HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

Bachelorarbeit

Herr
Robert Richard Zahn

Begehungsweisen von Cybercrime-Delikten

Mittweida, 2022

Fakultät Angewandte Computer- und Biowissenschaften

Bachelorarbeit

Begehungsweisen von Cybercrime-Delikten

Autor:
Herr Robert Richard Zahn

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO19w2-B

Erstprüfer:
Prof. Dr. rer. nat. Dirk Labudde

Zweitprüfer:
B. Sc. Martin Klöden

Einreichung:
Mittweida, 26.08.2022

Verteidigung/Bewertung:
Mittweida, 2022

Faculty Applied Computer Sciences &
Biosciences

BACHELORTHESIS

Committing of Cybercrime

author:
Mr. Robert Richard Zahn

course of studies:
General and Digital Forensic Science

seminar group:
FO19w2-B

first examiner:
Prof. Dr. rer. nat. Dirk Labudde

second examiner:
B. Sc. Martin Klöden

submission:
Mittweida, 26.08.2022

defence/ evaluation:
Mittweida, 2022

Bibliografische Beschreibung:

Zahn, Robert Richard
Begehungsweise von Cybercrime-Delikten. - 2022. - 4, 56, 3 S.
Mittweida, Hochschule Mittweida, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2022

Referat:

Die vorliegende Arbeit befasst sich mit dem Cybercrime-Phänomen Phishing. Durch die Analyse von echten Delikten im Bereich des Phishings wird betrachtet, inwieweit das Phänomen durch das Strafgesetzbuch erfasst wird. Dafür wird sich an Paragrafen orientiert, die aus der Cybercrime-Konvention hervorgegangen sind, beziehungsweise durch diese geändert wurden und dem Bereich *Cybercrime im engeren Sinn* zugeordnet werden können. Neben einer Definition des Begriffes Cybercrime werden eine begriffliche Einordnung des Phänomens Phishing vorgenommen und die Grundzüge dieses aufgezeigt. Anschließend wird mithilfe der Delikte erörtert, welche Tatbestandsmerkmale der einzelnen Paragrafen sich bei den Delikten detektieren lassen und inwieweit die Begehungsweise Einfluss auf die detektierbaren Tatbestandsmerkmale hat. Bei der Erörterung wird auch auf den Begriff *Daten* eingegangen und welche Definition diesem innerhalb der betrachten Paragrafen zugrunde liegt.

Inhalt

Tabellenverzeichnis

Abkürzungsverzeichnis

App	Applikation
APWG	Anti-Phishing Working Group
BKA	Bundeskriminalamt
BSI	Bundesamt für Sicherheit in der Informationstechnik
com	commercial
DOS	Denial of Service
EC	Electronic Cash
E-Mails	electronic mail
OLG	Oberlandesgericht
PKS	Polizeiliche Kriminalstatistik
SMS	Short Message Service
StGB	Strafgesetzbuch
TAN	Transaktionsnummer

1 Einleitung

Im Jahr 2021 konnte die polizeiliche Kriminalstatistik (PKS) einen Anstieg von über 12 % in den Zahlen der begannen Cyber-Straftaten festhalten, während die Aufklärungsquote bei unter 30 % lag. Das Cybercrime-Bundeslagebild des Bundeskriminalamts (BKA) sieht diese Entwicklung zum einen durch die voranschreitende Digitalisierung begründet, die durch die Corona-Pandemie zusätzlich beschleunigt wurde. Mit der Verlagerung der Kriminalität zum digitalen Raum und einer höheren Anzeigebereitschaft innerhalb der Bevölkerung werden weitere Begründungen genannt. Gleichzeitig wird auch auf eine Ausbreitung von Cyber-Straftaten und die vielfältigen Möglichkeiten bietende Underground Economy hingewiesen. Begrifflich erfasst die Betrachtung des Bundeslagebildes Cybercrime im engeren Sinn [1, S. 4]. Unter diesem Begriff werden alle Straftaten zusammengefasst, die sich gegen datenverarbeitende Systeme, deren Daten selbst oder das Internet richten. Cybercrime im weiteren Sinn hingegen erfasst alle Straftaten, in denen bei der Tatbegehung derartige Systeme in irgendeiner Form eine Aufgabe erfüllt haben [2]. Demnach wird beispielsweise auch der Verkauf von Drogen über das Internet von letztgenannter Definition erfasst. Bereits 2004 trat mit der Cybercrime-Konvention ein völkerrechtlicher Vertrag des Europarates in Kraft, der die Bekämpfung von Cyberkriminalität zur Aufgabe hat. Deren unterzeichnende Staaten haben sich verpflichtet, den Inhalt im innerstaatlichen Recht umzusetzen, darunter auch Deutschland [3]. Das Strafrecht betreffende Maßnahmen werden unter anderem in Kapitel zwei Abschnitt eins der Konvention gelistet und beinhalten sowohl Cybercrime im engeren als auch weiteren Sinn [4, S. 3-7]. Aufbauend auf diesen Vorgaben wurde durch das 41. Strafrechtsänderungsgesetz aus dem Jahr 2007 das Strafgesetz angepasst. Darüber hinaus wurde mit § 202d im Jahr 2015 die Datenhehlerei als Tatbestand aufgenommen. Entsprechend der Betrachtungsweise des Bundeslagebilds *Cybercrime im engen Sinn* beinhaltet nach diesen Gesetzesänderungen das Strafgesetzbuch (StGB) folgende Paragrafen:

- § 149 – Vorbereitung der Fälschung von Geld und Wertzeichen
- § 202a – Ausspähen von Daten
- § 202b – Abfangen von Daten
- § 202c – Vorbereitung des Ausspähens und Abfangens von Daten
- § 202d – Datenhehlerei
- § 263a – Computerbetrug
- § 269 – Fälschung beweiserheblicher Daten
- § 270 – Täuschung im Rechtsverkehr bei der Datenverarbeitung
- § 271 – Mittelbare Falschbeurkundung
- § 274 – Urkundenunterdrückung
- § 303a – Datenveränderung
- § 303b – Computersabotage [5, S. 36-37]

Wie gezeigt gibt es sowohl auf nationaler als auch internationaler Ebene Bemühungen Cyberkriminalität entgegenzutreten. Dennoch bekräftigen die eingangs aufgeführten Zahlen, dass das Phänomen Cybercrime auch weiterhin ein Problem innerhalb der Gesellschaft darstellen wird. Während der Begriff Cybercrime in der Literatur statisch definiert ist, warnt das BKA an anderer Stelle vor der Dynamik, die dieser Deliktbereich aufweist und welche Professionalität mit wirtschaftlichen Strukturen dahinter steht [2].

Teil dieser Struktur ist der bereits erwähnte Begriff *Underground Economy*. Darunter werden Dienstleistungen und Plattformen zusammengefasst, über die sich Cyber-Kriminelle Wissen, Programme sowie Daten austauschen können [1, S. 8]. Ein Bestandteil der Underground Economy im Bereich des Datenaustausches sind *Data-Leaks*. Mit diesem Begriff wird das unberechtigte Abgreifen von Anmeldungs- und Zahlungs- sowie sonstigen personenbezogenen Information beschrieben, die anschließend in Form von Datensätzen gebündelt und zum Verkauf angeboten werden [1, S. 12]. Neben dem Verkauf der Informationen wird durch den Begriff *Doxing* das öffentlich zugänglich machen solcher Informationen verstanden [6]. Eine 2021 häufig genutzte Angriffsform für das Erlangen von entsprechenden Daten war das *Phishing* [1, S. 13].

Das Wort *Phishing* ist eine Zusammensetzung aus den Begriffen *password* und *fishing* und beschreibt das Erlangen von entsprechenden Daten mit Hilfe technischer Kommunikationswege, zum Beispiel durch E-Mails. Um die Opfer zu einer Herausgabe zu bewegen, werden Sachverhalte vorgetäuscht [7]. Die E-Mails führen die Empfänger über Links zu Websites, auf denen sie diese Informationen preisgeben sollen. Eine weitere bekannte Form des Phishings stellt das Versenden von Schadsoftware dar. Diese befindet sich im Anhang der E-Mail, die von dem Empfänger geöffnet werden soll. Unter dem Begriff *Drive-by-Infection* wird als Verbreitungsmöglichkeit von Schadsoftware auch das automatische Herunterladen und Installieren beim Besuchen einer Website erfasst. Dies wird durch Sicherheitslücken im Browser des E-Mail-Empfängers ermöglicht [8, S. 28-30]. Neben dem Versenden von E-Mails stellt das *Smishing* eine Sonderform des Phishings dar und leitet sich aus den Wörtern *SMS* und *Phishing* ab. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) griff die Thematik auf und bemerkte im Frühjahr 2021 versendete SMS, die eine Paketsendung bzw. eine Rücksendung zum Absender ankündigen und einen Link enthalten. Der Link führt zu App-Downloads, über den die als App getarnte Schadsoftware verbreitet wird oder zu Phishing-Websites. Seit Herbst 2021 verzeichnet das BSI, dass auch Sicherheitsupdates für das Telefon und angeblich empfangene Sprachnachrichten über die Links angeboten werden [9].

Um Identitätsdiebstahl und Betrug zu bekämpfen, hat sich 2003 die Anti-Phishing Working Group (APWG), ein internationaler Zusammenschluss aus Strafverfolgungsbehörden, Forschern, Finanz- und Technologieunternehmen und weiteren Organisationen, gegründet [10]. In ihrem *Phishing Activity Trends Report* für das erste Quartal 2022 konnte die APWG zum ersten Mal seit Beginn der Aufzeichnung für ein Quartal über eine Million, von ihren Mitgliedern gemeldeten Phishing-Angriffe verzeichnen. Von unter 250.000 Angriffen im April 2021 stieg die Anzahl an monatlich gemeldeten Fällen in einem Jahr auf über

350.000 im März 2022 [11, S. 2]. Diese Zahlen lassen die Vermutung zu, das Phishing weiterhin ein relevantes Phänomen im Bereich der Cyberstraftaten bleiben wird.

Bereits 2004 gab es strafrechtliche Einordnungen des Phänomens Phishing. Unter dem Titel *Phishing for Money* erschien in der Zeitschrift *Multimedia und Recht* ein Beitrag auf Grundlage von Straftaten im Bereich des Online-Bankings in Zusammenhang mit Phishing [12]. Allerdings haben sich sowohl das Strafrecht als auch das Phänomen selbst seither verändert.

Ziel dieser Arbeit ist es, das Phänomen Phishing sowie das StGB in ihrer aktuellen Form zu untersuchen und aufzuzeigen, inwieweit sich die Begehungsweise von Phishing auf die Erfassung durch das StGB im Bereich Cybercrime im engeren Sinn auswirkt. Dafür werden die genannten Rechtsvorschriften mit Begehungsweisen begangener Phishing-Straftaten gegenübergestellt. Der Begriff *Begehungsweise* erfasst das Vorgehen einer Täterschaft bei der Verwirklichung einer Straftat, einschließlich der Vor- und Nachbereitung der Tat [13]. Im Rahmen dieser Arbeit wird sich bei der Gegenüberstellung auf das bloße Phishing als Bestandteil einer Begehungsweise einschließlich der Verwendung erlangter Informationen konzentriert. In einem Praktikum bei der Kriminalpolizeiinspektion Görlitz wurden dafür mehrere Begehungsweisen von echten Delikten im Bereich der Cyberkriminalität aus den zugehörigen Akten herausgeschrieben und in einem Praktikumsbericht erfasst. [14]. Angaben, die Rückschlüsse zu beteiligten Personen zulassen, wurden geändert. Eine vollständige Zitation aller beschriebener Sachverhalte befindet sich in den Anlagen. Innerhalb der jeweiligen Norm wird der objektive Tatbestand betrachtet. Dieser beschreibt mit Hilfe einzelner Tatbestandsmerkmale die äußere Gestalt der erfassten Tat [15, § 8 Rn. 3]. Der subjektive Tatbestand erfasst hingegen den innerlichen Zustand des Täters oder der Täterin und beschreibt das Motiv, die Vorstellung, die Absicht und die Gesinnung [15, § 8 Rn. 16]. Da diese Merkmale nicht aus den Akten hervorgegangen sind und somit eine abschließende Bewertung dieses Teils des Tatbestandes nicht möglich ist, wird in dieser Arbeit lediglich auf den objektiven Tatbestand eingegangen. Bei einer Prüfung, ob ein Sachverhalt den objektiven Tatbestand einer Norm erfüllt, wird dieser subsumiert. Dabei wird betrachtet, welche Merkmale durch den Sachverhalt erfüllt werden [15, § 11 Rn. 7].

Im Rahmen der zentralen Zielstellung sollen mit dieser Vorgehensweise folgende Fragen beantwortet werden:

- Welche Tatbestände erfassen Phishing?
- Hat die Begehungsweise von Phishing und eine mögliche Varianz dieser Einfluss auf die Tatbestandsmerkmale die detektierbar sind?
- Welche Erkenntnisse lassen sich daraus gewinnen?

Zentrales Element dieser Arbeit und des Phänomens Phishing ist der Begriff *Daten*. Neben der Beantwortung der vorangegangenen Fragen wird in dieser Arbeit auch betrachtet, wie das StGB mit dem Begriff *Daten* umgeht. Die verschiedenen Definitionen und

Auslegungen werden dafür miteinander verglichen. Zunächst wird in Kapitel 2 auf die einzelnen Rechtsnormen eingegangen. In Kapitel 3 erfolgt anschließend eine genauere Betrachtung des Phänomens Phishing, bevor in den Kapiteln 4 und 5 die Subsumtion der Sachverhalte unter die einzelnen Rechtsnormen erfolgt.

2 Objektive Tatbestände im StGB

Nachfolgend werden alle zu betrachtenden Normen aus Sicht ihrer objektiven Tatbestände erläutert. Dabei wird sich am Münchener Kommentar zum StGB orientiert und eine Abgrenzung zwischen Tatobjekt und Tathandlung vorgenommen. Da die Begehungsweisen keine Geld- und Wertzeichenfälschung zum Inhalt haben, wird § 149 bei der weiteren Betrachtung nicht berücksichtig.

2.1 § 202a Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.
[16, 202a]

Der § 202a hat den Schutz des Datengeheimnisses zur Aufgabe. Dieser Schutz setzt bei einem Geheimhaltungsinteresse des Verfügungsberechtigten der Daten ein. Ausschlaggebend für die Verfügungsberechtigung ist das Recht an dem gedanklichen Inhalt der Daten [17, 2]. Für das Tatobjekt ist die Definition des Begriffes *Daten* von Bedeutung, die in Abs. 2 vorliegt. Nach Abs. 2 schützt die Rechtsnorm nur übermittelte oder gespeicherte Informationen, die elektronisch, magnetisch oder anderweitig nicht wahrnehmbar vorliegen. Ihr Inhalt darf dabei ohne technische Hilfsmittel nicht ersichtlich sein [17, 15]. Weitere Merkmale sind die besondere Sicherung gegen unberechtigten Zugang und die Eigenschaft, dass die Daten nicht für die Täterschaft bestimmt sind [17, 10–53]. Die Tathandlung wird durch das unbefugte Verschaffen des Zugangs zu Daten dargestellt [17, 54–68].

2.2 § 202b Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.
[16, 202b]

Der § 202b bezieht sich wie auch § 202a auf das Datengeheimnisses und möchte das Rechtsgut der nichtöffentlichen Kommunikationen schützen [18, Rn. 2]. Innerhalb der Norm orientiert sich der Datenbegriff an den Erläuterungen aus § 202a Abs. 2 [18, Rn. 7]. Dies gilt ebenfalls für das Merkmal der Bestimmtheit der Daten, wobei diese auch die Empfänger der Daten einschließen kann [18, Rn. 8]. Im Mittelpunkt des § 202b steht die nichtöffentliche Datenübermittlung. Während dieser Kommunikation müssen die Daten abgefangen wurden sein [18, Rn. 9]. Alternativ kann auch das Abfangen von Daten aus einer elektromagnetischen Abstrahlung genannt werden, wobei die Abstrahlung nicht zwingend aus einer Datenübertragung resultieren muss [18, Rn. 13]. Innerhalb der Tathandlung wird das Verschaffen der Daten für sich oder einem anderen als Merkmal definiert. Auch hier wird, angelehnt an § 202a, sich der Kontrolle über die Daten zu verschaffen, verstanden [18, Rn. 16]. Zusätzlich dazu müssen technische Mittel zum Verschaffen eingesetzt wurden sein, wobei es keine Einschränkung bezüglich konkreter Mittel gibt [18, Rn. 18].

