

Master of Advanced Studies in Forensics (MAS Forensics)

Phishing und Skimming

Die Strafbarkeit aktueller Deliktsformen im elektronischen
Zahlungsverkehr

Masterarbeit

eingereicht am 16. April 2007
von

Markus Gisin

MAS Forensics, Klasse 1

betreut von

Prof. Dr. iur. Jürg-Beat Ackermann

Inhaltsverzeichnis

Inhaltsverzeichnis	III
Literaturverzeichnis	IV
Materialien	V
Abkürzungsverzeichnis	VI
Anhang	VI
Anmerkung	VI
Kurzfassung	VII

INHALTSVERZEICHNIS

1	EINLEITUNG	1
1.1	DELIKTE IM E-BANKING.....	2
1.2	DELIKTE BEIM KARTENGELD.....	2
2	PHISHING	3
2.1	BEGRIFF UND VORGEHENSWEISE.....	3
2.2	STRAFRECHTLICHE WÜRDIGUNG.....	5
2.2.1	<i>Veruntreuung – Art. 138 StGB</i>	5
2.2.2	<i>Diebstahl – Art. 139 StGB</i>	5
2.2.3	<i>Unbefugte Datenbeschaffung – Art. 143 StGB</i>	6
2.2.4	<i>Unbefugtes Eindringen in ein Datenverarbeitungssystem – Art. 143^{bis} StGB</i>	8
2.2.5	<i>Betrug – Art. 146 StGB</i>	9
2.2.6	<i>Betrügerischer Missbrauch einer Datenverarbeitungsanlage – Art. 147 StGB</i>	11
2.2.7	<i>Unbefugtes Beschaffen von Personendaten – Art. 179^{novies} StGB</i>	13
2.2.8	<i>Urkundenfälschung – Art. 251 StGB</i>	14
2.2.9	<i>Markenschutzgesetz</i>	18
2.2.10	<i>Konkurrenzen</i>	20
2.3	FALLBEISPIEL 1: PHISHING-ATTACKE AUS DEM JAHR 2005.....	21
2.3.1	<i>Sachverhalt</i>	21
2.3.2	<i>Strafrechtliche Würdigung</i>	22
2.3.3	<i>Kommentar zum Fallbeispiel</i>	22
2.4	FALLBEISPIEL 2: PHISHING-ATTACKE AUS DEM JAHR 2006.....	23
2.4.1	<i>Sachverhalt</i>	23
2.4.2	<i>Strafrechtliche Würdigung</i>	24
2.4.3	<i>Kommentar zum Fallbeispiel</i>	25
3	SKIMMING	26
3.1	BEGRIFF UND VORGEHENSWEISE.....	26
3.2	STRAFRECHTLICHE WÜRDIGUNG.....	28
3.2.1	<i>Diebstahl – Art. 139 StGB</i>	28
3.2.2	<i>Unbefugte Datenbeschaffung – Art. 143 StGB</i>	29
3.2.3	<i>Unbefugtes Eindringen in ein Datenverarbeitungssystem – Art. 143^{bis} StGB</i>	30
3.2.4	<i>Betrug – Art. 146 StGB</i>	30
3.2.5	<i>Betrügerischer Missbrauch einer Datenverarbeitungsanlage – Art. 147 StGB</i>	31
3.2.6	<i>Check- und Kreditkartenmissbrauch – Art. 148 StGB</i>	32
3.2.7	<i>Unbefugtes Beschaffen von Personendaten – Art. 179^{novies} StGB</i>	33
3.2.8	<i>Urkundenfälschung – Art. 251 StGB</i>	33
3.2.9	<i>Konkurrenzen</i>	34
3.3	FALLBEISPIEL 1: BANCOMAT-SKIMMING.....	35
3.3.1	<i>Sachverhalt</i>	35
3.3.2	<i>Strafrechtliche Würdigung</i>	36
3.3.3	<i>Kommentar zum Fallbeispiel</i>	36
3.4	FALLBEISPIEL 2: SKIMMING IM KLEIDERGEWÄNDLICHEN.....	37
3.4.1	<i>Sachverhalt</i>	37
3.4.2	<i>Strafrechtliche Würdigung</i>	38
3.4.3	<i>Kommentar zum Fallbeispiel</i>	38
4	FAZIT	38
4.1	FAZIT ZUM PHISHING.....	39
4.2	FAZIT ZUM SKIMMING.....	40

LITERATURVERZEICHNIS

- AMMANN** Matthias; Sind Phishing-Mails strafbar?; AJP 2006 S 195-203
- BAUDENBACHER** Carl; Lauterkeitsrecht – Kommentar zum Gesetz gegen den unlauteren Wettbewerb; Helbing & Lichtenhahn, Basel 2001
- BISWAS** Chanchal; Regeln 1 und 2: Passwort nicht verraten; NZZ am Sonntag vom 27. August 2006
- BOOG** Markus; Kommentar zu Art. 110 StGB, aus: Basler Kommentar, Strafgesetzbuch I, M.A. Niggli und H. Wiprächtiger (Hrsg.), Basel 2003 (zit. BSK StGB I)
- BOOG** Markus; Kommentar zu Art. 251 StGB, aus: Basler Kommentar, Strafgesetzbuch II, M.A. Niggli und H. Wiprächtiger (Hrsg.), Basel 2003 (zit. BSK StGB II)
- BRINER** Robert G.; Haftung der Internet-Provider für Unrecht Dritter; Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht, Ausgabe 6/2006, Seiten 383-400
- BUGGISCH** Walter / **KERLING** Christoph; Phishing, Pharming und ähnliche Delikte; Kriminalistik 2006, Heft 8-9, Seiten 531-536
- DAVID** Lucas; Markenschutzgesetz, Muster- und Modellgesetz; Helbing & Lichtenhahn, Zürich 1998
- ECKERT** Andreas; Die strafrechtliche Erfassung des Check- und Kreditkartenmissbrauchs; Schulthess Polygraphischer Verlag AG Zürich 1991
- FIOLKA** Gerhard; Kommentar zu Art. 147 StGB, aus: Basler Kommentar, Strafgesetzbuch II, M.A. Niggli und H. Wiprächtiger (Hrsg.), Basel 2003 (zit. BSK StGB II)
- FLURI** Anton; Bekämpfung des Kreditkartenmissbrauchs – Technische Aspekte; Kriminalistik 2003, Heft 8-9, Seiten 554-556
- FONTAINE** Joachim; Sicherheit an Geldautomaten; Retail Banking und Banktechnologie – Bundesverband deutscher Banken 2005
- GUGGENBÜHL** Heinrich; Bekämpfung des Kreditkartenmissbrauchs – gegenwärtige Verhältnisse; Kriminalistik 2003, Heft 8-9, Seiten 551-552
- KRONENBERG** Friedrich; Internet – das Taschenbuch; 4. überarbeitete Auflage. Verlag Moderne Industrie 2002
- NIGGLI** Marcel A. / **SCHWARZENEGGER** Christian; Strafbare Handlungen im Internet; SJZ 2002, Seiten 61-73
- NIGGLI** Marcel Alexander / **RIEDO** Christof; Kommentar zu Art. 139 StGB, aus: Basler Kommentar, Strafgesetzbuch II, M.A. Niggli und H. Wiprächtiger (Hrsg.), Basel 2003 (zit. BSK StGB II)
- OPPLIGER** Rolf; „Sichere“ Streichlisten; DIGMA-Zeitschrift für Datenrecht und Informationssicherheit, Heft 1/2005; Seiten 34-35
- PFEFFERLI** Peter; Bekämpfung des Kreditkartenmissbrauchs – Spurekundliche Aspekte; Kriminalistik 2003, Heft 8-9, Seiten 552-554
- SCHAAD** Peter; Kartenleser statt Nummernliste; Der Bund vom 19. Januar 2007
- SCHINDLER** Werner; Zum sicheren Umgang mit EC- und Kreditkarten; Bundesamt für Sicherheit in der Informationstechnik 2004
- SCHMID** Niklaus; Computer- sowie Check- und Kreditkarten-Kriminalität; Schulthess Polygraphischer Verlag Zürich 1994
- SCHNEIDER** Margit; Kartensicherheit.de; Referat der Konferenz Kartensicherheit vom 20.09.2006
- SCHWARZENEGGER** Christian; Der räumliche Geltungsbereich des Strafrechtes im Internet; Schweizerische Zeitschrift für Strafrecht, 118/2000, Seiten 109-130
- STULZ** Stephan / **REICHERT** Bernd; Rechtsunsicherheit im Internet-Banking; Neue Züricher Zeitung vom 22. September 2006
- STRATENWERTH** Günter; Schweizerisches Strafrecht, Besonderer Teil I: Straftaten gegen Individualinteressen; Stämpfli Verlag AG Bern 1995
- TRECHSEL** Stefan; Schweizerisches Strafrechtsgesetzbuch – Kurzkomentar; 2. neubearbeitete Auflage; Schulthess Polygraphischer Verlag Zürich 1997
- VON INS** Peter / **WYDER** Peter-René; Kommentar zu Art. 179^{novies} StGB, aus: Basler Kommentar, Strafgesetzbuch II, M.A. Niggli und H. Wiprächtiger (Hrsg.), Basel 2003 (zit. BSK StGB II)
- WEISSENBERGER** Philippe; Kommentar zu Art. 143 StGB, aus: Basler Kommentar, Strafgesetzbuch II, M.A. Niggli und H. Wiprächtiger (Hrsg.), Basel 2003 (zit. BSK StGB II)
- WEISSENBERGER** Philippe; Kommentar zu Art. 143^{bis} StGB, aus: Basler Kommentar, Strafgesetzbuch II, M.A. Niggli und H. Wiprächtiger (Hrsg.), Basel 2003 (zit. BSK StGB II)
- WESSELMANN** Bettina; Banken – Phishing und Gegenmassnahmen; SicherheitsForum Heft 1/2007; Seiten 15-18

MATERIALIEN

CENTER FOR SECURITY STUDIES - ETH; Informationssicherheit in Schweizer Unternehmen – eine Umfragestudie über Bedrohungen, Risikomanagement und Kooperationsformen; Zürich 2006

DIE SCHWEIZERISCHE POST; Jahresergebnis 2006 von PostFinance; Pressemitteilung vom 06. Februar 2007

DIE SCHWEIZERISCHE POST; Teilnahmebedingungen yellownet, August 2006

DIE SCHWEIZERISCHE POST; Teilnahmebedingungen Postcard, Juli 2006

MELDE- UND ANALYSESTELLE INFORMATIONSSICHERUNG; Informationssicherung – Lage in der Schweiz und International, Halbjahresbericht Juli bis Dezember 2005, Bundesamt für Polizei

MELDE- UND ANALYSESTELLE INFORMATIONSSICHERUNG; Informationssicherung – Lage in der Schweiz und International, Halbjahresbericht Januar bis Juni 2006, Bundesamt für Polizei

GESETZE

- Bundesgesetz vom 28. August 1992 über den Schutz von Marken und Herkunftsangaben; SR 232.11
- Bundesgesetz vom 19. Dezember 1986 gegen den unlauteren Wettbewerb; SR 241
- Schweizerisches Strafgesetzbuch vom 21. Dezember 1937; SR 311.0

BUNDESGERICHTSENTSCHEIDE

- BGE 98 IV 85
- BGE 101 IV 117
- BGE 104 IV 72
- BGE 116 IV 332
- BGE 116 IV 343
- BGE 127 IV 68
- BGE 129 IV 315
- BGE 6P.37/2005

INTERNETSEITEN

- Antiphishing.org: www.antiphishing.org
- Die Schweizerische Post: www.post.ch und www.postfinance.ch
- Heute-Online: www.heute-online.ch
- Kartensicherheit Deutschland: www.kartensicherheit.de
- Schweizerische Bankiervereinigung: www.swissbanking.org
- Swissreg – Eidg. Institut für Geistiges Eigentum: www.swissreg.ch

ABKÜRZUNGEN

a.a.O.	am angegebenen Ort
Abs.	Absatz
AJP	Allgemeine Juristische Praxis
Art.	Artikel
BGE	Bundesgerichtsentscheid, zitiert nach Band, Teil und Seitenzahl
BSK	Basler Kommentar
bzw.	beziehungsweise
CHF	Schweizer Franken
d.h.	das heisst
Erw.	Erwägung
EUR	Euro
ff.	folgende
i.d.R.	in der Regel
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
m.E.	meines Erachtens
NZZ	Neue Zürcher Zeitung
MELANI	Melde- und Analysestelle Informationssicherung des Bundesamtes für Polizei
MSchG	Markenschutzgesetz
resp.	respektive
S.	Seite
sog.	sogenannte(r)
StGB	Schweizerisches Strafgesetzbuch
SJZ	Schweizerische Juristen Zeitung
u.a.	unter anderem
usw.	und so weiter
UWG	Bundesgesetz gegen den unlauteren Wettbewerb
z.B.	zum Beispiel
Ziff.	Ziffer
zit.	zitiert

ANHANG

- Phishing-e-mail und Phishing-Internetseite aus Kapitel 2.4
- „PostFinance“ – spezifischer Markeneintrag im Swissreg

ANMERKUNG

In dieser Masterarbeit wird der einfacheren Lesbarkeit wegen grundsätzlich die männliche Form verwendet.

KURZFASSUNG

Der elektronische Zahlungsverkehr ist ein wichtiger Bestandteil des heutigen Wirtschaftssystems. Das zeit- und standortunabhängige Bezahlen von Rechnungen mittels E-Banking oder der bequeme Einsatz von Debit- und Kreditkarten an Automaten zum Bezug von Bargeld oder zur Bezahlung von Waren oder Dienstleistungen mit automatischer Belastung des eigenen Kontos sind weit verbreitet.

Diese Arbeit beschäftigt sich mit der Frage der Strafbarkeit von Phishing und Skimming als aktuelle Deliktsformen im elektronischen Zahlungsverkehr.

Gerade der sich laufend vergrößernde Benutzerkreis des Internet-Banking hat in seinem Sog auch kriminelle Elemente auf den Plan gerufen. Das sogenannte Phishing ist mittlerweile zu einer der aktuellsten und akutesten Deliktsformen in diesem Bereich avanciert. Jedes 93. e-mail, welches weltweit versendet wird, ist bereits ein Phishing-e-mail.

Das Phishing lässt sich in zwei voneinander unabhängige Schritte wie folgt unterteilen: Als ersten Schritt kontaktiert die Täterschaft das potentielle Opfer mittels einer e-mail, die es dazu verleiten soll, vertrauliche Informationen im Bezug auf seine E-Banking-Zugänge (Passwort, PIN-Code, weitere Sicherheitsmerkmale) preiszugeben. Häufig wird dabei das Opfer durch einen im e-mail aufgeführten Link auf eine Internetseite gelockt, welche das E-Banking-System seines Finanzinstitutes nachahmt. Sobald das Opfer dort seine Zugangsinformationen eingibt, stehen diese der Täterschaft zur Verfügung. In einem zweiten Schritt loggt sich dann die Täterschaft mit diesen Zugangsinformationen in das E-Banking-System des betreffenden Finanzinstitutes ein und löst im Namen des Opfers entsprechende Geldtransaktionen aus. Bevor der Kontoinhaber oder das Finanzinstitut etwas bemerken sind die Gelder überwiesen und abgehoben.

Somit sind für die rechtliche Würdigung folgende zwei Tathandlungen zu unterscheiden:

- Der Versand von Phishing-e-mails zum Erhalt der vertraulichen Daten.
- Die Verwendung dieser vertraulichen Daten zum Zwecke der unrechtmässigen Bereicherung.

Beim Versand der Phishing-e-mails gibt sich die Täterschaft als das jeweilige Finanzinstitut aus und verwendet dabei missbräuchlich Marken und Logos des betroffenen Institutes, welche im Regelfall entsprechend geschützt sind (einfach nachzuprüfen unter www.swissreg.ch). Dieses Vorgehen verstösst gegen Art. 62 des Markenschutzgesetzes, welcher den betrügerischen Markengebrauch unter Strafe stellt. Da zudem die Täterschaft beim Phishing in der Regel gewerbsmässig handelt, ist die Tat gemäss Abs. 2 dieser Bestimmung sogar von Amtes wegen zu verfolgen.

Phishing-e-mails, die selber mit konkreten Handlungsanweisungen zur Eingabe der Zugangsdaten versehen und vom Original des konkreten Finanzinstitutes nicht zu unterscheiden sind, erfüllen überdies den Straftatbestand der Urkundenfälschung nach Art. 251 StGB.

Die von den Phishern präparierte Internetseite zur Eingabe der Zugangsinformationen verstösst ebenfalls gegen das Markenschutzgesetz, da wiederum missbräuchlich Marken und Logos des betroffenen Institutes verwendet werden. Zudem kann die Internetseite eine Urkundenfälschung im Sinne von Art. 251 StGB sein, wenn das Erscheinungsbild dem Original des Finanzinstitutes täuschend ähnlich ist und auch die restlichen Anforderungen an eine Computerurkunde erfüllt sind.

Beim zweiten Teil der Tathandlung, der Verwendung der Zugangsinformationen um im E-Banking-System entsprechende Transaktionen zur unrechtmässigen Bereicherung auszulösen, handelt es sich klar um einen betrügerischen Missbrauchs einer Datenverarbeitungsanlage gemäss Art. 147 StGB.

Während nun in der Praxis der zweite Teil des Phishing problemlos als einen betrügerischen Missbrauch einer Datenverarbeitungsanlage nach Art. 147 StGB beurteilt wird, wird der erste Teil des Phishing vielfach fälschlicherweise als lediglich straflose Vorbereitungshandlung zum zweiten Teil missverstanden. Wie diese Arbeit aufzeigt, ist diese enge Betrachtungsweise nicht nur falsch, sondern aus Sicht der Prävention fragwürdig. Die Gesetzgebung stellt – insbesondere mit dem Markenschutzgesetz – genügend Grundlagen zur Verfolgung sämtlicher Tathandlungen des Phishing zur Verfügung. Diese müssen von der Praxis nur noch angewendet werden.

Infolge seiner breiten Streuung ist auch das Kartengeld (Debit- und Kreditkarten) Ziel von Kriminellen geworden. Das sogenannte Skimming von Zahlkarten an Automaten gehört heute leider zur alltäglichen Realität.

Beim Skimming präpariert die Täterschaft einen für die Verwendung von Zahlkarten vorgesehenen Automaten (häufig ein Geldausgabegerät). Es wird eine Lesevorrichtung installiert, welche bei Nutzung des Automaten sicherstellt, dass der Magnetstreifen der verwendeten Karte nicht nur vom Automaten sondern auch vom zusätzlich installierten Lesegerät eingelesen und kopiert wird. Zudem wird von der Täterschaft versucht, den vom Karteninhaber verwendeten PIN-Code auszuspiionieren. Dies erfolgt vielfach durch den Einsatz einer verdeckten Videoüberwachung. Nachdem die Täterschaft die Daten des Magnetstreifens zur Verfügung hat und den PIN-Code kennt, werden die Daten auf einen leeren Magnetstreifen kopiert und von der Täterschaft gemeinsam mit dem PIN-Code an verschiedenen Automaten eingesetzt. Im Regelfall erfolgen unrechtmässige Bezüge von Bargeld oder der Einkauf von Waren und Dienstleistungen.

Analog zum Phishing kann auch das Skimming für die rechtliche Würdigung in zwei unterschiedliche und voneinander unabhängige Tathandlungen unterteilt werden:

- Der erste Schritt besteht aus dem Beschaffen (Kopieren) der Daten des Magnetstreifens und des PIN-Codes.
- Im zweiten Schritt werden die Daten auf einen neuen Magnetstreifen kopiert und unter Verwendung des PIN-Codes zum Zwecke der unrechtmässigen Bereicherung an einem Automaten eingesetzt.

Der erste Schritt kann als unbefugte Datenbeschaffung nach Art. 143 StGB qualifiziert werden, zumal die Täterschaft beim Skimming immer in Bereicherungsabsicht handelt.

