kamera.
[100] Vgl. http://www.handelsblatt.com/technologie/it-tk/mobile-welt/it-sicherheit-smartphone-nutzer-fallen-haeufiger-auf-phishing-herein/6349776.html (recherchiert am 26.02.2014).
[101] Vgl. Handelsblatt a.a.O.

Ein weiterer Trend ist das Speichern von persönlichen Dateien nicht mehr auf lokalen Datenträgern wie dem eigenen PC oder dem USB-Stick, sondern im sogenannten Cloud Computing. [102] Die Sicherung der online abgespeicherten Daten ist im Vergleich zum heimischen Datenträger noch nicht so weit entwickelt.
Anhand der zu erwartenden technischen Entwicklungen muss durch die Ermittlungsbehörden eine intensive Beurteilung stattfinden und eine vorausschauende Analyse der Handlungserfordernisse.[103]

X. Vergleich mit der Gesamtstatistik der erfassten Straftaten

Während innerhalb der letzten 5 Jahre die Gesamtanzahl der erfassten Straftaten von 6.284.661 Straftaten im Jahre 2007[104], auf 5.997.040 im Jahre 2012 um fast 5 % abnahm und damit den Trend der meisten Straftatbestände auch gut wiederspiegelte, steigerte sich die engere Cybercrime im gleichen Zeitraum um 87 %.[105] Es wird damit für die Zukunft sehr deutlich, in welche Richtung sich ein Großteil der Kriminalität verlagert.

F. Strafverfolgung durch Behörden

Nachfolgend sollen das Arbeiten der Polizei und die praktischen Probleme einer Strafverfolgung im Internet verdeutlicht werden.

I. Ausgangssituation

Auf der einen Seite ist es natürlich äußerst problematisch, dass es sich hier um einen unbegrenzten, scheinbar regellosen Tatort handelt und die Spuren, die ein Täter hinterlässt, besonderes Sachverständnis bei der Ermittlung erfordern. Zum Anderen liegt aber auch eine ungemeine Chance in den Möglichkeiten, die die technische Vernetzung für die Ermittlungen mit sich bringt. Mit polizeilichen Vernetzungsprogrammen wie „SIS“ oder „Sirene“ ist z. B. ein europaweiter Informationsaustausch über laufende Ermittlungen möglich und auch die Verfolgung von Datenspuren im Netz.[106] Um den Kernbereich privater Lebensgestaltung zu schützen, müssen allerdings staatliche Regularien bestehen, welche die technischen Möglichkeiten zu Ermittlungen auf ein für die Allgemeinheit akzeptables Maß begrenzen.

---

[102] Vgl. Bundesministerium für Wirtschaft und Energie http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Navigation/Themen/cloud-computing.html (recherchiert am 15.02.2014).
[103] Vgl. Wernert S. 30.
[104] Polizeiliche Kriminalstatistik 2007.
[105] Polizeiliche Kriminalstatistik 2012.
[106] Vgl. Wernert S. 19.

Ein Hauptproblem vieler Polizeidienststellen ist strafbares Handeln im Internet überhaupt zu erkennen, richtig einzuordnen und unmittelbar eine geeignete Beweissicherung zu bewirken.[107]

II. Aufbau der Polizei bei Internetstraftaten

Ein aktuelles bundeseinheitliches Aus-/Fortbildungskonzept sieht vor, bei Internetstraftaten auf 3 verschiedenen personellen Ebenen vorzugehen, um eine Strafverfolgung zu optimieren.

Die erste Ebene stellen dabei die IuK-Ersteinschreiter dar. Dies soll jeder Polizeibeamte sein, der über ein fundiertes Grundwissen bzgl. des Internetstrafrechtes, der Einordnung und der Begehungsweise von Straftaten verfügt. Sie sollen eine Art Zuordnungsfunktion an nachgeordnete Stellen wahrnehmen und dabei erste Feststellungen und Maßnahmen treffen.[108]

Die normale Polizeistruktur sieht vor, eine Straftat in dem jeweiligen Bereich des Grunddeliktes zu bearbeiten. Es sind also pro Dezernat (z. B. Betrugsdezernat) speziell weitergebildete Polizeibeamte (IuK-Sachbearbeiter) auf die IuK-Kriminalität geschult. Diese treffen erste Beweissicherungsmaßnahmen.[109]

Die dritte Ebene bildet der Sachbearbeiter beim LKA und bei den Kreisdienststellen – zur IT – Beweissicherung. Er ist ausschließlich auf die IuK-Kriminalität angesetzt. Die Aufgaben der dritten Ebene sind dann die forensische Beweissicherung und Datenträgeruntersuchung sowie die beratende und unterstützende Hilfe bei Durchsuchungsmaßnahmen und komplexen Ermittlungen, um bei den erlangten Beweisen auch eine Gerichtsverwertbarkeit zu erlangen. Auch die Nachbereitung eines Falles, die Beurteilung von massenhaften Spam-Mails und den Kontakt mit privaten Stellen aus dem Bereich der IT nimmt die dritte Ebene war. Hier erfolgt auch die Marktbeobachtung, um neue Cybercrime-Methoden vorzeitig zu erkennen. Diese Kompetenzzentren werden „KIK“[110] genannt.

III. Polizeiliche Maßnahmen bei einem Phishing-Vorfall

Es ist sehr schwierig einen erfolgten Phishing-Vorfall als solchen zu erkennen, da es allein bei der Handlung des Phishings noch keinen Vermögensschaden gab. Oftmals erkennt man erst beim nachfolgenden Geldverlust die Vorbereitungshandlung. Die ersten Schritte sind die Anzeigenaufnahme und die Vernehmung. Dies wird durch die erste und zweite Ebene bei der Polizei abgedeckt.

---

[107] Vgl. Wernert S. 19.
[108] Vgl. Wernert a.a.O.
[109] Vgl. Wernert a.a.O.
[110] Vgl. Wernert ; Def.: KIK - Kompetenzzentren Internetkriminalität S.19 ff.

Das Feststellen von Auffälligkeiten und die Untersuchung der angewandten Malware sind der dritten Ebene vorbehalten.

Vorgehen der Polizei bei einem Phishingangriff[111]		
Anzeigenaufnahme und Vernehmung	**Feststellungen zum PC und zur PC-konfiguration**	**Auffälligkeiten**
- **Feststellung der Identität des Opfers** - **Feststellung der Bankverbindungen von Opfer und Finanzagenten (Bankinstitut; IBAN-Nummer)** - **Betrag** - **Wenn möglich, bei der Bank Personalien des Empfängers erfragen.**	- **Wo ist der Tatort?** - **Wer hat Zugang zu dem PC (Einzel- oder Mehrbenutzungssystem)?** - **Zugangsart (DSL; ISDN; UMTS)?** - **Betriebssystem und die darauf installierte Schutzsoftware?** - **Benutzter Browser (z. B. Internet-Explorer , Firefox) und Provider (T-Online, Vodafone)?** - **Bei welcher Bank betreibt der Geschädigte das Online-Banking?** - **Welches Sicherungsverfahren hat die Bank?** - **Wurden bereits die tatrelevanten Daten verändert oder gelöscht?**	- **Kann Zeitpunkt des Zugangs auf den PC ermittelt werden?** - **Wurden persönliche Daten durch die Schadsoftware abgefragt?** - **Sicherung der E-Mail, falls das Phishing über E-Mail erfolgte?** - **Wann wurde die Abbuchung auf dem Konto bemerkt?** - **Gefälschte Absenderadressen – Erkennung nur über eine polizeiliche Header-Auswertung möglich**

IV. Hauptprobleme bei den Ermittlungen

Neben der Internationalität und der unterschiedlichen Bewertung und Verfolgung von Straftaten im Internet durch andere Länder, stellt vor allem die Arglosigkeit und Unerfahrenheit der Nutzer ein großes Problem dar. Die oftmals einzige Möglichkeit an die Täter zu kommen, ist die Nachverfolgung des Geldverkehrs. Da dieser aber häufig über anonyme Geldtransfers (Western Union, U-Cash) läuft, welche nicht zur Auskunft verpflichtet sind und dies auch oftmals nicht können, laufen viele Ermittlungen nach den „Phishern“ ins Leere.[112] Da oftmals auch nicht ausreichend geschultes Personal für die komplexen technischen Vorgänge in der ersten und

[111] Eigene Zusammenstellung mit Hilfe von Wernert S. 28 ; Arbeitsgruppe Identitätsschutz im Internet a-i3, https://www.a-i3.org/content/view/932/203/ (recherchiert am 05.01.2014).
[112] Vgl. Gerke/Brunst S. 39, Rnr. 47.

zweiten Ebene vorhanden ist, kann häufig nicht die nötige schnelle Beweissicherung stattfinden und die Sachverhalte nicht richtig strafrechtlich eingeordnet werden.[113]
Bei den europäischen Cybercrime-Konferenzen werden zumindest für die EU einheitliche Gesetzesgrundlagen für die Strafverfolgung geschaffen. [114]

G. Prävention

Den größten Schutz vor einem Phishing-Angriff stellt die Prävention dar. Eine Kombination von aktueller Antivirensoftware und einer aufmerksamen Benutzung des Internets.
Viele staatliche Sicherheitsbehörden, private Vereine und Branchenverbände bieten kostenlose Informationen zum Phishing an. Beratungsmöglichkeiten bietet z. B. die Verbraucherzentrale, die Arbeitsgruppe „Identitätsschutz im Internet“ (Abkürzung: a-i3) und die Onlineauftritte der Polizei an. Diese sensibilisieren die Bürger in aktuellen Meldungen vor den derzeitigen Phishing-Mails. Auch das Bundesamt für Informationssicherheit „BSI“ bietet fortlaufend wichtige Programme an, mit denen ein Befall von Malware geprüft werden kann.
Möglich wird dies durch eine offene Zusammenarbeit zwischen staatlichen Institutionen und den IT-Dienstleistern der Wirtschaft. Nur ein aktuelles Virenprogramm ist in der Lage Schadsoftware zu blockieren. Veraltete Software erkennt lediglich Phishing-Mails und Malware, welche ihm bei der Erstellung einprogrammiert wurden.