2.3 § 202c Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er
1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,
herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) § 149 Abs. 2 und 3 gilt entsprechend.
[16, 202c]

Der § 202c schütz, wie seine Vorgänger auch, das Rechtsgut des Datengeheimnisses, wobei hier Vorbereitungshandlungen erfasst werden sollen, die dieses Rechtsgut gefährden [19, Rn. 2]. Im Rahmen der Tatobjekte muss angemerkt werden, dass die Passwörter und Sicherungscodes auch in visuell wahrnehmbarer Form vorliegen können. Aus dem Begriff *Ermöglichen* ergibt sich zudem, dass diese bei der Begehung gültig sein müssen. Die Beschaffung dieser durch technische Hilfsmittel ist nicht notwendig [19, Rn. 10]. Beim Tatobjekt *Computerprogramm* liegt die Problematik der Einordnung dieses nach seiner Zweckbestimmung vor, sofern es nicht zweifellos für eine illegale Verwendung erstellt wurde [19, Rn. 13]. Dies betrifft vor allem Programme, die sowohl für legale als auch illegale Zwecke eingesetzt werden können und beispielsweise im Bereich der Netzwerkadministration Aufgaben wie das Überwachen von Verbindungen erfüllen [19, Rn. 14]. Dieser doppelte Zweck erfüllt nicht den objektiven Tatbestand des § 202c. Zur Bewertung eines Programms ist es erforderlich, dass die Ziele des Programmierers bewertet werden, die sich auch in der äußerlichen Erscheinung des Programmes widerspiegeln müssen [19,

16]. Im Bereich der Tathandlungen werden verschiedene Möglichkeiten genannt. Das Herstellen erfasst das Abschließen des Fertigungsvorgangs, sodass das Tatobjekt einsatzbereit wird. Beim Verschaffen wird, wie auch in den §§ 202a und b das Erlangen der Verfügungskontrolle verstanden. Für die Erfüllung des Verkaufens ist es notwendig, dass diese Handlung in einem Vertrag festgehalten wurde. Das Erlangen der Kontrolle ist nicht notwendig. Beim Überlassen wird der Besitz ohne die Verfügungskontrolle zu einer anderen Person übertragen. Das Verbreiten hat zum Ziel, den Nutzerkreis durch mindestens einmalige Weitergabe zu vergrößern und beim Zugänglichmachen wird die Möglichkeit des Zugriffs geschaffen [19, Rn. 17-23].

2.4 § 202d Datenhehlerei

(1) Wer Daten (§ 202a Absatz 2), die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe.

(3) Absatz 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu gehören insbesondere

1. solche Handlungen von Amtsträgern oder deren Beauftragten, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen, sowie

2. solche beruflichen Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen, mit denen Daten entgegengenommen, ausgewertet oder veröffentlicht werden.

[16, 202d]

Inhalt dieser Norm ist, wie auch bei den §§ 202a-c, das Datengeheimnis. Das Ziel ist es, bereits rechtswidrig erlangte Daten zu schützen und eine Weitergabe zu verhindern, wenn durch eine Vortat der Verfügungsberechtigte der Daten bereits die Kontrolle verloren hat [20, Rn. 2a]. Im Bereich des Tatobjektes wird auf die Erläuterung in § 202a Abs. 2 verwiesen. Ein weiteres Merkmal besteht in der nicht allgemeinen Zugänglichkeit der Daten. Daten sind allgemein zugänglich, wenn diese für jede Person auf einem Weg rechtmäßig verfügbar sind. Zudem müssen die Daten im Vorfeld rechtswidrig erlangt wurden sein, wobei hier jeder Tatbestand des StGB geeignet ist [20, Rn. 10-13]. Bei den Tathandlungen dieser Norm wurde sich an § 202c orientiert. Unter dem Verschaffen wird die Übertragung der Verfügungskontrolle verstanden. Beim Überlassen geht der Besitz der Daten an eine andere Person über, ohne dass zugleich automatisch die Verfügungskontrolle übertragen wird. Das Verbreiten der Daten hat zum Ziel, den Personenkreis, der Zugang zu den Daten hat, zu vergrößern und das Zugänglichmachen erfasst das bloße Ermöglichen eines Zugriffs auf die Daten. Wegen der Streitfrage aus § 202c, ob der bloße Kaufvertrag über

Daten bereits für den Verkauf ausreicht, da bei einer Zustimmung in dieser Richtung noch nicht das zu schützende Datengeheimnis angegriffen wird, wurde auf eine Übernahme dieser Handlung aus § 202c verzichtet [20, Rn. 18-23].

2.5 § 263a Computerbetrug

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) § 263 Abs. 2 bis 6 gilt entsprechend.

(3) Wer eine Straftat nach Absatz 1 vorbereitet, indem er

1. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt oder

2. Passwörter oder sonstige Sicherungscodes, die zur Begehung einer solchen Tat geeignet sind, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(4) In den Fällen des Absatzes 3 gilt § 149 Abs. 2 und 3 entsprechend.

[16, 263a]

Das zu schützende Rechtsgut dieser Norm ist das Vermögen einer einzelnen Person [21, Rn. 1]. Erfasst werden Begehungsweisen, bei denen auf einen Datenverarbeitungsvorgang eingewirkt wird, wodurch eine Vermögensschädigung einer Person eintritt [21, Rn. 2]. Dabei wird sich am § 263 orientiert, wobei die aus einem Irrtum resultierende Vermögensverfügung durch den veränderten Datenverarbeitungsvorgang ersetzt wird [21, Rn. 5]. Innerhalb der Norm wird der Begriff *Daten* genannt. Da dieser nicht näher eingegrenzt wird, muss sich bei der Begriffsdeutung an Auslegungsgrundsätzen orientiert werden. Danach können alle codierten Informationen, die eine maschinenlesbare Form aufweisen, unter diesem Begriff zusammengefasst werden [21, Rn. 22-23]. Unter dem zweiten zentralen Begriff *Datenverarbeitungsvorgang* werden die Eingabe von Daten, deren Verarbeitung mittels Programmen und die anschließende Ausgabe von Ergebnissen zusammengefasst [21, Rn. 25]. Innerhalb der Tathandlung wird sämtliches Einwirken auf diese drei Phasen genannt. Das Einwirken auf die Eingabephase wird durch die Verwendung unrichtiger oder unvollständiger Daten eingeschlossen. Die unrichtige Gestaltung eines Programms deckt die Verarbeitungsphase ab und durch den sonstige unbefugten Ablaufeingriff wird auch die Ausgabephase eingeschlossen. Als weitere Tathandlung, die sich nicht explizit einer der drei Phasen zuordnen lässt, wird noch die unbefugte Verwendung von Daten genannt [21, Rn. 32]. Beim Begriff *Unbefugt* existieren verschiedenen Auslegungen. Nach der überwiegend vorherrschenden Meinung bedarf der Begriff einer betrugsähnlichen Deutung, wobei eine täuschungsähnliche Handlung vorliegen muss. Diese

Argumentation wird unter anderem durch die Anlehnung der Norm an § 263 gestützt. Zwar fehlt es beim Computerbetrug an einer täuschbaren Person, aufgrund dessen soll aber auf einer Interpretation des Verhaltens in Bezug auf eine täuschungsähnliche Handlung abgezielt werden [21, Rn. 78-79]. Zudem wird von der Norm der Eintritt eines Vermögensschadens vorausgesetzt. Dieser muss direkt aus dem veränderten Ergebnis des Datenverarbeitungsvorgangs resultieren. Durch einen Vergleich der Vermögenswerte zwischen den Zeitpunkten vor und nach dem Vorgang wird die Minderung bemessen [21, Rn. 179]. Ein weiterer Bereich des § 263a stellen die Vorbereitungshandlungen nach Abs. 3 dar. Beim ersten Tatobjekt *Computerprogramme* kann auf die gleiche Problematik wie in § 202c verwiesen werden. Auch hier muss sich aus der Gestaltung des Programms ein eindeutiger Zweck ergeben [21, Rn. 189]. Auch bei dem zweiten Tatobjekt *Passwörter und Sicherungscodes* kann auf § 202c verwiesen werden, wobei diese für die Begehung der Tat geeignet sein müssen [21, Rn. 196]. Bei den Handlungen im Rahmen einer Vorbereitung werden mehrere Möglichkeiten genannt. Unter dem Verschaffen wird auch hier das Erlangen der Verfügungskontrolle verstanden. Das Herstellen beschreibt das Abschließen des Fertigungsprozesses, sodass eine Verwendung möglich ist und das Verwahren beinhaltet, dass Programme oder Passwörter/Sicherungscodes bereitgehalten werden. Feilhalten beschreibt das Anbieten zum Verkauf und ein Überlassen überträgt die Möglichkeit des Gebrauchs, die zeitlich begrenzt sein kann [21, Rn. 199-203].

2.6 § 269 Fälschung beweiserheblicher Daten

(1) Wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, daß bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) § 267 Abs. 3 und 4 gilt entsprechend.

[16, 269]

Durch den § 269 sollen den Rechtsverkehr betreffende Entscheidungen von Personen geschützt werden. Betroffene Personen sollen nicht auf Grundlager falscher Erklärungen eine für sie schädliche Entscheidung treffen. Damit orientiert sich § 269 an § 267 [22, Rn. 1]. Im Mittelpunkt steht dabei die Datenurkunde. Eine Urkunde stellt eine Rechtswirkung entfaltende Erklärung dar, bei der die erklärende Person erkennbar ist. Im Unterschied zur Urkunde aus § 267 tritt die Datenurkunde, die Resultat der Erklärung ist, nicht in Form von visuell wahrnehmbaren Zeichen, sondern durch einen Datensatz auf [22, Rn. 8]. Von dem Begriff *Daten* werden dabei alle codierten Informationen erfasst, die maschinell verarbeitet werden können und deren Inhalt nicht über menschliche Kommunikationswege ohne technische Hilfsmittel erfasst werden kann [22, Rn. 13]. Eine mögliche Tathandlung stellt das Speichern solcher Daten dar. Darunter werden alle Vorgänge zum Erstellen oder Bearbeiten von Daten erfasst, die eine falsche Datenurkunde zum Ergebnis haben [14, Rn. 32].

Daneben existiert die Handlung des Veränderns. Dabei erhält eine echte Urkunde einen mindestens teilweise neuen Inhalt. Die letzte mögliche Handlung umfasst das Benutzen solcher Daten. Diese wird dadurch erfüllt, dass den Geschädigten der Zugang zu den entsprechenden Daten ermöglicht wird [22, Rn. 38].

2.7 § 270 Täuschung im Rechtsverkehr bei der Datenverarbeitung

Der Täuschung im Rechtsverkehr steht die fälschliche Beeinflussung einer Datenverarbeitung im Rechtsverkehr gleich.

[16, 270]

Diese Rechtsnorm bezieht sich auf alle Tatbestände, die die Täuschung im Rechtsverkehr beinhalten und stellt diese mit der Beeinflussung von Datenverarbeitungsvorgängen gleich. Die Diskussion um die Problematik, dass nur Personen getäuscht werden können, da Datenverarbeitungsvorgänge keine beeinflussbare Vorstellungskraft besitzen, wird damit gegenstandslos [23, Rn. 1]. Eine Subsumtion der Sachverhalte wird aufgrund der bloßen Gleichstellungsfunktion dieser Rechtsnorm nicht durchgeführt. An entsprechenden Stellen wird auf diese verwiesen.

2.8 § 271 Mittelbare Falschbeurkundung

(1) Wer bewirkt, daß Erklärungen, Verhandlungen oder Tatsachen, welche für Rechte oder Rechtsverhältnisse von Erheblichkeit sind, in öffentlichen Urkunden, Büchern, Dateien oder Registern als abgegeben oder geschehen beurkundet oder gespeichert werden, während sie überhaupt nicht oder in anderer Weise oder von einer Person in einer ihr nicht zustehenden Eigenschaft oder von einer anderen Person abgegeben oder geschehen sind, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer eine falsche Beurkundung oder Datenspeicherung der in Absatz 1 bezeichneten Art zur Täuschung im Rechtsverkehr gebraucht.

(3) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen Dritten zu bereichern oder eine andere Person zu schädigen, so ist die Strafe Freiheitsstrafe von drei Monaten bis zu fünf Jahren.

(4) Der Versuch ist strafbar.

[16, 271]

Diese Norm schützt, wie auch die §§ 267 und 269, den Rechtsverkehr betreffende Entscheidungen von Personen, mit dem Unterschied, dass hier der bloße Erklärungsinhalt im Mittelpunkt steht und nicht die gesamte Authentizität der Erklärung [24, Rn. 1]. Als Tatobjekte werden zunächst öffentliche Urkunden genannt, die im Rahmen amtlicher Berechtigungen von öffentlichen Behörden oder durch Personen öffentlicher Glaubwürdigkeit innerhalb ihres jeweiligen Geschäftsbereiches erstellt wurden sind [24, Rn. 5]. Letztere sind

Personen, die aufgrund von Gesetzten oder Anordnungen befugt sind, Urkunden zu bestimmten Sachverhalten auszustellen [24, Rn. 8]. Bücher und Register können zum zweiten Tatobjekt zusammengefasst werden und beschreiben öffentliche Informationssammlungen von Behörden. Maßgeblich ist dabei, dass diese der Öffentlichkeit zugänglich sind und die Beweiskraft durch die Angabe einer Gewähr auf Richtigkeit gegeben ist [24, Rn. 45]. Durch die Erweiterung der Norm um das dritte Tatobjekt *Dateien* wird auch die Beurkundung von Sachverhalten in einer nicht unmittelbar wahrnehmbaren Form, einem Datensatz erfasst [24, Rn. 47]. Im Bereich der Tathandlung wird unter dem Begriff *Bewirken* jede Handlung der Täterschaft verstanden, die eine Falschbeurkundung zur Folge hat [24, Rn. 50]. In Bezug auf das hier zu betrachtende Tatobjekt *Dateien* wird als Tathandlung das Bewirken einer Speicherung genannt. Damit sich die Handlung ausschließlich auf einer Beurkundung bezieht und nicht das äußerliche Einwirken und Speichern von Veränderungen erfasst wird, ist unter dieser Handlung ausschließlich das Veranlassen von Amtsträgern zur Speicherung von Veränderungen zu verstehen [24, Rn. 53]. Zusätzlich nennt die Norm in Abs. 2 noch eine alternative Handlungsmöglichkeit. Im Rahmen der Tathandlung des Gebrauchens kann sich an § 269 orientiert werden. Dabei wird die Handlungsmodalität erfasst, dass die Täterschaft gegenüber den Geschädigten auf entsprechende Einträge in zum Beispiel digitalen Registern verweist. Wie die Daten entstanden sind, ist unerheblich [24, Rn. 57-58].

2.9 § 274 Urkundenunterdrückung

(1) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer
1. eine Urkunde oder eine technische Aufzeichnung, welche ihm entweder überhaupt nicht oder nicht ausschließlich gehört, in der Absicht, einem anderen Nachteil zuzufügen, vernichtet, beschädigt oder unterdrückt,
2. beweiserhebliche Daten (§ 202a Abs. 2), über die er nicht oder nicht ausschließlich verfügen darf, in der Absicht, einem anderen Nachteil zuzufügen, löscht, unterdrückt, unbrauchbar macht oder verändert oder
3. einen Grenzstein oder ein anderes zur Bezeichnung einer Grenze oder eines Wasserstandes bestimmtes Merkmal in der Absicht, einem anderen Nachteil zuzufügen, wegnimmt, vernichtet, unkenntlich macht, verrückt oder fälschlich setzt.
(2) Der Versuch ist strafbar.
[16, 274]

Nach § 274 wird das Recht auf Beweiserbringung mittels Urkunden, technischen Aufzeichnungen und beweiserheblichen Daten geschützt [25, Rn. 1]. Nachfolgend soll die Norm in Bezug auf Abs. 1 Nr. 2 *beweiserhebliche Daten* erläutert werden. Zunächst verweist die Norm beim Begriff der Daten auf § 202a Abs. 2, wonach Daten nicht unmittelbar wahrnehmbare Informationen sind. Gleichzeitig wird der Begriff der Beweiserheblichkeit genannt, weshalb ein Bezug zum § 269 hergestellt werden kann. In letzter Konsequenz bedeutet dies, dass die betreffenden Daten die Eigenschaften einer Urkunde nach § 269 erfüllen müssen. Des Weiteren wird als Merkmal eine fehlende oder eine nicht alleinige

Verfügungsberechtigung genannt. Daraus kann abgeleitet werden, dass dieses Merkmal erfüllt wird, sobald eine fremde Verfügungsberechtigung vorliegt [25, Rn. 22-23]. Im Bereich der Handlung werden vier Möglichkeiten genannt. Beim Löschen werden die Daten unwiederbringlich vernichtet und im Rahmen des Unterdrückens wird die verfügungsberechtigte Person daran gehindert, die Beweiskraft der Urkunde zu nutzen. Das Unbrauchbarmachen schränkt die Beweiskraft ein oder hebt sie auf und beim Verändern wird die Beweiskraft durch einen neuen Inhalt eingeschränkt [25, Rn. 12-14].