Das Kopieren der Daten auf einen leeren Magnetstreifen zur anschliessenden gemeinsamen Verwendung mit dem PIN-Code erfüllt den Tatbestand der Urkundenfälschung nach Art. 251 StGB, da es sich bei den Originaldaten auf dem Magnetstreifen um eine Computerurkunde handelt und die Täterschaft beim Skimming in Vorteilsabsicht handelt.

Der Einsatz der kopierten Karten und des PIN-Code an einem Automaten zum unrechtmässigen Bezug von Bargeld oder zur Bezahlung von Waren oder Dienstleistungen gilt als betrügerischer Missbrauch einer Datenverarbeitungsanlage gemäss Art. 147 StGB.

Während im Zusammenhang mit Skimming die Anwendung von Art. 143 StGB für den ersten Schritt und Art. 147 StGB für den zweiten keine Probleme zu bereiten scheinen, geht in der Praxis häufig vergessen, dass die Herstellung einer Kopie des Magnetstreifens eine Urkundenfälschung nach Art. 251 StGB darstellt. Dies dürfte mit der nicht immer einfachen Definition des Urkundenbegriffes, respektive der Computerurkunde zu begründen sein.

Zusammenfassend kann zu den Deliktsformen Phishing und Skimming festgehalten werden, dass durch den bestehenden Gesetzesrahmen sämtliche Handlungen des Skimming und Phishing als Officialdelikte erfasst werden. Diese Erkenntnis ist jedoch in der Praxis noch nicht vollständig umgesetzt worden, was vor allem beim Versand von Phishing-e-mails zu falschen Schlüssen (straflose Vorbereitungshandlung) der Strafverfolgungsbehörden führt. Dies kann aber weder im Sinne der Verbrechensprävention noch der von den Deliktsformen betroffenen Personen und Unternehmen sein.

1 Einleitung

Checks, schriftliche Zahlungsaufträge und sogenanntes Kartengeld (Kredit- und Debitkarten) sind die wesentlichsten Produkte des heutigen bargeldlosen Zahlungsverkehrs. Mit der Einführung und Verbreitung des elektronischen Zahlungsverkehrs haben Checks und schriftliche Zahlungsaufträge jedoch an Bedeutung verloren, weshalb sie in der Praxis immer weniger benutzt werden.

Mit elektronischem Zahlungsverkehr ist im Rahmen dieser Arbeit das Bezahlen mittels informatikgestützter Geldtransfers gemeint. Darunter fällt die Zahlungsverarbeitung via Internetplattformen von Finanzinstituten (sog. E-Banking oder Online-Banking), aber auch der Bezug von Bargeld an Geldausgabegeräten oder das Bezahlen an elektronischen Terminals, von wo aus direkt das auf die verwendete Karte lautende Konto belastet wird.

Praktisch jeder Kontoinhaber verfügt heute über eine entsprechende Kontokarte (Debitkarte), welche es ihm ermöglicht an einem Geldausgabegerät Bargeld zu beziehen oder seinen Einkauf mittels Verwendung dieser Karte direkt ab seinem Konto abbuchen zu lassen.

Nebst Debitkarten gehören auch Kreditkarten zum Kartengeld und sind ebenfalls weit verbreitet. Auch die Kreditkarte kann – analog wie die Debitkarte – als elektronische Zahlkarte verwendet werden. Der grundsätzliche Unterschied zwischen Debit- und Kreditkarte besteht darin, dass bei einer Bezahlung mittels Debitkarte der fragliche Betrag jeweils direkt auf dem Konto des Karteninhabers belastet wird. Bei der Kreditkarte hingegen erfolgt die Bezahlung durch die Kreditgesellschaft, welche die Karte herausgegeben hat. Der Betrag wird – als Kredit für den Karteninhaber – durch die Kreditgesellschaft vorfinanziert und in der Regel monatlich dem Benutzer belastet.

Während die Kreditkarte seit jeher eine grosse Rolle im bargeldlosen Zahlungsverkehr gespielt hat, ist die Bedeutung der Debitkarte gemeinsam mit der Verbreitung des elektronischen Zahlungsverkehrs ständig gewachsen, da sie nebst dem Bargeldbezug auch als Zahlkarte an elektronischen Terminals im Handel, Gastronomie, Tourismus etc. eingesetzt werden kann. Zur Veranschaulichung dieser Bedeutung sei ein Beispiel der Kunden von PostFinance – dem Finanzinstitut der Schweizerischen Post – aufgezeigt: An einem einzigen Tag, am 23.12.2006, haben alleine PostFinance-Kontoinhaber ihre Karten in der Schweiz insgesamt 518'000 mal eingesetzt.¹

Mit der Verbreitung des Internets hat auch die Verbreitung des E-Banking oder Online-Banking stattgefunden, welches dem Kunden erlaubt, Dienstleistungen des Finanzinstitutes auf dem elektronischen Weg abzurufen. Namentlich Zahlungsaufträge lassen sich heutzutage unabhängig vom Standort und von der Uhrzeit auf diesem Weg erledigen.

Als Beispiel für die zunehmende Bedeutung des E-Banking kann wiederum das Finanzinstitut der Schweizerischen Post aufgeführt werden. Per 31.12.2006 wurden bei PostFinance 3'154'000 Kundenkonten geführt. Ebenfalls am gleichen Stichtag waren bei

¹ Die Schweizerische Post, PostFinance, Pressemitteilung vom 06.02.2007

PostFinance rund 761'000 Benutzer des „yellownet“ – der E-Banking-Plattform der Schweizerischen Post – angemeldet. Dies entspricht einer Zunahme von knapp 89'000 Personen gegenüber dem Vorjahr.²

Diese Masterarbeit konzentriert sich auf die Strafbarkeit spezifischer Deliktsformen im Bereich des E-Banking und beim Kartengeld: Phishing und Skimming.

1.1 Delikte im E-Banking

Das Internet ist ein vollwertiger virtueller Handelsplatz. Es kann praktisch alles gekauft, verkauft und gehandelt werden. Zudem können praktisch sämtliche Finanztransaktionen „online“ getätigt werden.

Aufgrund der immensen Möglichkeiten ist das Internet auch zum Tummelplatz für Kriminelle geworden. Gerade das Phishing stellt eine der aktuellsten und akutesten Deliktsformen dar. Alleine im Dezember 2006 wurden weltweit 28'532 Phishing-Seiten gemeldet.³ Phishing-Seiten sind Internetseiten, welche den echten Homepages von betroffenen Unternehmen zum Verwechseln ähnlich sehen und haben das Ziel, Kunden dieser Unternehmen zu täuschen und zur Eingabe vertraulicher Daten (z.B. Passwörter etc.) zu verleiten, welche anschliessend für kriminelle Zwecke verwendet werden können.

Im Jahr 2006 wurden rund 35 % aller festgestellten Phishing-Seiten von Internet-Providern mit Sitz in den USA gehostet⁴, gefolgt von China (7.2 %), Deutschland (6.58 %), Russland (2.9 %), Frankreich (2.7 %), Grossbritannien (2.4 %), Kanada (2.3 %) und diversen weiteren Staaten. In der Schweiz befanden sich lediglich 0.58 % der fraglichen Internetseiten.⁵

Das E-Banking ist das Hauptangriffsziel des Phishing. Alleine im Dezember 2006 hatten 89.7 % der weltweit erfassten Phishing-Attacken den Finanzsektor als Ziel.⁶ Gemäss der britischen IT-Sicherheitsfirma „MessageLabs“ war jedes 93. e-mail, welches im Januar 2007 weltweit versendet wurde, ein Phishing-e-mail.⁷ Über den finanziellen Schaden, den Phishing verursacht liegen keine Angaben vor. Dennoch ist davon auszugehen, dass zumindest das Schadensrisiko erheblich sein muss.

1.2 Delikte beim Kartengeld

² Die Schweizerische Post, PostFinance, Pressemitteilung vom 06.02.2007

³ www.antiphishing.org, Report for December 2006

⁴ Hosting in dieser Arbeit bedeutet, dass ein Internet-Provider jemanden den Zugang zum Internet - z.B. für dessen Internetseite - zur Verfügung stellt, siehe dazu KRONENBERG Friedrich, Internet – das Taschenbuch, Seite 749

⁵ www.antiphishing.org, Phishing and Crimeware Map, 05.01.2007

⁶ www.antiphishing.org, Report for December 2006

⁷ www.heute-online.ch, 06.02.2007

In der Schweiz und im umliegenden Ausland verfügt praktisch jede erwachsene Person mindestens über eine Debit- und Kreditkarte. Der mit diesen Karten generierte Umsatz ist beträchtlich und damit einhergehend auch das Deliktpotential.

Im Jahr 2005 entstand alleine in Deutschland bei ausgewählten Kreditkarten (Master-Card und Visa) ein Schaden in der Höhe von 43 Millionen EUR aus deliktischen Handlungen. Bei den Maestro-Karten (Debitkarten) in Deutschland waren es im gleichen Zeitraum rund 30 Millionen EUR. Während bei den Kreditkarten als häufigste Deliktsform das Kopieren angegeben wird (rund 64 % der 2005 verzeichneten Fälle), verhält es sich bei den Angaben zu den Debitkarten gerade umgekehrt (rund 34 % Karten-Kopien und 66 % Karten-Diebstähle etc.).⁸ Dieser Unterschied lässt sich hauptsächlich damit erklären, dass eine kopierte Kreditkarte einfacher einsetzbar ist als eine kopierte Debitkarte.

Solange der rechtmässige Kreditkartenbesitzer nicht bemerkt hat, dass seine Kreditkarte kopiert wurde, kann die Täterschaft die kopierten Daten ohne weitere Sicherheitsmerkmale auf einer anderen Kreditkarte verwenden. Sie kann problemlos im Internet Einkäufe tätigen oder die Karte zur direkten Bezahlung einsetzen. Die diesbezügliche, je nach Situation noch abzugebende Unterschrift stellt kein wesentliches Hindernis dar, weil sie vor Ort bei einer kopierten Karte nicht überprüft werden kann, respektive die Täterschaft selber die gewünschte Unterschrift auf der kopierten Karte zu Vergleichszwecken anbringen kann.

Bei den Debitkarten hingegen ist bei jeder Transaktion auch die Eingabe einer persönlichen Identifikationsnummer (sog. PIN-Code) notwendig. Eine Täterschaft muss also unbemerkt die Kartendaten kopieren und gleichzeitig den PIN-Code ausfindig machen um anschliessend Nutzen daraus ziehen zu können. Dies stellt bereits eine grössere Herausforderung dar. Weshalb es in diesem Zusammenhang häufiger noch zu Diebstählen ganzer Geldbörsen inklusive Debitkarten kommt. Vielfach findet die Täterschaft beim Durchsuchen der entwendeten Ware entsprechende Hinweise, welche auf einen PIN-Code schliessen lassen und setzt dann die Debitkarte ein, bis diese vom Geschädigten gesperrt wird.

2 Phishing

2.1 Begriff und Vorgehensweise

Der Begriff Phishing setzt sich aus den englischen Wörtern „Password“, „Harvesting“ und „Fishing“ zusammen.⁹ Frei übersetzt bedeuten dies in etwa nach Passwörter suchen (fischen) und diese einsammeln. Konkret gemeint ist damit, dass mittels Phishing versucht wird an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen.

In den am häufigsten vorkommenden Varianten des Phishing schickt die Täterschaft dem potentiellen Opfer offiziell wirkende e-mails, die es verleiten sollen, vertrauliche

⁸ SCHNEIDER Margit, Referat vom 20.09.2006 an der Konferenz „kartensicherheit.de“ in D-Frankfurt

⁹ Bundesamt für Polizei; Melde- und Analysestelle Informationssicherung, Halbjahresbericht 2006/1; Kapitel 10 Glossar, S. 31

Informationen im Bezug auf seine E-Banking-Zugänge (Passwörter, PIN-Code, weitere Sicherheitsmerkmale) zu offenbaren. Nebst dem Zusenden von e-mails besteht auch noch die Möglichkeit, das potentielle Opfer auszuspionieren, es telefonisch zu kontaktieren und sich als Vertreter seines Finanzinstitutes oder ähnliches auszugeben um so an die gewünschten Angaben zu gelangen. Ist der Täter erst einmal im Besitze der notwendigen Informationen, veranlasst er ab dem Konto seines Opfers unrechtmässige Überweisungen oder Auszahlungen zu seinen Gunsten. Bis der Geschädigte die Belastungen auf dem Konto feststellt ist es meistens schon zu spät und von Täter und Geld fehlt jede Spur.

In dieser Arbeit wird die verbreitetste Variante, das Zusenden von Phishing-e-mails und das anschliessende Auslösen unrechtmässiger Transaktionen mittels E-Banking, näher betrachtet.

Phishing-e-mails werden entweder auf gut Glück massenweise an x-beliebige e-mail-Adressen gesendet (vergleichbar mit SPAM-e-mails¹⁰) oder gezielt an vorgängig ausfindig gemachte e-mail-Adressen von Kunden eines bestimmten Finanzinstitutes. Beim betroffenen Kunden erwecken diese e-mails einen authentischen Eindruck. Die primär ersichtlichen Absenderangaben als auch die in den e-mails verwendeten Logos entsprechen normalerweise denjenigen des Finanzinstitutes des Kontoinhabers.

Im e-mail selber wird der Kunde aufgefordert seine Passwörter und die weiteren Sicherheitsmerkmale zur Prüfung auf einer Internetseite seines Finanzinstitutes einzugeben. Ein spezifischer Link¹¹ im e-mail führt den Kunden direkt zur erwähnten Internetseite. Als Grund für diese Aufforderung werden oftmals Sicherheitsprobleme oder ähnliches angegeben.

Folgt der Kunde dem angegebenen Link kommt er zu einer Internetseite, die vom Erscheinungsbild her ähnlich oder gleich derjenigen seines Finanzinstitutes ist. Als nächstes wird dann von ihm verlangt, dass er in der richtigen Reihenfolge Passwörter, PIN-Codes und die weiteren Sicherheitsmerkmale für seine E-Banking-Applikation eingibt.

Die eingegebenen Informationen stehen dabei umgehend dem Phisher zur Verfügung. Mit diesen Daten loggt¹² er sich ins E-Banking-System des betreffenden Finanzinstitutes ein und löst im Namen des Kontoinhabers entsprechende Transaktionen zu seinen Gunsten aus. Bevor der Betroffene oder das Finanzinstitut etwas davon bemerken sind die Gelder bereits überwiesen und abgehoben. In der Regel erfolgen die Überweisungen ins Ausland, entweder auf ein ausländisches Bankkonto oder werden gar per Western Union direkt bar ausbezahlt.

¹⁰ Massenweises Zusenden von e-mails an beliebige e-mail-Adressen mit unnützem Inhalt, siehe dazu: KRONENBERG Friedrich, Internet – das Taschenbuch; Seite 557

¹¹ Ein Verweis (Pfad), welcher automatisch auf eine andere Internetseite führt; siehe dazu KRONENBERG Friedrich, Internet – das Taschenbuch; Seite 751

¹² Einloggen ist ein Vorgang, den man beim Anmelden bei einem Computer im Internet durchläuft. Hierbei muss der Benutzername, das Passwort und eventuell weitere Sicherheitsmerkmale angegeben werden, siehe dazu KRONENBERG Friedrich, Internet – das Taschenbuch; Seite 747

Bisher sind keine bedeutenden Phishing-Seiten bekannt, welche von Schweizer Providern gehostet werden. Im Regelfall befinden sich die Provider mit den diesbezüglichen Internetseiten im Ausland (v.a. USA und Russland).

2.2 Strafrechtliche Würdigung

In den nachfolgenden Unterkapiteln wird der Frage nachgegangen, welche Straftatbestände durch den Versand von Phishing-e-mails zum Erhalt vertraulicher Daten und deren anschliessende Verwendung zum Zwecke der unrechtmässigen Bereicherung offensichtlich erfüllt sind.

Im Rahmen der strafrechtlichen Würdigung des Phishing sind also zwei wesentliche Tathandlungen zu betrachten:

- Der Versand von Phishing-e-mails zum Erhalt der vertraulichen Daten.
- Die Verwendung dieser vertraulichen Daten zur unrechtmässigen Bereicherung.

2.2.1 Veruntreuung – Art. 138 StGB

Eine Veruntreuung gemäss Art. 138 StGB begeht, wer sich ihm anvertraute bewegliche Sachen oder Vermögenswerte unrechtmässig zu seinem oder eines anderen Nutzen verwendet.

Anvertraut ist dabei die Sache oder der Vermögenswert, welche oder welcher explizit dem Täter übergeben oder überlassen worden ist um in einer bestimmten Weise damit zu verfahren.¹³ Da der Täter im Phishing-e-mail über seine wahre Identität täuscht und das Opfer in Wirklichkeit glaubt, dem Finanzinstitut seine vertraulichen Daten preiszugeben, sind ihm diese Daten offensichtlich nicht anvertraut. Überdies handelt es sich bei den offengelegten Daten weder um bewegliche Sachen noch um Vermögenswerte im Sinne von Art. 138 StGB (siehe dazu auch die nachfolgenden Ausführungen unter Kapitel 2.2.2 und 2.2.3).

Für die Erfüllung des Veruntreuungstatbestandes genügt es zudem nicht, wenn der Täter lediglich Zutritt zum Tatobjekt erhält, weil er zum Beispiel den Schlüssel zu seinem Aufbewahrungsort in seinen Händen hält.¹⁴ Auch wenn nun der Täter durch das Phishing im Besitze der notwendigen Zugangsdaten für das E-Banking des Opfers ist, er somit den „Schlüssel“ zu dessen Vermögenswerten erhält, sind ihm diese Vermögenswerte vom Opfer trotzdem nicht anvertraut.

Somit erfüllt das Phishing den Tatbestand der Veruntreuung offensichtlich nicht.

2.2.2 Diebstahl – Art. 139 StGB

¹³ STRATENWERTH Günter; Schweiz. Strafgesetzbuch – Besonderer Teil I; § 13 N 49

¹⁴ STRATENWERTH Günter; Schweiz. Strafgesetzbuch – Besonderer Teil I; § 13 N 52

Wer jemanden eine fremde bewegliche Sache zur Aneignung wegnimmt, um sich oder einen anderen damit unrechtmässig zu bereichern, macht sich des Diebstahls nach Art. 139 StGB schuldig.

Als Tatobjekt kommen dabei nur fremde, bewegliche Sachen in Frage. Als eigentliche Sache gelten nur körperliche Gegenstände, nicht Rechte, Forderungen oder Buchgeld.¹⁵ Zudem erfordert der Tatbestand des Diebstahls die Wegnahme dieser Sache. Dies bedeutet den Bruch fremden und Begründung neuen Gewahrsams.¹⁶

Alleine schon aufgrund der Definition des Tatobjektes lässt sich das Phishing nicht unter den Tatbestand des Diebstahls subsumieren. Bei den durch die e-mails erlangten Daten als auch bei der Überweisung von Geldern handelt es sich nicht um körperliche Gegenstände im Sinne von Art. 139 StGB. Analoges gilt im Übrigen auch für den Auffangtatbestand der unrechtmässigen Aneignung nach Art. 137 StGB.

Der Erhalt der Daten und deren nachfolgende Verwendung zur Vornahme unrechtmässiger Transaktionen stellt auch keine Wegnahme im Sinne von Art. 139 StGB dar, da Sinn und Zweck des Phishing-e-mails es ja gerade ist, das potentielle Opfer dazu zu verleiten, die Daten freiwillig herauszugeben. Daher kommt Diebstahl beim Phishing eindeutig nicht in Frage.

2.2.3 Unbefugte Datenbeschaffung – Art. 143 StGB

Nach Art. 143 StGB macht sich derjenige strafbar, der sich oder einem anderen in unrechtmässiger Bereicherungsabsicht elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, welche nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind.