[113] Vgl. Geschonneck S 323 ff.
[114] Einrichtung eines European Cybercrime Center im Jahr 2013 http://www.zdnet.de/88183922/europaeisches-cybercrime-zentrum-veroeffentlicht-taetigkeitsbericht/ (recherchiert am 13.02.2014)

Sicherheitsmaßnahmen gegen Phishing[115]		
Schutz	**Früherkennung Phishing-E-Mails**	**Früherkennung Phishing-Webseiten**
- **Computer und Smartphone sollten mit einer aktuellen Virenschutzsoftware, welche regelmäßig aktualisiert wird, ausgerüstet sein** - **Passwörter und Benutzerdaten nicht leichtfertig preisgeben**	- **Unpersönliche Anrede (Lieber Kunde der X-Bank!)** - **Dringender Handlungsbedarf wird vorgetäuscht, teils auch mit Drohungen (ohne Datenaktualisierung, wird das Online- Konto gesperrt)** - **Vertrauliche Daten (PINs und TANs) werden mittels eines Formulars abgefragt, bzw. einem Link, dem gefolgt werden, soll** - **Nachrichten sind manchmal im schlechten Deutsch verfasst (Täter sitzt im Ausland und benutzt ein Übersetzungsprogramm)** - **E-Mails enthalten kyrillische Buchstaben; Umlaute werden falsch dargestellt (statt „ä“ wird ein „ae“ gezeigt)**	- **Fehlen des Sicherheitskürzels https:// für eine vertrauliche Verbindung** - **Fast identische Adresszeile, aber mit unüblichen Zusätzen wie www.135x-Bank.com** - **Auf der Login-Seite werden TANs abgefragt** - **Das Sicherheitszertifikat (Schlosssymbol) in der Statusleiste fehlt oder ist gefälscht** - **Mehrfache Abfrage von TAN-Nummern**

H. Strafbarkeit des Phishing

Im Folgenden soll untersucht werden, ob die derzeitigen gesetzlichen Regelungen ausreichen, die Tathandlung des Phishing und seine vielfältigen Erscheinungsformen unter Strafe zu stellen. Es wird dabei geprüft, inwiefern weitere nachfolgende Straftatbestände verwirklicht werden müssen, um die Strafbarkeit gewährleisten zu können.

Bei der Prüfung der Strafbarkeit wird zwischen der Datenbeschaffung und der anschließenden Verwendung der Daten unterschieden.[116] Diese Teilung wird vorgenommen, da Phishing keinen eigenen Tatbestand erfüllt und so lediglich die

[115] Tabelle wurde erstellt mit dem Online-Dienst der Polizei http://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/phishing/tipps.html (recherchiert am 08.02.2014) ; der Arbeitsgruppe Identitätsschutz im Internet a-i3, welche sich auf den Schutz vor Cyberangriffen spezialisiert hat https://www.a-i3.org/content/view/932/203/ (recherchiert am 08.02.2014) ; Bundesamt für Sicherheit in der Informationstechnik https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Phishing/Schutzmassnamen/schutzmassnamen_node.html (recherchiert am 08.02.2014), Vgl. Abbildung Nr. 2 und Nr. 3.

[116] Vgl. Seidel, Hrr-Strafrecht (2010) S. 85 .

einzelnen Handlungsschritte auf die Erfüllung einer Strafnorm geprüft werden können. Des Weiteren ist noch die Tätigkeit des Finanzagenten zu untersuchen.
Einigkeit bestand lange Zeit lediglich darin, dass das Abgreifen der Passwörter und der Zugangsdaten auch ohne deren Verwendung zumindest strafwürdig ist.[117] Phishing wurde nicht als expliziter Tatbestand aufgenommen, da das Bundesministerium der Justiz am 20.09.2006 feststellte, dass das Phishing bereits durch bestehende Strafnormen abgedeckt ist.[118] Verwiesen wurde auf die Straftatbestände des Ausspähens von Daten (§ 202 a StGB), des Computerbetruges (§263 a StGB) und der Fälschung beweiserheblicher Daten (§ 269 StGB) sowie der unbefugten Datenerhebung und Verarbeitung (§§ 44, 43 BDSG). Auch mit dem 41. Strafrechtsänderungsgesetz ist Phishing nicht als eigenständiger Tatbestand aufgenommen worden.

I. Auslandsbezug / Tatortprinzip

Fraglich ist, ob für die Strafbarkeit überhaupt deutsches Recht anwendbar ist, da Versender der Malware und Ersteller der Webseiten sich oftmals im Ausland befinden. Gemäß § 3 StGB ist dt. Strafrecht anwendbar bei im Inland verübten Taten (Territorialitätsprinzip).[119] Es ist dabei ausreichend, dass entweder Erfolg oder Handlung der Tat im Inland stattfinden (§ 9 StGB). Wird beim Versenden der Mail eine Schadsoftware nachgeladen und auf dem Rechner des Opfers im Inland gespeichert, so unterliegt die Handlung nach § 303 a StGB dem dt. Strafrecht.
Zu prüfen ist aber, ob die versendeten Mails, welche auf Websites führen, die auf ausländischen Servern gespeichert sind, auch dem dt. StGB unterliegen. Es findet sich hierbei eine Vielzahl von vertretbaren Meinungen. Einer Ansicht nach haben diese abstrakten Gefährdungsdelikte im Inland keinen Erfolgsort. Es verbleibt bei einer Auslandstat, da es sich um eine Gefahr handelt, die an jedem Ort anders beurteilt werden muss und sich somit nach der Gesetzgebung des jeweiligen Landes richtet.[120]
Man muss sich allerdings für die Beurteilung den Zweck der Website in Erinnerung rufen. Es handelt sich um eine deutschsprachige Website, bei der deutsche Internetauftritte der jeweiligen Banken inkl. Logos und Embleme nachgebildet werden, um gezielt deutsche Konteninhaber zu täuschen. Es wird daher ein Hilfstatort an dem Ort gebildet, an dem der Schaden eintritt.[121] Kann festgestellt

[117] Vgl.Graf, NStZ 2007, 129 ff.
[118] Pressemitteilung BMJ vom 20.09.2006.
[119] Vgl. Fischer (2014) § 3 Rnr. 1.
[120] Vgl. Stuckenberg, ZStW S. 881 ff.
[121] Vgl. Geschonneck S. 327.

werden, dass sich die Website auf einem ausländischen Server befindet, so sollte auch eine Strafanzeige im Ausland erfolgen.[122]

Unproblematisch ist deutsches Strafrecht beim nachfolgenden Betrug nach § 263 StGB festzustellen, da das Phishing-Opfer in Deutschland getäuscht wurde, was für eine Inlandstat (siehe §§ 3; 9 StGB) ausreichend ist.[123] Gleiches ist für die Tätigkeit des Finanzagenten festzustellen.[124]

II. Strafbarkeit der Datenbeschaffung

Nachfolgend soll geprüft werden, ob die bestehenden und oben genannten Strafnormen ausreichend sind oder es eines expliziten Straftatbestandes bedarf. Zuerst wird dabei auf die Beschaffung der Kontozugangsdaten eingegangen.

1. § 202 a StGB - Ausspähen von Daten

Gemäß § 202 a StGB macht sich derjenige strafbar, der unbefugte Daten, welche nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft. Nach Absatz 2 sind allerdings nur solche Daten zu verstehen, welche nicht unmittelbar wahrnehmbar sind. Da die Daten (PIN/TAN) im Rechner digitalisiert werden, besteht hier bereits Streit.[125] Sie sind zwar nicht mehr „unmittelbar wahrnehmbar“, befinden sich aber nur kurzweilig im Arbeitsspeicher, bevor sie wieder erkennbar angezeigt werden eine Speicherung im Sinne des § 202 a Abs. 1 StGB ist nicht erfüllt. [126]

Das unwissende Opfer gibt dem Täter sichtbare Ziffern und Zahlen weiter. Auch nach der elektronischen Datenübermittlung kommen die Daten decodiert und als unmittelbar ersichtlich beim Täter an, der Tatbestand ist demnach nicht erfüllt.

Kritiker sehen auch nicht die Verwirklichung des Straftatbestandes, da die persönlichen Daten meist durch das Opfer selbst herausgegeben werden und dies in einer freiwilligen Annahme und nicht wie im Tatbestand beschrieben, unbefugt geschieht.[127]

Auch die besondere Sicherung der übermittelten Daten ist nicht gegeben, da dies allein nach objektiven Kriterien geschieht und die Daten ohne weitere Kontrolle oder Schutzmechanismus freiwillig vom Opfer an den Täter gesendet werden.[128]

---

[122] Vgl. Geschonneck S. 327.
[123] Vgl. Stuckenberg, ZStW S. 881 ff.
[124] BGH vom 23.04.2013 2 Ars 91/13, 2 AR 56/13.
[125] Vgl. Popp MMR (2006), 84, 85.
[126] Vgl. Fischer (2014) § 202 a Rnr. 5 ; Vgl. Popp MMR (2006), aaO.
[127] Stuckenberg, ZStW (2006) S. 878,884 ; Fischer (2014) § 202 a, Rnr. 7 a.
[128] Vgl. Seidel HRRS (2010) S. 85 ff. ;Vgl. Popp MMR (2006), 84, 85. ;

Die Beschaffung der Kontozugangsdaten beim klassischen Phishing / Pharming ist demnach nicht unter § 202 a StGB zu subsumieren.

2. § 202 b StGB - Abfangen von Daten

Der § 202 b StGB wurde durch das 41. Strafrechtsänderungsgesetz neu eingefügt und stellt das Abfangen von Daten unter Strafe. Voraussetzung des § 202 b StGB ist ein Abfangen der Daten aus einer nichtöffentlichen Datenübermittlung oder einer elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage. Ein Abfangen beim klassischen Phishing findet allerdings nicht statt. Hier kommt es vor der Übertragung vom Opfer zum Täter zu einer Täuschung durch die Phishing-E-Mail bzw. die Weiterleitung an die nachgebildete Website.[129] Da eine direkte Verbindung ohne ein Abfangen vorliegt, kommt § 202 b StGB nicht in Betracht.