2.10 § 303a Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.
(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.
[16, 303a]

§ 303a ist angelehnt an den § 303 Sachbeschädigung und schützt die Unversehrtheit von Daten im Interesse der berechtigten Person gegenüber Beschädigung und Zerstörung [26, Rn. 1-3]. Für den Datenbegriff wird auf § 202a verwiesen, wonach Daten auch hier nicht unmittelbar wahrnehmbar gespeicherte oder übermittelte Daten sein müssen. Seitens der Norm wird der Begriff nicht weiter eingeschränkt. Demnach werden auch Programme vom Begriff der Daten erfasst. Um eine Kollision der Norm mit dem Grundgesetz und eine falsche Auslegung zu verhindern, wird der Begriff der Daten weiterhin durch Verfügungs- und Nutzungsbefugnisse eingegrenzt. Diese müssen bei mindestens einer anderen Person als der Täterschaft liegen. Die Befugnisse können dabei auch in eingeschränkter Form vorliegen und sowohl die Inhaber der Daten, als auch die Inhaber der Speichermedien einschließen [26, Rn. 8-9]. Als Tathandlungen werden vier Möglichkeiten genannt. Das Löschen umfasst das unumkehrbare Zerstören der Daten, wobei es unerheblich ist, ob Kopien dieser Daten vorhanden sind, da sich die Norm auf eine konkrete Version bezieht. Beim Unterdrücken besitzt die berechtigte Person mindestens vorrübergehend keinen Zugang zu den Daten. Das Unbrauchbarmachen führt dazu, dass die Daten ihrer Funktion nicht mehr nachkommen können. Das Verändern wird erfüllt, wenn die Daten inhaltlich in irgend einer Form modifiziert wurden [26, Rn. 12-15]. In Abs. 3 wird zudem im Rahmen einer Vorbereitung auf § 202c verwiesen.

2.11 § 303b Computersabotage

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er
1. eine Tat nach § 303a Abs. 1 begeht,
2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder

3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. einen Vermögensverlust großen Ausmaßes herbeiführt,

2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,

3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.

(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

[16, 303b]

Diese Norm möchte die ordnungsgemäße Funktionalität von Datenverarbeitungen schützen. Das Delikt ist dabei so ausgestaltet, dass der Datenverarbeitungsvorgang gestört und damit ein konkreter Erfolg eingetreten sein muss [27, Rn. 1-2]. Der Begriff der Datenverarbeitung ist weitläufig und umfasst jegliche Nutzung von Daten. Um eine ausufernde Auslegung zu verhindern, wird der Begriff durch die Formulierung *von wesentlicher Bedeutung* eingegrenzt. Im privaten Bereich ist zu unterscheiden, ob der Vorgang im Leben der betreffenden Person eine bedeutsame Aufgabe im Rahmen einer Erwerbstätigkeit oder anderer kultureller oder bildender Betätigungen erfüllt hat [27, Rn. 9]. Innerhalb von Abs. 1 werden drei mögliche Handlungen zusammengefasst. Bei Nr. 1 muss § 303a Abs. 1 vollständig erfüllt werden. Diese Verknüpfung erfasst das Beeinflussen von Datenverarbeitungsvorgängen durch die Veränderung von Daten. Innerhalb von Nr. 2 wird die missbräuchliche Verwendung von Daten (Definition nach § 202a Abs. 2) erfasst und durch Nr. 3 wird auch das Einwirken auf Hardware eingeschlossen [27, Rn. 11-13]. Wie auch in § 303a wird in Abs. 5 auf eine Vorbereitung nach § 202c verwiesen.

3 Das Phänomen Phishing

Wie bereits in der Einleitung dargestellt, existieren verschiedene Varianten des Phishings. Neben dem Smishing kann auch das *Spear-Phishing* als weitere Sonderform unterschieden werden. Beim klassischen Phishing werden große Mengen an E-Mails wahllos an unbekannte Personen versendet. Das Spear-Phishing hingegen erfordert eine gezielte Vorbereitung und Recherche zu einer Person, damit eine personalisierte E-Mail zu einem Sachverhalt verschickt werden kann. Dadurch soll eine höhere Glaubwürdigkeit erzielt werden [28]. Neben den Unterschieden der verschiedenen Varianten sind aber auch Gemeinsamkeiten erkennbar. Jedes Phishing hat als gemeinsames Merkmal den Kontakt zur geschädigten Person bzw. jener, die Zugang zu Informationen gewährleisten soll. Auch bei einer Installation von Schadsoftware wird im ersten Schritt Kontakt zur Person aufgebaut, die über das anzugreifende Gerät verfügt. Dies kann beispielsweise durch SMS oder E-Mail erfolgen. Anschließend werden die Personen dazu bewegt, eine gewünschte Handlung durchzuführen. Dies kann darin bestehen, eine Website aufzurufen. Um dies zu ermöglichen, bedient sich Phishing einem anderen Phänomen, dem *Social Engineering*. Aus diesem Grund soll zunächst dieser Begriff erläutert und in Bezug zum Phishing verortet werden.

3.1 Social Engineering

Das BSI definiert *Social Engineering* als das Ausnutzen menschlicher Eigenschaften und die Manipulation von Personen für die Umsetzung krimineller Absichten, beispielsweise zum Erlangen von vertraulichen Informationen [29]. Diese Definition lässt den Rückschluss zu, dass Social Engineering ausschließlich ein Kriminalität-Phänomen ist. Dieser Auslegung kann allerdings widersprochen werden. In der deutschen Fassung des Buches *Die Kunst des Human Hacking* von Christopher Hadnagys wir der Begriff anhand seiner Bezeichnung definiert. Demnach ist Social Engineering die Wissenschaft, Menschen geschickt zu bestimmten Handlungen zu bewegen [30, S. 30]. Entsprechend dieser Definition kann Social Engineering in verschiedenen Bereichen des täglichen Lebens auftreten. Beispielsweise setzten Psychologen Social Engineering ein, um einer Person gezielt Informationen entlocken zu können. Ebenso nutzt ein Verkäufer diese Disziplin, um die Bedürfnisse eines Kunden zu erfragen, damit er diese in einem Verkaufsgespräch gezielt bedienen kann [30, S. 41]. Wird Social Engineering als Angriff im Rahmen krimineller Handlungen betrachtet, lassen sich zwei Arten unterscheiden. Beim *Human-based-social-engineering* erfolgt der Angriff durch persönlichen Kontakt, während beim *Computer-based-social-engineering* die Kommunikation ausschließlich digital mittels E-Mail erfolgt [8, S. 19]. Nach dieser Aufteilung kann das Phishing in seiner Anfangsphase gemäß der Definition auch als *Computer-based-social-engineering* bezeichnet werden. Christopher

Hadnagys definiert, übereinstimmend mit dieser Feststellung, das Phishing in seinem Buch als eine der drei Grundformen des Social Engineering [30, S. 63].

3.2 Phishing als Cybercrime und dessen Folgen

Das Ziel einer Phishing-Handlung ist das Erlangen von Informationen. Dabei können sowohl Informationen vieler verschiedener Personen im Vordergrund stehen als auch verschiedenen Informationen einer Person. In jedem Fall wird beim Phishing die digitale Identität mindestens einer Person angegriffen. Unter diesem Begriff wird die Gesamtheit aller Nutzer-Accounts, Zugangsdaten und sonstiger personenbezogener Daten und Aktivitäten einer Person im Internet verstanden [31, S. 12]. Welche Auswirkungen das Abgreifen von digitalen Identitäten bzw. einzelnen Bestandteilen haben kann, zeigt sich am 2020 aufgetretenen Fall der Website *Weleakinfo.com*. Dort wurden im Frühjahr 2020 über 12 Milliarden Datensätze zum Verkauf angeboten [32, S. 10]. Im Jahr 2021 wurden Daten von 30 Millionen Nutzern eines US-amerikanischen Mobilfunkanbieters für etwa 240.000 Euro zum Kauf angeboten [1, S. 6]. 2017 wurde das BKA auf eine über einen längeren Zeitraum zusammengetragene Datensammlung von ca. 500 Millionen Zugangsdaten aufmerksam in einem Forum [33]. Um zu überprüfen, ob eigene persönliche Informationen bereits im Internet veröffentlicht wurden, eignen sich spezielle Suchmaschinen. Eine entsprechende Funktion bietet das Hasso-Plattner-Institut an. Durch die Eingabe der eigenen E-Mail-Adresse in das entsprechende Feld auf der Website kann abgefragt werden, ob persönliche Informationen veröffentlicht wurden, die in einen Zusammenhang mit der E-Mail-Adresse gebracht werden können. Die Informationen stammen von bekannten Daten-Leaks [34]. Neben dem Sammeln von Informationen in Datensätzen und dem Verkauf dieser besitzt die Täterschaft allerdings auch die Möglichkeit der direkten Verwendung der erlangten Informationen. Das BSI warnt beispielsweise vor Phishing im Zusammenhang mit Bankbetrug [35]. Auch Banken selbst nehmen sich dieser Thematik an und warnen vor Phishing-Angriffen auf Online-Banking-Konten. Die Münchener Bank beispielsweise unterhält eine Website, auf der regelmäßig bekannte Vorgehensweisen von Phishing veröffentlicht werden [36]. Vorgehensweisen, die Bankkonten angreifen, sind auch Bestandteil der Sachverhalte, die in den folgenden Kapiteln erörtert werden. Wird das Phänomen Phishing mit allen Sonderformen als Cybercrime definiert, bleibt zu betrachten, ob sich dieses Phänomen dem engeren oder weiteren Sinn zuordnen lässt. Manfred Wernert geht in seinem Buch *Internetkriminalität* von Strafgesetz selbst aus und fasst alle Straftaten unter diesen Begriff zusammen, bei dessen Normen innerhalb der Tatbestandsmerkmale elektronische Datenverarbeitungsanlagen auftreten. Weiter fügt er an, dass Phishing sich diesem Bereich zuordnen lässt [5, S. 35]. Inwieweit diese Definition mit jener aus der Einleitung korrespondiert und ob sich Phishing uneingeschränkt Cybercrime im engeren Sinn zuordnen lässt, wird innerhalb der Diskussion dieser Arbeit erläutert.

4 Phishing ohne Datenverwendung

In diesem Kapitel sollen die Sachverhalte näher betrachtet werden. Nachfolgend werden die aufgetretenen Phishing-Phasen dieser erläutert. Bei der Betrachtung kann zwischen dem Beschaffen und dem Verwenden von Daten unterschieden werden [26, S. 58]. Aufgrund dessen wird in diesem Kapitel gemäß der Phishing-Definition lediglich das Beschaffen der Daten und die Phishing-Phase als einzelner Bestandteil betrachtet. Eine Analyse der vollständigen Sachverhalte, einschließlich der Datenverwendung, erfolgt im Kapitel 4. Beim dritten Sachverhalt *Smishing* wird die Datenverwendung in der Betrachtung durch das Ausführen der Schadsoftware entsprechend ersetzt und diese getrennt vom bloßen Installieren dieser betrachtet. Nachfolgend wird sowohl das Beschaffen von Daten als auch das Installieren der Schadsoftware einheitlich als Phishing-Phase und Phishing-Handlung bezeichnet. Alle Sachverhalte sind vollständig in den Anlagen erläutert.

Sachverhalt 1 – Smishing mit Telefonat

Im ersten gelisteten Sachverhalt (Anlagen 1.1) wurde der Geschädigte mittels Smishing auf eine Website geleitet. Sowohl SMS als auch Website versuchten mit ihrem Aussehen den Anschein zu wecken, dass sie die Volksbank repräsentieren. Der Geschädigte besaß zu diesem Zeitpunkt ein Konto bei der Volksbank. In der SMS wurde von einem Gesetzesverstoß und einem sofort notwendigen Handeln gesprochen. Auf der Website gab der Geschädigte in einem auszufüllenden Formular seine EC-Kartennummer, das Gültigkeitsdatum, seine Telefonnummer sowie E-Mail-Adresse an. Ergänzend zu der SMS wurde auf der Website von einer Kontosperre gesprochen, wenn der Geschädigte nicht innerhalb von 14 Tagen das Formular ausfüllt.

Sachverhalt 2 - Phishing

Auch im zweiten Sachverhalt (Anlagen 1.2) wurden Daten von einem Volksbankkonto abgegriffen. Die Weiterleitung auf eine vermeintliche Volksbank-Website erfolgte in diesem Fall über eine E-Mail. Durch den Link könne die Geschädigte ein *Secure-Go* – Verfahren aktivieren. Neben Bankdaten gab die Geschädigte auch eine TAN ein, die ihr in ihrer Banking App angezeigt wurde. Diesen Vorgang wiederholte sie ein zweites Mal, ehe sie den Vorgang abbrach.

Sachverhalt 3 - Smishing

Beim dritten Sachverhalt (Anlagen 1.3) wurde sich ebenfalls dem Smishing bedient. Die SMS informierte die Geschädigte über einen vermeintlichen Paketversand des Dienstleisters FedEx. Nach dem die Geschädigte dem Link und weiteren Anweisungen folgte,

installiert sich eine Schadsoftware auf dem Telefon der Geschädigten. Diese hatte die Funktion weitere gleichartige SMS an verschiedene Telefonnummern zu senden.

4.1 § 202a Ausspähen von Daten

Datenbegriff

Innerhalb der Sachverhalte 1 und 2 kann zunächst festgehalten werden, dass die Geschädigten bei der Eingabe ihrer jeweiligen Informationen in einen Computer bzw. in ein Telefon diese in nicht unmittelbar wahrnehmbarer Form erstellen. Ob es sich bei diesen Informationen um Daten nach Abs. 2 handelt, wurde in der Literatur allerdings angezweifelt, da bei einer Eingabe der Informationen innerhalb einer Phishing-Website aufseiten der Geschädigten keine Speicherung dieser im Sinne einer Aufbewahrung vorliegt. Begründet wird diese dadurch, dass Daten nur über einen kurzen Zeitraum im Arbeitsspeicher des Computers der Geschädigten nach der Eingabe über die Tastatur verbleiben. [37, S. 85]. Auch für ein Telefon kann diese Erläuterung übernommen werden. Dieser Argumentation kann allerdings auch widersprochen werden, da das Gesetz zum Datenträger und der Speicherung keine weiteren Einschränkungen vornimmt [17, Rn. 20]. Allerdings erhält die Täterschaft keinen Zugriff auf die Arbeitsspeicher der Geschädigten, weshalb diese Anforderung nicht erfüllt ist. Der Begriff *Übermitteln* beinhaltet hingegen auch das Versenden gespeicherte Daten an Dritte. Eine Einschränkung ist dennoch vorzunehmen, wenn die entsprechenden Informationen im Klartext an die Täterschaft übermittelt werden. In diesem Fall sind die Daten unmittelbar wahrnehmbar [17, Rn. 20]. Mit dieser Argumentation handelt es sich bei den auf der Website eingegeben Informationen aus den Sachverhalten 1 und 2 nicht um Daten nach Abs. 2, da diese im Klartext auf der Website eingegeben werden und serverseitig für die Täterschaft genauso erscheinen. Für die Bewertung weiterer Merkmale wird dennoch davon ausgegangen, dass die Informationen vom Datenbegriff im Sinne des Abs. 2 erfasst werden. Innerhalb des dritten Sachverhaltes können die Informationen auf dem Telefon der Geschädigten als gespeicherte Daten betrachtet werden, da diese entsprechend der Definition in nicht unmittelbar wahrnehmbarer Form vorliegen.