Als Daten im Sinne von Art. 143 StGB gelten alle Notate, die überhaupt Gegenstand menschlicher Kommunikation sein können.¹⁷ Also alle Informationen, die von einer Datenverarbeitungsanlage verarbeitet, gespeichert oder übermittelt werden können, ab dem Moment, in dem sie von der visuell erkennbaren in die codierte Form überführt werden, über alle Verarbeitungs- und Übermittlungsstadien hin bis zur Rückführung in die visuell erkennbare Form.¹⁸

Gestützt auf diese Definition fallen sämtliche Zugangsinformationen für das E-Banking, wie Passwort, PIN-Code und die weiteren Sicherheitsmerkmale sowie die im E-Banking ersichtlichen Informationen wie Kunden- und Kontenangaben unter den Datenbegriff gemäss Art. 143 StGB.

Um den Tatbestand zu erfüllen, müssen die Daten nicht für den Täter bestimmt sein, d.h. der Täter muss unbefugt über die Daten verfügen. Hierbei ist entscheidend, ob nach dem Willen des Datenherren (respektive des Datenberechtigten), die Daten dem Täter für seine Zwecke zur Verfügung stehen sollen oder nicht.¹⁹ Beim Phishing sind die ver-

¹⁵ STRATENWERTH Günter; Schweiz. Strafgesetzbuch – Besonderer Teil I; § 13 N 5

¹⁶ BSK StGB II – NIGGLI Marcel Alexander/RIEDO Christof; Art. 139 Ziff. 1 N 11

¹⁷ STRATENWERTH Günter; Schweiz. Strafgesetzbuch – Besonderer Teil I; § 14 N 24

¹⁸ SCHMID Niklaus; Computer- sowie Check- und Kreditkarten-Kriminalität; § 2 N 25

¹⁹ SCHMID Niklaus; Computer- sowie Check- und Kreditkarten-Kriminalität; § 4 N 25

wendeten Daten – sowohl die Zugangsinformationen als auch die Kunden- und Kontodaten des E-Banking-Portals - nicht für den Täter bestimmt, weshalb auch dieses Tatbestandsmerkmal erfüllt ist.

Ferner müssen die Daten gegen den unbefugten Zugriff besonders gesichert sein. Hier gilt es zwischen den Daten des eigentlichen E-Banking-Kunden und den Daten des Finanzinstitutes zu unterscheiden. An die Sicherung von Kundendaten einer Bank sind höhere Massstäbe zu setzen als an die Sicherung privater Daten beispielsweise auf einem persönlichen Notebook.²⁰ Da die E-Banking-Portale in der Schweiz mit Passwort, PIN-Code und weiteren Sicherheitsmerkmalen besonders geschützt sind, würde ein Angriff auf diese Daten das entsprechende Tatbestandselement sicherlich erfüllen. An den Kunden – als eigentlich datenberechtigte Person – werden nicht die gleich hohen Anforderungen bezüglich dem besonderen Schutz seiner Daten gestellt. Womit also der Kunde bereits durch Aufbewahrung der Daten in einer verschlossenen Schublade oder in einem mit Passwort geschützten PC die Anforderung ebenfalls erfüllt.

Als letzter wesentlicher Punkt muss sich der Täter gemäss Wortlaut von Art. 143 StGB die Daten aktiv beschaffen. Dies wäre dann vorstellbar, wenn er die Zugriffsschranken überwinden oder umgehen und sich die Daten dadurch unrechtmässig beschaffen kann.²¹

Die Tathandlung des Beschaffens bedeutet, dass der Täter für sich oder einen andern unmittelbar die Verfügungsmacht über die Daten, die aus dem Datenbestand eines andern stammen, erlangt. Beschafft hat er sich die Daten, wenn er oder der Dritte selbst physisch über die Daten verfügt, d.h. wenn er sie also ausserhalb der Datenverarbeitungsanlage, des Datenträgers oder der Datenübermittlungseinrichtung des Berechtigten, aus der sie stammen, für seine Zwecke einsetzen kann. Nicht erforderlich für die Vollendung des Straftatbestandes ist, dass er sie tatsächlich für seine Zwecke einsetzt.²²

Art. 143 StGB wurde den Aneignungstatbeständen nachempfunden. Somit lassen sich unter den Begriff der Datenbeschaffung nur entsprechende Verhaltensweisen subsumieren, welche in Symmetrie zu diesen – namentlich zum Diebstahlstatbestand – liegen. Wo diese Symmetrie fehlt, kann nicht von einem Beschaffen im Sinne von Art. 143 StGB gesprochen werden.²³

In subjektiver Hinsicht wird ein vorsätzliches Handeln in unrechtmässiger Bereicherungsabsicht verlangt. Dies trifft beim Phishing auf jeden Fall zu.

Lässt sich also das potentielle Opfer von einem Phishing-e-mail täuschen und leitet dem Täter seine – ansonsten – besonders geschützten Zugangsdaten weiter, kann nach dem Gesagten zwar von einer erfolgreichen Beschaffung durch den Täter gesprochen werden. Gleichwohl ist der Tatbestand von Art. 143 StGB für den ersten Teil des Phishing nicht erfüllt, da nicht der Täter sich selber aktiv mittels Überwindung der besonderen Sicherung die Daten beschafft hat, sondern ihm diese durch einen Irrtum über den wahren Empfänger vom Opfer freiwillig zur Verfügung gestellt werden.

²⁰ BSK StGB II – WEISSENBERGER Philippe; Art. 143 N 12

²¹ BSK StGB II – WEISSENBERGER Philippe; Art. 143 N 15

²² SCHMID Niklaus; Computer- sowie Check- und Kreditkarten-Kriminalität; § 4 N 41

²³ SCHMID Niklaus; Computer- sowie Check- und Kreditkarten-Kriminalität; § 4 N 56

Es fehlt somit in diesem Fall an der vorgängig erwähnten Symmetrie zum Diebstahlstatbestand. Der Täter hatte nicht selber spezifischen Mechanismen oder Sicherheitssysteme, welche die Zugangsdaten schützen, zu überwinden.²⁴ Näher liegt in diesem Fall der Vergleich zum Betrugstatbestand, wo der Täter durch arglistige Täuschung sein Ziel erreicht (mehr dazu im Kapitel 2.2.5).

Im ersten Teil des Phishing ist somit der Tatbestand der unbefugten Datenbeschaffung nicht erfüllt.

Die auf diese Weise erhaltenen Daten setzt der Täter dann im zweiten Teil des Phishing ein, um auf das E-Banking-Portal Zugriff nehmen zu können. Da er nun im Besitze der Zugangsinformationen ist, gelingt es ihm im Rahmen der weiteren Tathandlungen das Sicherheitssystem des Finanzinstitutes aktiv zu überwinden und an die Kontodaten zu gelangen.

Fraglich ist, ob der erfolgreiche Zugriff auf das E-Banking-Portal und somit auf sämtliche entsprechenden Kontodaten des Kunden den Tatbestand von Art. 143 StGB erfüllt. Der Täter greift zwar gegen den Willen des Verfügungsberechtigten auf das – als besonders gesichert geltende - E-Banking-Portal und auf die dort vorhandenen Kunden- und Kontodaten zu und verwendet diese Daten für seine Transaktionen. Wenn er dabei aber die Daten weder kopiert noch ausdruckt, sondern sie nur für seine Zwecke benützt, ohne dass er sie in seinen eigenen Datenbestand überführt, handelt er nicht tatbestandsmässig im Sinne von Art. 143 StGB.²⁵

Der Täter erfüllt also den Tatbestand von Art. 143 StGB beim zweiten Teil des Phishing nur, wenn er die Daten nicht nur benutzt, sondern auch kopiert oder zumindest ausdruckt. Separat geprüft wird die Konkurrenzfrage zu anderen in Frage kommenden Straftatbeständen unter Kapitel 2.2.10.

2.2.4 Unbefugtes Eindringen in ein Datenverarbeitungssystem – Art. 143^{bis} StGB

Gemäss Art. 143^{bis} StGB wird auf Antrag bestraft, wer unbefugterweise – ohne Bereicherungsabsicht - auf dem Wege von Datenübertragungseinrichtungen in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt.

Als Datenverarbeitungssysteme gelten technische Einrichtungen, über welche Informationen in nicht direkt lesbarer, üblicherweise kodierten Form entgegengenommen, automatisiert bearbeitet und wieder abgegeben werden. Dies kann eine mit dem Internet verbundene Rechneranlage, aber auch ein einzelner PC sein, wenn deren Verwendung beispielsweise durch ein Passwort gesichert ist.²⁶

Weiter muss das Datenverarbeitungssystem für den Täter fremd sein. Unter Fremdheit ist hier die fehlende Zugangsberechtigung zum System zu verstehen.²⁷ Ebenfalls hat das Datenverarbeitungssystem gegen den unberechtigten Zugriff besonders gesichert zu

²⁴ AMMANN Matthias; Sind Phishing-Mails strafbar?; AJP 2006 S. 195 ff.

²⁵ SCHMID Niklaus; Computer- sowie Check- und Kreditkarten-Kriminalität; § 4 N 60

²⁶ BSK StGB II – WEISSENBERGER Philippe; Art. 143^{bis} N 5

²⁷ BSK StGB II – WEISSENBERGER Philippe; Art. 143^{bis} N 6

sein. Als Sicherheitsmassnahmen sind hier lediglich elektronische Massnahmen – wie Passwörter, PIN-Codes, Verschlüsselungssoftware etc. – zu verstehen. Entgegen dem vorgängig behandelten Tatbestand der unbefugten Datenbeschaffung genügt es bei Art. 143^{bis} StGB nicht, wenn zum Beispiel das Datenverarbeitungssystem in einem verschlossenen Raum steht, aber über keinen elektronischen Zugangsschutz verfügt. Dies ergibt sich aus der Formulierung „auf dem Wege von Datenübertragungseinrichtungen“.²⁸

Konkret ist damit gemeint, dass der Täter über einen drahtverbundenen (z.B. Telefonnetz) oder auch drahtlosen (z.B. UMTS) Kanal die Zugangsschranken aktiv überwinden muss um den Tatbestand erfüllen zu können.²⁹ Ferner muss unbefugt in das Datenverarbeitungssystem eingedrungen werden. Dies bedeutet, dass der Täter gegen den Willen des Verfügungsberechtigten handeln muss.³⁰

Phishing-e-mails – wie alle e-mails – werden mittels Datenverarbeitungssystem versendet und auf einem fremden – demjenigen des potentiellen Opfers – Datenverarbeitungssystem empfangen. Analog zum bereits unter Kapitel 2.2.3 erwähnten, überwindet der Täter dadurch jedoch nicht aktiv elektronische Zugangsschranken. Er benutzt lediglich das e-mail als Kommunikationsmedium um sein potentielles Opfer zu täuschen und ihn so dazu zu bringen, von sich aus die benötigten Zugangsinformationen bekannt zu geben. Der Versand von Phishing-e-mails und die beabsichtigte Reaktion des Empfängers erfüllen demnach den objektiven Tatbestand von Art. 143^{bis} nicht.

Es ist noch zu prüfen, ob der Tatbestand allenfalls dadurch erfüllt sein könnte, dass sich der Täter mit den „gephisheten“ Informationen anschliessend Zugang zum E-Banking-Portal seines Opfers verschafft. Aus Sicht des Täters handelt es sich beim E-Banking-System um ein fremdes Datenverarbeitungssystem, für welches ihm die Zugriffsberechtigung fehlt. Da er gegen den Willen des Verfügungsberechtigten auf das E-Banking-Portal - welches als besonders gesichert bezeichnet werden kann - zugreift, ist sein Eindringen auch als unbefugt einzustufen.³¹ Somit handelt es sich hierbei objektiv um ein unbefugtes Eindringen in eine Datenverarbeitungsanlage im Sinne von Art. 143^{bis} StGB.

Das Ziel der Phishing-Attacke ist jeweils der Zugriff auf die Vermögenswerte des Opfers, der Täter handelt also stets in Bereicherungsabsicht. Da jedoch der subjektive Tatbestand des unbefugten Eindringens in eine Datenverarbeitungsanlage ausdrücklich ein Handeln ohne Bereicherungsabsicht verlangt, ist aus diesem Grund der Art. 143^{bis} StGB auch für den zweiten Teil des Phishing nicht gegeben.

2.2.5 Betrug – Art. 146 StGB

Wer in der Absicht sich oder einen anderen unrechtmässig zu bereichern, jemanden durch Vorspielung oder Unterdrückung von Tatsachen arglistig irreführt oder ihn in einem Irrtum arglistig bestärkt und so den Irrenden zu einem Verhalten bestimmt, wodurch dieser sich selbst oder einen anderen am Vermögen schädigt, macht sich des Betrugs nach Art. 146 StGB schuldig.

²⁸ BSK StGB II – WEISSENBERGER Philippe; Art. 143^{bis} N 8

²⁹ SCHMID Niklaus; Computer- sowie Check- und Kreditkarten-Kriminalität; § 5 N 21

³⁰ STRATENWERTH Günter; Schweiz. Strafgesetzbuch – Besonderer Teil I; § 14 N 39

³¹ AMMANN Matthias; Sind Phishing-Mails strafbar?; AJP 2006 S. 195 ff

Der Betrug zeichnet sich dadurch aus, dass das Opfer durch die motivierende Einwirkung des Täters dazu veranlasst wird, sich selbst (bzw. seiner Verfügung unterliegendes Vermögen) zu schädigen.³² Der objektive Tatbestand kann somit in vier Elemente³³ aufgeteilt werden:

- Das motivierende Verhalten, das im Normalfall eine Täuschung ist, aber nicht zu sein braucht;
- als Erfolg dieses Verhaltens die Setzung eines Motivs beim anderen, das auf einem Irrtum beruhen muss;
- eine dadurch motivierte Vermögensverfügung des anderen, und endlich
- einen durch die Verfügung herbeigeführten Vermögensschaden.

Beim Phishing bezieht sich das motivierende Verhalten des Täters auf die Täuschung des Opfers mittels Zusendung einer e-mail des vermeintlichen Finanzinstitutes und der ebenfalls vom vermeintlichen Finanzinstitut stammenden Internetseite, auf welche das Opfer per Link im e-mail gelangt und zur Eingabe der Zugangsinformationen für das E-Banking verleitet wird.

Die für die Täuschung notwendige arglistige Irreführung wird dadurch erreicht, dass sowohl e-mail als auch Internetseite hinsichtlich Erscheinungsform und Inhalt den Anschein erwecken, wirklich vom betreffenden Finanzinstitut zu stammen.

Eine erfolgreiche Täuschung ruft beim Opfer einen Irrtum bezüglich Empfänger und Sinn und Zweck der Eingabe der vertraulichen Zugangsinformationen hervor. Basierend auf diesem Irrtum liefert das Opfer dem Phisher sämtliche notwendigen Zugangsinformationen für das E-Banking, wodurch der Täter Zugriff auf die entsprechenden Vermögenswerte seines Opfers erhält und sich unrechtmässig bereichern kann.

Während durch diese Vorgehensweise die Tatbestandselemente der Täuschung und des darauf beruhenden Irrtums des Geschädigten erfüllt werden und im Normalfall auch ein Schaden aufgrund der Vermögensdisposition eintritt, ist das Erfordernis der direkt auf dem Irrtum basierenden Vermögensdisposition durch den Geschädigten nicht gegeben.

Namentlich wird die Vermögensdisposition beim Phishing nicht vom Opfer selber erbracht. Sie ist deshalb auch nicht direkt auf seinen Irrtum zurückzuführen, da das Opfer durch seinen Irrtum und die Preisgabe der entsprechenden Zugangsdaten dem Täter nur den Einstieg ins E-Banking-System ermöglicht. Die Vermögensverschiebung wird schlussendlich vom Täter selbst veranlasst.

Es kann noch die Meinung vertreten werden, dass bereits das Erlangen der vertraulichen Zugangsinformationen durch die arglistige Täuschung der Phisher als Vermögensdisposition des Opfers zu werten ist, da diese Daten mit grösstmöglicher Wahrscheinlichkeit im Anschluss daran zu dessen Schaden genutzt werden. Diese Auslegung ist jedoch zu verneinen, da das Risiko, respektive die Wahrscheinlichkeit, dass die Täterschaft die ihr überlassenen Zugangsdaten zum Schaden des Opfers verwenden wird, noch keinen rechtlich relevanten Vermögensschaden darstellt. Ein solcher Vermögensschaden tritt

³² STRATENWERTH Günter; Schweiz. Strafgesetzbuch – Besonderer Teil I; § 15 N 4

³³ BGE 101 IV 117

erst dann ein, wenn die Täterschaft in einer weiteren – selbständigen – Handlung, die Zugangsdaten im E-Banking-System zur Auslösung von Transaktionen einsetzt. Diese Auslegung wird sinngemäss in der Rechtspraxis im Verhältnis von Art. 146 zu Art. 148 StGB angewendet und ist m.E. ebenfalls in der Konstellation des Phishing anzuwenden.³⁴

Zu prüfen bleibt, ob durch diese Vorgehensweise allenfalls ein Betrug gegenüber dem Finanzinstitut vorliegen könnte. Bei der unrechtmässigen Verwendung der Zugangsinformationen für das E-Banking täuscht der Täter nämlich die Identität des Kunden vor, welche ihm ermöglicht, auf diese Weise die entsprechenden Vermögensdispositionen im Auftrag zu geben. Dennoch ist Art. 146 StGB nicht anwendbar, da der traditionelle Tatbestand des Betruges vom Bild des Opfers ausgeht, welches durch Täuschung dazu bewogen wird, sich selbst zu schädigen. Das E-Banking-System eines Finanzinstitutes – als Datenverarbeitungssystem – kann man jedoch in diesem Sinne nicht täuschen.³⁵ Die unrechtmässige Vermögensverschiebung beruht somit nicht auf einem vom Täter hervorgerufenen Irrtum bei einem menschlichen Opfer, sondern wird mittels Manipulation einer Datenverarbeitungsanlage bewirkt.³⁶

Folglich kann nicht von einem Betrug im Sinne von Art. 146 StGB gesprochen werden. Der Straftatbestand von Art. 146 StGB ist damit nicht für das Phishing anwendbar.

2.2.6 Betrügerischer Missbrauch einer Datenverarbeitungsanlage – Art. 147 StGB

Laut Art. 147 StGB macht sich strafbar, wer in der Absicht sich oder einen anderen unrechtmässig zu bereichern, durch unrichtige, unvollständige oder unbefugte Verwendung von Daten oder in vergleichbarer Weise auf einen elektronischen oder vergleichbaren Datenverarbeitungs- oder Datenübermittlungsvorgang einwirkt und dadurch eine Vermögensverschiebung zum Schaden eines anderen herbeiführt oder eine Vermögensverschiebung unmittelbar danach verdeckt.

Der Tatbestand des betrügerischen Missbrauchs einer Datenverarbeitungsanlage wurde weitgehend dem Tatbestand des Betruges nachempfunden. Im Hinblick auf Art. 146 StGB kommt dem auch als Computerbetrug bezeichneten Art. 147 StGB lediglich subsidiärer Charakter zu.³⁷

Als für die Deliktsform des Phishing primär relevante Tathandlung ist die unrichtige, unvollständige oder unbefugte Verwendung von Daten analog der arglistigen Täuschung beim Betrug anzusehen. Die Verwendung dieser Daten im Rahmen eines Datenverarbeitungs- oder Datenübermittlungsvorganges hat zum Ziel, dass der eigentliche Akt der Datenverarbeitung oder –übermittlung im Ergebnis unrichtig sein muss. Diese Handlungsweise entspricht beim Tatbestand des Betruges der Irreführung bezüglich dem wahren Sachverhalt.³⁸ Die daraus folgende Vermögensverschiebung entspricht der Vermögensverfügung beim Betrug. Dies bedeutet, dass die Vermögensverschiebung wiederum direkt kausal zum Datenverarbeitungs- oder

³⁴ BGE 127 IV 68

³⁵ STRATENWERTH Günter; Schweiz. Strafgesetzbuch – Besonderer Teil I; § 16 N 2

³⁶ SCHMID Niklaus; Computer- sowie Check- und Kreditkarten-Kriminalität; § 7 N 1

³⁷ SCHMID Niklaus; Computer- sowie Check- und Kreditkarten-Kriminalität; § 7 N 15

³⁸ STRATENWERTH Günter; Schweiz. Strafgesetzbuch – Besonderer Teil I; § 16 N 6

Datenübermittlungsvorgang stehen muss. Somit hat das betreffende Vermögen der automatisierten Datenverarbeitung oder –übermittlung zu unterliegen. Aus der Vermögensverschiebung hat direkt kausal ein entsprechender Schaden zu entstehen. Bedarf es für den Täter weiterer selbständiger Handlungen um den erstrebten Vermögensvorteil zu erlangen, so scheidet Art. 147 StGB automatisch aus. Ebenfalls analog zum Betrugstatbestand bezüglich dem Verfügenden und dem Geschädigten gilt beim Computerbetrug, dass derjenige in dessen Dienst der Computer steht und derjenige, den der Schaden trifft, nicht identisch sein müssen.³⁹

Als unrichtige Daten im Sinne von Art. 147 StGB sind Daten zu verstehen, welche im Zeitpunkt des Datenverarbeitungsvorganges in ihrem Informationsgehalt im Widerspruch zur objektiven Sach- und Rechtslage stehen.⁴⁰ Bezüglich der unbefugten Verwendung von Daten wird auf die Ausführungen in den Kapiteln 2.2.3 und 2.2.4 verwiesen.