3. § 263 StGB - Betrug

Es ist umstritten, ob beim Phishing eine Strafbarkeit des Betruges nach § 263 StGB vorliegt. § 263 StGB setzt eine aktive Beteiligung des getäuschten Opfers voraus, welches Irrtums bedingt eine Vermögensverfügung trifft und sich selbst finanziellen Schaden zufügt.[130] Allein das Erlangen persönlicher Daten und der Bankverbindung stellt aber noch keinen finanziellen Schaden dar, sondern lediglich die Voraussetzung.[131] Das Wissen über die PIN und Tan stellt also für sich genommen noch keine Vermögensminderung dar.[132] Der Vermögenswert wird erst mit einer nachfolgenden, davon abzugrenzenden Handlung möglich. Beim § 263 StGB ist daher auch die Unmittelbarkeit der Vermögensverfügung zu prüfen.[133]

Auch eine Weiterleitung oder Verkauf der Zugangsdaten in der „Underground Economy“ stellt noch keine Vermögensverfügung dar.[134]

Durch die Täuschung an sich ist auch noch nicht die endgültige Benutzung der Daten geklärt.[135] Der Täter hat sich beim Versenden der Mail oder des Trojaners noch nicht entschieden, die Daten auch zu verwenden (z. B. bei einer zweifelhaften Kontendeckung, die er mittels Malware prüft).

Bei der Datenbeschaffung der PIN und TAN - Daten handelt es sich demnach nicht um einen Betrug nach § 263 StGB.

Vgl. Goeckenjan wistra (2008) S. 128 130.
[130] Vgl. Fischer (2014), § 263 Rnr. 113 ff.
[131] Vgl. Popp, NJW 2004 S. 3517-3518.
[132] Vgl. Goeckenjan wistra a.a.O.
[133] Vgl. Stuckenberg, ZStW (2006) S. 878,899.
[134] Vgl. Gercke CR 2005 S. 606, 607.
[135] Vgl. Fischer (2014), § 263 Rnr. 156.

4. § 240 StGB - Nötigung

Zu prüfen ist, ob eine Strafbarkeit wegen Nötigung in Betracht kommt. Dieser Fall könnte vorliegen, wenn dem Opfer auf telefonische Weise oder in der E-Mail angedroht wird, dass bei einer Nichtweiterleitung der Zugangsdaten wegen einer regulären Überprüfung oder Ähnlichem, dessen Konto gesperrt wird bzw. sein Geld verloren geht. Allein in diesen Fällen wäre eine Strafbarkeit des Phishings nach § 240 StGB gegeben, da hier rechtswidrig dem Opfer angedroht wird, dass er ohne eine entsprechende Handlung (Verschaffen der PIN und TAN) einen empfindlichen finanziellen Schaden erleiden werde.[136] Dies ist einer der aktuellsten Trends des Phishings. Bei der Umstellung auf das SEPA – Verfahren wurden aus dem benachbarten Ausland viele Leute benachrichtigt, dass es bei der Umstellung zu Datenverlusten gekommen ist und die Zugangsdaten auf ihre Richtigkeit geprüft werden müssten. Anschließend erhielten die Angerufenen eine vorgedruckte E-Mail. Der Bürger wurde darin aufgefordert, seine Daten einzugeben und die E-Mail zurückzusenden. Ohne entsprechende Weiterleitung drohe finanzieller Schaden und Datenverlust.

Auch bestimmte Fälle des Vishings können unter den Straftatbestand der Nötigung fallen.

5. § 263 a StGB - Computerbetrug

Zu prüfen ist, ob es sich beim Phishing um eine Vorbereitungshandlung im Sinne des § 263 a StGB Abs. 3 handelt. Der § 263 a StGB sieht vor, dass eine Beeinflussung eines Computerprogrammes stattfindet. Dies ist nicht zutreffend. Die Täuschungs-E-Mail stellt kein Computerprogramm im Sinne des § 263 a StGB dar.[137] Ein Computerprogramm nimmt eine Reihe von Befehlen entgegen und verarbeitet sie selbstständig nach bestimmten Abläufen, mit dem Ziel, ein entsprechendes Ergebnis zu erzielen.[138] Auch die Phishing-Website erfüllt nicht den Tatbestand des § 263 a Abs. 3 StGB, da die Daten nicht unmittelbar für den Computerbetrug verwendet werden.[139]

6. §§ 143, 143 a MarkenG und § 106 UrhG - Kennzeichenverletzung

In den meisten klassischen Phishing-Fällen nutzt der Phisher zur Täuschung die offiziellen Embleme und geschäftlichen Bezeichnungen der Banken. Er macht sich

[136] Vgl. Stuckenberg, ZStW (2006) S. 878,884.
[137] Vgl. Fischer (2014), § 263 a Rnr. 3.
[138] Vgl. mögliche rechtliche Definition eines Computerprogrammes http://www.linksandlaw.de/linkingundframing6.htm (recherchiert am 22.02.2014).
[139] Vgl. Gercke CR 2005 S. 606, 608.

daher nach §§ 143, 143 a MarkenG und §§ 106 UrhG strafbar, da es sich um markenrechtlich eingetragene Kennzeichen handelt.[140]

7. § 44 Abs. 1, 43 Abs. 2 Nr. 1 und 4 BDSG - Datenverarbeitung und Erhebung

Die unbefugte Datenverarbeitung und Erhebung kommt in den meisten Fällen nicht in Betracht, da individuelle Zugangscodes und TAN/PIN keine personenbezogenen Daten im Sinne des § 3 I BDSG darstellen.[141]

8. §§ 303 a, b StGB - Datenveränderung und Computersabotage

Auf den ersten Blick kämen auch die Datenveränderung und die Computersabotage beim Phishing in Betracht. Dies ist jedoch zu verneinen. Der § 303 a StGB spricht von geschützten Daten im Sinne des § 202 a StGB.[142] TAN und PIN fallen nicht unter diese Definition.

Des Weiteren setzt § 303 b StGB eine Störung einer Datenverarbeitung voraus[143], die Weiterleitung an die täuschende Website stellt allerdings keine Störung dar, sondern ist genau so gewollt.[144]

9. § 269 StGB - Fälschung beweiserheblicher Daten

Bei der Fälschung beweiserheblicher Daten muss zwischen der Phishing-Mail und der Website unterschieden werden. Voraussetzung des § 269 StGB ist, dass es sich um beweiserhebliche Daten handelt und diese durch die Tathandlung des Speicherns oder Veränderns eine falsche Wahrnehmung hervorrufen und somit eine verfälschte Urkunde vorliegt. Eine dritte Variante der Tathandlung wäre das Gebrauchen derart gespeicherter oder veränderter Daten.[145]

a) Phishing-Mail

Es ist umstritten, ob sich der Phisher / Pharmer beim Versenden der Mail nach § 269 StGB strafbar macht. Zu prüfen ist vorerst, ob es sich um beweiserhebliche Daten handelt. Beweiserheblich bedeutet, dass die Daten bestimmt und geeignet sind, für ein Rechtsverhältnis Beweis zu erbringen.[146]

---

[140] Vgl. Goeckenjan wistra (2008) S. 128 130.
[141] Vgl. Popp, NJW 2004 S. 3517-3518.
[142] Vgl. Fischer (2014) § 303 a Rnr. 3 , 4 ; Fahl/Winkler zu § 303 a StGB.
[143] Vgl. Fischer (2014) § 303 b Rnr. 4.
[144] Vgl. Goeckenjan wistra (2009) S. 47, 52.
[145] Fahl/Winkler zu § 269 StGB.
[146] Fahl/Winkler zu § 269 StGB.

Eine Meinung vertritt die Auffassung, dass eine rechtlich relevante und im Rechtsverkehr ausreichende Gedankenerklärung vorliegt, da der Phisher den Anschein erweckt das Opfer zu einer vertragsgemäßen Mitwirkung aufzufordern.[147] Vertragsgemäß deshalb, da in der Mail alles dafür spricht, dass diese durch den legitimen Vertragspartner und unter dessen Namen versendet wurde (Logo der Bank; Angabe der Abteilung der Bank; Namen des Bearbeiters).[148] Das Abspeichern der Mail im Postfach des Opfers ist die Tathandlung.[149]

Folgt man der Gegenansicht, so handelt es sich bei der Mail nicht um eine rechtlich relevante Gedankenerklärung, welche beweiserhebliche Daten enthält. Zum einen, weil diese millionenfach versendet werden und häufig leicht durchschaubare falsche Absender enthalten. Demnach fehle es an einem konkreten Aussteller.[150]

Der Bearbeiter schließt sich der ersten Meinung an. Selbst bei millionenfacher Übersendung ist die offensichtliche Erkennbarkeit der Phishing-Mails in den letzten Jahren weitaus schwieriger geworden. Das Social-Engineering der Ersteller hat sich extrem verbessert, sodass es den Empfängern oftmals nicht möglich ist zu erkennen, dass es sich bei dem Absender um eine Phantasiefirma handelt. Es ist dem juristisch nicht vorgebildeten Opfer auch nicht zuzumuten, dass es möglicherweise falsch zugeordnete Rechtsformzusätze nicht erkennt. [151] Des Weiteren wird dem Opfer eine Mitwirkungspflicht vorgespielt, von seiner vermeintlichen Bank. Auch wenn das Ansehen der Banken in der letzten Zeit stark gelitten hat, so strahlen sie dennoch genug Seriosität aus, so dass viele Menschen, ausgehend von ihrem allgemeinen Empfängerhorizont, antworten würden. Allenfalls wenn es eine offensichtliche Täuschung gibt, welche dem normal gebildeten Internetnutzer auffallen müsste, ist § 269 StGB zu verneinen. Es ist demnach eine Einzelfallentscheidung unter Berücksichtigung der Qualität der E-Mail zu treffen. Eine Strafbarkeit nach § 269 StGB ist aber vor allem unter Berücksichtigung der heutigen Zeit und den vorgenommenen Entwicklungen realitätsnaher.

b) Die Phishing-Website

Die objektiven Voraussetzungen zur Phishing-Mail sind identisch und auch bei der Website gibt es gegenteilige Auffassungen.

Die Richtigkeit des Adressaten lässt sich anhand der Website lediglich über die IP-Adresse zurückverfolgen. Diese IP-Adresse ist aber nicht falsch zugeordnet, da der Täter ja genau diese Täuschungswebsite erstellt hat. Falsch ist lediglich der auf

[147] Vgl. Seidel HRRS (2010) S. 85 ff.
[148] Vgl. Stuckenberg, ZStW (2006) S. 878,886.
[149] Vgl. Stuckenberg a.a.O.
[150] Vgl. Graf, NStZ 2007, 129 ff.
[151] OLG Koblenz Urteil vom 10.10.2007 – 1 SS 267 / 07. , NStZ-RR 2008, 120 ff.