Wille der verfügungsberechtigten Person

Nach Abs. 1 bedarf es der Eigenschaft, dass die Daten nicht für die Täterschaft bestimmt sind. Über die Bestimmtheit entscheidet der Verfügungsberechtigte der Daten [17, Rn. 21]. Dieses Merkmal ist eng verknüpft mit den Merkmalen der Zugangssicherung gegen Unberechtigte und des unbefugten Verschaffens des Zugangs aus der Tathandlung, wobei bei der Zugangssicherung nicht diese selbst, sondern der Begriff *Unberechtigt* gemeint ist. Unberechtigt sind all jene, die keine Bestimmtheit an den Daten besitzen. Demzufolge liegt eine Berechtigung vor, wenn eine Bestimmtheit vorliegt [17, Rn. 38]. Ähnlich

verhält es sich mit dem unbefugten Verschaffen des Zugangs. Dies liegt nicht vor, wenn die Täterschaft Kenntnis über die Informationen erlangen darf [17, Rn. 65]. Daraus kann geschlussfolgert werden, dass der Verfügungswille der berechtigten Person ausschlaggebend für diese Merkmale ist. Bei der Frage nach dem erfüllten Tatbestandsmerkmal der fehlenden Bestimmtheit sind nun die Verfügungsberechtigten zu betrachten. Bei den Sachverhalten 1 und 2 kann angenommen werden, dass die Geschädigten von einer Kommunikation mit der Bank ausgehen. In der Literatur wurde sich dazu bereits wie folgt geäußert: Glauben die Geschädigten, dass die herausgegeben Informationen der Bank bekannt sind, liegen keine übertragenen Befugnisse an die Täterschaft vor, da die Geschädigten bezüglich ihres Geheimhalteinteresses irrten. Ist den Geschädigten hingegen bekannt, dass diese Informationen gegenüber der Bank geheim sind, übertragen sie diese Befugnisse bei vollem Bewusstsein über die Eigenschaft eines Geheimnisses und dass dieses aufgegeben wird. Dass die Geschädigten in Bezug auf die Identität des Kommunikationspartners irren, ist für die Nichterfüllung dieses Tatbestandsmerkmals unerheblich [38, S. 3518]. Aus den Sachverhalten 1 und 2 ist nicht zu entnehmen, in welchem Glauben die Geschädigten zu den Informationen und ihrer Bank standen, weshalb diese hinsichtlich dieses Merkmals nicht abschließend bewertet werden können. Beim dritten Sachverhalt kann davon ausgegangen werden, dass die Geschädigte an eine Kommunikation mit dem Versanddienstleister FedEx glaubte. Gemäß dem geschilderten Sachverhalt gab die Geschädigte zu keinem Zeitpunkt willentlich und bewusst Informationen an andere Personen heraus. Ebenso war der Geschädigten nicht bekannt, dass sich auf ihrem Telefon eine Schadsoftware installiert hat, die möglicherweise Zugriff auf ihre Daten haben könnte. Dementsprechend kann ebenso davon ausgegangen werden, dass keine Bestimmtheit aufseiten der Täterschaft vorlag.

Überwindung der besonderen Zugangssicherung

Das letzte Merkmal in Bezug zum Tatobjekt wird ebenfalls durch die besondere Zugangssicherung genannt, wobei hier nicht der Begriff *Unberechtigt* im Fokus steht, sondern die Zugangssicherung selbst. Während der Tatbegehung muss dieser Schutz der Daten gegeben sein [17, Rn. 36]. Daraus ergibt sich seitens der Täterschaft die Notwendigkeit, dass diese während der Durchführung der Tat den Schutz durchdringen müssen [17, Rn. 61]. In den Sachverhalten 1 und 2 werden die Informationen freiwillig durch die Geschädigten herausgegeben. Aufgrund dieser Herausgabe wird die Zugangssicherung aufgehoben, da die Täterschaft eine mögliche Sicherung nicht mehr überwinden muss. Dass die Freiwilligkeit auf einer Täuschung beruht, ist dabei irrelevant [17, Rn. 64]. Beim dritten Sachverhalt kann von einem Vorhandensein mehrere Zugangssicherung im Sinne des Tatbestandsmerkmals ausgegangen werden. Zu möglichen Schutzvorkehrungen, die durch das Merkmal eingeschlossenen werden, gehören unter anderem biometrische Erkennungsverfahren, Software-Schutzmaßnahmen sowie Passwörter [17, Rn. 44–46], wobei moderne Mobiltelefone je nach Baujahr und Konfiguration mehrere dieser Möglichkeiten aufweisen können. Allerdings kann aufgrund der Aktenlage ebenso davon

ausgegangen werden, dass die Schadsoftware freiwillig von der Geschädigten installiert wird. Zwar beruht diese Handlung auch auf einer Täuschung, dennoch ist der Sachverhalt ähnlich gelagert wie die anderen. Durch die freiwillige Installation muss die Täterschaft mittels der Schadsoftware keine Sicherung durchdringen, weshalb dieses Merkmal nicht erfasst wird.

4.2 § 202b Abfangen von Daten

Beziehungen zu § 202a

Beim Datenbegriff wird innerhalb der Norm auf die Einschränkungen in § 202a verwiesen. Entsprechend kann sich an den Erläuterungen in Kapitel 4.1 orientiert werden, wonach in Sachverhalt 1 und 2 die Informationen im Klartext übermittelt werden und deshalb nicht vom Begriff erfasst werden. In Sachverhalt 3 kann hingegen von einer Speicherung von Daten auf dem Telefon der Geschädigten ausgegangen werden. Ebenso ist die Orientierung für das Merkmal der Bestimmtheit und den Begriff *Unbefugt* möglich, wobei die Bestimmtheit auch die Empfänger der Daten einschließen kann [18, Rn. 8]. Gemäß den Erläuterungen aus dem vorangegangenen Abschnitt kann nur in Sachverhalt 3 von einer fehlenden Bestimmtheit ausgegangen werden.

Nichtöffentliche Kommunikation, technische Abstrahlung und technische Mittel

Als neue Merkmale sind zum einen das Abfangen von Daten aus nichtöffentlichen Datenübermittlung oder aus elektromagnetischer Abstrahlung und zum anderen das Benutzen technischer Mittel zum Abfangen festzuhalten. Diese Merkmale werden von keiner Begehungsweise erfüllt, da die Kommunikation jeweils direkt zwischen den Geschädigten und der Täterschaft erfolgt und eine Datenübermittlung die Täterschaft selbst zum Empfänger hätte. Anderweitige findet keine Datenübermittlung oder Abstrahlung statt, die mithilfe technischer Mittel abgefangen wird.

4.3 § 202c Vorbereiten des Ausspähens und Abfangens von Daten

Tatobjekt Passwörter und Sicherungscodes

Die Phishing-Phase aus Sachverhalt 1 beinhaltet keine Passwörter oder Sicherungscodes, da gemäß den Schilderungen der Begehungsweise lediglich Telefonnummer, E-Mail-Adresse sowie EC-Kartennummer und das Gültigkeitsdatum dieser übermittelt wurden. Unter der Annahme, dass es sich bei den Informationen, die innerhalb von Sachverhalt 2 unter dem Begriff Bankdaten zusammengefasst werden, auch um Zugangsdaten für Online-Banking handelt, werden diese Informationen von der Norm erfasst [19, Rn. 9]. Als

Tathandlung kann dabei das Verschaffen als erfüllt betrachtet werden, da die Täterschaft die Verfügungsmacht über die möglichen Online-Banking-Informationen erlangt [19, Rn. 19]. Wie bereits im Abschnitt 4.1 beschrieben, fehlt bei einer freiwilligen Herausgabe der Informationen allerdings das Merkmal der Zugangssicherung nach § 202a. Unabhängig davon, ob es sich bei den erlangten Informationen aus dem ersten und zweiten Sachverhalt um Passwörter und Zugangsdaten handelt, kann das Merkmal als unerfüllt betrachtet werden, da aufgrund der freiwilligen Herausgabe dieser keine Zugangssicherung bei Benutzung dieser überwunden wird und somit auch keine Vorbereitung vorliegt [19, Rn. 10]. Innerhalb von Sachverhalt 3 ist nicht bekannt, dass mit der bloßen Installation der Schadsoftware Passwörter und Sicherungscodes durch eine der möglichen Tathandlungen Gegenstand des Sachverhaltes werden, weshalb das Tatobjekt nicht bestätigt werden kann.

Tatobjekt Computerprogramm

Bezüglich der Frage, ob es sich bei den verwendeten Websites um Computerprogramme handelt, kann an einen Beschluss des OLG Rostock verwiesen werden. In diesem wird zusammengefasst, dass ein Computerprogramm die Eigenschaft besitzt, Programmabläufe zu steuern. Des Weiteren wird daraus geschlussfolgert, dass Websites, die keine ablauffähigen Anweisungen zum Ausführen bestimmter Computerfunktionen enthalten, keine Programme sind [39, S. 2]. Die tatsächliche Ausgestaltung der Websites ist nicht bekannt. Aufgrund der Beschreibung aus den Akten kann allerdings beim ersten Sachverhalt davon ausgegangen werden, dass diese Website nicht die Anforderungen an ein Programm erfüllt. Im zweiten Sachverhalt ergibt sich aus den Schilderungen die Vermutung, dass während der Eingabe der Kontodaten durch die Geschädigte bzw. im Anschluss daran eine Software automatisch Überweisungen veranlasste, die mit Hilfe der TANs bestätigt werden sollten. Dieser mögliche Ablauf ist wahrscheinlicher, als dass eine Person im Hintergrund wartet, bis jemand auf die E-Mail reagiert und seine Informationen eingibt. Entsprechend dieser Erläuterung wird in der weiteren Betrachtung von einer Hintergrundsoftware ausgegangen. Diese würde gemäß den Schilderungen des OLG Rostock die Anforderungen an ein Computerprogramm erfüllen. Hierbei ist entscheiden, ob die Website und Software als Einheit oder getrennt betrachtet werden. Nach der genannten Definition von Phishing umfasst diese Phase das Erlangen der Daten. Eine weitere Verarbeitung wird nicht geschildert. Nach dieser Schlussfolgerung erfüllt die Website der einzeln betrachten Phishing-Phase nicht das Merkmal eines Computerprogramms. Im dritten Sachverhalt wird durch die versendete SMS und den darin enthaltenen Link Schadsoftware, die die Anforderungen an Programme des OLG Rostock erfüllt, verbreitet. Der Sachverhalt kann den objektiven Tatbestand des § 202c erfüllen, wenn die Schadsoftware nach der Installation entsprechende weitere Funktionen ausführt, die zum Ausspähen oder Abfangen von Daten dienen. Dabei wird durch den SMS-Versand die Tathandlung der Verbreitung erfüllt [19, Rn. 22]. Ebenso können weitere Handlung wie das Verschaffen oder Herstellen bei entsprechendem Vorgehen der Täterschaft erfüllt werden. Da aufgrund der Erläuterungen zum Sachverhalt allerdings abschließend nicht bestätigt werden kann, dass

die Schadsoftware weitere Funktionen außer das Versenden von SMS ausführt, kann auch die Erfüllung des objektiven Tatbestandes im Zusammenhang mit Computerprogrammen nicht bestätigt werden.

4.4 § 202d Datenhehlerei

Da die Phishing-Handlungen in allen Sachverhalten die Vortat selbst repräsentiert, in der Daten möglicherweise rechtswidrig erlangt wurden, scheitert die Subsumtion dieser am Tatobjekt. Durch den beim Daten-Begriff verwendeten Verweis auf § 202a Abs. 2 ergibt sich zudem die gleiche Diskussion wie auch im § 202a selbst, ob die Informationen aus den Sachverhalten 1 und 2 überhaupt von der Definition erfasst werden, da eine Übermittlung dieser im Klartext stattfindet. Innerhalb von Sachverhalt drei ist nicht bekannt, dass durch eine bloße Installation der Schadsoftware überhaupt Daten erlangt werden.

4.5 § 263a Computerbetrug

Datenverarbeitungsvorgang und Vermögensverschiebung

Zunächst ist zu betrachten, inwieweit ein Datenverarbeitungsvorgang vorhanden ist. Die erste Phase, die Dateneingabe, wird durch die Geschädigten im ersten und zweiten Sachverhalt erfüllt, da es sich bei den Konto- und Bankinformationen um codierte Informationen handelt, die durch die Eingabe erzeugt werden. Mit der Begründung aus Abschnitt 4.3, dass die einzeln betrachteten Websites der Phishing-Phase keine Programme darstellen und keine Programmabläufe steuern können, besitzen diese auch nicht die Eigenschaften eines Datenverarbeitungsvorgangs. Aus diesem Grund scheitert die Subsumtion der Sachverhalte 1 und 2 am Tatobjekt. Aus der Akte des Sachverhaltes 3 geht nicht hervor, in welcher Form der Download der Schadsoftware erfolgte und ob die Täterschaft bei der Bereitstellung des Downloads auf andere Vorgänge eingewirkt hat, weshalb eine Bewertung des Sachverhaltes in dieser Hinsicht nicht vorgenommen werden kann. Neben den Datenverarbeitungsvorgängen fehlt es zudem an Vermögensverschiebungen, die innerhalb der Phishing-Phase Bestandteil der Begehungsweise sind.

Vorbereitungshandlungen nach Abs. 3

Das zweite zu betrachtende Gebiet betrifft die Vorbereitungen nach § 263a. Bei der Vorbereitung einer Straftat müssen zunächst die beiden genannten Tatobjekte betrachtet werden. Entgegen der Aussage des OLG Rostock wird im Münchener Kommentar zwar die Website als Programm eingeordnet, allerdings wird hier der fehlende Zweck des Programms, direkt den Computerbetrug zu begehen, als Ausschlusskriterium genannt, weshalb die Phishing-Website die Vorbereitung im Sinne eines Programms nach Abs. 3 nicht erfüllt [21, Rn. 193]. Innerhalb des dritten Sachverhaltes muss bezüglich einer

Subsumtion unter das Tatobjekt *Computerprogramm* gegenüber den Erläuterungen aus Kapitel 5 vorgegriffen werden. Wie in bei der Betrachtung des gesamten Sachverhaltes erläutert, wird die Zweckbestimmung des Programms, eine solche Tat zu begehen erfüllt, weshalb die Schadsoftware vom Tatobjekt des Computerprogramms erfasst wird. Dementsprechend kann der Umgang mit dieser Schadsoftware aufseiten der Täterschaft auch die Vorbereitung nach Abs. 3 Nr. 2 erfüllen. Je nachdem, ob sich die Täterschaft die Software lediglich verschafft oder selbst hergestellt hat, können verschiedene Handlungsmöglichkeiten unterschieden werden. Anzumerken ist hierbei allerdings, dass diese Handlungen bereits im Vorfeld, vor der Phishing-Handlung und nicht durch diese selbst erfüllt werden, weshalb eine Subsumtion trotzdem erfolglos bleibt. Da im Gegensatz zum Computerprogramm die Passwörter und Sicherungscodes nach dem Wortlaut der Norm zur Begehung der Tat lediglich geeignet sein müssen, wird auch das Erlangen dieser im Rahmen einer Vorbereitungshandlung durch Phishing erfasst [21, Rn. 196-197]. Passwörter und Sicherungscodes umfassen dabei alle Zeichenkombinationen, durch die der Zugriff auf bestimmte Daten ermöglichen wird [21, Rn. 195]. Nach dieser Definition können die möglicherweise erlangten Zugangsdaten zum Onlinebanking aus Sachverhalt 2 als Passwörter und Sicherungscodes bezeichnet werden. Sowohl die Installation der Schadsoftware aus Sachverhalt 3 als auch die Phishing-Phase aus Sachverhalt 1 beinhalten keine Passwörter oder Sicherungscodes.