Mittels Versand der Phishing-e-mails und der vermeintlichen Internetseite des Finanzinstitutes soll der E-Banking-Kunde getäuscht werden. Die im e-mail und auf der Internetseite verwendeten Informationen sind inhaltlich unrichtige Daten, womit ein erstes Tatbestandselement erfüllt wäre. Jedoch wird mit dem Versand der unrichtigen Daten per e-mail nicht auf einen elektronischen Datenverarbeitungs- oder Datenübermittlungsvorgang eingewirkt um automatisch eine Vermögensverschiebung auszulösen, sondern lediglich der Empfänger getäuscht.

Die im Anschluss an die erfolgreiche Täuschung und die Herausgabe der Zugangsinformationen folgende Vermögensverschiebung im E-Banking durch den Täter ist nicht direkt kausal zum Versand der unrichtigen Daten. Sie beruht auf einer weiteren, selbständigen Handlung des Täters, welcher sich mit den erhaltenen Daten im E-Banking-System einloggt und die Vermögensverschiebung auslöst.

Der Versand der Phishing-e-mails und das Sammeln der Zugangsdaten kann als Vorbereitungshandlung für den zweiten Teil des Phishing betrachtet werden. Diese Vorbereitungshandlungen fallen jedoch nicht unter Art. 260^{bis} StGB, weshalb sie straflos bleiben.

Gestützt auf die vorgängigen Erwägungen ist Art. 147 StGB für den ersten Teil des Phishing nicht anwendbar. Der erste Teil des Phishing kann auch nicht als unvollendeter Versuch von Art. 147 StGB gewertet werden, da dieser Tatbestand erst ab Beginn der Tatausführung des zweiten Teils des Phishing Relevanz entwickelt. Der Täter überschreitet die Schwelle zum Versuch erst, wenn er sich mittels Verwendung der erhaltenen Zugangsinformationen in das E-Banking-System einloggt um eine Vermögensverschiebung vorzunehmen.

Die Vorgehensweise im zweiten Teil des Phishing entspricht dem in diesem Kapitel behandelten Tatbestand wie nachfolgende Ausführungen aufzeigen.

Beim Tatbestand des Computerbetruges ist es – im Unterschied in etwa zu Art. 143 StGB – unerheblich, wie der Täter an die von ihm verwendeten Daten gekommen ist.⁴¹

³⁹ STRATENWERTH Günter; Schweiz. Strafgesetzbuch – Besonderer Teil I; § 16 N 11

⁴⁰ SCHMID Niklaus; Computer- sowie Check- und Kreditkarten-Kriminalität; § 7 N 45

⁴¹ SCHMID Niklaus; Computer- sowie Check- und Kreditkarten-Kriminalität; § 7 N 65

Zur Erfüllung des Tatbestandes ist es zu Beginn lediglich relevant, dass die verwendeten Daten unrichtig, unvollständig oder eben unbefugt verwendet werden. Wie bereits in den Kapiteln 2.2.3 und 2.2.4 ausgeführt, ist das Eindringen des Täters in das E-Banking-System mit den Zugangsinformationen des wahren Verfügungsberechtigten als unbefugte Datenverwendung zu bezeichnen.

Nachdem sich der Täter den Zugang verschafft hat, löst er im E-Banking-System einen an sich richtigen Datenverarbeitungsvorgang aus, welcher aber im Ergebnis unzutreffend ist. Konkret bedeutet dies, dass der Täter aufgrund der Verwendung der korrekten Zugangsinformationen gegenüber dem E-Banking-System als autorisiert gilt um elektronische Transaktionen auslösen zu können. Ohne die Verwendung der entsprechenden Zugangscodes könnten alleine schon systembedingt keine Datenverarbeitungsvorgänge durch den Täter im E-Banking ausgelöst werden. Die ausgelösten Transaktionen sind aber dennoch im Ergebnis unzutreffend, da dem Täter die entsprechende Befugnis des rechtmässig Berechtigten fehlt. Der Vermögensschaden als weiteres Tatbestandselement ist ebenfalls gegeben, da durch die ausgelöste Transaktion das Guthaben des Phishing-Opfers gegenüber dem Finanzinstitut reduziert wird.⁴²

Zusammenfassend kann also festgehalten werden, dass beim zweiten Teil des Phishing der Täter durch eine unbefugte Verwendung von Daten im Rahmen eines Datenverarbeitungsvorganges eine Transaktion auslöst, welche direkt zu einer Vermögensverschiebung zu seinen Gunsten und somit zu einem Schaden des Betroffenen führt. Setzt man nun noch die Bereicherungsabsicht und den Vorsatz der Täterschaft voraus, sind sämtliche Tatbestandselemente erfüllt und die Tathandlung kann unter Art. 147 StGB subsumiert werden.

Die Frage der Konkurrenzen wird im Kapitel 2.2.10 behandelt.

2.2.7 Unbefugtes Beschaffen von Personendaten – Art. 179^{novies} StGB

Gemäss Art. 179^{novies} StGB wird auf Antrag bestraft, wer unbefugt besonders schützenswerte Personendaten oder Persönlichkeitsprofile, die nicht frei zugänglich sind, aus einer Datensammlung beschafft.

Die für diesen Tatbestand wesentlichen Begriffe „besonders schützenswerte Personendaten“, „Persönlichkeitsprofile“ und „Datensammlung“ sind in Art. 3 Datenschutzgesetz (DSG) definiert. Das StGB stützt sich bezüglich diesen Tatbestandsmerkmalen auf das DSG ab.⁴³

Besonders schützenswerte Personendaten werden durch Art. 3 lit. c DSG als Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, Gesundheit, Intimsphäre oder Rassenzugehörigkeit, Massnahmen der sozialen Hilfe und administrative oder strafrechtliche Verfolgung oder Sanktionen definiert.⁴⁴ Ein Persönlichkeitsprofil ist gemäss Art. 3 lit. d DSG eine Zusammenstellung von Daten, welche eine Beurteilung wesentlicher Aspekte einer natürlichen Person erlaubt.⁴⁵

⁴² AMMANN Matthias; Sind Phishing-Mails strafbar?; AJP 2006 S. 195 ff.

⁴³ BSK StGB II – VON INS Peter/WYDER Peter-René; Art. 179^{novies} N 8

⁴⁴ BSK StGB II – VON INS Peter/WYDER Peter-René; Art. 179^{novies} N 9

⁴⁵ BSK StGB II – VON INS Peter/WYDER Peter-René; Art. 179^{novies} N 11

Gestützt auf diese Definitionen können die gehishten Zugangsinformationen für das E-Banking klar ausgeschlossen werden, da diese sich auf Passwörter, PIN-Code und weitere Sicherheitsmerkmale beschränken und weder die Anforderungen als besonders schützenswerte Personendaten noch als Persönlichkeitsprofile erfüllen. Somit erfüllt der erste Teil des Phishing den Straftatbestand von Art. 179^{novies} nicht.

Man könnte nun argumentieren, dass die im E-Banking vorhandenen Informationen über das potentielle Opfer den Begriff eines Persönlichkeitsprofils erfüllen könnten. Namentlich hat der Täter aufgrund der Zugangsinformationen volle Einsicht in gewisse Personalien und in sämtliche über das betroffene Finanzinstitut getätigte Transaktionen des Opfers. Über einen längeren Zeitraum betrachtet lassen diese Transaktionen (Höhe, Einzahler, Begünstigter, Bemerkungen etc.) allenfalls die Erstellung eines Persönlichkeitsprofils gemäss Art. 3 lit. d DSG zu.

Sinn und Zweck des Phishing ist jedoch die unrechtmässige Bereicherung. Der Täter wird sich also im E-Banking eine Übersicht über die verschiedenen Saldi und allenfalls vorhandenen Bezugslimiten auf den angeschlossenen Konten verschaffen und baldmöglichst versuchen entsprechende Transaktionen auszulösen. Die vom Täter benötigten Informationen fallen weder unter den Begriff der besonders schützenswerten Personendaten noch unter den Begriff des Persönlichkeitsprofils. Somit ist Art. 179^{novies} StGB auch nicht für den zweiten Teil des Phishing anwendbar.

2.2.8 Urkundenfälschung – Art. 251 StGB

Wer in der Absicht, jemanden am Vermögen oder an anderen Rechten zu schädigen oder sich oder einem anderen einen unrechtmässigen Vorteil zu verschaffen, eine Urkunde fälscht oder verfälscht, die echte Unterschrift oder das echte Handzeichen eines anderen zur Herstellung einer unechten Urkunde benützt oder eine rechtlich erhebliche Tatsache unrichtig beurkundet oder beurkunden lässt oder eine Urkunde dieser Art zur Täuschung gebraucht, macht sich der Urkundenfälschung im Sinne von Art. 251 StGB schuldig.

Im Zusammenhang mit dem Tatbestand der Urkundenfälschung dürfte nur der erste Teil des Phishing, also der Versand der Phishing-e-mails und der damit beabsichtigte Erhalt der Zugangsinformationen zum E-Banking, relevant sein. Dabei steht insbesondere der Begriff der Urkunde im Vordergrund.

Urkunden sind gemäss Art. 110 Ziff. 5 StGB Schriften oder Zeichen die bestimmt und geeignet sind, eine Tatsache von rechtlicher Bedeutung zu beweisen. Die Aufzeichnung auf Bild- und Datenträgern steht der Schriftform gleich, sofern sie demselben Zwecke dient.

Eine Schrift wird also dann zur Urkunde, wenn sie nebst einer menschlichen Gedankenäusserung, der Zurechenbarkeit zu einem Aussteller, der Perpetuierungsfunktion und als Beweismittel für rechtserhebliche Tatsachen genügt.

Gemäss der Rechtsprechung gelten Tatsachen dann als rechtlich erheblich, wenn sie alleine oder in Verbindung mit anderen Tatsachen die Entstehung, Veränderung, Aufhebung oder Feststellung eines Rechts bewirken, wobei auch blosser Indizien, die den

Schluss auf rechtserhebliche Tatsachen zulassen, als rechtlich erheblich eingestuft werden.⁴⁶ Grundsätzlich ist eine Schrift zur Urkunde geeignet, wenn sie nach Gesetz oder Verkehrsübung als Beweismittel anerkannt wird. Beweisfunktion bedeutet, dass die Urkunde zum Beweis geeignet und bestimmt sein muss.⁴⁷ Entscheidend ist das Vertrauen, welches das Schriftstück im Verkehr genießt.⁴⁸ Zudem muss die Schrift vom Aussteller mit dem Willen geschaffen worden sein, ein Beweismittel zu sein oder als solches zu dienen, wobei der Wille des Ausstellers darauf ausgerichtet sein muss, das Schriftstück nicht nur für den internen Gebrauch zu verwenden, sondern es objektiv erkennbar als Beweismittel im Rechtsverkehr zu schaffen und auch als solches zu verwenden.⁴⁹ Bezüglich der Beständigkeit müssen auch elektronisch aufgezeichnete Daten gewissen Anforderungen entsprechen (Perpetuierungsfunktion). Die Rechtsprechung stellt dabei darauf ab, ob die Daten durch eine mehr oder minder strikte Beschränkung des Zugangs (z.B. Legitimationskarte, Zugangscodes etc.) zu ihnen genügend gegen unbeabsichtigte Löschung oder Veränderung gesichert sind.⁵⁰

Es stellt sich nun zuerst die Frage, ob ein Phishing-e-mail als Urkunde gemäss Art. 110 Ziff. 5 StGB gelten kann oder nicht.

Das Phishing-e-mail lässt sich aufgrund der Aufmachung (z.B. Logo des Finanzinstitutes) und der Absenderdaten (z.B. E-Banking-Team oder Sicherheitsbeauftragte des Finanzinstitutes) einem vermeintlichen Aussteller zuordnen. Dieser Aussteller muss dabei nicht zwingend namentlich erwähnt werden. Der Empfänger darf dabei darauf vertrauen, dass nur spezifische Mitarbeitende seines Finanzinstitutes Zugang zum entsprechenden e-mail-Account, mit welchem das fragliche e-mail versendet wurde, haben. So hat bei einer vergleichbaren Konstellation bezüglich einem nicht namentlich erwähnten Aussteller das Bundesgericht auch entschieden, dass bei einer elektronisch geführten Bankbuchhaltung die notwendige Garantiefunktion damit begründet ist, dass aufgrund des internen Sicherheitssystems nur bestimmte Personen – nämlich die zugriffsberechtigten Bankangestellten - entsprechende Buchungen vornehmen können.⁵¹

Nachdem die Zurechenbarkeit des Ausstellers erfüllt ist, gilt es abzuklären, ob das Phishing-e-mail eine menschliche Gedankenäusserung zum Inhalt hat. Eine Gedankenäusserung, respektive Gedankenerklärung ist jede verständliche Mitteilung von Mensch zu Mensch.⁵² Im e-mail befinden sich vom Versender verfasste Informationen darüber, weshalb der Empfänger kontaktiert wird. Beispielsweise werden oftmals Sicherheitsprobleme im E-Banking als Auslöser genannt. Weiter werden dem Empfänger konkrete Handlungsanweisungen gegeben: Anwählen des im e-mail beigefügten Internetlink und Eingabe der Zugangsinformationen für das E-Banking. Bei diesen Informationen und Handlungsanweisungen handelt es sich zweifellos um menschliche Gedankenäusserungen.

⁴⁶ BGE 6P.37/2005

⁴⁷ BSK StGB I – BOOG Markus; Art. 110 Ziff. 5 N 4

⁴⁸ BSK StGB I – BOOG Markus; Art. 110 Ziff. 5 N 29

⁴⁹ BSK StGB I – BOOG Markus; Art. 110 Ziff. 5 N 31

⁵⁰ BGE 116 IV 343

⁵¹ BGE 116 IV 343

⁵² BSK StGB I – BOOG Markus; Art. 110 Ziff. 5 N 13

Das Merkmal der Beständigkeit dürfte als erfüllt gelten, weil die e-mails auf dem e-mail-Account des Empfängers empfangen und gespeichert werden. Dieser Account ist jeweils mittels Passwort vor unbefugtem Zugriff und somit auch durch unbefugte Veränderung oder Löschung geschützt.

Als weitere Voraussetzung muss das e-mail nun noch als Beweismittel für eine rechtlich erhebliche Tatsache genügen.

Im regulären Geschäftsverkehr sind heutzutage e-mails weit verbreitet. Geschäftspartner kommunizieren per e-mail schnell und einfach miteinander. Es ist üblich, dass über das Internet getätigte Bestellungen oder Einkäufe per e-mail vom Lieferanten bestätigt werden oder Aufträge bei bereits bestehenden Geschäftsbeziehungen per e-mail erteilt und bestätigt werden. Gerade auch beim E-Banking wird den Kunden nebst dem telefonischen auch ein e-mail-Support angeboten, an den sie sich jederzeit wenden können und von wo sie entsprechend weiterführende Informationen wiederum per e-mail zugesendet erhalten (beispielsweise bei der Schweizerischen Post: yellownet@postfinance.ch).

Beim Phishing-e-mail soll dem Empfänger aufgezeigt werden, dass aufgrund der Absenderangaben und dem verwendeten Logo sein E-Banking-Vertragspartner mit ihm Kontakt aufnimmt und ihm gestützt auf wichtige sicherheitsrelevante Vorkommnisse und/oder gestützt auf den E-Banking-Vertrag wesentliche Informationen und Handlungsanweisungen zukommen lässt.

Bezüglich der Beweiskraft von e-mails könnte entgegengehalten werden, dass aufgrund der zahlreichen SPAM-e-mails, welche früher oder später praktisch jeden e-mail-Account einmal treffen und zu überfluten drohen, grundsätzlich sämtlichen e-mails zu misstrauen wäre und ihnen deshalb keine Beweiseignung und –bestimmtheit zukommen kann. Dem kann jedoch entgegengehalten werden, dass praktisch alle SPAM-e-mails rasch auch als solche erkennbar sind (z.B. aufgrund des Inhaltes oder des Absenders) und somit nicht mit den im Geschäftsverkehr üblichen e-mails verglichen werden können.

Einem qualitativ schlecht erstellten Phishing-e-mail (z.B. falsche Sprache, falsches Logo etc.) dürfte effektiv keine Beweiskraft zukommen, da es wohl von der Glaubwürdigkeit her mit einem SPAM-e-mail vergleichbar ist. Obwohl es bei einer Urkunde im Grundsatz nicht auf deren Qualität ankommt, ist ein solches e-mail aufgrund seiner Einfältigkeit gar nicht in der Lage den Anschein einer Urkunde zu erwecken.⁵³

Ein glaubwürdig erstelltes Phishing-e-mail ist jedoch durchaus mit einem im Geschäftsverkehr üblichen e-mail zu vergleichen. Basierend auf diesen Erwägungen erfüllt ein solches e-mail somit auch die Beweisfunktion für eine rechtlich erhebliche Tatsache und kann somit als Urkunde im Sinne von Art. 110 Ziff. 5 StGB angesehen werden.

Mit der Erstellung eines qualitativ hochstehenden Phishing-e-mails (korrekte Sprache, korrektes Logo, korrekte Absenderangaben etc.) erfüllt der Täter zumindest einmal den objektiven Tatbestand der Urkundenfälschung gemäss Art. 251 StGB. Er täuscht den Empfänger über die eigentliche Urhebererschaft des Phishing-e-mails und stellt so eine unechte Urkunde aus.

⁵³ BSK StGB II – BOOG Markus; Art. 251 N 7

Auf der subjektiven Seite verlangt Art. 251 StGB nebst Vorsatz ein Handeln in Schädigungs- oder Vorteilsabsicht. Im Zusammenhang mit dem Phishing steht klar die Vorteilsabsicht des Täters im Vordergrund. Als unrechtmässiger Vorteil gilt dabei gemäss Rechtssprechung jede Besserstellung, wobei die Besserstellung vermögensmässiger oder sonstiger Natur sein kann.⁵⁴ Unrechtmässig ist ein Vorteil dann, wenn er rechtswidrig ist oder wenn der Täter darauf keinen Anspruch hat.⁵⁵

Stellt man sich nun auf den Standpunkt, dass aufgrund des Phishing-e-mails der Empfänger seine Zugangsinformationen zum E-Banking offen legt und diese anschliessend zur unrechtmässigen Bereicherung genutzt werden können, so ist der unrechtmässige Vorteil gegeben und somit Art. 251 StGB auch in subjektiver Hinsicht erfüllt.