Benutzerebene sichtbare „Domain Name“. Dieser stellt statt des unübersichtlichen Zahlencodes in der Adressleiste, einen täuschenden Namen dar. Eine Fälschung von beweiserheblichen Daten ist somit nicht gegeben.

Dieser Auffassung kann aber wie bereits bei der Phishing-Mail nicht gefolgt werden, da auch die Website eine unechte Datenurkunde darstellt. Es würde eine über die normalen Maße hinausgehende Sorgfaltspflicht des Benutzers voraussetzen, die IP-Adresse und den Domain Namen im Vorfeld zu vergleichen. Zumal auch das Emblem des Sicherheitsschlosses, welches für eine gesicherte https.// - Verbindung steht, mit modernen Methoden leicht zu fälschen ist.

Die Phishing-Website erfüllt auch den Tatbestand des § 269 StGB. In den Augen des Bearbeiters sogar in den meisten Fällen noch offensichtlicher als die Mail, da das Vertrauensverhältnis zur gesicherten Website einer Bank bei den meisten Benutzern noch höher sein dürfte, als es bei einer E-Mail der Fall ist.

Bei der Beschaffung der Zugangsdaten durch die Hilfsmittel einer E-Mail bzw. einer Website ist im Ergebnis § 269 StGB, die Fälschung beweiserheblicher Daten als Straftatbestand, in den meisten Fällen erfüllt. Diese starke Tendenz kann und darf allerdings nicht die Einzelfallprüfung ersetzen.

III. Strafbarkeit der Datenverwendung

Der zweite Handlungsschritt des Phishers ist die Überweisung eines Geldbetrages vom Konto des ausgespähten Opfers auf das Konto des Finanzagenten. Nachfolgend soll geprüft werden, ob auch dieser Vorgang ausreichend unter bestehende strafrechtliche Normen subsumierbar ist.

1. § 202 a StGB - Ausspähen von Daten

Es ist umstritten, ob § 202 a StGB bei der Überweisung und dem Zugriff auf das Konto des Opfers Anwendung findet. Die Norm setzt das Überwinden einer besonderen Zugangssicherung voraus. Bei der Zugangssicherung gibt es keine Beschränkung hinsichtlich ihrer Art und lediglich minimale Anforderungen an ihre Qualität (mechanisch, Software- oder Hardware-integrierte Sicherungen).[152]

Eine Meinung ist der Annahme, dass der objektive Tatbestand nicht erfüllt ist, da der Phisher die Zugangsdaten (PIN und TAN) direkt vom Opfer erhalten hat, eine Zugangssicherung mithin gar nicht mehr besteht. Die Zugangsbeschränkung ist in

[152] Vgl. Fischer (2014) § 202 a Rnr. 9.

dem Moment der Weitergabe aufgehoben worden.[153] Es ist dabei auch unerheblich, dass das Opfer bei der Weitergabe auf eine Täuschung hereingefallen ist.[154]
Der anderen Ansicht nach handelt es sich bei PIN und Tan allerdings um eine ausreichende Vorkehrung, die objektiv geeignet und subjektiv dazu bestimmt ist, den Zugriff auf die Daten auszuschließen bzw. zu erschweren.[155] Das Opfer sah in der Ausgangssituation durch die vorgeschaltete Kennwortabfrage eine ausreichende Zugangssicherung für seine Depotinformationen. Der Wegfall dieser Sicherung, aufgrund eigenen Weiterleitens der Daten, ist für das Opfer zu keinem Zeitpunkt ersichtlich.
Der Ansicht des Bearbeiters nach ist es auch nicht die Aufgabe des Opfers, weitere Zugangssicherungen für das Onlinekonto vorzunehmen. Dies dürfte einem beliebigen Benutzer auch überhaupt nicht möglich sein. Der Onlinekonten-Benutzer darf sich insoweit auf das Sicherungssystem der Bank verlassen.
Möglich wäre ggf. eine Diskussion über das Tatbestandsmerkmal „unter Überwindung“. Inwiefern darf dem Opfer also ein selbstschädigendes Verhalten angerechnet werden. Der § 202 a StGB sieht allerdings keine Ausnahme in der unbewussten Weitergabe der Bankdaten. Eine Strafbarkeit der Datenverwendung nach § 202 a StGB ist gegeben.[156]

2. § 202 b StGB - Abfangen von Daten

Wie bereits oben beschrieben findet beim klassischen Phishing kein „Mitschneiden“ der Daten zwischen dem Opfer und einem Dritten statt, welches für die Erfüllung des objektiven Tatbestandes aber notwendig wäre. Eine Strafbarkeit nach § 202 b StGB beim Benutzen der erschlichenen Daten ist nicht gegeben, da die Daten aus einer Direktverbindung zwischen Opfer und Phisher stammen.

3. § 202 c StGB - Vorbereiten des Ausspähens und Abfangens von Daten

Bei der Datenbeschaffung konnte noch keine Prüfung des § 202 c StGB erfolgen, da §§ 202 a, b StGB keine Anwendung fanden. Da bei der erfolgreichen Verwendung der Daten eine Strafbarkeit gemäß § 202 a StGB gegeben ist, kommt auch eine Strafbarkeit nach § 202 c StGB in Betracht. § 202 c StGB tritt allerdings in Konkurrenz zu § 202 a StGB und demnach hinter diesen zurück.[157]

---

[153] Vgl. Graf, NStZ 2007, 129, 131.
[154] Vgl. Graf a.a.O. ; Vgl. auch Fischer (2014) § 202 a Rnr. 9a.
[155] Vgl. Fahl / Winkler zu § 202 a StGB.
[156] Vgl. Seidel HRRS (2010) S. 85 ff.
[157] Vgl. Fischer (2014) § 202 c Rnr. 10.

4. § 263 a StGB - Computerbetrug

Bei der Verwendung ist nun hinsichtlich des objektiven Tatbestandes zu prüfen, welche der 4 Tatvarianten in Betracht kommt. Tathandlungsvariante Nr. 3 beschreibt das unbefugte Verwenden von Daten. Es ist nach herrschender Meinung eine betrugsspezifische Auslegung bzgl. der unbefugten Verwendung vorzunehmen. Bedeutet, die Tathandlung läge dann vor, wenn die Verwendung gegenüber einer Person eine Täuschung und damit einen Betrug nach § 263 StGB darstellen würde. [158]

Fraglich ist demnach, ob die Eingabe der zu unrecht erworbenen Kontaktdaten eine Täuschung darstellt. Beim Online-Banking musste ein Äquivalent geschaffen werden zur manuellen Überweisung am Bankschalter. Dort weist der Kunde sich durch seine Bankkarte und seinen Personalausweis aus. Im Onlinebanking erfolgt diese Identitätsprüfung gegenüber der Software der Bank durch die Eingabe von PIN und TAN. Die Kontaktdaten werden dann dem vermeintlichen Vertragspartner zugewiesen, eine Identitätstäuschung ist für die Software nicht ersichtlich. Ein Einverständnis des wirklichen Vertragspartners liegt allerdings gar nicht vor, eine Anweisung seinerseits ist nie geschehen. [159] Die Verwendung ist demnach gleichzusetzen mit einer Identitätstäuschung im Sinne des § 263 StGB.

Die dritte Tatalternative des unbefugten Verwendens ist demnach gegeben und auch die Beeinflussung des Ergebnisses einer Datenverarbeitungsanlage, da es dem Phisher ohne Eingabe der Daten nicht möglich wäre, eine Überweisung zu tätigen.[160]

§ 263 a StGB setzt einen unmittelbaren Vermögensschaden voraus. Da die Freigabe eines vermögensrelevanten Zugangs ausreicht, ist auch dieser Teil erfüllt.[161] Fraglich ist, wer den Vermögensschaden dann trägt.

Gemäß § 675 j Abs. 1 BGB ist ein Zahlungsvorgang gegenüber dem Kontoinhaber nur wirksam, wenn er diesem zugestimmt hat. Eine derartige Autorisierung gab es allerdings nie vom Kontoinhaber. Die Bank muss dann nach § 675 u BGB den entstandenen Schaden komplett ersetzen. Eine Ausnahme dieser Regelung ist der § 675 v I, II BGB. Die Bank hat demnach wiederum einen Zahlungsanspruch gegenüber dem Kontoinhaber, wenn dieser seine Daten (PIN und TAN – seine personalisierten Sicherheitsmerkmale) nicht sicher aufbewahrt hat oder der Schaden durch eine grob fahrlässige Pflichtverletzung im Sinne des § 675 Abs. 1 BGB entstanden ist. § 675 Abs. 1 BGB verpflichtet den Kontoinhaber dazu, nach

---

[158] Fahl / Winkler zu § 263 a StGB; Fischer (2014) StGB § 263 a Rnr. 11.
[159] Vgl. Beck/Dornis CR 2007, 642.
[160] Fahl/Winkler a.a.O. ; Fischer 2014 § 263 a Rnr. 20.
[161] Fischer (2014) § 263 a Rnr. 22.

Erhalt der Zugangsdaten alle zumutbaren Vorkehrungen zu treffen, um diese Daten vor unbefugtem Zugriff zu schützen. Kommt es zu einer Weitergabe der Daten, hat der Kontoinhaber dies unverzüglich anzuzeigen, nachdem er davon Kenntnis erlangt hat.

Die Frage für die Bank ist demnach, in welcher Höhe sie einen Anspruch gegen den Kontoinhaber hat gemäß § 675 v BGB. Nach § 675 v Abs. 1 S. 2 ist der Anspruch auf 150 € beschränkt, wenn die Zugangsdaten gestohlen, abhanden gekommen oder verloren gegangen sind. Dieser Zahlungsanspruch besteht für die Bank auch ohne Nennung weiterer Gründe oder Verschulden des Kontoinhabers.[162]

Eine unbegrenzte Haftung des Konteninhabers sieht § 675 v Abs. 2 BGB vor. In diesem Fall muss dem Kontoinhaber grobe Fahrlässigkeit vorgeworfen werden können. Ob grobe Fahrlässigkeit vorliegt, muss immer am Einzelfall entschieden werden und unter Beachtung von §§ 276, 277 BGB.[163] Auch hier spielt wieder der Trend des „Social-Engineering“ eine große Rolle.

Der am häufigsten auftretende Fall ist § 675 Abs. 1 S. 2 BGB. Eine grobe Fahrlässigkeit wird selten nachgewiesen werden können und der Anspruch der 150 € wird regelmäßig zu bejahen sein, da dieser verschuldensunabhängig ist.