4.6 § 269 Fälschung beweiserheblicher Daten

Datenurkunde

Alle nicht codierten Informationen werden vom Datenbegriff erfasst. Innerhalb dieser Norm sind nicht die erlangten Informationen zu betrachten, die im Mittelpunkt der vorangegangenen Tatbestände standen, sondern jene, die durch SMS, E-Mail und Website dargestellt werden. Diese Beschreibung des Datenbegriffes trifft auf alle diese Informationen zu, weshalb alle Sachverhalte dieses Merkmal erfüllen. Ein rechtwirksame Erklärung wird durch die E-Mail aus Sachverhalt 2 mit Bezug auf einen bestehenden Vertrag zwischen Bankkunden und Bank ebenso vorgetäuscht [40, S. 885]. Um rechtswirksam zu sein, muss von der Erklärung selbst ein Beweisinteresse ausgehen [22, Rn. 10]. Das Beweisinteresse wird dadurch begründet, dass die Täterschaft mit der Erklärung den Beweis erbringen möchte, die Bank zu sein und auf diesem Wege mit der geschädigten Person kommunizieren zu wollen. Diese Argumentationskette kann auch für die SMS aus Sachverhalt 1 übernommen werden. Im Münchener Kommentar zu StGB wird der Erfassung einer Phishing-Mail als rechtserhebliche Erklärung zugestimmt [22, Rn. 33]. Findet sich die gleiche Erklärung auf der Phishing-Website, wird das Merkmal gleichzeitig von dieser erfüllt [40, S. 890]. Prinzipiell wird eine Website mit falscher Identitätsangabe von der Norm erfasst [22, Rn. 34]. Da die Daten die entsprechende Rechtswirksamkeit der Erklärung nachweisen können, erfüllen sie auch die Eigenschaft der Beweiserheblichkeit [22, Rn. 12]. Im dritten Sachverhalt möchte die Täterschaft durch die SMS den Beweis

erbringen, dass sie den Versanddienstleister darstellt und die empfangende Person ein Paket zu erwarten hat. Deshalb stellt auch diese eine rechtswirksame Erklärung dar und erfüllt die Eigenschaft der Beweiserheblichkeit. Aufgrund der Rechtswirksamkeit der Erklärung bedarf es zudem der eindeutigen Feststellbarkeit der erklärenden Person, wobei diese Person die Daten nicht selbst maschinell erzeugt haben muss. Stattdessen ist die Notwendigkeit gegeben, dass die Identität der erklärenden Person direkt aus den Daten feststellbar ist [22, Rn. 11]. Innerhalb der Sachverhalte 1 und 2 wird die Erkennbarkeit durch den Namen der Bank und weiteren entsprechenden Angaben realisiert [40, S. 888-889]. Diese Betrachtungsweise kann auch für den Versanddienstleisters aus Sachverhalt 3 übernommen werden. Abschließend können E-Mail, SMS und Website als unechte Datenurkunde betrachtet werden.

Tathandlungen

Bei den möglichen Tathandlungen kann zunächst das Speichern als erfüllt betrachtet werden. Durch das Versenden von SMS und E-Mail seitens der Täterschaft finden in allen Sachverhalten mehrere Speichervorgänge auf den Computern und Telefonen der Beteiligten und den Mailservern statt [40, S. 886]. Auch die Websites erfüllen die Speicherung auf den jeweiligen Servern [40, S. 890]. Durch das Versenden der E-Mail und SMS wird ebenfalls das Gebrauchen solcher Daten in allen Delikten erfüllt [40, S. 886]. Über die Links werden in diese Tathandlung zudem die Phishing-Websites eingeschlossen [40, S. 890].

4.7 § 271 Mittelbare Falschbeurkundung

Keine der genannten Phishing-Handlungen erfüllt den objektiven Tatbestand dieser Norm. Die Subsumtion in den Sachverhalten scheitert bereits am Tatobjekt der öffentlichen Urkunde. Die unbefugte Erstellung von Datensätzen wird nicht nach § 271 erfasst, da für den Schutzzweck der inhaltlichen Richtigkeit der Norm zunächst eine amtliche Gewähr auf entsprechende Richtigkeit vorliegen muss [24, Rn. 6]. Aus diesem Grund wird auch das Erstellen der E-Mail, SMS und Websites im Namen von Banken oder Paketversanddienstleistern nicht Abs. 1 der Norm erfüllen. Anderweitige wurde nach Abs. 1 nicht bewirkt, dass entsprechende öffentliche Urkunden erstellt wurden. Ebenso wird in keinem der Delikte im Sinne des Abs. 2 auf entsprechende Einträge verwiesen.

4.8 § 274 Urkundenunterdrückung

Wie bereits erläutert, müssen die beweiserheblichen Daten die Eigenschaften einer Urkunde erfüllen. Gleichzeitig gilt zu beachten, dass lediglich echte Urkunde mit der wahrhaftigen Erklärung der ausstellenden Person von der Norm erfasst werden [25, Rn. 3]. Mit dieser Begründung stellen E-Mail, SMS und Websites der Sachverhalte keine

beweiserheblichen Daten dar, da diese von der Täterschaft fälschlicherweise im Namen von Bank und Paketdienstleister erstellt wurden. Somit scheitert die Erfüllung dieses objektiven Tatbestandes wie auch beim § 271 am Tatobjekt.

4.9 § 303a Datenveränderung

Datenveränderung im dritten Sachverhalt

Aufgrund des weit gefassten Datenbegriffs der Norm werden innerhalb von Sachverhalt 3 alle nicht unmittelbar wahrnehmbare Informationen auf dem Telefon der Geschädigten als Daten erfasst. Zudem liegt die Verfügung unter anderem bei der Geschädigten und damit bei mindestens einer anderen Person als bei der Täterschaft. Das Installieren von Schadsoftware auf dem Telefon erfüllt das Verändern der Daten unter anderem dadurch, dass beim Einschleusen der Schadsoftware Daten hinzugefügt werden [26, Rn. 15]. Die anderen Handlungsmöglichkeiten können nur als potenziell erfüllt betrachtet werden, da aus der Beschreibung die genauen Umstände der Schadsoftwareinstallation nicht bekannt sind. Das Löschen von Daten kann durch das Installieren erfüllt werden, wenn Daten mittels anderer Daten überschrieben werden [26, Rn. 12]. Zugleich kann die Löschung und das Verändern der Daten auch die Handlung des Unbrauchbarmachens der Daten erfüllen [26, Rn. 14]. Werden Daten der Geschädigten gleichzeitig dauerhaft oder zeitweise entzogen, ist auch die Tathandlung des Unterdrückens erfüllt [26, Rn. 13].

Datenveränderung im ersten und zweiten Sachverhalt

Innerhalb der Sachverhalte 1 und 2 wird § 303a nicht erfüllt. Zum einen erhält die Täterschaft keinen Zugriff auf die Geräte der Geschädigten. Durch das Betreiben der Website, das Versenden von E-Mail und SMS sowie die Eingabe der Daten durch die Geschädigten wird keine der genannten Handlungsmöglichkeiten erfüllt, da kein dadurch erzieltes Einwirken auf Daten bekannt ist.

Vorbereitungshandlung nach § 202c Abs. 1

Durch die erlangten Zugangsinformationen zum Online-Banking aus Sachverhalt 2 kann eine Vorbereitungshandlung erfüllt werden, da diese als Tatobjekt *Passwörter und Sicherungscodes* Zugang zu Daten in Form des Kontozugriffs ermöglichen. Dabei wird die Tathandlung des Verschaffens erfüllt. Die Schadsoftware selbst, die im dritten Sachverhalt installiert wird, kann unter den Begriff des Computerprogramms subsumiert werden. Auch hier muss auf die Erläuterungen aus Kapitel 5 vorgegriffen werden. Demnach ist die Software für eine Begehung einer solchen Tat geeignet und erfüllt dementsprechende die Eigenschaft eines Computerprogramms im Rahmen einer Vorbereitung. Auch hier ist die

Erfüllung mehrerer Handlungen möglich. Es muss allerdings angemerkt werden, dass diese Handlungen nicht durch die Phishing-Handlung selbst, sondern im Vorfeld erfüllt werden, weshalb auch hier einer erfolgreichen Subsumtion nicht zugestimmt werden kann.

4.10 § 303b Computersabotage

Computersabotage in den drei Sachverhalten

Zwar wird im Abs. 1 Nr. 1 die Tathandlung § 303a Abs. 1 als zu erfüllender objektiver Tatbestand genannt, weshalb auf Abschnitt 4.9 verwiesen werden kann, wonach Sachverhalt 3 diesen erfüllt und somit auch die Handlung nach Abs. 1 Nr. 1 verwirklicht. Allerdings ist nicht bekannt, dass durch die bloße Installation der Schadsoftware und den vorangehenden SMS-Versand Datenverarbeitungsvorgänge gestört werden, die für die geschädigte Person von erheblicher Bedeutung sind, weshalb die Erfüllung des objektiven Tatbestandes aufgrund des fehlenden Tatobjektes bereits nicht bestätigt werden kann. Gleiches kann auch für das Versenden von SMS, E-Mail und das Betreiben der Website aus den Sachverhalten 1 und 2 festgestellt werden.

Vorbereitungshandlungen nach § 202c Abs. 1

Im Rahmen von Sachverhalt 3 kann eine Vorbereitungshandlung nach 202c nicht bestätigt werden, da die Schadsoftware nicht für die Begehung einer Computersabotage geeignet ist. Für die Online-Banking-Informationen aus Sachverhalt 2 kann sich an der Erläuterung aus dem vorangegangenen Abschnitt zu § 303a orientiert werden. Dabei stellt sich die Frage, inwieweit eine Computersabotage mit diesen Informationen vorbereitet werden sollte. Da dies durch die Erläuterungen des Sachverhaltes nicht abschließend beantwortet werden, kann einer derartigen Subsumtion nicht zugestimmt werden.

5 Vollständige Betrachtung der Sachverhalte

Entsprechend der Unterscheidungsnotwendigkeit wird in diesem Kapitel eine Betrachtung der vollständigen Sachverhalte durchgeführt. Dabei gehen die Begehungsweisen über das alleinige Erlangen von Daten und somit auch über Phishing gemäß der Definition aus der Einleitung hinaus. Aufgrund der Komplexität der Delikte wird die Betrachtung geordnet nach den einzelnen Sachverhalten durchgeführt.

5.1 Sachverhalt 1 – Smishing mit Telefonat

Wie aus der Schilderung in den Anlagen zu entnehmen, stellt das Phishing im Gegensatz zu Sachverhalt 2 hier lediglich einen Teil der Begehungsweise dar. Den zweiten Teil bildet das Gespräch zwischen dem vermeintlichen Bankmitarbeiter und dem Geschädigten. Im Rahmen der Vorbereitung wurde zudem eine E-Mail-Adresse sowie eine Domäne auf falsche Identität generiert. Außerdem besteht die Verbindung zu einer realen Person, auf dessen Konto das Geld überwiesen werden sollte. Es kann vermutet werden, dass es sich bei dieser um einen Finanzagenten handelt. Ein Finanzagent wird von der Täterschaft über Stellenanzeigen angeworben und hat die Aufgabe, die Gelder von seinem zur Verfügung gestellten Konto in das Ausland zu transferieren [41]. Da der vermutete Finanzagent aber kein wesentlicher Bestandteil des Phishings ist, wird dieser bei der weiteren Betrachtung des Sachverhaltes nicht berücksichtigt. Gleiches gilt für die Registrierungshandlungen der Domäne.

§ 202a Ausspähen von Daten

Zunächst verwendet die Täterschaft die erlangte Information aus der Phishing-Handlung, um Kontakt mit dem Geschädigten aufzunehmen und zu halten. Erfolgreich geschieht dies zunächst telefonisch. Aus der späteren SMS ist zu entnehmen, dass mithilfe der Bankdaten eine Überweisung generiert wurde. An dieser Stelle müssen zwei Möglichkeiten unterschieden werden. Die erste Möglichkeit wird dadurch dargestellt, dass sich die Täterschaft mit den erlangten Informationen in das Online-Banking Konto des Geschädigten einloggt. Bezüglich dieser Begehungsweise existieren konträre Meinungen. Nach der ersten Meinung kann der objektive Tatbestand des § 202a hier als erfüllt betrachtet werden [40, S. 906]. Das Tatobjekt der Daten stellen hierbei die Informationen innerhalb des Online-Kontos da. Diese erfüllen zunächst die Beschreibung von Daten nach Abs. 2 vollständig, da es sich um nicht wahrnehmbare Informationen handelt, die auf den Servern der Bank gespeichert sind. Darüber hinaus kann davon ausgegangen werden, dass der Verfügungswille des Geschädigten den Täterkreis nicht einschließt und damit die Daten

sowohl nicht für die Täterschaft bestimmt sind als auch unbefugt erlangt wurden. Die Log-In-Informationen stellen eine Zugangssicherung dar [17, Rn. 36]. Entgegen dieser Argumentation wurde auf Grundlage des Münchener Kommentars schon in Kapitel 4.3 angemerkt, dass durch die freiwillige Herausgabe der Daten seitens der Geschädigten bereits in einer möglichen Vorbereitungshandlung nach § 202c jene Zugangssicherung ausgehebelt wird und aus diesem Grund der objektive Tatbestand nach § 202a nicht erfüllt wird [19, Rn. 10]. Unabhängig dieser Diskussion kann gemäß den Schilderungen aus der Fallakte nicht bestätigt werden, dass die Täterschaft Online-Banking-Informationen erlangte, sich in das entsprechende Konto einloggte und dort die Überweisung generierte. Auf welchem Wege dies mit den erlangten Informationen (EC-Kartennummer, Gültigkeitsdatum, E-Mail-Adresse, Telefonnummer) geschah, lässt sich den Schilderungen ebenso nicht entnehmen. Aus diesem Grund kann eine Erfüllung des objektiven Tatbestandes auf diesem Weg nicht bestätigt werden. Anderweitig erfüllen das Telefongespräch und das Versenden der Überweisungs-SMS nicht den objektiven Tatbestand nach 202a. Die Subsumtion scheitert bereits am Tatobjekt, da keine weiteren Daten erlangt wurden.

§ 202b Abfangen von Daten

Wie bereits in der einzelnen Phishing-Phase festgestellt, beinhaltet diese Norm im Unterschied zu § 202a das Abfangen von Daten aus einer nichtöffentlichen Kommunikation oder elektromagnetischen Abstrahlung und das Benutzen von technischen Mitteln dafür, während der Datenbegriff sowie die Merkmale *Unbefugt* und *Bestimmtheit* übertragbar sind. Auch die Erweiterung des Blickwinkels über den gesamten Sachverhalt ändert nichts daran, dass die Erfüllung des objektiven Tatbestandes an einer fehlenden Datenübermittlung der Geschädigten mit einer weiteren Partei außerhalb der Täterschaft oder einer abgefangenen elektromagnetischen Abstrahlung scheitert.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

Außerhalb der Phishing-Handlung sind weder Passwörter oder Sicherungscodes, die den Zugang zu Daten ermöglichen, noch Computerprogramme, deren Zweck die Begehung einer solchen Tat sind Bestandteil der Begehungsweise. Aus diesem Grund wird auch bei einer gesamten Betrachtung des Sachverhaltes der objektive Tatbestand nicht erfüllt.

§ 202d Datenhehlerei

Zunächst ist auch hier der Datenbegriff zu betrachten. Darunter fallen durch den Verweis auf § 202a Abs. 2 alle nicht unmittelbar wahrnehmbaren Daten. Unter den Begriff Daten können zunächst die EC-Kartennummer, das Gültigkeitsdatum, die E-Mail-Adresse und

die Telefonnummer betrachtet werden, da diese Informationen in nicht unmittelbar wahrnehmbarer Form bei der Täterschaft, die die Informationen erlangte, gespeichert vorliegen. Ebenso sind die Daten nicht öffentlich zugänglich, wenn davon ausgegangen wird, dass diese durch den Geschädigten im Vorfeld nicht veröffentlicht wurden. In diesem Fall können die Informationen nicht durch jede Person rechtmäßig erlangt werden. Das letzte Tatobjekt bezogene Merkmal betrifft das Erlangen der Daten durch eine andere rechtswidrige Tat. Da jeder objektive Tatbestand des StGB dieses Merkmal erfüllen kann, ist die Verwirklichung des objektiven Tatbestandes von § 269 beim Verschaffen der Informationen durch die Phishing-Handlung ausreichend. Allerdings enthält dieses Merkmal die weitere Bedingung, dass dies durch eine andere Person geschehen ist. An dieser Stelle scheitert die Erfüllung des objektiven Tatbestandes, wenn es sich bei der Täterschaft der Phishing-Phase und jener, die die Daten nutzen, nicht um mindestens zwei verschiedene Personen handelt. Handelt eine Täterschaft sowohl bei der Beschaffung als auch bei der Verwendung der Daten, wird keine Tathandlung erfüllt. Nach § 202d wird das Zugänglichmachen sowie das Übertragen von Verfügungsmacht und Besitz erfasst. Diese Eigenschaften an den Daten liegen allerdings bereits bei der Täterschaft. Dass eine andere dem objektiven Tatbestand entsprechende Konstellation in diesem Sachverhalt vorliegt, lässt sich nicht bestätigten, weshalb die Norm als nicht erfüllt betrachtet werden kann.