Abweichend davon wird die Meinung vertreten, dass mit dem Phishing-e-mail lediglich der Empfänger mittels einem Internetlink auf eine Internetseite gelockt und dort nochmals mittels falschen Angaben getäuscht und zur Eingabe der Zugangsdaten verleitet werden soll. Unter diesem Aspekt wäre der einzige Nutzen des Phishing-e-mails, dass der Empfänger den fraglichen Internetlink anwählt. Alleine mit dieser Handlung ist jedoch nicht ersichtlich, inwiefern der Täter in vermögensrechtlicher oder sonstiger Hinsicht bessergestellt sein sollte. Es fehlt in dieser Konstellation somit am Vorteil, weshalb Art. 251 StGB in subjektiver Hinsicht nicht erfüllt wäre und somit nicht zum Tragen kommen würde.⁵⁶ In subjektiver Hinsicht würde also erst die vom Täter gefälschte Internetseite verbunden mit der daraus folgenden Offenlegung der Zugangsdaten dem Element des unrechtmässigen Vorteils genügen.

Basierend auf diese Konstellation ist somit noch zu prüfen, ob die fragliche Internetseite als Computerkurkunde gilt oder nicht. Es sind hierbei die gleichen Massstäbe wie beim e-mail anzuwenden.

Die Elemente der Zurechenbarkeit an einen Aussteller (Impressum, Logo etc.) und die menschliche Gedankenäusserung (Information und Handlungsanweisungen) sind identisch mit dem vorgängig behandelten e-mail und können somit als erfüllt angesehen werden. Ebenso ist die Beständigkeit gegeben, da die Internetseite selber – bis auf die durch das Opfer auszufüllenden Felder – schreibgeschützt ist und einzig durch den Verfügungsberechtigten gelöscht oder verändert werden kann.

Somit bleibt in objektiver Hinsicht noch die Beweismittelfunktion in Verbindung mit der rechtlich erheblichen Tatsache zu prüfen. Eine rechtliche Bedeutung im Sinne der Computerurkunde liegt nur bei relevanten Vorgängen oder Zuständen vor, die bestimmt und geeignet sind, die aufgezeichnete Tatsache zu beweisen. Es muss sich also um Daten handeln, die dazu bestimmt sind bei einer Verarbeitung im Rechtsverkehr als Beweisdaten benutzt zu werden.⁵⁷ Hierfür in Frage kommen vorab Daten im Zusammenhang mit kaufmännischer Buchführung sowie Daten zur Abwicklung wirtschaftlicher Transaktionen im Bereich von Banken und ähnlichen Institutionen.⁵⁸

⁵⁴ BSK StGB II – BOOG Markus; Art. 251 N 93

⁵⁵ BSK StGB II – BOOG Markus; Art. 251 N 95

⁵⁶ AMMANN Matthias; Sind Phishing-Mails strafbar?; AJP 2006 S. 195 ff.

⁵⁷ SCHMID Niklaus; Computer- sowie Check- und Kreditkarten-Kriminalität; § 3 N 68

⁵⁸ SCHMID Niklaus; Computer- sowie Check- und Kreditkarten-Kriminalität; § 3 N 71

Es ist davon auszugehen, dass das potentielle Opfer gestützt auf das erhaltene e-mail direkt auf die fragliche Internetseite gelangt. Die Internetseite ist im Hinblick auf Layout und Vorgehensweise zum Einloggen identisch mit dem üblicherweise genutzten E-Banking-System. Ebenso entsprechen die Eingabeaufforderungen in ihrer Art der normalerweise beim E-Banking verwendeten Autorisierung als Verfügungsberechtigter.

Der E-Banking-Kunde muss somit davon ausgehen, dass die Internetseite seinem Finanzinstitut zugeordnet werden muss. Da diese Internetseite, respektive der darin aufgeführte Inhalt aber nicht dem Willen des E-Banking-Institutes entspricht und die Internetseite nur vorgibt vom betreffenden Finanzinstitut zu stammen, liegt eine unechte Erklärung vor. In Analogie der Schrifturkunde kann in diesem Fall von einem der Blankettfälschung angenäherten Sachverhalt gesprochen werden.⁵⁹

Basierend auf diesen Ausführungen kann die von der Täterschaft beim Phishing erstellte Internetseite zur Erlangung der Zugangsinformationen unter den Tatbestand der Urkundenfälschung nach Art. 251 StGB subsumiert werden, sofern sie – analog zum Phishing-e-mail – in objektiver Hinsicht von genügender Qualität ist um die Beweisfunktion einer rechtlich erheblichen Tatsache zu erfüllen.

Nochmals rekapitulierend kann festgehalten werden, dass der Tatbestand der Urkundenfälschung beim Phishing-e-mail erfüllt ist, wenn dieses die objektiven Tatbestandsmerkmale gemäss den vorgängigen Ausführungen erfüllt und gestützt auf dieses e-mail die Zugangsdaten offen gelegt werden.

Der Tatbestand ist nicht erfüllt, wenn das Phishing-e-mail den Kunden lediglich dazu verleitet mit dem aufgeführten Internetlink die fragliche Internetseite aufzurufen und er dort nochmals getäuscht werden muss um die Zugangsdaten offen zu legen.

Dafür erfüllt die für die Eingabe der Zugangsdaten verwendete Internetseite der Phisher ebenfalls den Tatbestand der Urkundenfälschung sofern sie in objektiver Hinsicht gemäss den vorgängigen Ausführungen Urkundenqualität aufweist.

Die Frage der Konkurrenzen zu anderen Straftatbeständen wird in Kapitel 2.2.10 separat behandelt.

2.2.9 Markenschutzgesetz

Die strafrechtliche Würdigung des Phishing hat ergeben, dass beim Zugriff auf das E-Banking des Opfers und die Veranlassung unrechtmässiger Transaktionen der Straftatbestand der missbräuchlichen Verwendung einer Datenverarbeitungsanlage (Art. 147 StGB) anwendbar ist.

Hinsichtlich des ersten Teils des Phishing, dem Versand der e-mails zur Erlangung der Zugangsinformationen kommt im Rahmen des StGB lediglich der Tatbestand der Urkundenfälschung (Art. 251 StGB) in Frage und dies auch nur unter bestimmten Voraussetzungen.

⁵⁹ SCHMID Niklaus; Computer- sowie Check- und Kreditkarten-Kriminalität; § 3 N 99

Das StGB stellt somit nicht in jedem Fall sämtliche Handlungen des Phishing unter Strafe. Aus diesem Grund bleibt zu prüfen, ob der Versand der Phishing-e-mails womöglich durch das Nebenstrafrecht erfasst wird.

Beim Phishing verwendet der Täter im Rahmen des e-mail-Versandes aber auch auf der Internetseite zur Täuschung die in der Regel geschützte Marke (z.B. PostFinance, yellownet.ch etc.) des betroffenen Finanzinstitutes. Dem Inhaber einer geschützten Marke kommt jedoch gemäss dem Bundesgesetz vom 28. August 1992 über den Schutz von Marken und Herkunftsangaben (Markenschutzgesetz) das ausschliessliche Recht der Markenverwendung zu. Als Marke ist jedes Kennzeichnungsmittel (Wörter, Buchstaben, Zahlen, bildliche Darstellungen, dreidimensionale Formen) anzusehen, welches Markenschutz genießt, also alle im entsprechenden Markenregister eingetragenen und gebrauchten Marken. Entscheidend dabei ist die rein formelle Tatsache der Eintragung ins entsprechende Markenregister.⁶⁰ Diese Eintragungen im Markenregister können unter www.swissreg.ch abgerufen, respektive überprüft werden.

Ein betrügerischer Markengebrauch gemäss Art. 62 Ziff. 1 lit. a Markenschutzgesetz (MSchG) begeht, wer Waren oder Dienstleistungen zum Zwecke der Täuschung widerrechtlich mit der Marke eines anderen kennzeichnet und auf diese Weise den Anschein erweckt, es handle sich um Originalwaren oder –dienstleistungen.

Ziel des betrügerischen Markengebrauchs ist es also, eine Markendienstleistung zu produzieren, die von der Originalleistung kaum unterscheidbar ist und für diese gehalten wird. Ziel der vom Täter begangenen Täuschung ist die Schaffung der Illusion, die von ihm angebotenen Dienstleistungen seien echt, d.h. mit den betreffenden Originaldienstleistungen identisch.⁶¹ Art. 62 MSchG schützt nicht nur den Markeninhaber vor skrupelloser Aneignung und Ausnutzung seiner Rechte, sondern ebenso sehr den Abnehmer und Konsumenten, dessen Vermögen geschützt werden soll.⁶²

Beim Phishing wird auf der Internetseite und in den e-mails die Marke des betroffenen Finanzinstitutes verwendet um den Empfänger über den wirklichen Urheber hinweg zu täuschen. Mit dieser Vorgehensweise missbraucht der Täter die Marke eines anderen – nämlich des Finanzinstitutes – unrechtmässig. Dabei genügt es, wenn der Täter die geschützten Zeichen des Finanzinstitutes in seinen e-mails oder auch der Internetseite verwendet um damit den Eindruck zu erwecken, es handle sich um eine vom betroffenen Finanzinstitut angebotene Dienstleistung. Der Kunde geht in der Folge davon aus, dass die Dienstleistung vom betroffenen Finanzinstitut und nicht vom Täter angeboten wird.

Bei Art. 62 MSchG handelt es sich um ein Antragsdelikt, welches bei gewerbsmässiger Begehung von Amtes wegen zu verfolgen ist. Gewerbsmässigkeit ist bei berufsmässigem Handeln der Täterschaft gegeben. Solches liegt dann vor, wenn sich aus der Zeit und den Mitteln, die der Täter für die deliktische Tätigkeit aufwendet, als auch aus der Häufigkeit der Einzelakte innerhalb eines bestimmten Zeitraumes sowie aus den angestrebten und erzielten Einkünften ergibt, dass er die deliktische Tätigkeit nach der Art eines Berufes ausübt und aus den deliktischen Handlungen relativ regelmässige Ein-

⁶⁰ DAVID Lucas; Markenschutzgesetz, Muster- und Modellgesetz; Art. 61 N 6

⁶¹ DAVID Lucas; Markenschutzgesetz, Muster- und Modellgesetz; Art. 62 N 7

⁶² DAVID Lucas; Markenschutzgesetz, Muster- und Modellgesetz; Art. 62 N 4

nahmen anstrebt und erzielt, die einen namhaften Kostenbeitrag an seine Lebensgestaltung darstellen.⁶³

Da der Täter beim Phishing in der Regel mit grossem Mittel- und Zeiteinsatz vorgeht, viele potentielle Opfer kontaktiert und einen entsprechend grossen Gewinn durch sein Handeln anstrebt, kann aufgrund der aktuellen Rechtsprechung von einer gewerbsmässigen Tatbegehung ausgegangen werden. Folglich ist gemäss Art. 62 Abs. 2 MSchG das Phishing von den Strafverfolgungsbehörden von Amtes wegen – ohne Einreichung eines expliziten Strafantrages – zu verfolgen.

Abschliessend ist also festzuhalten, dass normalerweise bereits beim Versand von Phishing-e-mails selbst dann, wenn allenfalls die strafrechtliche Voraussetzung der Urkundenfälschung nicht erfüllt ist, eine Strafbarkeit aufgrund von Art. 62 Abs. 1 lit. a MSchG gegeben ist. Da Phishing grundsätzlich gewerbsmässig erfolgt, verfügen die Strafverfolgungsbehörden gemäss Abs. 2 der gleichen Bestimmung über die Möglichkeit von Amtes wegen auch schon gegen Phishing-e-mails vorzugehen.

Der Frage der Konkurrenz zu den anderen Straftatbeständen des StGB wird im nachfolgenden Kapitel nachgegangen.

2.2.10 Konkurrenzen

Bereits der Versand von Phishing-e-mails ist – unter bestimmten Voraussetzungen – strafbar nach Art. 251 StGB wegen Urkundenfälschung. Da bei den fraglichen e-mails die Marke der betroffenen Finanzinstitute missbräuchlich verwendet wird, liegt ebenfalls ein Verstoss gegen das Markenschutzgesetz aufgrund von Art. 62 MSchG vor.

Die Internetseite der Phisher erfüllt analog den Ausführungen zu den Phishing-e-mails ebenfalls den Tatbestand der Urkundenfälschung und begründet unter den gleichen Voraussetzungen die Strafbarkeit nach Markenschutzgesetz, da sie ja auch einer breiten Öffentlichkeit zugänglich gemacht wird.

Während der Straftatbestand der Urkundenfälschung das Vertrauen schützt, welches im Rechtsverkehr sowohl der Echtheit als auch der Wahrheit von Urkunden entgegengebracht wird, stellt der Straftatbestand des betrügerischen Markengebrauchs insbesondere den Markenschutz in den Vordergrund. Somit steht Art. 251 StGB in echter Konkurrenz zu Art. 62 MSchG.

Die Verwendung der erhaltenen Zugangsinformationen um in den besonders gesicherten Bereich des E-Banking einzudringen kann erst dann als unbefugte Datenbeschaffung nach Art. 143 StGB qualifiziert werden, wenn der Täter die vertraulichen Kunden- und Kontodaten im E-Banking-System für sich kopiert oder ausdrückt. Sinn und Zweck des Phishing ist jedoch nicht die unbefugte Datenbeschaffung sondern die unrechtmässige Bereicherung.

Die Verwendung der Zugangsdaten zur Auslösung entsprechender Vermögensverschiebungen im E-Banking zu Gunsten des Täters erfüllt den Straftatbestand des Missbrauchs einer Datenverarbeitungsanlage nach Art. 147 StGB.

⁶³ BGE 116 IV 332

Hat der Täter die Kunden- und Kontodaten für sich kopiert oder ausgedruckt steht Art. 147 StGB in Konkurrenz zu Art. 143 StGB. Eine echte Konkurrenz ist dabei denkbar, wenn die unbefugt beschafften Daten für sich selbst einen ökonomischen Wert darstellen. Entsteht keine über die bloße Datenbeschaffung hinausgehende Vermögensverschiebung, ist lediglich Art. 143 StGB anwendbar.⁶⁴ Dient die unbefugte Datenbeschaffung der Begehung eines betrügerischen Missbrauchs einer Datenverarbeitungsanlage gilt Art. 143 StGB als mitbestrafte Vor- bzw. Nachtat, da Art. 147 StGB jedenfalls mittelbar auch die ungestörte Verfügungsberechtigung der Daten schützt.⁶⁵

Eine echte Konkurrenz zwischen Art. 143 und Art. 147 StGB wäre m.E. allenfalls bei der Konstellation denkbar, in welcher der Täter die beschafften Daten nicht nur zum betrügerischen Missbrauch einer Datenverarbeitungsanlage nutzt, sondern auch noch andere Zwecke mit Bereicherungsabsicht damit verfolgen will (z.B. Verkauf vertraulicher Finanzdaten von berühmten Personen an die Medien).

Beim zweiten Teil des Phishing ist gestützt auf diese Erwägungen im Regelfall lediglich Art. 147 StGB anwendbar.

Der erste Teil des Phishing kann nicht als Versuch zum betrügerischen Missbrauch einer Datenverarbeitungsanlage betrachtet werden, da es sich bei der Vorgehensweise des Phishing um zwei von einander unabhängige Tathandlungen handelt. Der erste Teil ist im Bezug auf Art. 147 StGB lediglich straflose Vorbereitungshandlung. Ein strafbarer Versuch liegt erst ab dem Einloggen ins E-Banking-System vor.

2.3 Fallbeispiel 1: Phishing-Attacke aus dem Jahr 2005

2.3.1 Sachverhalt⁶⁶

Im Juni und im August 2005 wurden schweizweit E-mails mit dem Vermerk „PostFinance Online Service“ mit einer vermeintlichen Absenderadresse von PostFinance an eine unbestimmte Anzahl Personen versendet. Die e-mails enthielten die Botschaft, dass E-Banking-Kunden von PostFinance den im e-mail enthaltenen Link lautend auf www.yellow-net.ch anwählen sollten.

Wählte man den erwähnten Link an, gelangte man auf eine Internetseite, welche dem E-Banking-System der Schweizerischen Post (www.yellownet.ch) zum verwechseln ähnlich sah. Auf der Internetseite wurde man in englischer Sprache aufgefordert, seine yellownet-Benutzernummer, das Passwort und die nächsten 6 Sicherheitsnummern der verwendeten Streichliste (ein weiteres Sicherheitsmerkmal des E-Banking-Systems der Schweizerischen Post) anzugeben. Als Begründung wurde wenig aufschlussreich eine Überprüfung der Nutzungsrechte aufgeführt.

⁶⁴ BSK – StGB II; FIOLKA Gerhard; Art. 147 N 39

⁶⁵ BSK – StGB II; WEISSENBERGER Philippe; Art. 143 N 30

⁶⁶ Untersuchungsrichteramt III Bern-Mittelland; Fall-Nr. U 06 21222

Aufgrund der Phishing-e-mails vom Juni 2005 legte eine unbekannte Anzahl von PostFinance-Kunden die gewünschten Zugangsdaten offen. Als die Schweizerische Post Kenntnis von der Phishing-Attacke erhielt, versuchten in einem ersten Schritt die internen Fachstellen gemeinsam mit der Melde- und Analysestelle Informationssicherung (MELANI) des Bundesamtes für Polizei die Internetseite der Phisher deaktivieren zu lassen. Die fragliche Internetseite wurde von einem Server in Asien gehostet, welcher nach wenigen Stunden tatsächlich reagierte und die Seite vom Internet entfernte.

Dennoch gelang es der Täterschaft ab 13 Konten Überweisungen via Western Union nach Russland und Estland auszulösen und in 10 Fällen dort das Geld auch in Empfang zu nehmen. In drei Fällen blieb es beim Versuch, weil PostFinance nach Bekanntwerden der Vorgehensweise sämtliche Transaktionen im Western Union-Kanal der Post blockierte und jede weitere gewünschte Transaktion detailliert nachprüfte.

Im August 2005 wurde nochmals eine identische Phishing-Attacke auf PostFinance-Kunden gestartet. Wiederum wurde die Internetseite von einem Server in Asien gehostet und wiederum legten einzelne Kunden ihre Zugangsdaten offen. Es kam jedoch zu keinen Transaktionen, weil in der Zwischenzeit PostFinance das Sicherheitssystem angepasst hatte und die 6 offen gelegten Streichlisten-Nummern nicht mehr für den Zugriff genügten. Zudem konnten auch keine unrechtmässigen Login-Versuche festgestellt werden. Die fragliche Internetseite wurde innert weniger Stunden deaktiviert und die Kunden nochmals mittels Pressemitteilungen darüber informiert, dass ein Finanzinstitut niemals diesen Weg zur Kontaktnahme mit seinen Kunden wählen würde.

2.3.2 Strafrechtliche Würdigung

Die Strafuntersuchung wurde von einem Untersuchungsrichteramt im Kanton Bern geführt.

Die Phishing-Attacke vom Juni 2005 wurde vom zuständigen Untersuchungsrichter in 10 Fällen als strafbare Handlung nach Art. 147 StGB und in 3 Fällen als vollendeter Versuch dazu gewertet. Das Verfahren wurde mittlerweile gestützt auf Art. 235 der bernischen Strafprozessordnung bis zur Ermittlung der Täterschaft eingestellt, da sämtliche ergriffenen Massnahmen zu deren Ermittlung bisher ergebnislos verlaufen waren.

Das anlässlich der analogen Attacke vom August 2005 eröffnete Verfahren wegen Art. 147 StGB wurde vom gleichen Untersuchungsrichter mit der Begründung eingestellt, dass die Täterschaft im straflosen Vorbereitungsstadium steckengeblieben sei und die Schwelle zum strafbaren Versuch somit nie überschritten habe.

2.3.3 Kommentar zum Fallbeispiel

Die in dieser Arbeit vorgenommene strafrechtliche Würdigung bestätigt die strafrechtliche Subsumtion der Untersuchungsbehörde dahingehend, dass der zweite Teil des Phishing nach Art. 147 StGB strafbar ist.

Hingegen wurden vom zuständigen Untersuchungsrichter keine weiteren Straftatbestände geprüft. Es wurde beispielsweise nicht geklärt, ob die von den Phishern verwendete Internetseite zur Täuschung der Kunden auch den Tatbestand von Art. 251 StGB erfüllt und somit in echter Konkurrenz zu Art. 147 StGB stehen würde.