Zusammenfassend ist demnach in den meisten Fällen ein Schaden sowohl beim Inhaber des Kontos in Höhe von 150 € entstanden, wie auch bei der Bank, welche den restlichen Schaden tragen, muss nach § 675 u S. 2 BGB. Allein beim Nachweis grober Fahrlässigkeit ist der Kontoinhaber alleiniger Geschädigter.

5. § 269 StGB - Fälschung beweiserheblicher Daten
§ 270 StGB - Täuschung im Rechtsverkehr bei Datenverarbeitung

Zu prüfen ist, ob bei der Verwendung der Bankdaten, der Tatbestand der Fälschung beweiserheblicher Daten gemäß § 269 StGB erfüllt ist.

Voraussetzung ist wieder das Speichern beweiserheblicher Daten, welche den Anschein einer Urkunde entwickeln und den Rechtsverkehr täuschen. Mit der Eingabe der Daten legitimiert sich der Phisher gegenüber der Bank. Die Bank legt sowohl einen Vorgang beim Einloggen als auch bei der Überweisung an und speichert die Information, dass sich der vermeintliche Kunde durch PIN und TAN ausgewiesen hat. [164] Da aber lediglich die Software der Datenverarbeitung der Bank getäuscht wird und keine Person, ist § 269 StGB in Verbindung mit § 270 StGB anzuwenden.

---

[162] Vgl. Palandt (2014) § 675 v, Rnr. 3 ff, Sprau.
[163] Vgl. Palandt (2014) § 675 v, Rnr. 5,6 , Sprau.
[164] Vgl. Goeckenjan wistra (2008) S. 128, 132; Vgl. Stuckenberg, ZStW (2006) S. 878,906.

Gemäß § 270 StGB ist das Merkmal der „Täuschung im Rechtsverkehr“ auch dann gegeben, wenn beim Einsatz einer Software eine menschliche Kontrolle der eingegebenen Daten nicht stattfindet und ein täuschungsgleicher Effekt durch die Beeinflussung der Software gegeben ist. [165]

6. § 303 a StGB - Datenveränderung

Bei der Datenverwendung der TAN könnte es zu einer Unbrauchbarkeit im Sinne des § 203 a StGB kommen. Selbst bei den neuesten Banksystemen, bei der mit einer TAN mehrere Verfügungen getroffen werden können, ist die TAN am Ende der „Sitzung“ verbraucht. Eine erneute Verwendung durch den wahren Berechtigten ist ausgeschlossen. Der Begriff des Unbrauchbarmachens ist als die elektronische Variante des Beschädigens nach § 303 StGB zu sehen.[166] Eine Beschädigung liegt in diesem Sinne allerdings nicht vor, da die TAN bestimmungsgemäß für eine Banküberweisung genutzt wurde. [167] Ein Unterdrücken der Zugangsdaten als Tatbestandsalternative des § 303 a StGB liegt auch nicht vor, da der legitime Benutzer auch Zugang hat, wenn der Phisher im Onlinebanking eingeloggt ist.[168] Des Weiteren setzt ein Unterdrücken voraus, dass das Opfer nach dem Übergriff wieder frei über seine Daten verfügen kann. Dies ist zu verneinen da die genutzte TAN nicht nur vorübergehend, sondern gänzlich gesperrt ist.[169]

7. § 303 b StGB - Computersabotage

Bei der Datenverarbeitung kommt es zwar zu einer Eingabe von Daten, mit der Absicht dem Opfer finanziellen Schaden zuzufügen. Allerdings mangelt es aber wie bereits oben genannt bei der Datenbeschaffung an einer Beeinträchtigung einer Datenverarbeitung.[170]

8. Anwerben des Finanzagenten

Für die Überweisung des Geldes bedient sich der Phisher eines Mittelsmannes. Diesen bezeichnet man als Finanzagenten. Er wird als Werkzeug benutzt und über die wahren Absichten des Phishers hinweggetäuscht.

Die im Anhang befindliche Anwerbungsmail (Abbildung Nr. 5) könnte einen Betrug nach § 263 StGB darstellen. Die Täuschungshandlung liegt in der falschen

---

[165] Vgl. Fischer (2014) § 270 Rnr 2.
[166] Vgl. Fischer (2014) § 303 a Rnr. 11.
[167] Vgl. Goeckenjan wistra (2009) S. 47, 53.
[168] Eigene Feststellung.
[169] Vgl. Fischer (2014) § 303 a Rnr. 10.
[170] Vgl. Goeckenjan wistra (2009) S. 47, 53.

Darstellung der „legalen“ Tätigkeiten des Finanzagenten.[171] Fraglich ist, inwiefern ein definierbarer Vermögensschaden beim Finanzkurier vorliegt, da die Vermögensminderung grds. In Geld quantifizierbar sein muss.[172] Der § 263 StGB ist dennoch nicht anwendbar, da es sich zwischen dem eintretenden Schaden des Finanzagenten und dem Vermögensvorteil beim Phisher um identische Beträge handeln muss.[173] Dies ist nicht der Fall, da der Phisher nicht den vollen Betrag vom Finanzagenten bekommt.

IV. Besonderheiten bei der Datenbeschaffung durch Malware

Das Phishing wird in diesen Fällen durch die Benutzung der Schadsoftware erweitert. Geprüft werden muss, ob auch dieses Verwenden weiterer Tatmittel strafbar ist.

1. § 263 a Abs. 3 StGB - Computerbetrug

Wie auf Seite 32 beschrieben, setzt § 263 a Abs. 3 StGB die Verwendung eines Computerprogrammes voraus, dessen Zweck die Begehung eines Computerbetruges ist. Die Schadsoftware stellt unzweifelhaft einen durch Daten vorgeschriebenen Arbeitsbefehl an den Computer dar.[174] Es handelt sich demnach unzweifelhaft um ein Computerprogramm.

Zu prüfen ist, ob der objektive Zweck dieses Programmes das Begehen eines Computerbetruges ist. Demnach darf das Programm lediglich auf seinen Inhalt strafrechtlich geprüft werden und nicht auf seine Verwendung. Die Schadsoftware müsste daher vom Ersteller ausschließlich für die Begehung eines Computerbetruges im Sinne des § 263 a I StGB geschrieben sein. Dies ist aber nicht der Fall. Ein Trojaner oder ein Keylogger dient nicht der unmittelbaren Begehung eines Computerbetruges, sondern zur Erlangung der Kontodaten.[175] Eine Strafbarkeit ist bei den ausspähenden Arten der Malware nach § 263 a Abs. 3 StGB nicht gegeben.Es stellt sich hier auch ein praktisches Problem. Wenn § 263 a StGB auch Vorbereitungsprogramme umfassen sollte für eine möglicherweise stattfindende Betrugshandlung, so ergäbe sich eine viel zu weitreichende Präjudizierung der Programme.[176]

---

[171] Vgl. Goeckenjan wistra (2008) S. 128, 132.
[172] Vgl. Fischer (2014) § 263 Rnr. 110; 111; 114.
[173] Vgl. Goeckenjan wistra (2008) S. 128, 132; Schönke / Schröder, § 263 Rnr. 168 Cramer / Peron.
[174] Vgl. Fischer (2014) § 263 a Rnr. 6 ; Schönke / Schröder § 236 a Rnr. 1 ff Cramer / Peron.
[175] Fischer (2014) § 263 a Rnr. 32.
[176] Vgl. Gercke CR 2005 S. 606, 608.

2. § 303 a StGB - Datenveränderung

Zu prüfen ist, ob bei der Installation eines Keyloggers oder eines Trojaners eine Strafbarkeit nach § 303 a StGB möglich ist. Als Tatvariante kommt das Verändern, die Löschung, das Unterdrücken oder das Unbrauchbarmachen der Daten in Betracht.

Eine Veränderung der Daten kommt bei Keyloggern und Trojanern nur unter bestimmten Bedingungen vor. In erster Linie dienen sie lediglich der Informationsbeschaffung der Kontozugangsdaten. Auch verändern sie keine Datenverarbeitung innerhalb der Transaktion, sondern belegen lediglich Speicherplatz auf der Festplatte.[177] Eine Datenveränderung kommt in den Fällen in Betracht, wenn der Phisher die Host-Datei[178] verändert und den Benutzer auf eine Pharming-Website führt.

Da eine TAN-Nummer nur einmal verwendet werden kann, könnte auch das Unbrauchbarmachen oder das Unterdrücken in Betracht kommen. Ein Unterdrücken liegt vor, wenn die Daten dem berechtigten entzogen werden und dadurch Ihre Verwendbarkeit ausgeschlossen wird. [179] Dieser Fall liegt vor, wenn die Funktionsweise des Trojaners eine Kommunikation zwischen offiziellem Benutzer und der Bank verhindert. Ein Unbrauchbarmachen liegt nach der Benutzung vor. Es genügt dabei eine zeitweilige Entziehung, da bereits in minimaler Zeit erheblicher Schaden angerichtet werden kann.[180]

Eine Strafbarkeit nach § 303 a StGB ist demnach auch gegeben. Bei der Zuordnung der Tatvariante muss auf die Funktionsweise der Malware eingegangen werden.

I. Zuviel des Guten - Beeinträchtigung der Softwareentwicklung

Wenn man darüber nachdenkt, ob derzeitige Straftatbestände zu weit gefasst und es möglicherweise eine Gesetzesänderung / Ergänzung geben sollte, so muss auch immer das Gesamtbild und die einzelnen Interessenslagen der Beteiligten berücksichtigt werden. Denn neben Opfern und Tätern gibt es auch eine IT-Branche, welche durch neue Gesetze nicht in ihrem Handlungsraum beschränkt werden sollte, um in Deutschland international konkurrenzfähig bleiben zu können.