§ 263a Computerbetrug

Grundlage dieser Norm ist die Beeinflussung eines Datenverarbeitungsvorgangs. Wird der gesamte Sachverhalt betrachtet, kann ein Datenverarbeitungsvorgang innerhalb der Bank detektiert werden. Dieser wird durch die Verarbeitung von Überweisungsaufträgen durch die Bank dargestellt. Die Eingabephase wird durch die Täterschaft initialisiert. Anschließend erfolgt aufseiten der Bank die Verarbeitung der Informationen mittels Programme und abschließend die Ausgabe in Form von Ergebnissen durch die ausgeführte Überweisung, durch die ein Vermögensschaden erzielt wird. Die Täterschaft erfüllt dabei das Einwirken auf diesen Vorgang durch die unbefugte Verwendung von Daten. Gemäß der vorherrschenden Meinung in Bezug auf den Begriff „Unbefugt“ kann als täuschungsähnliche Handlung das Vortäuschen einer falschen Identität gegenüber der Bank betrachtet werden. Zwar wurde die Überweisung in Auftrag gegeben, durch die fehlende Übermittlung der TAN durch den Geschädigten scheiterte die Vollendung allerdings. Demnach kann nur der Versuch des Abs. 1 als erfüllt betrachtet werden. Nach § 22 StGB unternimmt einen Versuch, „[…] wer nach seinen Vorstellungen von der Tat zur Verwirklichung des Tatbestandes unmittelbar ansetzt.“ [16, 22]. Diese Beschreibung trifft auf den Sachverhalt zu. Die Strafbarkeit des Versuches wird in Abs. 2 der Norm mit dem Verweis auf die Abs. 2-6 von § 263 genannt. Vorbereitungshandlungen nach § 263a werden außerhalb der Phishing-Handlung nicht durchgeführt. Aus der Beschreibung der Begehungsweise geht nicht hervor, inwieweit Computerprogramme für die Initialisierung der Überweisung genutzt wurden. Eine anderweitige Nutzung ist ebenfalls nicht bekannt. Ebenso wird Nr. 2 nicht erfüllt. Zwar handelt es sich bei der TAN um einen Sicherungscode, der zur

Begehung einer solchen Tat geeignet ist, allerdings wird keine Tathandlung erfüllt, da der Geschädigte die TAN nicht übermittelt. Ein Versuch liegt bei einer Vorbereitungshandlung nicht vor, da bei dieser nicht unmittelbar zur Verwirklichung des objektiven Tatbestandes angesetzt wird.

§ 296 Fälschung beweiserheblicher Daten

Im Mittelpunkt von § 296 stehen Datenurkunden, wobei mit der Norm vor einem falschen Erklärungsinhalt und darauf aufbauenden Entscheidungen geschützt werden sollen. In der Literatur existiert die Ansicht, dass als relevante Handlung das in Auftrag geben der Überweisung betrachtet werden kann. Durch diese wird bei der Bank im Zusammenspiel mit der TAN eine falsche Datenurkunde gespeichert. Inhalt dieser ist die Erklärung, dass die Täterschaft der Kontobesitzer sei [40, S. 906]. Zunächst kann der Inhalt der Informationen nicht ohne technische Hilfsmittel erfasst werden, weshalb die Definition des Datenbegriffs diese einschließt. Ebenso wird innerhalb dieser eine Erklärung abgegeben. Das Beweisinteresse und die damit verbundene Rechtswirkung und Beweiserheblichkeit werden hier durch das Interesse der Täterschaft dargestellt, die Identität als Geschädigter zu begründen. Allerdings entfällt die Täuschung im Rechtsverkehr, da kein Mensch getäuscht wird. Durch die Gleichstellungsfunktion dieser mit der fälschlichen Beeinflussung von Datenverarbeitungen durch § 270 wird diese Problematik allerdings aufgelöst [40, S. 906]. Da die Täterschaft die TAN allerdings nicht erhält, wird der objektive Tatbestand nicht erfüllt. Deshalb bleibt es bei einer Versuchsstrafbarkeit nach Abs. 2 der Norm.

§ 271 Mittelbare Falschbeurkundung

Auch die Verwendung der durch Phishing erlangten Daten scheitert bei dieser Norm am Tatobjekt der öffentlichen Urkunde, da durch die unbefugte Verwendung der Daten durch die Täterschaft wie in § 269 beschrieben eine falsche Urkunde vorliegt und nur öffentliche Urkunden mit einer amtlichen Gewähr auf Richtigkeit von der Norm erfasst werden (siehe Abschnitt 4.7). Anderweitig sind weder nach Abs. 1 noch nach Abs. 2 der Norm öffentliche Urkunden Inhalt der Begehungsweise.

§ 274 Urkundenunterdrückung

Genau wie die bloße Phishing-Phase scheitert die Verwendung der erlangten Informationen am Tatobjekt der echten Urkunde, die lediglich von der Norm erfasst wird. Anderweitig ist keine echte Urkunde im Fall enthalten.

§ 303a Datenveränderung

Die Erfüllung dieses objektiven Tatbestandes scheitert auch außerhalb des Erlangens von Daten, da weder der Überweisungsauftrag noch das Telefonat mit der versuchten TAN-Abfrage Daten verändern, löschen, unterdrücken oder unbrauchbar machen. Obwohl nach einer Benutzung der abgefragten TAN der Geschädigte diese nicht noch einmal verwenden kann, würde dies nicht den objektiven Tatbestand im Sinne eines Unbrauchbarmachens erfüllen. Die Bestimmung der TAN besteht gerade in ihrer Verwendung, weshalb diese nicht von Norm erfasst wird. Begründet werden kann diese durch die Nähe der Norm zum § 303, wonach Gegenstände, die ihren Zweck in einer Verwendung haben, nicht unter den objektiven Tatbestand einer Sachbeschädigung fallen [42, S. 89]. Dementsprechenden ist im vorliegenden Sachverhalt auch keine Versuchsstrafbarkeit nach Abs. 2 gegeben. Da keine entsprechenden Passwörter und Sicherungscodes, die Zugang zu Daten ermögliche oder Computerprogramme, die für die Begehung einer solchen Tat geeignet sind, vorhanden sind, werden keine Vorbereitungshandlungen erfüllt.

§ 303b Computersabotage

Zunächst kann Abs. 1 Nr. 1 als Tathandlung ausgeschlossen werden, da wie aufgezeigt, weder die Phishing-Handlung noch die Datenverwendung den objektiven Tatbestand von § 303a erfüllen. Innerhalb des Sachverhaltes wird keine Datenträger oder eine entsprechende Anlage angegriffen, weshalb auch diese Tathandlung nach Nr. 3 scheitert. Zwar kann durch das generieren der Überweisung mit der Nachteilsabsicht Abs. 1 Nr. 2 der Norm betrachtet werden, allerdings scheitert auch diese Handlung am benötigten Tatobjekt der gestörten Datenverarbeitung [42, S. 89]. Der Unterschied zu § 263a und der dort genannten Datenverarbeitung besteht darin, dass dort das Ergebnis einer Datenverarbeitung und hier diese selbst im Mittelpunkt steht. Vorbereitungshandlungen werden, wie auch in Kapitel 4 nicht erfüllt, da mögliche Tatobjekte fehlen.

5.2 Sachverhalt 2 - Phishing

Im Gegensatz zu erstem Sachverhalt wird hier auch die TAN-Abfrage innerhalb der Phishing-Handlung durchgeführt. Außerhalb dieser bildet die bereits in Kapitel 4 angesprochenen Software, die mit den eingegebenen Daten die Überweisung veranlasst, den weiteren Teil der Begehungsweise. Demnach wird mit dieser die Datenverwendung realisiert. Außerhalb dieser Handlung ist nur bekannt, dass das Geld auf ein französisches Bankkonto überwiesen werden sollte, dass per Online-Authentifizierungsverfahren eröffnet wurde.

§ 202a Ausspähen von Daten

Auch dieser Sachverhalt stößt auf die Diskussion, ob durch die freiwillige Herausgabe der Zugangsdaten für Online-Banking die Zugangssicherung ausgehebelt wird, wie sie bereits im Rahmen einer Vorbereitungshandlung nach § 202c (Kapitel 4.3) und innerhalb von Sachverhalt 1 (Kapitel 5.1) geführt wurde. An dieser Problematik ändert auch der Umstand nichts, dass der Log-In Vorgang im Gegensatz zum ersten Sachverhalt möglicherweise durch die Software realisiert wurde. Abschließend kann eine Erfüllung des objektiven Tatbestandes wie auch in Sachverhalt 1 nicht bestätigt werden.

§ 202b Abfangen von Daten

Da der Sachverhalt wie auch Sachverhalt 1 keine nichtöffentlichen Datenübermittlung zwischen Parteien außerhalb der Täterschaft oder eine elektromagnetische Abstrahlung beinhaltet, die abgefangen werden könnten, wird auch hier der objektive Tatbestand nicht erfüllt wird.

§ 202c Vorbereitung des Ausspähens und Abfangens von Daten

Wie auch im Sachverhalt 1 sind außerhalb des Erlangens von Informationen durch die Phishing-Phase keine Passwörter oder Sicherungscode Bestandteil des Sachverhaltes. Wie in Kapitel 4.3 erläutert, besteht eine Trennung zwischen der Phishing-Phase und der Software, die die Informationen verarbeitet. Nach der Definition des OLG Rostock handelt es sich bei der Software um ein Computerprogramm. Aufgrund des Verwendungszweckes, automatisch eine Überweisung zu generieren und anschließend die benötigte TAN über die Website abzufragen, kann die Anforderung, einem illegalen Zweck zu dienen, angenommen werden. Dennoch kann eine Erfüllung des objektiven Tatbestandes nicht bejaht werden, da die Software für die Begehung einer Tat nach 202a oder 202b geeignet sein muss. Aus der Funktion der Software, sich in das Konto einzuloggen, automatisch Überweisungen zu generieren und die benötigten TANs weiterzuleiten, geht nicht hervor, dass diese gleichzeitig dafür geeignet ist, nach 202a eine Zugangssicherung zu überwinden und Daten auszuspähen oder eine nichtöffentliche Datenübermittlung oder elektromagnetischen Abstrahlung nach 202b abzufangen.

§ 202d Datenhehlerei

Genauso wie Sachverhalt 1 scheitert dieser Fall an dem Merkmal, dass die Daten durch eine andere Person erlangt wurden. Aus der Begehungsweise ist anzunehmen, dass es

um eine Täterschaft handelt, die die Informationen erlangt und benutzt. Aus diesem Grund kann auf die entsprechenden Erläuterungen zu Sachverhalt 1 verwiesen werden.

§ 263a Computerbetrug

Der Unterschied zwischen Sachverhalt 1 und 2 besteht darin, dass bei Letzterem die für die Überweisung benötigte TAN automatisch und nicht per Telefon abgefragt wird. Auf die Erfüllung des objektiven Tatbestandes wirkt sich dieser Unterschied nicht aus. Auch hier wird die Notwendigkeit eines Datenverarbeitungsprozesses durch den bankintern bearbeiteten Überweisungsauftrag und als Tathandlung die unbefugte Verwendung von Daten erfüllt, weshalb auf die Erläuterungen in Kapitel 5.1 verwiesen werden kann. Da die Täterschaft die TANs erlangte und eine der beiden Überweisungen ausgeführt wurde, was zu einem Vermögensschaden führte, ist im Gegensatz zu Sachverhalt 1 der Erfolg eingetreten und nicht nur ein Versuch detektierbar. Der Umgang mit der Software, die die Überweisung im Hintergrund initialisiert, kann ebenso die Vorbereitungshandlung nach Abs. 3 Nr. 1 erfüllen, da die Software für die Begehung einer solchen Tat geeignet ist. Dabei wird die Handlung des Verwahrens erfüllt. Andere Handlungen, beispielsweise das Herstellen, sind denkbar, können aber nicht bestätigt werden.

§ 269 Fälschung beweiserheblicher Daten

Bei der Subsumtion dieses Sachverhaltes kann ebenso vollständig auf die Erläuterungen von Sachverhalt 1 in Kapitel 5.1 verwiesen werden. Genau wie in diesem täuscht die Täterschaft mit der Erklärung vor, dass sie die kontobesitzende Person sei. Die daraus resultierende, unechte Urkunde liegt ebenso in Datenform vor, dessen Inhalt ohne Hilfsmittel nicht erfassbar ist und wird aufseiten der Bank gespeichert.

§ 271 Mittelbare Falschbeurkundung

Mit der Begründung, dass nur öffentliche Urkunden mit amtlicher Gewähr auf Richtigkeit von der Norm erfasst werden, scheitert die Subsumtion von diesem Sachverhalt auch bereits am Tatobjekt, da keine solche Urkunde Bestandteil der Begehungsweise ist.

§ 274 Urkundenunterdrückung

Genau wie Sachverhalt 1 scheitert die Subsumtion dieser Norm am Tatobjekt der echten Urkunde, da es sich bei der von der Täterschaft erstellten Urkunde gegenüber der Bank um eine falsche Urkunde handelt und anderweitig der Fall keine echte Urkunde beinhaltet.

§ 303a Datenveränderung

Unter dem Verweis auf Kapitel 5.1 kann auch hier festgehalten werden, dass die abgefragte TAN nicht von der Norm erfasst wird. Bezüglich der Datenverwendung und des sonstigen Sachverhaltes kann sich demnach an Sachverhalt 1 orientiert werden, wonach der objektive Tatbestand nicht erfüllt wird. Bezüglich möglicher Vorbereitungshandlungen kann zunächst auf die Erläuterungen in Kapitel 4 verwiesen werden, wonach innerhalb des gesamten Sachverhaltes das Verschaffen von Passwörtern und Sicherungscodes in Form der Online-Banking-Informationen erfüllt wird. Aus der Beschreibung des Sachverhaltes geht nicht hervor, dass die Hintergrundsoftware selbstständig dazu in der Lage ist, Daten zu verändern. Aus diesem Grund wird diese vom Tatobjekt *Computerprogramm* nicht erfasst.

§ 303b Computersabotage

Auch im Rahmen von § 303b kann vollumfänglich auf den Sachverhalt 1 und die dortige Erläuterung verwiesen werden. Die Verwendung von Software zur Generierung der Überweisung und dem weiteren Ablauf ändert nichts daran, dass die in Abs. 1 Nr. 2 der Norm genannte Tathandlung nicht erfüllt wird, da hier die Datenverarbeitung selbst und nicht deren Ergebnis erfasst wird. Demnach wird der objektive Tatbestand nicht erfüllt. Vorbereitungshandlungen werden nicht erfüllt, da die Hintergrundsoftware gemäß den Schilderungen des Sachverhaltes nicht den Zweck besitzt, eine Computersabotage durchzuführen. Anderweitig sind keine Programme oder Passwörter und Sicherungscodes Bestandteil des Sachverhaltes.

5.3 Sachverhalt 3 – Smishing

Neben dem SMS-Versand, der Bereitstellung der Schadsoftware über den Link und der Installation dieser auf dem Telefon der Geschädigten stellt das Benutzen dieser den zweiten Teil der Tathandlung dar. Dabei agierte die Software eigenständig und veranlasste, dass weitere gleichartige SMS versendet wurden, wie sie auch die Geschädigte erhielt. Es kann nicht ausgeschlossen werden, dass die SMS, die die Geschädigte erhielt, auch von einer Schadsoftware versendet wurde. Aufmerksam auf den Sachverhalt wurde die Geschädigte durch eine Rechnung ihres Mobilfunkanbieters, der die entstandenen Kosten für den SMS-Versand in Rechnung stellte. Weitere Erkenntnisse und Funktionen der Schadsoftware sind nicht bekannt.