Die zweite Phishing-Attacke vom August 2005 wurde als strafrechtlich nicht relevant beurteilt und deshalb auch nicht weiter untersucht. Die Ausführungen im Kapitel 2.2 dieser Arbeit haben aber ergeben, dass bereits der Versand von Phishing-e-mails eine mögliche Strafbarkeit nach Art. 251 StGB sowie nach Art. 62 MSchG begründet. Aufgrund der weiten Verbreitung der Phishing-e-mails und der Vorgehensweise der Täterschaft dürfte es sich zudem um eine gewerbsmässige Tatbegehung gehandelt haben, weshalb die Untersuchungsbehörde schon von Amtes wegen bezüglich der Verletzung des Markenschutzgesetzes hätte ermitteln müssen.

Ob nun tatsächlich der Versand der Phishing-e-mails in diesem konkreten Fall die erwähnten Straftatbestände erfüllt hätte oder die fragliche Internetseite Urkundenqualität hatte, muss schlussendlich offen bleiben. Aufgrund der Einstellung erfolgten keine weiteren Untersuchungshandlungen oder eine Sicherung der e-mails oder des Inhaltes der Internetseite. Eine vertiefte Prüfung kann deshalb nicht mehr nachgeholt werden.

Aus meiner Sicht wurde daher das fragliche Strafverfahren zu schnell eingestellt. Es hätte mindestens eine Überprüfung der Strafbarkeit nach den erwähnten Straftatbeständen erfolgen müssen. Ob eine umfassendere Überprüfung am spezifischen Endergebnis – der Einstellung – etwas geändert hätte, ist hingegen auch wieder fraglich und der Entscheidung des Untersuchungsrichters aus Sicht der anderweitigen Geschäftslast nachvollziehbar.

2.4 Fallbeispiel 2: Phishing-Attacke aus dem Jahr 2006

2.4.1 Sachverhalt⁶⁷

Im Juli 2006 erhielten zahlreiche E-Banking-Kunden der Schweizerischen Post ein e-mail mit dem vermeintlichen Absender: „support@postfinance.ch“ und dem Betreff: „Achtung! Für alle Postfinance Kunden“.

Das fragliche e-mail forderte die Kunden in deutscher Sprache auf, sich mittels dem beigefügten Link: „<https://www.yellownet.ch/app/welcome.do>“ im E-Banking-System der Post zu identifizieren und 20 Sicherheitsnummern der aktuellen Streichliste einzugeben. Als Grund wurde die Einführung neuer Sicherheitsmassnahmen wegen der in letzter Zeit immer wieder vorkommenden Betrugsversuche im Internet angegeben und die Kunden um Verständnis für diese Massnahme gebeten. Ferner wurde ihnen mitgeteilt, dass wenn die Authentifizierung nicht innert eines Tages erfolge, das PostFinance-Konto gesperrt werden müsse.

Das versendete e-mail entsprach in der Aufmachung dem Bild von PostFinance und die Internetseite war eine qualitativ sehr gute Kopie der Originalseite „www.yellownet.ch“.

⁶⁷ Untersuchungsrichteramt III Bern-Mittelland; Fall-Nr. U 06 68304

Dies führte dazu, dass zahlreiche Kunden dem e-mail Glauben schenkten und die Anweisungen befolgten.

Nachdem die Kunden die Internetseite aufgerufen, sich mittels Benutzernummer und Passwort eingeloggt hatten, wurden sie aufgefordert die 20 verlangten Sicherheitsnummern der Streichliste einzugeben. Nach erfolgter Eingabe erschien eine Fehlermeldung mit dem Aufruf 20 weitere Sicherheitsnummern einzugeben. Durch diese Vorgehensweise gelangte die Täterschaft in den Besitz von 40 Sicherheitsnummern und hatte somit genügend Daten für einen erfolgreichen Zugriff auf das E-Banking-System der Post.

Nach Bekanntwerden der Attacke wurde umgehend der normalerweise durch die Täterschaft verwendete Western Union-Kanal geschlossen und jede Transaktion detailliert geprüft. Weiter wurden Warnmeldungen veröffentlicht, geahishte Kunden wurden gebeten sich zu melden und in einer gemeinsamen Aktion des Bundesamtes für Polizei und der postinternen IT-Experten neun Server in Russland, in Südamerika und in Asien ausfindig gemacht, welche alle als Host für die fragliche Internetseite dienten. Da die Täterschaft bei ihrer Phishing-Attacke mehrere identische e-mails aber mit Links auf unterschiedliche Internetseiten versendet hatte, dauert es rund zwei Tage bis alle Seiten blockiert werden konnten.

Zum Bezug der Gelder verwendete die Täterschaft dieses Mal nicht direkt den Western Union-Kanal. Sie heuerte vorgängig mittels Ausschreibung im Internet sogenannte Finanzagenten an. Deren Aufgabe war es, ihre Bank- und Postkonten für den Empfang von Überweisungen zur Verfügung zu stellen, anschliessend die Gelder abzuheben und abzüglich einer Provision von 5 bis 10 % per Western Union an bestimmte Orte ins Ausland zu überweisen.

Rund 20 Personen mit Wohnsitz in der Schweiz stellten daraufhin ihre Post- und Bankkonten für entsprechende Überweisungen zur Verfügung. Die Täterschaft löste mittels den geahishten Zugangsinformationen entsprechende Transaktionen auf diese Konten aus. Aufgrund der mehreren Millionen Transaktionen pro Tag fielen diese Inlandüberweisungen beim Monitoring nicht auf und konnten erfolgreich durchgeführt werden. Im Anschluss daran bezogen die Empfänger umgehend die überwiesenen Gelder und veranlassten – nach Abzug ihrer Provision - entsprechende Überweisungen per Western Union in verschiedene Länder.

In 25 Fällen war diese Vorgehensweise erfolgreich bis sie von der PostFinance entdeckt und das Überwachungssystem angepasst wurde.

2.4.2 Strafrechtliche Würdigung

Das auch in diesem Fall verfahrensleitende Untersuchungsrichteramt aus dem Kanton Bern eröffnete eine Strafuntersuchung gegen die unbekannte (Phishing-)Täterschaft gestützt auf Art. 147 StGB und wegen Geldwäscherei (Art. 305^{bis} StGB). Bisher verlief die Identifikation der Phishing-Täterschaft ergebnislos, was den Schluss zulässt, dass auch dieses Verfahren in absehbarer Zeit aufgrund Art. 235 der bernerischen Strafprozessordnung mit analoger Begründung zu Praxisbeispiel 1 eingestellt werden wird.

Ferner wurden Strafverfahren wegen Gehilfenschaft zu Art. 147 StGB und wegen Geldwäscherei gegen die 20 als „Finanzagenten“ agierenden Personen eröffnet, welche ihre Konten zur Überweisung zur Verfügung gestellt hatten.

Die zuständige Untersuchungsrichterin begründete die Verfahreneröffnung wegen Gehilfenschaft zu Art. 147 StGB gegen die Finanzagenten damit, dass diese der unbekanntes Täterschaft ihre Konten für Überweisungen von „gephishen“ Konten zur Verfügung stellten und anschliessend auf Anweisung der unbekanntes Täterschaft die überwiesenen Gelder – abzüglich ihrer Provision – über Western Union an weitere Personen im Ausland überwiesen hatten.

Der Geldwäscherei-Vorwurf nach Art. 305^{bis} StGB an die Finanzagenten wurde analog dazu damit begründet, dass die Angeschuldigten mit ihren Handlungen dazu beigetragen hätten, den Zugriff und die Ermittlung der Herkunft der durch das Phishing überwiesenen Gelder zu vereiteln.

Die Strafverfahren gegen die 20 Finanzagenten befinden sich noch im Untersuchungsstadium. Es ist gemäss der zuständigen Untersuchungsrichterin vorgesehen, die weitere Untersuchungsführung an die für die Wohnsitze der Finanzagenten zuständigen Untersuchungsbehörden (12 verschiedene Kantone) abzutreten.

2.4.3 Kommentar zum Fallbeispiel

Es kann in diesem Fall grundsätzlich auf den Kommentar zum Fallbeispiel 1 in Kapitel 2.3.3 verwiesen werden.

Zweifellos ist die Anwendung von Art. 147 StGB für die unbekanntes (Phishing-)Täterschaft korrekt. Ferner hätte in diesem Fall aus meiner Sicht zusätzlich Art. 251 StGB bezüglich der Internetseiten und der e-mails angewendet werden müssen. Diese Erkenntnis ergibt sich aus der hervorragenden Qualität der e-mails und der als äusserst authentisch wirkenden und in sich schlüssigen Internetseiten. Diesbezüglich wird auch auf den Anhang dieser Arbeit verwiesen.

Ein Vergleich der beim Phishing verwendeten Marken mit den im Markenregister unter www.swissreg.ch eingetragenen Originalmarken der Schweizerischen Post ergab eine vollkommene Übereinstimmung.

Die Schweizerische Post hat es auch in diesem Fall unterlassen, einen separaten Strafantrag bezüglich eines vermuteten Verstosses nach Art. 62 MSchG zu stellen. Der betrügerische Markengebrauch der Marke „PostFinance“ der Schweizerischen Post durch die Täterschaft hätte dies gerechtfertigt. Jedoch hätte auch ohne separaten Strafantrag die Eröffnung einer Strafuntersuchung wegen des Verdachts der gewerbsmässigen Tatbegehung von Amtes wegen erfolgen müssen.

Die Verfahren wegen Geldwäscherei und Gehilfenschaft zum betrügerischen Missbrauch einer Datenverarbeitungsanlage gegen die sogenannten Finanzagenten sind berechtigt. Mit dem Abheben der Gelder auf ihren Konten und der anschliessenden Überweisung mittels Western Union ins Ausland scheinen die Finanzagenten zumindest in objektiver Hinsicht den klassischen Tatbestand der Geldwäscherei zu erfüllen.

Mit dem zur Verfügung stellen ihrer Konten gegen entsprechende Provision leisteten die Finanzagenten einen kausalen Beitrag zur Straftat⁶⁸ und begünstigten deren Erfolg. Aufgrund des derzeitigen Verfahrensstandes kann ebenfalls davon ausgegangen werden, dass die Finanzagenten in irgendeiner Art und Weise wissen mussten, dass sie mit ihrer Handlungsweise eine Straftat unterstützen würden. Dafür spricht zum einen die relativ hohe Provision für einen relativ kleinen Aufwand und zum anderen die eher fadenscheinigen Begründungen, weshalb ihr Konto benötigt würde.

Es kann jedoch auch davon ausgegangen werden, dass die Phishing-Handlung auch ohne die Unterstützung der Finanzagenten in irgendeiner Art und Weise stattgefunden hätten, weshalb ihr Beitrag richtigerweise nicht als eigentliche Mittäterschaft angesehen werden kann. Ferner dürfte ihre Tathandlung keinen Zusammenhang mit den anderen strafbaren Handlungen im Vorfeld haben (Phishing-e-mail und Phishing-Internetseite) und somit diesbezüglich auch keine Strafbarkeit vorliegen.

Obwohl auch bei diesem Beispiel nicht alle in Frage kommenden Straftatbestände berücksichtigt wurden, liegt die Vermutung nahe, dass auch bei einer umfassenden Untersuchung das Resultat dasselbe geblieben wäre.

Insofern ist die Konzentration auf die Tatbestände von Art. 147 und 305^{bis} StGB bei der unbekanntem Täterschaft auch hinsichtlich der allgemeinen Geschäftslast nachvollziehbar.

3 *Skimming*

3.1 Begriff und Vorgehensweise

Der englische Begriff Skimming dürfte vom Verb „to skim“ abgeleitet sein, was unter anderem „gleiten“ bedeutet. Damit dürfte die im klassischen Sinn bei dieser Tathandlung vorgenommene Handbewegung gemeint sein, bei der die echte Karte durch den Kartenleser hindurchgeführt wird um die sich auf der Karte befindlichen Daten zu kopieren⁶⁹. Dem Begriff Skimming kommt im Englischen aber auch die Bedeutung von „Abschöpfen“ zu, was ebenfalls als treffend – im Sinne von Geld abschöpfen - angesehen werden könnte.

Es gibt verschiedene Varianten von Skimming. Im Rahmen dieser Arbeit wird nur die aktuellste Variante davon behandelt. Nämlich das Kopieren von Karten in ihrer Funktion als Zahlkarten unter gleichzeitiger Ausspionierung des dafür notwendigen PIN-Codes und die Verwendung dieser zum Bezug von Bargeld oder zum Einkauf von Waren sowie Dienstleistungen an Automaten (z.B. sogenannte EFTPOS-Geräte), welche im Anschluss daran automatisch eine Belastung auf dem Konto des rechtmässigen Karteninhabers zur Folge haben.

Eine Kredit- oder Debitkarte kann mit dem dazugehörigen PIN-Code an jedem dafür vorgesehenen Automaten zum Bezug von Bargeld oder zum Einkauf von Waren oder

⁶⁸ BGE 98 IV 85

⁶⁹ GUGGENBÜHL Heinrich; Bekämpfung des Kreditkartenmissbrauchs – gegenwärtige Verhältnisse; Kriminalistik Heft 8-9 Jg. 2003; S. 551 f.

Leistungen eingesetzt werden. Nach dem Einsatz am Automaten erfolgt durch diesen, respektive (bei Offline-Betrieb) durch den Automaten-Besitzer automatisch eine Belastung auf dem durch die Zahlkarten bezogenen Konto.

Als Basis für die dafür notwendige elektronische Datenverarbeitung wird heutzutage in der Regel der sich auf der Rückseite der Karten befindliche Magnetstreifen verwendet. Der Aufbau und die Struktur dieses Magnetstreifens ist für den weltweiten Einsatz standardisiert. Gerade aufgrund dieser weltweiten Standardisierung sind kombinierte Lese- und Schreibgeräte für diese Magnetstreifen vielerorts erhältlich (beispielsweise können sie im Internet bestellt werden). Mittels diesen Geräten kann ein beschriebener Magnetstreifen einer Karte problemlos eingelesen und anschliessend auf einen anderen noch unbeschriebenen Magnetstreifen kopiert werden. Diese Kopie verhält sich dabei gleich wie das Original und kann wiederum von jedem dafür vorgesehenen Automaten (Geldautomat, Kassenterminal beim Einkauf etc.) gelesen werden.⁷⁰

Als Sicherung dieser an sich einfach zu verwendenden Daten wird aus diesem Grund eine persönliche Identifikationsnummer (der PIN-Code) verwendet. Die im Magnetstreifen enthaltenen Daten können nur im Sinne ihres Zweckes verwendet werden, wenn gleichzeitig eine Autorisierung des Nutzers gegenüber dem betroffenen Automaten mittels PIN-Code erfolgt.

Aus diesem Grund hat es die Täterschaft beim Skimming nebst den Daten auf dem Magnetstreifen der jeweiligen Zahlkarte auch auf den PIN-Code des rechtmässigen Nutzers abgesehen. Um an sämtliche Informationen zu gelangen wird im Regelfalle wie folgt vorgegangen:

Die Täterschaft präpariert einen für die Verwendung von Zahlkarten vorgesehenen Automaten (häufig ein Geldausgabegerät). Es wird eine Lesevorrichtung installiert, welche bei Nutzung des Automaten sicherstellen soll, dass der Magnetstreifen der verwendeten Karte nicht nur vom Automaten sondern auch vom zusätzlich installierten Lesegerät eingelesen und kopiert wird. Zudem wird von der Täterschaft versucht, den vom rechtmässigen Karteninhaber verwendeten PIN-Code auszuspionieren. Dies kann durch Beobachten der Eingabe von blossen Auge oder mittels verdeckter Videoüberwachung erfolgen. Eine weitere – bisher wenig verbreitete, da technisch aufwändigere – Möglichkeit, ist die gleichzeitige Präparierung des für die Eingabe des PIN-Codes vorgesehenen numerischen Zahlenblockes am Automaten.

Nachdem die Täterschaft den Magnetstreifen für sich eingelesen und den PIN-Code erhältlich gemacht hat, kopiert sie die erhaltenen Daten auf einen Magnetstreifen einer neuen Karte und verwendet diese gemeinsam mit dem PIN-Code im Regelfall zum Bezug von Bargeld oder zum Einkauf von Waren und Dienstleistungen.

Aufgrund der weiten Verbreitung dieser Deliktsart wurde in den letzten Jahren nebst dem nach wie vor immer vorhandenen Magnetstreifen zusätzlich ein Prozessor-Chip auf den Kredit- und Debitkarten eingeführt. Diese Prozessor-Chips gelten im Vergleich zu den Magnetstreifen als deutlich sicherer, da sie nicht so einfach eingelesen und kopiert werden können. D.h. selbst wenn der Täter im Besitze des PIN-Codes ist, ist es auf-

⁷⁰ FLURI Anton; Bekämpfung des Kreditkartenmissbrauchs – technische Aspekte; Kriminalistik Heft 8-9 Jg. 2003; S. 554 f

grund der Chip-Technologie deutlich schwieriger die auf dem Chip gespeicherten Daten zu kopieren.

Der Chip enthält die gleichen Informationen wie der Magnetstreifen und hat zum Ziel diesen mittel- bis langfristig gänzlich zu ersetzen. Seit kurzem gilt in der Schweiz bereits der Standard, dass Geldausgabegeräte bei schweizerischen Zahlkarten (Maestro und Postcard) nur noch den Chip lesen, falls dieser nicht gelesen werden kann, wird die Karte eingezogen. Wird eine ausländische Karte eingesetzt, welche keinen Chip hat oder dieser ist nicht lesbar, wird durch den Automaten auf den Magnetstreifen zugegriffen um die Zahlungshandlung gleichwohl zuzulassen.

Im Ausland ist man bezüglich Umstellung auf die Prozessor-Chips für die Automaten noch nicht soweit wie in der Schweiz. In Westeuropa dürfte der Prozessor-Chip als grundsätzlicher Standard in den nächsten Jahren erreicht werden. Ausserhalb Westeuropas dürfte noch über längere Zeit hinaus der Magnetstreifen der einzige Standard bleiben. Solange sich der neue Standard nicht weltweit durchgesetzt hat wird in der Schweiz weiterhin der Magnetstreifen bei ausländischen Karten und im Ausland der Magnetstreifen schweizerischer Karten verwendet werden können.

3.2 Strafrechtliche Würdigung

In den nachfolgenden Unterkapiteln wird der Frage nachgegangen, welche Straftatbestände durch das Skimming erfüllt werden. Ähnlich wie beim Phishing ist auch das Skimming für die strafrechtliche Würdigung in zwei Schritte zu unterteilen:

- Der erste Schritt des Skimming besteht aus dem Beschaffen (Kopieren) der Daten und des PIN-Codes.
- Im zweiten Schritt werden die eingelesenen Daten auf einen neuen Magnetstreifen kopiert und unter Verwendung des PIN-Codes mit dem Ziel der unrechtmässigen Bereicherung eingesetzt.

3.2.1 Diebstahl – Art. 139 StGB

Bezüglich den grundsätzlichen Ausführungen wird auf das Kapitel 2.2.2 verwiesen.

Als Tatobjekt beim Diebstahl kommt lediglich die Wegnahme körperlicher Gegenstände in Frage. Aus diesem Grunde kann der erste Schritt des Skimming - das Kopieren der Daten und das Ausspionieren des PIN-Codes - nicht unter Art. 139 StGB subsumiert werden.

Sofern die Folge des zweiten Schrittes des Skimming eine unrechtmässige Bereicherung des Täters mit einer fremden beweglichen Sache (z.B. Bargeld aus Geldautomat) ist, wäre zumindest das Tatobjekt des Diebstahls gegeben.

In diesem Fall ist noch zu prüfen, ob es sich bei der für den Diebstahl notwendigen Tat handlung (Wegnahme zur Aneignung) um den Bruch fremden und die Begründung

neuen, in der Regel eigenen Gewahrsams handelt.⁷¹ Ein Bruch des Gewahrsams ist nur vorstellbar ohne die Einwilligung des Gewahrsamsinhabers.⁷² Sobald eine Einwilligung des Gewahrsamsinhabers vorliegt muss ein Gewahrsamsbruch ausgeschlossen werden.