In der Praxis stößt § 202 c Abs. 1 Nr. 2 StGB auf Kritik. Im Jahr 2009 reichten mehrere Personen unter anderem Softwareentwickler eine Verfassungsbeschwerde

---

[177] Vgl. Sch / Schr. § 303 a Rnr. 8 StGB Stree / Hecker.
[178] Siehe Erklärung unter Abschnitt C.IV.c – „DNS-Spoofing“.
[179] Fahl / Winkler zu § 303 a StGB.
[180] Vgl. Sch / Schr. § 303 a Rnr. 6 Stree / Hecker.

ein, da sie eine Behinderung der Arbeit in der IT-Branche sahen.[181] Der § 202 c StGB stellt die Programme unter Strafe, welche bestimmt sind für das Ausspähen und Abfangen von Daten. Bei weiter Auslegung umfasst der § 202 c StGB auch die Entwicklung im Bereich der IT-Sicherheit. Systemadministratoren benutzen häufig ähnlich aufgebaute Software, um Sicherheitslücken überhaupt erkennen zu können. Da man mit dieser oder einer leicht veränderten Variante der Software aber auch umgekehrt Straftaten begehen kann, nennt man sie Dual-Use-Tools.[182]

I. Beispiele für Dual-Use-Tools/objektiver Tatbestand des § 202 c StGB

Passwort-Scanner, Netzwerksniffer, Portscanner und Fernwartungssysteme sind nur ein paar Werkzeuge der Netzwerkadministratoren und IT-Sicherheitsbeauftragten.

Passwort-Scanner prüfen bei der Neueinrichtung eines Passwortes, ob es den vorgeschriebenen Sicherheitsstandards entspricht, ist dies nicht der Fall bekommt der Nutzer einen Hinweis. Die Software kann aber genauso gut eingesetzt werden, um das Passwort widerrechtlich zu speichern und zu übermitteln. [183] Ähnlich verhält es sich mit sogenannten Netzwerksniffern. Diese dienen an sich zur Netzwerkoptimierung und Fehlerdiagnose, können aber auch den gesamten Datenverkehr aufzeichnen und als Schadprogramm auf dem PC des Opfers ohne große Umstände und oftmals ohne deren Wissen installiert werden. [184] Ein Portscanner zeigt offene „Türen“ zu einem Netzwerk an. Diese werden von Systemadministratoren geschlossen von potenziellen Cyberkriminellen allerdings dazu genutzt Schadsoftware nachzuladen (z. B. beim DNS-Spoofing).

Im Ergebnis ist festzustellen, dass der objektive Tatbestand des § 202 c StGB bei den Programmen fast immer verwirklicht wird.

II. Subjektiver Tatbestand des § 202 c StGB

„Programme haben keine Zwecke, sondern nur Eigenschaften, Zwecke werden ihnen durch Personen gegeben“ – eine Abgrenzung ist daher nur aufgrund subjektiver Merkmale möglich.[185]

§ 202 c StGB bezieht sich zwar explizit auf §§ 202 a, b StGB, dennoch genügt dolus eventualis.[186] Softwareentwickler wissen, dass es nicht auszuschließen ist, dass die

[181] Vgl. Fischer zu § 202 c Rnr. 2.
[182] Vgl. Borges, Stellungnahme zum Gesetzesentwurf der Bundesregierung v. 19.03.2007.
[183] Vgl. Stellungnahme Borges aaO
[184] Vgl. Stellungnahme Borges aaO ; bekanntes Sniffing-Programm: Bundestrojaner
[185] Vgl. Ernst, NJW (2007) S. 2661,2663.

Software illegal zur Anwendung kommt. Daher ist ein Inkaufnehmen einer Vorbereitungshandlung im Sinne des § 202 c StGB immer gegeben bei der Weiterentwicklung und Verbreitung der Programme. Auch der subjektive Tatbestand wäre demnach anzunehmen.[187]

III. Zwischenergebnis

Lediglich die sogenannten Hacker-tools sollen dem Gesetzgeber nach von der Norm erfasst werden. Eine Abgrenzung in der Praxis ist allerdings nicht realisierbar, ohne die flexible Handlungsfähigkeit der Sicherheitsbeauftragten komplett einzuschränken.[188] Es wäre daher zweckmäßig, den § 202 c StGB genauer zu definieren. Objektiv sollte er dahingehend eingeschränkt werden, dass nur Programme erfasst werden, welche ausschließlich der Begehung von Straftaten dienen und Testsoftware explizit ausgeschlossen wird.[189] Hinsichtlich des Phishings ist es zu empfehlen, die zentralen Delikte (§§ 269, 263 a StGB) als Verweisung -wie bereits mit den §§ 202 a, b StGB erfolgt -mit aufzunehmen. Der subjektive Tatbestand sollte lediglich dolus directus[190] und nicht dolus eventualis beinhalten, um eine Vereinfachung für Softwareentwickler zu schaffen.

J. Finanzagent / Finanzkurier

Im Vorfeld wurde bereits festgestellt, dass allein das Erlangen der Kontodaten noch keine Vermögensverfügung ist. Eine direkte Überweisung auf das eigene Konto stellt für den Phisher ein hohes Risiko der Strafverfolgung dar. Der Pharmer / Phisher muss daher einen Weg finden, wie er gefahrlos und unkompliziert an das Geld kommt.

Dafür schaltet der Phisher einen oftmals inländischen „Partner“ (den Finanzagenten) ein, der ein Konto bereithalten muss. Ist das Geld auf dessen Konto gelangt, muss dieser es über das Bargeldtransfersystem der Western Union Bank an seinen „Geschäftspartner“ (der oftmals zufällig in Osteuropa gerade auf Dienstreise ist), übersenden. Dort wird das Geld dann unter Vorlage eines falschen Ausweises in Empfang genommen.[191]

---

[186] Bedingter Vorsatz.
[187] Vgl. Borges, Stellungnahme zum Gesetzesentwurf der Bundesregierung v. 19.03.2007.; Vgl. auch Fischer (2014) § 202 C Rnr. 8.
[188] Vgl. Ai3 Arbeitsgruppe Identitätsschutz im Internet „StGB Änderung des Computerstrafrechts“.
[189] Vgl. Stuckenberg, ZStW (2006) S. 878 ff.; Vgl. Borges a.a.O.
[190] Absicht.
[191] Vgl. Graf, NStZ (2007), 129, 131. ; Neuheuser NStZ (2008) 492.

I. Anwerben des Finanzagenten / Finanzkurier

Es gibt verschiedenste Methoden einen arglosen Mittelsmann anzuwerben. Zum einen werben die Phisher mit lukrativsten Jobangeboten im Internet - getarnt als Firmenwerbung -; verschicken massenhaft E-Mails an potenzielle Mittelsmänner[192] oder schalten Anzeigen in Jobbörsen. Bei allen Varianten wird versprochen, für vergleichsweise wenig einzusetzende Zeit, ohne Vorbildung eine nicht in Relation stehende hohe Vergütung (6-10 % vom überwiesenen Geld) zu erhalten.

Um einen seriösen Eindruck zu erlangen, häufen sich die Fälle, in denen der Phisher an z. B. kleine Softwareunternehmen herantritt und sich einfachste Dienstleistungen erstellen lässt. Kommt es dann zur Bezahlung wird ein erheblich höherer Betrag an den seriösen Dienstleister überwiesen als vorher vereinbart war. Die Differenz soll das getäuschte Unternehmen dann per Western Union an eine bestimmte Person im Ausland überweisen. Dieser Ablauf ist im besonderen Maße finanziell schmerzhaft für den Getäuschten, da zum einen nun gegen ihn ermittelt wird und er für seine Arbeit auch keine Vergütung erhält, da er seinen Lohnanspruch gegen den Phisher im Ausland durchsetzen müsste.[193]

II. Strafbarkeit des Finanzagenten

Fraglich ist, inwiefern eine Strafbarkeit des Finanzagenten besteht, auch unter der Berücksichtigung seiner Gutgläubigkeit und einer Täuschungshandlung durch den Phisher.

III. §§ 263 a, 25 StGB - Strafbarkeit wegen Mittäterschaft zum Computerbetrug

Der Finanzagent ist nicht über den Tatplan informiert, mithin kann er nicht das für § 25 StGB erforderliche Wissen besitzen. Er wird sogar über die Herkunft des Geldes; dessen Legitimität und die Transaktion in den meisten Fällen getäuscht. Es liegen weder Tatherrschaft noch Täterwillen vor, eine Strafbarkeit wegen Mittäterschaft schließt sich demnach aus.[194]

---

[192] Anwerbung Finanzagent – Anhang, Abbildung Nr. 5 - https://www.a-i3.org/content/view/908/138 (recherchiert am 16.02.2014)
[193] Vgl. Biallaß ZUM (2006), S. 879,880.
[194] Vgl. Neuheuser NStZ (2008) 492.

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

Zu prüfen ist eine Strafbarkeit hinsichtlich der Beihilfe zum Computerbetrug. Als beihilfetaugliche Unterstützungshandlung kommt das Bereithalten eines inländischen Kontos, die Abhebung des Geldes und die Transferierung ins Ausland in Betracht.[195] Fraglich ist dabei vor allem, ob man auf eine Beihilfehandlung abstellen kann, da der Computerbetrug mit dem Eintritt des Schadens vollendet ist,[196] allerdings der Geldtransfer weiter läuft, bis der Vermögensvorteil auf dem Konto des Phishers eintrifft.[197] Es ist daher zu untersuchen ob eine Beihilfehandlung zwischen Vollendung des Computerbetruges und Beendigung des Geldtransfers möglich ist. Den Vermögensvorteil erlangt der Phisher erst mit Überweisung durch den Finanzagenten. Der Schaden wird hingegen bereits durch die Überweisung an den möglichen Gehilfen ausgelöst. Diese Problematik kann allerdings dahin gestellt bleiben, da die Anforderung an ein Hilfeleisten bereits in jedem Beitrag gesehen wird der die Haupttat ermöglicht oder erleichtert.[198] Sie muss nicht ursächlich für den Taterfolg im Sinne einer „conditio sine qua non sein".[199] Ein ausreichender Gehilfenbeitrag liegt demnach bereits in der Bereitstellung des Kontos und nicht erst in der Transaktion an den Phisher.