§ 202a Ausspähen von Daten

Wie bereits erläutert, stellt die Verwendung der Schadsoftware das erneute Versenden weiterer gleichartiger SMS dar, weshalb sich an den Erläuterungen in Kapitel 4.1 orientiert werden kann. Neben dem Datenbegriff, der auch alle Informationen auf weiteren Telefonen potenzieller Geschädigten einschließt, die eine der versendeten SMS erhielten und die Schadsoftware installierten, können ebenso die Erläuterungen für den Verfügungswillen der Geschädigten übertragen werden. Aus diesem Grund scheitert auch das Benutzen der Schadsoftware am Merkmal der Zugangssicherung, da für den SMS Versand keine überwunden werden muss.

§ 202b Abfangen von Daten

Genauso wie bei den anderen Sachverhalten kann auch hier auf die Problematik verwiesen werden, dass keine nichtöffentliche Datenübermittlung zwischen zwei Parteien außerhalb der Täterschaft vorhanden ist oder eine elektromagnetische Abstrahlung abgefangen wird.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

Aufgrund der Ähnlichkeit zwischen dem Installieren und Verwenden der Schadsoftware kann sich auch hier an den Erläuterungen aus Kapitel 4.3 orientiert werden. Demnach scheitert eine Erfüllung des objektiven Tatbestandes daran, dass zum einen keine Passwörter oder Sicherungscodes Bestandteil der Begehungsweise sind und zum anderen nicht bekannt ist, dass die Schadsoftware als Computerprogramm weitere Funktionen ausführt, die den Zweck zur Begehung einer Tat nach den §§ 202a und 202b erfüllen.

§ 202d Datenhehlerei

Die Subsumtion dieser Norm scheitert am Tatobjekt *Daten*. Aus der Schilderung des Sachverhaltes geht nicht eindeutig hervor, dass tatsächlich Daten erlangt wurden, da die Schadsoftware möglicherweise lediglich den Zugang zu Daten gewährt. Zudem kann davon ausgegangen werden, dass es sich um eine Täterschaft handelt, die die Verfügung über die potenziell erlangten Daten erhält, weshalb dieser objektive Tatbestand nicht erfüllt wird.

§ 263a Computerbetrug

Zunächst stellt ein SMS-Versand einen Datenverarbeitungsvorgang beim Mobilfunkanbieter dar, der die versendete SMS auf dem Zieltelefon zum Ergebnis hat. Die Initialisierung dieses Vorgangs mittels Schadsoftware stellt zudem die Tathandlung des unbefugten Einwirkens auf diesen Vorgang dar. Die täuschungsähnliche Handlung wird durch die Ausführung der Schadsoftware realisiert, da diese vorgibt, dass der SMS-Versand von der Geschädigten ausgeführt wurde. Auch das letzte Merkmal *Vermögensschaden* wird bedient. Dies wird dadurch erfüllt, dass der Mobilfunkanbieter seine Ressourcen für das Versenden der SMS bereitstellt und diesen Vorgang letztlich auch ausführt. Zwar hat dieser den Versand bei der Telefonbesitzerin in Rechnung gestellt, allerdings ist bei diesem zunächst der Schaden entstanden. Durch die nicht bezahlte Ressourcennutzung ist bei einem Vergleich vor und nach dem Datenverarbeitungsvorgang eine unmittelbare Verringerung des Vermögens festzuhalten. Demzufolge kann der objektive Tatbestand als erfüllt betrachtet werden, indem nicht die Telefonbesitzerin als geschädigt betrachtet wird, sondern der Anbieter. Innerhalb der Vorbereitungshandlungen aus Abs. 3 ändert das Benutzen der Schadsoftware nichts daran, dass Passwörter und Sicherungscodes aus Nr. 2 nicht fester Bestandteil des Sachverhaltes sind. Bezüglich einer Subsumtion der Schadsoftware unter das Tatobjekt *Computerprogramm* bleibt es bei einer Erfüllung möglicher Handlung im Vorfeld der eigentlichen Phishing-Handlung. Nach der Phishing-Handlung wird keine Tathandlung mit Bezug auf das Objekt Computerprogramm erneut erfüllt.

§ 269 Fälschung beweiserheblicher Daten

Da mit dem Benutzen der Schadsoftware weitere gleichartige SMS versendet werden, wie sie auch die Geschädigte erhielt, kann die Argumentation aus Kapitel 4.6 übernommen werden. Demnach wird die versendete SMS auch hier vom Datenbegriff erfasst. Gleichzeitig stellt jede einzelne SMS wieder eine rechterhebliche Erklärung dar. Auch die Merkmale der Beweiserheblichkeit und der Erkennbarkeit der Person sowie die geschilderten Tathandlungen werden von jeder versendenten SMS erfüllt, weshalb jeder dieser Vorgänge für sich genommen von der Norm erfasst wird.

§ 271 Mittelbare Falschbeurkundung

Auch einschließlich der Verwendung der Software findet sich in diesem Sachverhalt keine öffentliche Urkunde mit amtlicher Gewähr auf Richtigkeit, weshalb die Subsumtion am Tatobjekt scheitert.

§ 274 Urkundenunterdrückung

Da dieser Sachverhalt zu keinem Zeitpunkt eine echte Urkunde beinhaltet, wird der objektive Tatbestand nicht erfüllt.

§ 303a Datenveränderung

Die Aufgabe der Schadsoftware, gleichartige SMS zu versenden, ändert nichts an der Betrachtungsweise, wie sie in Kapitel 4.9 erläutert wurde. Nach wie vor stellt die Installation der Schadsoftware eine Datenveränderung nach § 303a da. Die Ausführung der Schadsoftware mit dem Versenden der SMS erfüllt für sich genommen den objektiven Tatbestand erneut, da durch den SMS-Versand ebenfalls Daten unbefugt verändert werden. Dies geschieht durch das Hinzufügen von Daten innerhalb des Postausgangs auf dem Telefon. Innerhalb der Vorbereitungshandlungen kann sich ebenso an den Erläuterungen aus Kapitel 4 orientiert werden. Durch den Umgang mit der Schadsoftware aufseiten der Täterschaft können mehrere Handlungsmöglichkeiten im Rahmen einer Vorbereitung erfüllt werden. Dies geschieht allerdings im Vorfeld der Phishing-Handlung und wird nach der Installation der Schadsoftware nicht erneut erfüllt.

§ 303b Computersabotage

Für den Begriff des Datenverarbeitungsvorgangs lassen sich mehrere mögliche Tatobjekte detektieren. Zunächst findet sich ein Datenverarbeitungsvorgang aufseiten des Mobilfunkanbieters. Wie auch im Rahmen von § 263a umfasst dieser das Verarbeiten und Senden von SMS. Ebenso erfüllt dieses Tatobjekt das Merkmal der wesentlichen Bedeutung, da diese Vorgänge innerhalb der geschäftlichen Tätigkeiten des Unternehmens einen Bereich darstellen. Durch die Benutzung der Schadsoftware werden kein Datenträger oder eine entsprechende Verarbeitungsanlage nach Abs. 1 Nr. 3 angegriffen, mit dem Ziel, den erläuterten Verarbeitungsvorgang zu stören. Allerdings wird der Vorgang dadurch beeinflusst, dass nach Nr. 2 durch die Initialisierung des SMS-Versandes Daten übermittelt werden. Dabei wird unter dem Begriff „Übermitteln“ ein möglicher Handlungsbereich zusammengefasst, wobei dieser jegliches Versenden von Informationen zwischen Datenverarbeitungsanlagen auf elektronischem Weg erfasst [27, Rn. 12]. Vorausgesetzt der subjektive Tatbestand, dass die Täterschaft dies in der Absicht der Nachteilszufügung durchführt, wird erfüllt, wird diese Tathandlung erfasst. Ebenfalls betrachtet werden muss, inwieweit dieser Datenverarbeitungsvorgang erheblich gestört wird. Eine mögliche Begehungsweise stellen dabei Denial-of-Service-Angriffe (DOS-Angriffe) dar [26, Rn. 12]. Eine solche DOS-Attacke richtet sich gegen die Verfügbarkeit von Diensten und versucht diese durch einen hohen Datenverkehr zum Zusammenbruch zu bringen [43]. Aus den Schilderungen geht nicht hervor, dass durch das mehrfache Versenden dieser SMS nach dem Schema eine DOS-Attacke der Dienst des Mobilfunkanbieters als

Datenverarbeitungsvorgang gestört wurde. Aus diesem Grund kann eine Erfüllung des objektiven Tatbestandes nicht bestätigt werden. In Nr. 1 wird die Norm mit § 303a verknüpft. Demnach erfüllt das in § 303a genannte Verändern von Daten innerhalb des Postausgangs auf dem Telefon der Geschädigten gleichzeitig die Tathandlung nach Nr. 1. Allerdings ist den Erläuterungen aus Kapitel 2.11 zu entnehmen, dass Datenverarbeitungsvorgänge im Zusammenhang mit erwerbstätigen, kulturellen oder bildenden Aufgaben stehen müssen. Aufgrund der geschilderten Begehungsweise geht nicht eindeutig hervor, inwieweit entsprechende Vorgänge beeinträchtig wurden sind, weshalb eine Bewertung dieses Sachverhaltes nicht abschließend vorgenommen werden kann. Da im Rahmen möglicher Vorbereitungshandlungen nicht bekannt ist, dass die Schadsoftware als Computerprogramm dem Zweck dient, eine Computersabotage zu begehen, wird dies als Tatobjekt nicht erfasst, weshalb eine Vorbereitungshandlung nicht erfüllt wird.

6 Diskussion der Ergebnisse

In diesem Kapitel sollen die Ergebnisse unter Betrachtung der in der Einleitung genannten Fragen evaluiert werden. Dafür werden zunächst die Ergebnisse aus den vorangegangenen Kapiteln zusammengefasst und in Tabellen gelistet. Anschließend erfolgt eine Betrachtung dieser.

6.1 Zusammenfassung der Subsumtion

Die nachfolgenden Tabellen listen auf, welcher objektive Tatbestand von welchem Sachverhalt erfüllt wird. Bei einer Erfüllung ist die entsprechende Zelle mit einem Kreuz markiert. Die Zahlen in der äußersten linken Spalte repräsentieren die drei Sachverhalte.

Tabelle 1 - Erfüllung objektiver Tatbestände beim Erlangen von Daten

	202a	202b	202c	202d	263a	Vorbereitung 263a	269	271	274	303a	303b	Vorbereitung 303a	Vorbereitung 303b
1							X						
2						X	X					X	
3							X			X			

Tabelle 2 - Erfüllung objektiver Tatbestände innerhalb der gesamten Sachverhalte

	202a	202b	202c	202d	263a	Vorbereitung 263a	269	271	274	303a	303b	Vorbereitung 303a	Vorbereitung 303b
1					X		X						
2					X	X	X					X	
3					X	X	X			X		X	

Die Zusammenfassung erfolgt sortiert nach den einzelnen Sachverhalten. Dabei wird für jeden objektiven Tatbestand geschildert, warum dieser als erfüllt oder nicht erfüllt zu bewerten ist.

6.1.1 Sachverhalt 1 – Smishing mit Telefonat

§ 202a Ausspähen von Daten

Der objektive Tatbestand dieser Norm wird weder durch die eigentliche Phishing-Phase noch durch das Verwenden der erlangten Informationen erfüllt. Zunächst werden die Informationen, die der Geschädigte an die Täterschaft übermittelt, nicht vom Datenbegriff erfasst, da jene Übermittlung im Klartext erfolgt und somit die Informationen in unmittelbar wahrnehmbarer Form vorliegen. Das zweite Merkmal, das den Verfügungswillen des Berechtigten betrifft, kann nicht bewertet werden, da nicht bekannt ist, inwieweit die Daten unter Kenntnis des Geheimhaltungsinteresses aufseiten der Geschädigten übermittelt wurden. Zuletzt muss auch das dritte Merkmal der Zugangssicherung und die damit verknüpfte Tathandlung der Überwindung dieser als nicht erfüllt betrachtet werden, da durch die freiwillige Herausgabe der Informationen keine Zugangssicherung von der Täterschaft überwunden werden muss. Vom Datenbegriff erfasst werden sämtliche Informationen, die gespeichert auf den Servern der Bank vorliegen. Ebenso schließt der Verfügungswille des Geschädigten den Täterkreis nicht ein. Allerdings wird durch eine freiwillige Herausgabe von Log-In-Informationen bezüglich eines möglichen Online-Bankkotos eine Zugangssicherung ausgehebelt. Darüber hinaus ist eine Log-In-Handlung seitens der Täterschaft in ein entsprechendes Konto nicht bestätigbar und nicht bekannt, inwieweit durch eine Verwendung der Informationen eine Überweisung generiert wurde, weshalb einer Erfüllung des objektiven Tatbestandes auch durch eine Datenverwendung nicht zugestimmt werden kann.

§ 202b Abfangen von Daten

Entsprechend der Orientierung der Norm an § 202b werden die Informationen, die die Täterschaft durch die Phishing-Phase erlangte, auch hier nicht vom Datenbegriff erfasst. Ebenso kann einer Bewertung des Verfügungswillens nicht vorgenommen werden. Da die Kommunikation sowohl während der Phishing-Phase als auch außerhalb dieser direkt zwischen der Täterschaft und dem Geschädigten stattfindet und anderweitig keine nichtöffentliche Datenübermittlung oder elektromagnetische Abstrahlung abgefangen wird, ist der objektive Tatbestand als nicht erfüllt zu betrachten.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

Zu keinem Zeitpunkt sind Passwörter oder Sicherungscodes Bestandteil der Begehungsweise, da lediglich eine EC-Kartennummer, das Gültigkeitsdatum der Karte sowie Telefonnummer und E-Mail-Adresse des Geschädigten erlangt wurden und anderweitig ein Vorhandensein entsprechende Informationen nicht bekannt ist. Mit der Begründung, dass

Websites nicht vom Begriff Computerprogramm erfasst werden, scheitert der Sachverhalt auch an diesem Tatobjekt.

§ 202d Datenhehlerei

Neben der Problematik, dass durch den Verweis auf den Datenbegriff aus § 202a die Informationen, die durch die Phishing-Handlung erlangt wurden, nicht erfasst werden, stellt jene Handlung die Tat zur Erlangung selbst da. Anderweitig wurden durch eine Vortat keine Daten erlangt. Auch die Erweiterung auf den gesamten Sachverhalt erfüllt den objektiven Tatbestand nicht. Zwar liegen die erlangten Informationen gespeichert in nicht wahrnehmbarer Form aufseiten der Täterschaft vor, allerdings ist von einer Täterschaft auszugehen, die bereits durch eine Vortat nach § 269 die Verfügungsgewalt über die Informationen erlangt und dementsprechend diese nicht durch eine andere Person im Vorfeld erlangt wurden.

§ 263a Computerbetrug

Innerhalb der Phishing-Handlung scheitert die Subsumtion am Tatobjekt des Datenverarbeitungsvorgangs, da dieser Begriff die Verarbeitung von Daten mittels Programme umfasst und Websites nicht als diese betrachtet werden können. Aus diesem Grund fehlt dieses Tatobjekt auch innerhalb einer Vorbereitungshandlung. Wie bereits erläutert, sind Programme und Sicherungscodes zu keinem Zeitpunkt Bestandteil dieser Phase, weshalb auch auf diese Weise eine Vorbereitungshandlung nicht erfüllt wird. Zudem fehlt es an einem Vermögensschaden. Außerhalb der Phishings-Handlung wird ein Datenverarbeitungsvorgang durch die Bank in Form der Überweisung durchgeführt. Durch die unbefugte Verwendung von Daten wird auf diesen Vorgang seitens der Täterschaft eingewirkt. Zwar fehlt es an einer Vollendung der Tat, da der Geschädigte die TAN nicht übermittelt, allerdings wird ein Versuch nach Abs. 2 der Norm erfüllt, weshalb der Sachverhalt vollständig unter den objektiven Tatbestand subsumiert werden kann.