Die Einwilligung kann an Bedingungen und Auflagen geknüpft sein, was insbesondere bei Waren- und Geldautomaten Bedeutung erlangt. Diesbezüglich kann die Einwilligung insbesondere auch von Bedingungen abhängig gemacht werden, die der Automat nicht überprüfen kann.⁷³ Beim Einsatz des kopierten Magnetstreifens und des PIN-Codes kann der Automat nicht überprüfen, ob der effektiv Berechtigte den Waren- oder Geldbezug tätigt, also die Bedingungen für die Einwilligung erfüllt sind oder nicht. Folglich liegt in diesem Fall auch keine Einwilligung in die Gewahrsamsaufgabe durch den entsprechenden Bezug vor, weshalb m.E. ein Gewahrsamsbruch erfolgt. Mit der Behändigung der bezogenen Sache begründet der Täter auch neuen Gewahrsam. Da beim Skimming dies immer mit der Absicht der unrechtmässigen Bereicherung erfolgt, ist der Tatbestand des Diebstahls sowohl objektiv wie subjektiv erfüllt.⁷⁴

In diesem Zusammenhang sei noch erwähnt, dass mit der gleichen Begründung der Tatbestand des Erschleichens einer Leistung nach Art. 150 StGB gegeben ist, wenn es sich beim Tatobjekt um eine Leistung anstelle einer fremden beweglichen Sache handelt. In der Regel steht das Erschleichen einer Leistung jedoch beim Skimming nicht im Vordergrund.

Die Frage der Konkurrenzen zu weiteren Straftatbeständen wird im Kapitel 3.2.9 separat behandelt.

3.2.2 Unbefugte Datenbeschaffung – Art. 143 StGB

Hinsichtlich den grundsätzlichen Ausführungen sei auf Kapitel 2.2.3 hingewiesen.

Die auf dem Magnetstreifen der Zahlkarte gespeicherten Informationen und der PIN-Code entsprechen – analog den Zugangsinformationen zum E-Banking – dem Datenbegriff nach Art. 143 StGB. Ferner sind die vom Täter beim Skimming verwendeten Daten nicht für ihn bestimmt, weshalb er unbefugt über sie verfügt und damit ein weiteres Tatbestandselement erfüllt.

Da die auf dem Magnetstreifen gespeicherten Daten ohne die Eingabe des PIN-Codes zwar kopiert aber nicht ausgelesen werden können, dürfte das Merkmal der besonderen Sicherung ebenfalls erfüllt sein.

Art. 143 StGB bedingt zudem, dass der Täter bestehende Zugangsschranken aktiv überwindet oder umgeht und sich dadurch die gewünschten Daten beschafft. Beim Skimming präpariert der Täter die für Zahlkarten verwendeten Automaten und installiert versteckte Lese- und Überwachungsgeräte um an die Kartendaten und den PIN-Code zu kommen. In diesem Sinne ergreift er also Massnahmen um sich die Daten aktiv und –

⁷¹ BSK – StGB II; NIGGLI Marcel Alexander/RIEDO Christof; Art. 139 N 11

⁷² STRATENWERTH Günter; Schweiz. Strafgesetzbuch – Besonderer Teil I; § 13 N 82

⁷³ BSK- StGB II; NIGGLI Marcel Alexander/RIEDO Christof; Art. 139 N 50

⁷⁴ ähnlich BGE 104 IV 72

im Gegensatz zum Phishing – ohne freiwillige Offenlegung des Karteninhabers zu beschaffen.

Davon ausgehend, dass der Täter vorsätzlich und in Bereicherungsabsicht handelt, erfüllt gestützt auf diese Vorgehensweise der erste Schritt des Skimming den Tatbestand der unbefugten Datenbeschaffung nach Art. 143 StGB. Die Frage allfälliger Konkurrenzen zu anderen Straftatbeständen wird in Kapitel 3.2.9 behandelt.

Die anschliessende Verwendung der kopierten Zahlkarte und des PIN-Codes zum Bezug von Bargeld oder der elektronischen Bezahlung von Einkäufen oder Dienstleistungen erfüllt den Tatbestand nicht, da die Tathandlung lediglich in einer vermeintlichen Zahlungsfreigabe für einen Bezug von Geld, Waren oder Dienstleistungen mündet und, entgegen dem unbefugten Eindringen in ein E-Banking-System beim Phishing, dadurch keine weiteren Daten für den Täter beschafft werden.

3.2.3 Unbefugtes Eindringen in ein Datenverarbeitungssystem – Art. 143^{bis} StGB

In Bezug auf die grundsätzlichen Ausführungen zum Straftatbestand sei auf Kapitel 2.2.4 verwiesen.

In Ergänzung zu diesen Ausführungen kann vermerkt werden, dass bereits der objektive Tatbestand beim ersten Schritt des Skimming nicht erfüllt ist, weil der Täter gar nicht in eine fremde Datenverarbeitungsanlage eindringt, sondern lediglich am Automaten Lese-einrichtungen installiert um an die Daten der vom Opfer verwendeten Zahlkarte zu gelangen. Diese Daten sind jedoch nicht Bestandteil der Datenverarbeitungsanlage des präparierten Automaten, sondern lediglich auf einem Datenträger (Magnetstreifen) gespeicherte Datenbestände.

Der Magnetstreifen für sich ist keine Datenverarbeitungsanlage, sondern lediglich ein Datenspeicher (wie beispielsweise auch Disketten), welcher nicht unter den Schutz von Art. 143^{bis} StGB fällt.⁷⁵ Mit dem Kopieren der Daten auf dem Magnetstreifen dringt der Täter nicht in ein Datenverarbeitungssystem ein. Zudem erfolgt das Lesen der Daten nicht über den für Art. 143^{bis} StGB notwendigen Weg von drahtverbundenen oder drahtlosen Übermittlungskanälen⁷⁶, sondern durch direkten Kontakt mit dem Lesegerät.

Auch in subjektiver Hinsicht ist beim Skimming der Straftatbestand des unbefugten Eindringens in ein Datenverarbeitungssystem grundsätzlich nicht anwendbar, da er nur ohne Bereicherungsabsicht begangen wird und Sinn und Zweck des Skimming – analog des Phishing – ja gerade die unrechtmässige Bereicherung ist.

3.2.4 Betrug – Art. 146 StGB

Betreffend den grundsätzlichen Ausführungen wird auf Kapitel 2.2.5 verwiesen.

⁷⁵ SCHMID Niklaus; Computer- sowie Check- und Kreditarten-Kriminalität; § 5 N 16

⁷⁶ SCHMID Niklaus; Computer- sowie Check- und Kreditkarten-Kriminalität; § 5 N 21

Der erste Schritt des Skimming kann den Betrugstatbestand schon daher nicht erfüllen, als dass keinerlei motivierende Einwirkung auf das Opfer stattfindet. Dieses setzt seine Zahlkarte aus eigenem Antrieb ein und ermöglicht es dabei – unwissend – dem Täter die Daten zu kopieren. Zudem erfolgt wiederum, wie bereits bei der strafrechtlichen Würdigung des Phishing festgehalten, die Vermögensverfügung nicht durch das Opfer selbst, sondern durch eine zusätzliche, selbständige Handlung des Täters (nämlich durch Einsatz der kopierten Zahlkarte).

Zu prüfen ist nun noch, ob durch die Vorgehensweise im zweiten Schritt des Skimming allenfalls ein Betrug hinsichtlich dem Einsatz der kopierten Zahlkarte und des PIN-Codes vorliegen könnte. Durch die unrechtmässige Verwendung der Karte und des PIN-Codes an einem Automaten täuscht der Täter die Identität des Opfers vor und veranlasst so die entsprechende Vermögensdispositionen.

Obwohl diese Vorgehensweise den aufgeführten Tatbestandselementen weitgehend entspricht, ist Art. 146 StGB analog wie beim Phishing auch für diesen Fall nicht anwendbar, da der Tatbestand des Betruges vom Bild eines Opfers ausgeht, das durch Täuschung dazu bewogen wird, sich selbst zu schädigen. Ein Datenverarbeitungssystem kann man nicht täuschen und es kann auch nicht über Vermögen verfügen.⁷⁷

Weil der Täter sich mit den kopierten Daten und dem PIN-Code lediglich gegenüber einem Datenverarbeitungssystem identifiziert und die Vermögensverschiebung im Rahmen dieser Datenverarbeitung selber auf elektronischem Wege auslöst, kann auch beim Skimming nicht von einem Betrug im herkömmlichen Sinne gesprochen werden.

Art. 146 StGB ist somit auch nicht für Skimming anwendbar.

3.2.5 Betrügerischer Missbrauch einer Datenverarbeitungsanlage – Art. 147 StGB

In Bezug auf die grundsätzlichen Ausführungen sei auf Kapitel 2.2.6 hingewiesen.

Als wesentliches Erfüllungserfordernis des Art. 147 StGB gilt, dass als Folge der Handlungen das Ergebnis der Datenverarbeitung oder –übermittlung unrichtig sein muss. Dies wäre der Fall bei der Eingabe unrichtiger oder unvollständiger Daten, aber auch bei der Manipulation des verwendeten Programms oder schliesslich nur des Resultats der Datenverarbeitung.⁷⁸ Dies ist jedoch beim ersten Schritt des Skimming nicht der Fall.

Mit der Installation entsprechender Lese- und Aufzeichnungsgeräte an einem Automaten wird nicht auf einen Datenverarbeitungsvorgang eingewirkt, sondern nur die Daten, welche den entsprechenden Datenverarbeitungsvorgang autorisieren (Daten der Zahlkarte und PIN-Code), ausspioniert und kopiert. Der eigentliche, vom rechtmässigen Karteninhaber ausgelösten Datenverarbeitungsvorgang wird dadurch weder unrichtig noch unvollständig beendet. Der Vorgang ist an sich vergleichbar mit jeder unrechtmässigen Erstellung einer Datenkopie bei jeder anderen Gelegenheit und steht nicht zwingend im direkten Zusammenhang mit der Datenverarbeitung am vom Opfer benutzten Automaten.

⁷⁷ STRATENWERTH Günter; Schweiz. Strafgesetzbuch – Besonderer Teil I; § 16 N 2

⁷⁸ STRATENWERTH Günter; Schweiz. Strafgesetzbuch – Besonderer Teil I; § 16 N 6

Weiter erfüllt der erste Schritt des Skimming – analog dem ersten Teil des Phishing – auch nicht die Bedingung der direkt kausal zur erfolgreichen Täuschungshandlung folgenden Vermögensverschiebung. Diesbezüglich ist der zweite und wiederum selbstständig vom ersten Schritt erfolgende Teil des Skimming notwendig.

Mit Bezug auf den zweiten Schritt des Skimming kann die unrechtmässige Datenbeschaffung des ersten Schrittes als Vorbereitungshandlung angesehen werden, welche analog zum Phishing den Tatbestand von Art. 147 StGB jedoch nicht erfüllt und als Vorbereitungshandlung ohne Strafe bleibt (siehe dazu auch Kapitel 2.2.6).

Mittels Einsatz der kopierten Zahlkarte und des PIN-Codes löst der Täter im zweiten Schritt bei einem entsprechenden Automaten einen an sich richtigen Datenverarbeitungsvorgang aus, welcher aber im Ergebnis unzutreffend ist. Konkret bedeutet dies, dass der Täter aufgrund der unrechtmässigen Verwendung der kopierten Daten und des PIN-Codes gegenüber dem Automaten als autorisiert gilt um elektronische Transaktionen auslösen zu können. Ohne die Verwendung des entsprechenden Codes könnten alleine schon systembedingt keine Datenverarbeitungsvorgänge ausgelöst werden. Die ausgelösten Transaktionen sind aber dennoch im Ergebnis unzutreffend, da dem Täter die entsprechende Befugnis des rechtmässig Berechtigten fehlt. Der Vermögensschaden als weiteres Tatbestandsmerkmal ist ebenfalls gegeben, da durch die ausgelöste Transaktion das Guthaben des Skimming-Opfers bzw. des betroffenen Finanzinstitutes reduziert wird.⁷⁹

Zusammenfassend kann festgehalten werden, dass beim zweiten Schritt des Skimming – aufgrund analoger Voraussetzungen wie beim Phishing - der Täter durch eine unbefugte Verwendung von Daten im Rahmen eines Datenverarbeitungsvorganges eine Transaktion auslöst, welche direkt zu einer Vermögensverschiebung zu seinen Gunsten und somit zu einem Schaden des Betroffenen führt. Setzt man nun auch hier noch die Bereicherungsabsicht und den Vorsatz der Täterschaft voraus, sind sämtliche Tatbestandsmerkmale erfüllt und die Tathandlung kann unter Art. 147 StGB subsumiert werden.

Die Frage der Konkurrenzen wird im Kapitel 3.2.9 behandelt.

3.2.6 Check- und Kreditkartenmissbrauch – Art. 148 StGB

Nach Art. 148 StGB wird bestraft, wer – obschon zahlungsunfähig oder –unwillig – eine ihm vom Aussteller überlassene Check- oder Kreditkarte oder ein gleichartiges Zahlungsinstrument verwendet, um vermögenswerte Leistungen zu erlangen und den Aussteller dadurch am Vermögen schädigt, sofern dieser und das Vertragsunternehmen die ihnen zumutbaren Massnahmen gegen den Missbrauch der Karte ergriffen haben.

Das in diesem Tatbestand für die Beurteilung des Skimming relevante Element ist die Formulierung „vom Aussteller überlassen“. Damit wird ausgedrückt, dass der Tatbestand nur vom eigentlich Berechtigten an der Karte erfüllt werden kann.⁸⁰ Es kann sich

⁷⁹ AMMANN Matthias; Sind Phishing-Mails strafbar?; AJP 2006 S. 195 ff.

⁸⁰ STRATENWERTH Günter; Schweiz. Strafgesetzbuch – Besonderer Teil I; § 16 N 26

also nur strafbar machen, wer die verwendete Karte mit dem Einverständnis der Kartenorganisation oder einer sie vertretenden Partei erhalten hat.⁸¹

Da der Täter beim Skimming weder eine Einwilligung der Kartenorganisation noch eine des Berechtigten hat, ist Art. 148 StGB nicht anwendbar.

3.2.7 Unbefugtes Beschaffen von Personendaten – Art. 179^{novies} StGB

Hinsichtlich den grundsätzlichen Ausführungen wird auf Kapitel 2.2.7 verwiesen.

Analog zum Phishing fallen auch die beim Skimming verwendeten Daten (PIN-Code und Kontoinformationen der Zahlkarte) nicht unter den Begriff der besonders schützenswerte Personendaten und auch nicht unter den Begriff der Persönlichkeitsprofile und erfüllen somit den Straftatbestand von Art. 179^{novies} StGB nicht.

Auch ein detailliertes Auslesen dieser Daten oder deren Einsatz an einem Automaten erfüllen den Tatbestand nicht, zumal sie bezüglich dem betroffenen Kontoinhaber nur Informationen über die maximale Bezugslimite und allenfalls über seine letzten Bezüge zu enthüllen vermögen.

3.2.8 Urkundenfälschung – Art. 251 StGB

Bezüglich den grundsätzlichen Ausführungen wird auf Kapitel 2.2.8 verwiesen. Die Daten auf der vom Kunden rechtmässig verwendeten Zahlkarte fallen gemäss den dort gemachten Ausführungen unter den Urkundsbegriff gemäss Art. 110 Ziff. 5 StGB.

Es muss nun zuerst geprüft werden, ob auch bereits das Lesen dieser Zahlkarte im Rahmen des ersten Schrittes des Skimming als Urkunde qualifiziert werden kann. Dies kann jedoch aufgrund der nachfolgenden Erläuterungen rasch verneint werden.

Alleine das Einlesen der Daten auf der Zahlkarte in ein Lesegerät erfüllt die für die Urkunde notwendige Perpetuierungsfunktion nicht, da diese Lesegeräte nicht gegen unbefugte Zugriffe oder Veränderungen spezifisch geschützt sind. Jede Person mit Zugriff auf das Lesegerät könnte die entsprechenden Daten löschen oder verändern.

Weiter mangelt es beim Einlesen auch der Beweiskraft der Daten. Die im Lesegerät aufgezeichneten Daten müssen zuerst auf einen Magnetstreifen kopiert und gemeinsam mit dem PIN-Code eingesetzt werden um dann erst im rechtlich erheblichen Sinne ihre Beweiskraft entfalten zu können.

Nachdem der erste Schritt des Skimming nicht für den Tatbestand der Urkundenfälschung in Frage kommt, ist das weitere Vorgehen im zweiten Schritt detaillierter unter diesem Aspekt zu prüfen.

Da die auf der Zahlkarte vorhandenen Daten – wie erwähnt – die Eigenschaften einer Computerurkunde erfüllen, stellt das Kopieren dieser Daten auf einen leeren Magnet-

⁸¹ STRATENWERTH Günter; Schweiz. Strafgesetzbuch – Besonderer Teil I; § 16 N 27

streifen einer anderen Karte eine klassische Urkundenfälschung dar. Dies jedoch nur dann, wenn sichergestellt ist, dass die kopierten Daten nicht einfach für jedermann zugänglich sind. Dies wird durch die Sicherung der Daten mittels PIN-Code erreicht.

Eine falsche, d.h. eine unechte Computerurkunde liegt vor, wenn diejenige Person, welche die Dateneingabe oder –registrierung veranlasst hat, nicht mit jener identisch ist, die vorab gegen aussen als Aussteller und somit als Garant für ihre Richtigkeit in Erscheinung tritt.⁸² Dies ist explizit bei unrechtmässig duplizierten (kopierten) Daten von Magnetstreifen bei Zahlkarten der Fall.⁸³

Konkret wird durch den Täter eine unechte Urkunde hergestellt, indem er den Anschein erweckt, die Daten würden von einem anderen Urheber stammen und er somit über die wahre Identität des Urhebers täuscht.⁸⁴ Durch Datenverarbeitungsanlagen erstellte und fixierte Erklärungen – wie sie die Daten auf einem Magnetstreifen darstellen – gelten auch deshalb als Urkunden, weil sie normalerweise dem angegebenen Aussteller rechtswirksam zugerechnet werden können.⁸⁵ Mit dem Kopieren dieser Daten auf einen neuen Magnetstreifen und dem anschliessenden Einsatz des ausspionierten PIN-Codes täuscht der Täter über den eigentlichen Urheber der kopierten Daten.

Davon ausgehend, dass die kopierte Zahlkarte und der PIN-Code von der gleichen Person auch verwendet wird, gilt der Gebrauch einer falschen Urkunde als mitbestrafte Nachtat zur eigentlichen Urkundenfälschung.⁸⁶

Auf der subjektiven Seite verlangt Art. 251 StGB nebst Vorsatz ein Handeln in Schädigungs- oder Vorteilsabsicht. Im Zusammenhang mit dem Skimming steht klar die Vorteilsabsicht des Täters im Vordergrund. Als unrechtmässiger Vorteil gilt dabei gemäss Rechtsprechung jede Besserstellung, wobei die Besserstellung vermögensmässiger oder sonstiger Natur sein kann.⁸⁷ Unrechtmässig ist ein Vorteil dann, wenn er rechtswidrig ist oder wenn der Täter darauf keinen Anspruch hat.⁸⁸

Zusammenfassend kann festgestellt werden, dass das Erstellen eines Karten-Duplikates – wie es beim Skimming üblich ist – den Tatbestand von Art. 251 StGB erfüllt. Die Frage der Konkurrenzen wird im nachfolgenden Kapitel behandelt.

3.2.9 Konkurrenzen

Der erste Schritt des Skimming – das Einlesen der Daten und die Beschaffung des PIN-Codes – ist gemäss Kapitel 3.2.2 eine unbefugte Datenbeschaffung und somit nach Art. 143 StGB strafbar.