Ein doppelter Gehilfenvorsatz nach § 27 Abs. 1 StGB wird sich wohl in fast allen Fällen verneinen lassen müssen. Der Finanzkurier wird ja gerade durch den Phisher über dessen wahre Absichten und seinen vollständigen Transferierungsplan des Geldes getäuscht. Die wesentlichen Merkmale des vollständigen Planes bleiben ihm verborgen. Der Vorsatz geht meist nur so weit, fremdes Handeln zu erleichtern bzw. zu fördern.[200]

Hegt der Finanzagent allerdings Zweifel an der legalen Herkunft des Geldes und ist in der Annahme, er sichere unmittelbare Beute eines Vermögensdeliktes (Betrug, Computerbetrug, Untreue usw.), so ist er wegen Beihilfe zum Computerbetrug zu bestrafen.[201]

---

[195] Vgl. Heckmann Kapitel 8 Rnr. 133 ; Vgl. Neuheuser NStZ (2008) 492.
[196] Vgl. Schönke / Schröder Cramer/Peron § 263 a Rnr. 38; Fischer (2014)§ 262 a StGB Rnr. 22.
[197] Vgl. Fischer (2014) § 262 a Rnr. 22.
[198] Vgl. Fischer (2014) § 27 Rnr. 14.
[199] Vgl. Fischer (2014) § 27 Rnr. 14.
[200] Vgl. Neuheuser NStZ (2008) 492.; Vgl. BGH vom 29.11.2006 - 2 StR 301/06.
[201] Vgl. Fischer (2014) § 27 Rnr. 22; differenzierter und kritisch dazu BGH vom 28.02.2012 - 3 StR 435/11.

V. § 261 StGB - Geldwäsche; Verschleierung unrechtmäßig erlangter Vermögenswerte

Nur wenn die Beteiligung an der Vermögensvortat ausgeschlossen wird, kommt eine Strafbarkeitsprüfung nach § 261 StGB in Betracht.[202]

Der Tatbestand der Geldwäsche ist erfüllt, wenn jemand einen aus einer rechtswidrigen Vortat (§ 261 Abs. 1 Satz 2 Nr. 1-5 StGB) erlangten Gegenstand verbirgt, dessen Herkunft verschleiert oder die Ermittlung der Herkunft, das Auffinden, den Verfall, die Einziehung oder die Sicherstellung eines solchen Gegenstandes vereitelt oder gefährdet.

Es ist festzustellen, dass das abgephishte Geld aus einer rechtswidrigen Vortat, einem Vergehen nach § 261 Abs. 1 Satz 2 Nr. 4 a StGB herrührt. Bei der Weiterleitung des Geldes an den Phisher könnte dann ein Verbergen / Verschleiern nach § 261 Abs. 1 StGB gegeben sein.[203] Ein Verbergen ist jede Tätigkeit, die mittels einer nicht üblichen örtlichen Unterbringung oder einer den Gegenstand verdeckenden Handlung den Zugriff der Strafverfolgungsbehörden erschwert.[204] Dies ist gegeben, da eine Geldüberweisung ins Ausland erfolgt.[205] Ein Verschleiern liegt vor, wenn durch irreführende Machenschaften der Nachweis erschwert wird, dass das Geld aus einer Straftat stammt.[206] Auch das Verschleiern ist gegeben, da der Finanzagent das illegale Geld auf seinem zur Verfügung stehenden Konto in Empfang nimmt.

Der objektive Tatbestand ist erfüllt.

Zu prüfen ist nun der subjektive Tatbestand. Gemäß § 261 Absatz 5 StGB wird lediglich auf ein leichtfertiges Erkennen abgestellt in Bezug auf die Herkunft des Geldes. Leichtfertig handelt derjenige, der grob fahrlässig handelt und nicht beachtet, was sich jedermann aufdrängen muss.[207] Fraglich ist demnach, ob sich dem Finanzagenten Zweifel hätten aufdrängen müssen bei der Relation von versprochenem Lohn zur vergleichbar niedrigen Schwierigkeit der Tätigkeit und erforderlichem Vorwissen. Es muss hier jeweils eine Einzelfallentscheidung erfolgen. Der Finanzagent hat hier die Pflicht sich genauer zu informieren.[208] Hat er bereits ein „Bauchgefühl“, welches Zweifel anmeldet und die Vermutung besteht

---

[202] Neuheuser NStZ (2008) 492– siehe dort auch persönliche Strafausschließungsgründe.
[203] Vgl. NStZ 2008 aaO.
[204] Fahl / Winkler zu § 261 StGB.
[205] Fischer (2014) § 261 Rnr. 20.
[206] Fahl / Winkler zu § 261 StGB.
[207] Fahl / Winkler a.a.O.
[208] Fischer (2014) § 261 Rn. 42.

eine kriminelle Handlung zu unterstützen, so ist dies ausreichend um einen Eventualvorsatz festzustellen. [209]

VI. Verstoß gegen das Kreditwesengeschäft

Des Weiteren ergibt sich eine Strafbarkeit gegen das Kreditwesengeschäft nach §§ 54 Abs. 1 Nr. 2, 32 Abs. 1 S. 1, 1 Abs. 1 a Nr. 6 KWG, da es sich um Zahlungsaufträge gegen Entgelt handelt und somit eine Finanzdienstleistung besteht. Der Finanzagent handelt aber ohne die erforderliche Genehmigung nach § 32 Abs. 1 S. 1 KWG, der Bundesanstalt für Finanzdienstleistungsaufsicht.[210]

VII. Zusammenfassung Finanzagent

Es ist bei der Strafzumessung immer vom jeweiligen Einzelfall auszugehen. Die Vorstellungswelt des Finanzagenten, seine Reife und Einsichtsfähigkeit zur Transferhandlung ist dabei besonders zu berücksichtigen. Allein wenn er leichtfertig übersieht, dass das Geld aus einer Straftat stammt, macht er sich der Geldwäsche nach § 261 StGB strafbar. Eine Strafbarkeit nach §§ 263a, 27 StGB wird regelmäßig am erweiterten Vorsatz scheitern. Nicht in jeder Fallkonstellation (Arbeitslohn für den Kleinunternehmer) ist es dem Finanzagenten möglich, die Einsicht zu erlangen, ein Werkzeug zu sein. Die Staatsanwaltschaft, als unabhängiges Ermittlungsorgan, hat hier besondere Prüfpflicht, um den subjektiven Tatbestand festzustellen.

Der Finanzagent spielt bei der Bekämpfung und bei Aufklärung von Phishing und Computerbetrug eine zentrale Rolle. Für die Ermittlungsbehörden vor Ort ist er der erste Ansatzpunkt, um die Geldtransferkette zu verfolgen. Über die Gesprächs- und Nachrichtenprotokolle des Handys und der E-Mails ist es in seltenen Fällen auch möglich, Spuren ins Ausland aufzudecken.

K. Zusammenfassung der Diplomarbeit

Die aufgezeigten Statistiken über die Nutzung des Internets zeigen ein deutliches Bild. Das Internet und auch die darin stattfindenden Geldströme sind aus der heutigen Konsum- und Informationsgesellschaft nicht mehr wegzudenken.

Es ist dabei auch nicht verwunderlich, dass sich bei einer sehr geringen Aufklärungsquote, im Vergleich zur Gesamtkriminalstatistik, eine blühende Kriminalität entwickelt. Diese setzt sich nicht wie vielfach angenommen aus einzelnen, isolierten Hackern zusammen, sondern tritt als Underground Economy in

[209] Vgl. Neuheuser NStZ (2008) 492 ff.
[210] Vgl. Neuheuser a.a.O.

den verdeckten Foren, wie ein riesiger Marktplatz für illegale Software und Informationen auf. Das Wissen über die Hintergründe der Täter und deren Handlungsweisen, müssen die Polizei, die IT-Branche und die Banken bei der Entwicklung ihren Bekämpfungs- und Präventionsmethoden berücksichtigen.
Das größte Problem der heutigen Phishing-Attacken stellt die zielgerichtete Malware dar. Ein abschließender Überblick über die verschiedenen Arten der Malware ist nicht möglich, da ständig neue Programme durch die Cyberkriminellen entwickelt werden.
Auf der rechtlichen Ebene wurde festgestellt, dass derzeitig kein Straftatbestand explizit das Phishing erfasst. Die Handlungsschritte mussten daher unterteilt werden in die Datenbeschaffung und die Datenverwendung.
Die Datenbeschaffung fällt lediglich bei der Nötigung klar unter eine anwendbare Strafnorm. Bei § 269 StGB ist eine Einzelfallbewertung vorzunehmen. Anders verhält es sich bei der Datenverwendung. Diese lässt sich unter mehrere Straftatbestände subsumieren. Die im Vorfeld aufgeworfene Frage, ob der rechtliche Rahmen für die Erfassung des Phishing ausreichend ist, kann positiv beantwortet werden. Auch unter Berücksichtigung der neuen Malwareprogramme ist das Phishing keine straffreie Handlung.

L. Resümee

Das Internet ist schon lange kein Ort mehr, den man als abgeschottete Parallelwelt betrachten kann. Ein wachsender Anteil unseres täglichen Lebens, sei es Beruf oder Freizeit, findet unausweichlich im Netz statt. Man sollte das Internet daher auch nicht meiden oder der Nutzung mit Angst begegnen. Die aktuellen Statistiken zeigen deutlich, dass dieser Trend anhalten wird. Die bargeldlosen Onlineüberweisungen stellen in meinen Augen eine sehr große Errungenschaft dar. Das Wissen darüber, möglicherweise Opfer eines Cyberkriminellen zu werden, sollte allerdings bei jedem vorhanden sein. Dies erfordert eine gewisse Aufmerksamkeit, welche allerdings in jedem Geldgeschäft auch außerhalb des Internets geboten ist. Die mediale Aufklärung und die meisten Präventionsmethoden sind unter den gegebenen schwierigen und sich ständig verändernden Erscheinungsformen des Phishing bereits als gut zu bewerten.

Bei der rechtlichen Wertung des Phishing kann ein klares Ergebnis gefasst werden. Da die Datenverwendung unter mehrere Strafnormen subsumiert werden kann, ist es eher ein theoretisches Problem, dass die Datenbeschaffung in den meisten Fällen straffrei bleibt. Die Einführung eines Phishing-Tatbestandes in das dt.

Strafgesetzbuch ist nicht notwendig. Auch kann sich mit der Aufnahme eines Straftatbestandes keine leichtere polizeiliche Ermittlung erhofft werden. In der Schwierigkeit der Bekämpfung ist die schlechte Aufklärungsquote zu sehen und nicht die komplizierte Zuweisung einer Strafnorm. Eine speziellere Definition des § 202 c StGB ist aber dennoch wünschenswert. Es sollte explizit die Software ausgeschlossen werden, welche als Arbeitsmittel täglich durch die Systemadministratoren genutzt wird. Um die Arbeit der Softwareentwickler nicht im Vorfeld einzuschränken, darf lediglich „dolus directus“ zu einer Strafbarkeit führen.

Abschließend sei festzuhalten, dass der strafrechtliche Rahmen der dt. Gesetzgebung die Kriminalitätsform Phishing und die Handlungen des Finanzagenten ausreichend und vollständig erfasst.