⁸² BSK StGB II – BOOG Markus; Art. 251 N 80

⁸³ SCHMID Niklaus; Computer- sowie Check- und Kreditkarten-Kriminalität; § 3 N116

⁸⁴ BSK StGB II – BOOG Markus; Art. 251 N 3

⁸⁵ BSK StGB II – BOOG Markus; Art. 251 N 4

⁸⁶ BSK StGB II – BOOG Markus; Art. 251 N 74

⁸⁷ BSK StGB II – BOOG Markus; Art. 251 N 93

⁸⁸ BSK StGB II – BOOG Markus; Art. 251 N 95

Der zweite Schritt des Skimming – das Kopieren der Daten auf einen Magnetstreifen und die Verwendung dieser und des PIN-Codes mit dem Ziel der unrechtmässigen Bereicherung – erfüllt hingegen mehrere Straftatbestände.

Die Daten auf dem Magnetstreifen der Zahlkarte gelten als Computerurkunde nach Art. 110 Ziff. 5 StGB. Mit dem unrechtmässigen Kopieren dieser Daten auf einen neuen Magnetstreifen wird eine unechte Urkunde erstellt. Diese Handlung ist – subjektiver Tatbestand vorausgesetzt - gemäss den Ausführungen in Kapitel 3.2.8 nach Art. 251 StGB als Urkundenfälschung zu qualifizieren und somit strafbar.

Der in Bereicherungsabsicht erfolgende Einsatz des kopierten Magnetstreifens unter gleichzeitiger Verwendung des ausspionierten PIN-Codes an einem Automaten zur Erreichung einer Vermögensverschiebung zum Schaden eines anderen erfüllt gemäss Kapitel 3.2.5 den Straftatbestand von Art. 147 StGB. Dieser steht – analog beispielsweise zum Betrug nach Art. 146 StGB – angesichts der unterschiedlichen Rechtsgüter in echter Konkurrenz zur Urkundenfälschung nach Art. 251 StGB.⁸⁹

Unter bestimmten Voraussetzungen kann die Vorgehensweise des Skimming allenfalls auch den Tatbestand des Diebstahls nach Art. 139 StGB erfüllen. Da jedoch Sinn und Zweck des Skimming in der Manipulation der Datenverarbeitung zum erhältlich machen von Bargeld oder anderen Leistungen besteht, geht der Tatbestand des Art. 147 StGB dem Diebstahlstatbestand vor.⁹⁰ Somit ist im Falle des Skimming nebst Art. 251 StGB noch die alleinige Strafbarkeit nach Art. 147 StGB gegeben.⁹¹

3.3 Fallbeispiel 1: Bancomat-Skimming

3.3.1 Sachverhalt⁹²

Im Zeitraum vom 30. November 2004 bis 08. März 2005 präparierte G.S., rumänischer Staatsangehöriger, ohne Domizil in der Schweiz, zuerst in Bern, anschliessend in Solothurn, Olten, Luzern und in Lugano verschiedene Geldausgabegeräte der UBS AG, der Bank Coop und der Valiant Bank. Dabei installierte er jeweils ein Datenlesegerät beim Kartenschlitz der jeweiligen Bancomaten und eine Videokamera mit Aufzeichnungsfunktion oberhalb der Tastatur der Automaten.

Im fraglichen Zeitraum gelang es G.S. mittels den eingesetzten Gerätschaften die Kartendaten von 44 Personen zu kopieren und deren PIN-Code auszuspionieren. Anschliessend erstellte er Kartendoubletten indem er die Daten auf neue Magnetstreifen kopierte und diese an verschiedenen Geldausgabegeräten in Bern, Olten und Lugano gemeinsam mit den jeweiligen PIN-Codes zum Bezug von Bargeld verwendete. So gelangen ihm unrechtmässige Geldbezüge in der Höhe von rund CHF 65'000.

Anlässlich einer Routinekontrolle der Kantonspolizei TI wurden bei G.S. die Gerätschaften zum Skimming vorgefunden worauf er in Untersuchungshaft versetzt wurde.

⁸⁹ STRATENWERTH Günter; Schweiz. Strafgesetzbuch – Besonderer Teil I; § 16 N 20

⁹⁰ BSK – StGB II; NIGGLI Marcel Alexander/RIEDO Christof; Art. 139 N 50

⁹¹ SCHMID Niklaus; Computer- sowie Check- und Kreditkarten-Kriminalität; § 7 N151

⁹² Untersuchungsrichteramt III Bern-Mittelland; Fall-Nr. U 05 1056

Nach der Auswertung der vorgefundenen Kartendaten konnten mit Unterstützung der betroffenen Finanzinstitute die 44 Karteninhaber ausfindig gemacht und die einzelnen Tatorte rekonstruiert werden. Als zuständiger Gerichtsstand übernahm der Kanton Bern die Weiterführung des Verfahrens.

Die betroffenen Finanzinstitute übernahmen den Schaden der betroffenen Karteninhaber und beteiligten sich als Zivilpartei im Strafverfahren. Am 10. August 2006 wurde G.S. schuldig gesprochen wegen mehrfachen, gewerbsmässigen betrügerischem Missbrauchs einer Datenverarbeitungsanlage. Er wurde zu 18 Monaten Gefängnis bedingt, fünf Jahren Landesverweisung unbedingt und zudem zur Rückzahlung des verursachten Schadens verurteilt.⁹³

3.3.2 Strafrechtliche Würdigung

Der zuerst im Kanton Bern für das Verfahren zuständige Untersuchungsrichter hatte eine Strafuntersuchung wegen unbefugter Datenbeschaffung (Art. 143 StGB) und wegen betrügerischem Missbrauch einer Datenverarbeitungsanlage eröffnet.

In einem in diesem Zusammenhang vom Kanton Solothurn übernommenen Skimming-Fall war noch ein Verfahren wegen Diebstahls (Art. 139 StGB) und in einem anderen wegen Betruges (Art. 146 StGB) gegen G.S. eröffnet worden.

Im Verlaufe der Untersuchung wurde das Verfahren wegen Diebstahl aufgehoben. Die entsprechende Begründung des zuständigen Verfahrensleiters lautete, dass wo ein An eignungsdelikt mittels Computerbetrug begangen wird Art. 147 StGB Vorrang vor Diebstahl beanspruchen würde.

Auch das Verfahren wegen Betruges wurde aufgehoben. Die diesbezügliche Begründung lautete, dass der traditionelle Tatbestand des Betruges nicht geeignet sei, betrügerische Missbräuche an einem Automaten strafrechtlich zu erfassen. Der Betrugstatbestand gehe vom Bild eines Opfers aus, das durch Täuschung dazu bewogen wird, sich selbst zu schädigen. Einen Automaten könne man aber nicht täuschen und er könne auch nicht über Vermögenswerte verfügen.

Vor Abschluss der Untersuchung wurde dann auch noch das Verfahren wegen unbefugter Datenbeschaffung aufgehoben. Dies wurde damit begründet, dass wenn die unbefugte Datenbeschaffung zur Begehung eines betrügerischen Missbrauchs einer Datenverarbeitungsanlage diene, diese Datenbeschaffung als mitbestrafte Vor- beziehungsweise Nachtat gelten müsse, da Art. 147 StGB jedenfalls mittelbar auch die ungestörte Verfügungsberechtigung über Daten schütze.

3.3.3 Kommentar zum Fallbeispiel

Aufgrund der Ausführungen dieser Arbeit zum Skimming sind die Aufhebungen der Straftatbestände des Diebstahls und Betruges zu Recht erfolgt.

⁹³ Kreisgericht VIII Bern Laupen; Fall-Nr. U 05 1056; Urteil vom 10.08.2006

Bezüglich der Aufhebung des Tatbestandes von Art. 143 StGB muss ergänzt werden, dass bei G.S. keine Daten vorgefunden wurden, welche nicht bereits mittels Kartendubletten auch an Geldautomaten eingesetzt worden waren. Somit standen in diesem Fall Art. 143 StGB und Art. 147 StGB in direkter Konkurrenz zu einander. Die Begründung der Aufhebung deckt sich mit den Ausführungen zur Konkurrenz von Art. 143 und 147 StGB im Kapitel 3.2.9 dieser Arbeit.

Die Subsumtion der Tathandlungen unter Art. 147 StGB ist somit auch aus Sicht dieser Arbeit korrekt.

Hingegen wurde die Strafbarkeit nach Art. 251 StGB während dem ganzen Strafverfahren nie geprüft. Da bei G.S. diverse „White Cards“ – Weisse Karten mit kopierten Magnetstreifen - beschlagnahmt wurden, wäre aufgrund der vorgängigen Ausführungen im Kapitel 3.2.8 zusätzlich noch eine Strafbarkeit nach Art. 251 StGB gegeben gewesen.

3.4 Fallbeispiel 2: Skimming im Kleidergeschäft

3.4.1 Sachverhalt⁹⁴

Im Januar und Februar 2006 meldeten sich drei Kunden der PostFinance und bestritten Bargeldbezüge vom Dezember 2005 und Januar 2006 in der Höhe von jeweils ca. CHF 12'000. Nachdem festgestellt worden war, dass die bestrittenen Bezüge aller drei Kunden jeweils in Zürich, Weil am Rhein (Deutschland) und der Dominikanischen Republik erfolgt waren, wurde aufgrund der Gemeinsamkeiten der postinterne Ermittlungsdienst beigezogen.

Eine detaillierte Auswertung ergab, dass alle drei Kunden am 12.12.2005 in einem bestimmten Kleidergeschäft an der Bahnhofstrasse in Zürich eingekauft hatten. Die nachfolgenden Ermittlungen führten zur Entdeckung weiterer sechs Kunden von PostFinance, welche am gleichen Tag oder am darauffolgenden Tag in diesem Geschäft eingekauft hatten und mittlerweile ebenfalls Belastungen in Zürich, Weil am Rhein und der Dominikanischen Republik aufwiesen. Nach Rücksprache mit den betroffenen Kunden wurde eine Strafanzeige eingereicht.

Die weiteren Abklärungen der zuständigen Behörden führte zu Tage, dass J.L., dominikanischer Staatsangehöriger, welcher als Lehrling in besagtem Kleidergeschäft beschäftigt war, sämtliche der verzeichneten Verkäufe getätigt hatte. Die befragten Karteninhaber hatten alle zu Protokoll gegeben, dass J.L. vor der Verwendung der Zahlkarte im EFTPOS-Gerät, diese jeweils noch durch einen „Kartenreiniger“ gezogen hätte und als Begründung einen verschmutzten Magnetstreifen erwähnt hatte.

Gestützt auf diese Erkenntnisse wurde J.L. von der Polizei angehalten und befragt. J.L. gestand ein, mittels Lesegerät die Magnetstreifen der Kunden kopiert zu haben. Dank einer in der Decke versteckten Videokamera hatte er zudem die jeweilige PIN-Code-Eingabe aufgezeichnet. Anlässlich einer Hausdurchsuchung wurden die besagten Gerätschaften mit kopierten Daten und 6 Kartendubletten beschlagnahmt.

⁹⁴ Staatsanwaltschaft Zürich-Sihl; Fall-Nr. E-SU1/2006/657

Die weiteren Auswertungen führten zur Erkenntnis, dass J.L. im Zeitraum von Dezember 2005 bis Januar 2006 bei über 35 Personen die Daten ihrer Debitkarten kopiert und den PIN-Code ausspioniert hatte. Im Anschluss daran hatte er bereits die Daten von 20 Kunden auf die Magnetstreifen der „White Cards“ kopiert und diese in Zürich und Weil am Rhein eingesetzt und die Daten auch einem noch unbekanntem Komplizen in der Dominikanischen Republik zur Verfügung gestellt.

Gesamthaft wurde durch diese Vorgehensweise 122 unrechtmässige Bargeldbezüge mit einem Deliktsbetrag von CHF 103'000 getätigt. Die Finanzinstitute entschädigten die betroffenen Kunden umfassend. Die Strafuntersuchung gegen J.L. sowie gegen Unbekannt ist noch nicht abgeschlossen.

3.4.2 Strafrechtliche Würdigung

Die Staatsanwaltschaft Zürich-Sihl führt gegen J.L. sowie gegen Unbekannt ein Strafverfahren wegen Art. 147 StGB im Zusammenhang mit den 20 kopierten und bereits verwendeten Daten zum Bargeldbezug. Im Hinblick auf die vorgefundenen „White Cards“ wurde zudem ein Strafverfahren wegen Art. 251 StGB eröffnet. Weiter führt die Staatsanwaltschaft ein Verfahren wegen Art. 143 StGB im Bezug auf die zusätzlich vorgefundenen, aber noch nicht verwendeten Daten.

3.4.3 Kommentar zum Fallbeispiel

Aufgrund der hängigen Strafuntersuchung kann noch nicht abschliessend beurteilt werden, ob die erwähnten Straftatbestände allesamt erfüllt sind oder nicht.

Die erste rechtliche Beurteilung des zuständigen Staatsanwaltes deckt sich bezüglich der Subsumtion mit den Ausführungen dieser Arbeit. Wonach der erste Teil des Skimming – also das unrechtmässige Beschaffen der Kartendaten und des PIN-Codes – den Straftatbestand von Art. 143 StGB erfüllen. Während der Einsatz von Kartendubletten zum Bezug von Bargeld an Geldautomaten nach Art. 251 StGB und Art. 147 StGB strafbar ist.

4 Fazit

Phishing und Skimming sind im Bereich des elektronischen Zahlungsverkehrs regelmässig auftretende Deliktsformen. Der bereits heute vom Gesetzgeber zur Verfügung gestellte Strafraum reicht aus, um sämtliche Handlungen der beiden Erscheinungsformen unter Strafe zu stellen und von Amtes wegen verfolgen zu können.

Phishing ist wie folgt strafbar:

- Der Versand von Phishing-e-mails zum Erhalt vertraulicher Zugangsdaten ist nach Art. 62 MSchG und je nach Ausgestaltung des e-mails auch nach Art. 251 StGB strafbar. Gleiches gilt für die von den Phishern verwendete Internetseite.
- Die Verwendung dieser Zugangsdaten im E-Banking-System zur unrechtmässigen Bereicherung ist unter Art. 147 StGB zu subsumieren.

Skimming ist wie folgt strafrechtlich zu ahnden:

- Das Einlesen der Daten und das Ausspionieren des PIN-Codes ist eine unbefugte Datenbeschaffung und gemäss Art. 143 StGB zu bestrafen.
- Das Kopieren dieser Daten auf leere Magnetstreifen und die anschliessende Verwendung gemeinsam mit dem PIN-Code zur unrechtmässigen Bereicherung ist nach Art. 251 StGB und nach Art. 147 StGB strafbar.

4.1 Fazit zum Phishing

Der erste Teil des Phishing scheint bezüglich der Frage einer möglichen Strafbarkeit Mühe zu bereiten. Diesbezüglich sei explizit auf den Aufsatz von Matthias Ammann zum Thema „Sind Phishing-Mails strafbar?“ (AJP 2006 S. 195-2003) aber auch auf die untersuchten Straftatbestände in den Fallbeispielen unter Kapitel 2.3 und 2.4 verwiesen.

Entgegen diesen Erkenntnissen ist meiner Meinung nach der erste Teil des Phishing grundsätzlich strafbar. Im Regelfall liegt zumindest ein Verstoss gegen die Bestimmungen des Markenrechts vor. Einzige Voraussetzung dafür ist der Eintrag ins Markenregister, was bei sämtlichen bedeutenden Finanzinstituten der Fall sein wird (respektive sich jeweils rasch via www.swissreg.ch überprüfen lässt).

Glaubwürdig erstellte Phishing-e-mails mit konkreten Handlungsanweisungen können bereits als Urkundenfälschungen nach Art. 251 StGB qualifiziert werden. Enthalten sie lediglich den Link auf die Phishing-Internetseite und die Aufforderung, diesen anzuwählen, können sie immer noch nach Art. 62 MSchG bestraft werden, da die Phisher in betrügerischer Absicht unrechtmässig die Marken der betroffenen Finanzinstitute verwenden. Dabei ist Art. 62 MSchG im Sinne eines Offizialdeliktes anzuwenden, weil der Versand von Phishing-e-mails grundsätzlich gewerbsmässiger Natur sein dürfte.

Die von den Phishern verwendete Internetseite kann unter den gleichen Strafnomen wie bereits die versendeten e-mails subsumiert werden, da diese in den meisten Fällen die Anforderungen an eine unechte Computerurkunde erfüllt und immer missbräuchlich die Marke des betroffenen Finanzinstitutes verwendet.

Unbestritten – auch in der Praxis – ist die Anwendung von Art. 147 StGB für den zweiten Teil des Phishing. Die erhaltenen Daten werden in unrechtmässiger Bereicherungsabsicht unbefugt verwendet um im E-Banking-System eine Vermögensverschiebung zum Schaden des Kontoinhabers auszulösen.

Zusammenfassend kann festgehalten werden, dass es für jede Tathandlung des Phishing entsprechende Strafnormen gibt unter welche diese subsumiert werden können. Während in der Praxis die Anwendung von Art. 147 StGB für den zweiten Teil des Phishing

keine Mühe zu bereiten scheint, wird der Strafbarkeit der fraglichen e-mails und der Internetseite noch zu wenig Beachtung geschenkt.

Diese Praxis ist aus Sicht des Schreibenden fragwürdig. Es wäre gerade auch im Sinne der Prävention wünschenswert, würde bereits der bisher als lediglich straflose Vorbereitungshandlung betrachtete Versand der fraglichen e-mails konsequent strafrechtlich verfolgt werden. Die entsprechenden Strafnormen sind vorhanden und könnten (müssten) eigentlich bereits von Amtes wegen verfolgt werden.

4.2 Fazit zum Skimming

Der erste Schritt des Skimming, das in Bereicherungsabsicht erfolgende Kopieren der Daten mit gleichzeitigem Ausspionieren des PIN-Codes ist gemäss Art. 143 StGB als unbefugte Datenbeschaffung zu qualifizieren. Die Anwendung dieses Straftatbestandes ist auch in der Praxis anerkannt.

Die Verwendung der kopierten Daten gemeinsam mit dem PIN-Code an einem Automaten zum unrechtmässigen Bezug von Bargeld oder anderweitigen Leistungen ist nach Art. 147 StGB als betrügerischer Missbrauch einer Datenverarbeitungsanlage strafbar. Diese Beurteilung erfolgt auch in der Rechtspraxis grossmehrheitlich.

Das Kopieren der Daten auf einen leeren Magnetstreifen in der Absicht diesen – gemeinsam mit dem PIN-Code – an einem entsprechenden Automaten zu verwenden, erfüllt den Straftatbestand der Urkundenfälschung nach Art. 251 StGB. Die Feststellung, dass es sich bei den verwendeten Daten um eine Computerurkunde nach Art. 110 Ziff. 5 StGB handelt, hat sich gemäss Fallbeispielen in den Kapiteln 3.3 und 3.4 aber auch den weiteren Feststellungen des Schreibenden bisher nicht umfassend durchgesetzt. Die Anwendung von Art. 251 StGB dürfte in der Praxis wohl nicht daran scheitern, dass die Konkurrenzfrage nicht richtig geklärt würde, sondern vielmehr an der nicht immer offensichtlichen Frage, wann Computerdaten als Computerurkunden zu qualifizieren sind und wann nicht.

Abschliessend kann festgestellt werden, dass die strafrechtliche Würdigung des Skimming problemlos eine Subsumtion unter bestehende Straftatbestände des StGB zulässt. Während der erste Schritt als unbefugte Datenbeschaffung nach Art. 143 StGB zu würdigen ist, macht sich die Täterschaft beim zweiten Schritt wegen eines betrügerischen Missbrauchs einer Datenverarbeitungsanlage nach Art. 147 StGB sowie wegen Urkundenfälschung im Sinne von Art. 251 StGB strafbar.

Ich erkläre hiermit, dass ich die vorliegende Arbeit resp. die von mir ausgewiesene Leistung selbständig, ohne Mithilfe Dritter und nur unter Ausnützung der angegebenen Quellen verfasst resp. erbracht habe.

Aarau, 16. April 2007

.....
Markus Gisin