Anhang

Abbildung Nr. 1

Preisliste für Underground-Artikel

Die Übersicht enthält Preise für Waren und Dienstleistungen, wie sie im Zeitraum von Juni und Juli 2009 in Untergrundforen gehandelt wurden. Es gibt eine weite Preisspanne, die von Rabatten und gutem Verhandlungsgeschick bestimmt wird.

Produkt	Min. Preis	Max. Preis
RAT – abhängig von Features	20,00 €	100,00 €
Stealer – s.o.	5,00 €	40,00 €
Gefälschte Ausweise/Führerscheine – abhängig von Qualität der Fälschung	50,00 €	2.500,00 €
Bot-Datei – Preis nach Features und Programmierer	20,00 €	100,00 €
Bot-Quellcode	200,00 €	800,00 €

Dienstleistung	Min. Preis	Max. Preis
Hosting – nach Umfang der Dienstleistung, von Webspace bis zu mehreren Servern alles möglich	5,00 €	9.999,00 €
FUD-Service	10,00 €	40,00 €
DDoS-Attacke pro Stunde	10,00 €	150,00 €
Bot-Installs pro 1000 – die Preise richten sich nach der geografischen Lage	50,00 €	250,00 €
1 Million Spam-Mails an spezielle Adressaten, z.B. Spieler erhöhen den Preis	300,00 €	800,00 €

Daten	Min. Preis	Max. Preis
Datenbanken – für den Preis relevant sind genaue Inhalte und Umfang der Datenbank, es geht um den Kauf einer Datenbank	10,00 €	250,00 €
Kreditkartendaten – Preise richten sich nach Vollständigkeit der Daten. Nur eine CC-Nummer und Datum sind nicht viel Wert. Je mehr Daten mitgeliefert werden, desto höher ist der Preis.	2€	300€
1 Million E-Mail-Adressen – verifizierte Adressen oder von Interessen-Gruppen kosten mehr	30,00 €	250,00 €

Accounts	Min. Preis	Max. Preis
Steam-Account – Preis richtet sich nach Menge der installierten Spiele	2,00 €	50,00 €
WoW-Account – je nach Umfang der Daten und Level der Charaktere im Account	5,00 €	30,00 €
Packstation-Account – Preise richten sich nach Umfang der vorhanden	50,00 €	150,00 €

Abbildung Nr. 2

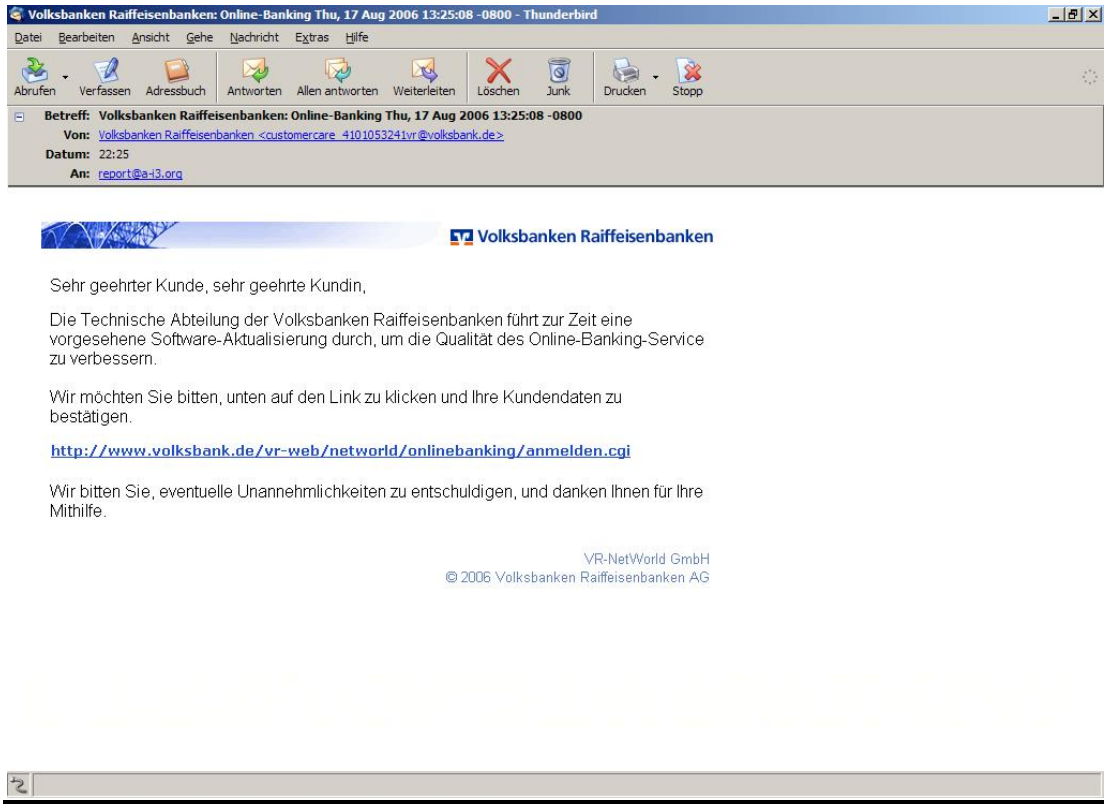


Abbildung Nr. 3

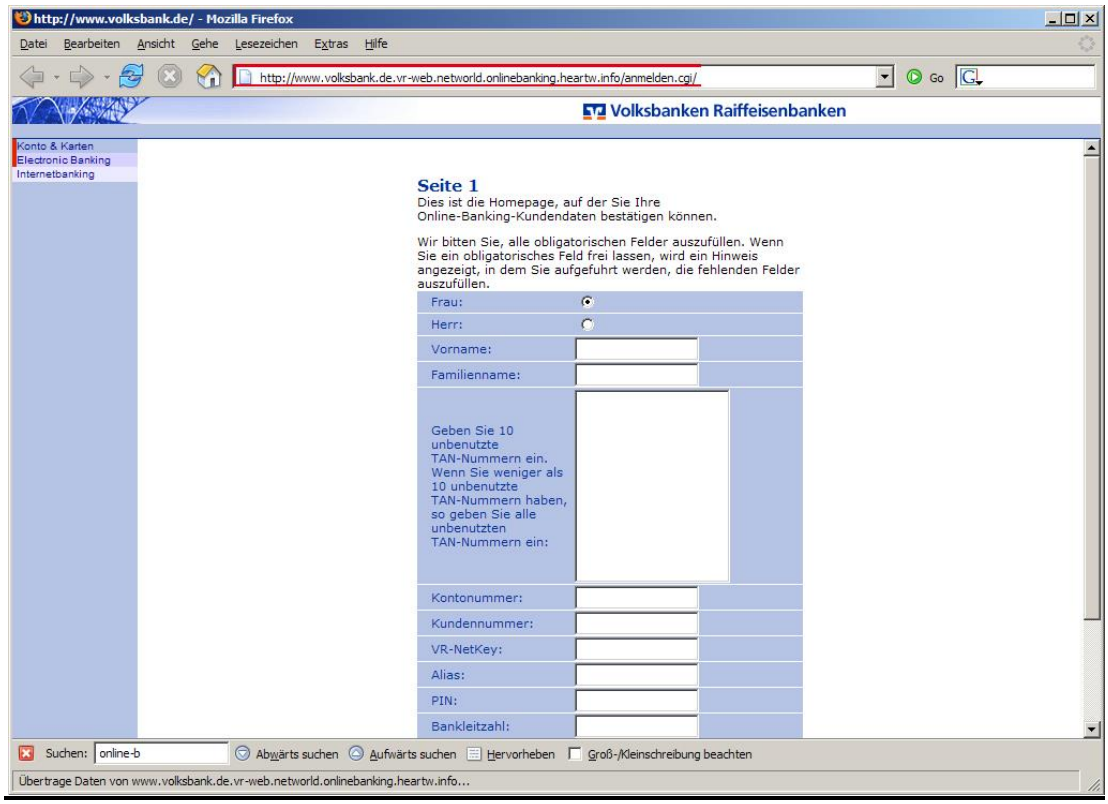


Abbildung Nr. 4

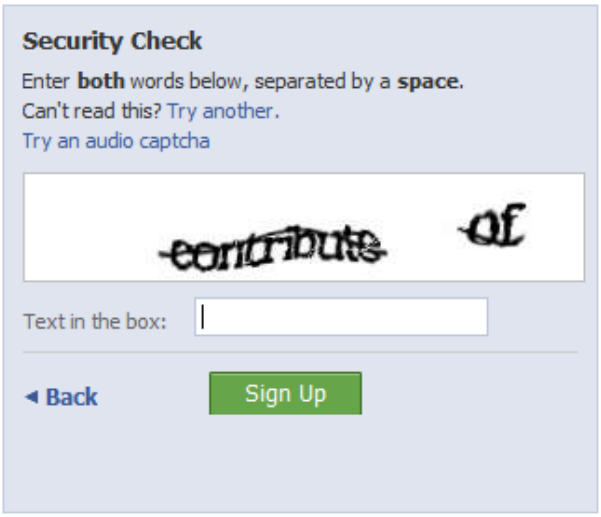


Abbildung Nr. 5

Sehr geehrte Damen und Herren, wir danken für die Möglichkeit uns Ihnen kurz vorstellen zu können

Unsere Gesellschaft ist seit mehreren Jahren auf dem Grossmarkt bekannt. Der Kernpunkt unserer Interessen liegt im Edelmetalmarkt, wobei wir auch in vielen benachbarten Branchen tätig sind. Sei es Börse, weltbekannte Auktionen, oder Forschung , ist es unser Ziel für uns und unsere Kunden immer die besten Ergebnisse zu erzielen. Im Moment ist die Entscheidung getroffen worden auf den deutschen Markt zu kommen, da dieser einen hohen Entwicklungspotenzial und höchstmöglichen Gewinnerziehlung erwarten lässt. Zur Zeit wird eine limitierte Anzahl Angestellte unter Vertrag genommen, oder auch als freie Mitarbeiter eingesetzt.

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 Beförderungsmöglichkeiten
- 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 unserer 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.

Impressum

Herausgeber der Reihe
Dekan Fachbereich Rechtspflege

ISBN
978-3-943579-49-9

Auflage
100

Druck
HWR Berlin

Berlin, August 2014

www.hwr-berlin.de