§ 269 Fälschung Beweiserheblicher Daten

Zunächst werden die Informationen, die durch SMS und Website innerhalb der Phishing-Handlung dargestellt werden, vom Datenbegriff der Norm erfasst. Durch die SMS möchte die Täterschaft vorgeben, dass sie die Bank sind und mit Bezug auf einen bestehenden Vertrag zum Geschädigten auf diesem Weg in Kontakt treten möchte. Das Merkmal der rechtserheblichen Erklärung wird ebenso von der Website erfüllt. Gleichzeitig ist die Identität der erklärenden Person sowohl aus SMS als auch Website eindeutig feststellbar, weshalb Datenurkunden vorliegen. Im Bereich der Tathandlungen werden das Speichern

sowie das Gebrauchen solcher Daten erfüllt. Außerhalb der Phishing-Handlung liegt eine Datenurkunde durch den Überweisungsauftrag in Verbindung mit der TAN vor. Dabei liegt das Beweisinteresse darin, dass sich die Täterschaft als Kontoinhaber ausweisen möchte, wodurch auch die erklärende Person erkennbar ist. Durch § 270 wird die Beeinflussung des Datenverarbeitungsvorgang des Sachverhaltes mit der Täuschung einer Person aus § 269 gleichgestellt, weshalb dieser Sachverhalt von der Norm erfasst wird. Da die Täterschaft die TAN nicht erhält, wird ein Versuch nach Abs 2 erfüllt.

§ 271 Mittelbare Falschbeurkundung

Aufgrund des fehlenden Tatobjektes der öffentlichen Urkunde erfüllt weder die Phishing-Handlung noch der restliche Sachverhalt den objektiven Tatbestand dieser Norm.

§ 274 Urkundenunterdrückung

Da nur echte Urkunden von der Norm erfasst werden, die Datenurkunde innerhalb und außerhalb der Phishing-Handlung allerdings falsche Urkunden darstellen, wird der objektive Tatbestand nicht erfüllt.

§ 303a Datenveränderung

Der objektive Tatbestand dieser Norm wird nicht erfüllt. Zu keinem Zeitpunkt erhält die Täterschaft Zugriff auf das Telefon des Geschädigten. Durch das Betreiben der Website und das Versenden der SMS werden keine Daten verändert. Außerhalb des Erlangens der Informationen stellt eine TAN zwar eine Information dar, die nach der Benutzung für eine Überweisung nicht noch einmal vom Geschädigten verwendet werden kann, weshalb diese unbrauchbar gemacht wurde, allerdings liegt die Zweckbestimmung einer TAN in der Verwendung dieser Informationen. Solche werden nicht vom Begriff des Unbrauchbarmachens geschützt. Da anderweitig keine Daten verändert werden, wird der objektive Tatbestand nicht erfüllt. Vorbereitungshandlungen werden sowohl innerhalb dieser Norm als auch in der darauffolgenden Norm aufgrund fehlender Tatobjekte nicht erfüllt.

§ 303b Computersabotage

Da wie bereits im Zusammenhang mit § 263a erläutert, innerhalb der Phishing-Handlung kein Datenverarbeitungsvorgang vorhanden ist, scheitert die Subsumtion hier am Tatobjekt. Gleiches kann auch bei einer Verwendung der Daten festgehalten werden, da im

Rahmen dieser Norm im Gegensatz zu § 263a nicht das Ergebnis, sondern der Datenverarbeitungsvorgang selbst im Mittelpunkt steht.

6.1.2 Sachverhalt 2 – Phishing

§ 202a Ausspähen von Daten

Wie auch in Sachverhalt 1 werden die übermittelten Informationen aufgrund der Übermittlung im Klartext nicht von der Norm erfasst. Ebenso kann der Verfügungswille der Person aus der Sachverhaltsschilderung nicht eindeutig bestimmt werden und es fehlt an einer Überwindung einer Zugangssicherung aufgrund der freiwilligen Herausgabe der Daten. Auch die Datenverwendung scheitert bei einer Subsumtion an der Zugangssicherung, da hier wie in Sachverhalt 1 die Daten freiwillige herausgegeben werden und beim Log-In in das Online-Banking Konto keine Zugangssicherung überwunden werden muss.

§ 202b Abfangen von Daten

Sowohl beim Erlangen als auch beim Verwenden von Informationen kann sich auch in § 202b an Sachverhalt 1 orientiert werden. Der objektive Tatbestand wird aufgrund des fehlenden Abfangens einer nichtöffentlichen Datenübermittlung oder elektromagnetischen Abstrahlung nicht erfüllt, wobei auch hier die übermittelten Informationen bereits nicht vom Datenbegriff erfasst werden und der Verfügungswillen des Geschädigten nicht bewertet werden kann.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

Die Phishing-Handlung hat keine Computerprogramme zum Inhalt. Die Online-Banking-Informationen können zwar unter dem Tatobjekt *Passwörter und Sicherungscodes* zusammengefasst werden, allerdings wird eine Erfüllung des objektiven Tatbestandes dadurch ausgeschlossenen, dass bei einer Verwendung der Informationen aufgrund der freiwilligen Herausgabe dieser keine Zugangssicherung überwunden werden muss. Eine Erfüllung des objektiven Tatbestandes von § 202a ist ausgeschlossen, weshalb auch eine Vorbereitungshandlung nicht erfüllt wird. Anderweitig sind keine Passwörter und Sicherungscodes Bestandteil des gesamten Sachverhaltes. Die Software, die automatische die Überweisung generiert, erfüllt zwar die Anforderungen an ein Computerprogramm, ist aber nicht dafür geeignet, eine Tat nach den §§ 202a oder 202b zu begehen, weshalb auch außerhalb des Erlangens von Informationen der objektive Tatbestand nicht erfüllt wird.

§ 202d Datenhehlerei

Wie auch der erste Sachverhalt scheitert dieser bei einer Subsumtion daran, dass Informationen vom Datenbegriff nicht erfasst werden und das Erlangen dieser durch die Phishing-Handlung die Vortat selbst darstellt. Ebenso erlangt die Täterschaft bereits durch die Vortat die Verfügungsgewalt.

§ 263a Computerbetrug

Auch in der Phishing-Handlung dieses Sachverhaltes findet sich kein Datenverarbeitungsvorgang, weshalb eine Erfüllung des objektiven Tatbestandes auf diesem Weg am Tatobjekt scheitert. Passwörter und Sicherungscodes werden durch die Online-Banking-Informationen dargestellt, weshalb das Erlangen dieser die Vorbereitung nach Abs. 3 erfüllt. Computerprogramme sind, wie auch bei § 202c, nicht Bestandteil der Phishing-Handlung. Außerhalb dieser Handlung ist die Begehungsweise auf die gleiche Art zu bewerten wie auch Sachverhalt 1. Auf einen Datenverarbeitungsvorgang der Bank wird durch die unbefugte Verwendung von Daten und den somit ausgelösten Überweisungsauftrag eingewirkt, wodurch beim Geschädigten unmittelbar eine Vermögensminderung stattfindet. Der objektive Tatbestand ist somit als erfüllt zu betrachten. Auch eine Vorbereitungshandlung kann hier durch den Umgang mit der Hintergrundsoftware erfüllt werden. Dies geschieht allerdings im Vorfeld der Phishing-Handlung.

§ 269 Fälschung Beweiserheblicher Daten

In Bezug auf die Phishing-Handlung besteht der wesentliche Unterschied zu Sachverhalt 1 darin, dass zu Beginn keine SMS, sondern eine E-Mail verschickt wird. Dennoch kann diese Begehungsweise gleich bewertet werden. Die E-Mail stellt eine Datenurkunde dar und bei einer entsprechenden Gestaltung der Website kann auch diese vom Begriff erfasst werden. Die Täterschaft erfüllt die Tathandlungen des Speicherns sowie des Gebrauchens solcher Daten. Ebenso gleich gelagert ist der Sachverhalt außerhalb der Phishing-Handlung. Durch den Überweisungsauftrag wird eine Datenurkunde bei der Bank gespeichert. Dabei ist für die Subsumtion unter diesen objektiven Tatbestand unerheblich, dass die Überweisung durch eine Software initialisiert wurde.

§ 271 Mittelbare Falschbeurkundung

Die Subsumtion dieser Norm scheitert am Tatobjekt der öffentlichen Urkunde, da zu keinem Zeitpunkt eine entsprechende Urkunde Bestandteil des Sachverhaltes ist.

§ 274 Urkundenunterdrückung

Da durch die Täterschaft lediglich falsche Urkunden erstellt werden, aber die Norm nur echte Urkunden erfasst, wird der objektive Tatbestand nicht erfüllt.

§ 303a Datenveränderung

Wie auch Sachverhalt 1 erfüllt diese Begehungsweise nicht den objektiven Tatbestand nach § 303a, da die Täterschaft keinen Zugriff auf das Telefon der Geschädigten erhält und anderweitig durch E-Mail und Website sowie die Eingabe der Informationen durch die Geschädigte keine Daten verändert werden. Ebenso wird die verwendete TAN aufgrund ihrer Zweckbestimmung nicht von der Norm geschützt. Allerdings wird das Verschaffen von Passwörtern und Sicherungscodes erfüllt, da die Online-Banking-Informationen Zugang zu Daten auf das Konto der geschädigten Person ermöglichen. Die Software hingegen wird außerhalb der Phishing-Handlung nicht von Tatobjekt des Programmes im Rahmen deiner Vorbereitung erfasst, da dieser der Zweck fehlt, selbstständig Daten zu verändern.

§ 303b Computersabotage

Abschließend wird dieser objektive Tatbestand nicht erfüllt, da die Phishing-Handlung keinen sabotierten Datenverarbeitungsvorgang beinhaltet. Im Gegensatz zu § 263a wird nicht das Ergebnis eines Datenverarbeitungsvorgangs, sondern jener selbst geschützt, weshalb eine Subsumtion wie in § 263a nicht erfolgreich durchgeführt werden kann. Da nicht bekannt ist, dass der Zweck der Software die Computersabotage ist und die Online-Banking-Informationen als Passwörter und Sicherungscodes im Sinne einer Computersabotage erlangt wurden, kann eine Erfüllung einer möglichen Vorbereitungshandlung nicht bestätigt werden.

6.1.3 Sachverhalt 3 – Smishing

§ 202a Ausspähen von Daten

Dieser objektive Tatbestand wird nicht erfüllt. Zwar werden die Informationen auf dem Telefon der Geschädigten vom Datenbegriff erfasst und ebenso schließt der Verfügungswille die Täterschaft nicht ein, allerdings installiert die Geschädigte die Schadsoftware selbst auf ihrem Telefon. Wie auch bei der freiwilligen Herausgabe der Daten ist es unerheblich, dass diese Freiwilligkeit auf einer Täuschung beruht. Die Täterschaft muss für die Installation keine Zugangssicherung überwinden, um sich Zugang zu Daten zu verschaff. Durch das Versenden der SMS werden anderweitig keine Daten ausgespäht. Da durch das Benutzen der Software auch wieder SMS versendet werden, mit denen dann lediglich

Zugang zu Schadsoftware verbreitet werden kann, erfüllt das Benutzen der Software ebenso wenig den objektiven Tatbestand.

§ 202b Abfangen von Daten

Wie bereits erläutert, kann sich beim Datenbegriff und dem Verfügungswillen an den Feststellungen zu § 202a orientiert werden. Da wie auch bei den anderen Sachverhalten eine nichtöffentliche Datenübermittlung fehlt, die nicht mit der Täterschaft stattfindet und auch sonst keine elektromagnetische Abstrahlung angefangen wird, ist der objektive Tatbestand als nicht erfüllt zu betrachten.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

Das erste mögliche Tatobjekt *Passwörter und Sicherungscodes* ist kein Bestandteil der Phishing-Handlung. Zwar stellt die Schadsoftware ein Computerprogramm dar, allerdings geht aus den Schilderungen zum Sachverhalt nicht hervor, dass diese auch für das Ausspähen und Abfangen von Daten geeignet ist, weshalb der objektive Tatbestand nicht erfüllt wird. Diese Erläuterungen können auch für das Benutzen der Schadsoftware übernommen werden.

§ 202d Datenhehlerei

Die Phishing-Handlung stellt die Vortat selbst dar, in der Daten erlangt wurden, weshalb diese den objektiven Tatbestand nicht erfüllen kann. Auch das Benutzen der Schadsoftware erfüllt diesen nicht, da zum einen Daten tatsächlich erlangt wurden sein müssen und zum anderen eine Verfügungsmacht übertragen wurden sein muss. Dies ist wie zuvor gezeigt auch außerhalb der Phishing-Handlung nicht der Fall.

§ 263a Computerbetrug

Die bloße Phishing-Phase erfüllt den objektiven Tatbestand nicht, da nicht bekannt ist, dass bei der Installation der Schadsoftware auf einen Datenverarbeitungsvorgang eingewirkt wurden ist. Zudem fehlt es an einer unmittelbar daraus resultierenden Vermögensminderung. Im Bereich der Vorbereitungshandlungen ist das Tatobjekt *Computerprogramm* relevant. Da die Schadsoftware dazu geeignet ist, einen Betrug zu begehen, kann der Umgang mit dieser mehrere Tathandlungsmöglichkeiten erfüllen. Dies geschieht allerdings außerhalb der Phishing-Handlung, weshalb diese selbst nicht unter eine mögliche Vorbereitungshandlung subsumiert werden kann. Außerhalb der Phishing-Phase wird

durch das Versenden einer SMS ein Datenverarbeitungsvorgang beim Mobilfunkanbieter dargestellt. Die ausgeführte Schadsoftware täuscht vor, die Telefonbesitzerin zu sein und wirkt unbefugt auf den Vorgang des SMS-Versand ein. Dadurch, dass der Telefonanbieter seine Ressourcen für den SMS-Versand bereitstellt, liegt nach diesem Vorgang eine unmittelbare Vermögensminderung vor. Das Benutzen der Schadsoftware erfüllt keine erneute Handlung im Rahmen des Tatobjektes *Computerprogramm*. Die bisherigen Erläuterungen dazu sind weiterhin relevant.

§ 269 Fälschung Beweiserheblicher Daten

Innerhalb der Phishing-Handlung erfüllt die SMS die Eigenschaften einer Datenurkunde und ist somit beweiserheblich. Innerhalb der Tathandlungen wird das Speichern sowie Gebrauchen erfüllt. Da das Verwenden der Schadsoftware auch wieder einen SMS-Versand mit gleichem Inhalt veranlasst, erfüllt dies ebenso den objektiven Tatbestand.

§ 271 Mittelabre Falschbeurkundung

Wie auch die anderen Sachverhalte scheitert die Subsumtion am Tatobjekt der öffentlichen Urkunde.

§274 Urkundenunterdrückung

Auch dieser Sachverhalt erfüllt die Norm nicht, da die versendeten SMS falsche Urkunden darstellen und anderweitig keine echten Urkunden im Sachverhalt vorhanden sind.

§ 303a Datenveränderung

Innerhalb dieses Sachverhalts wird der objektive Tatbestand dieser Norm durch die Tathandlung des Veränderns von Daten erfüllt. Dies geschieht durch die Installation der Schadsoftware auf dem Telefon der Geschädigten, da Daten hinzugefügt werden. Durch die Benutzung der Software und dem damit einhergehenden Versenden von SMS wird der objektive Tatbestand erneut erfüllt, da die versendeten SMS im Postausgang des Telefons erscheinen und somit auch Daten hinzugefügt wurden. Ebenso kann der Umgang mit der Schadsoftware Vorbereitungshandlungen erfüllen. Wie auch bei § 263a geschieht dies allerdings außerhalb der Phishing-Phase.

§ 303b Computersabotage

Es ist nicht bekannt, dass durch die Phishing-Handlung Datenverarbeitungsvorgänge gestört werden. Bei einem Benutzen der Schadsoftware werden mehrere SMS versendet. Geschieht dies in der Absicht, einem anderen einen Nachteil zuzufügen, können diese SMS den objektiven Tatbestand nach § 303b erfüllen. Durch das Versenden der SMS werden Daten übermittelt und somit auf das Versenden vom SMS als Datenverarbeitungsvorgang des Mobilfunkanbieters eingewirkt. Da aus den Schilderungen des Sachverhaltes allerdings nicht bestätigt werden kann, dass dieser Datenverarbeitungsvorgang erheblich gestört wurde, wird der objektive Tatbestand nicht erfüllt. Ebenso ergibt sich aus der Begehungsweise nicht, dass im Rahmen der Datenveränderung nach § 303a auf Datenverarbeitungsvorgänge auf dem Telefon der Geschädigten eingewirkt wurden ist, weshalb auch hier der objektive Tatbestand nicht erfüllt wird. Da der Schadsoftware der Zweck fehlt, Computersabotage zu begehen, wird diese im Rahmen möglicher Vorbereitungshandlungen vom Tatobjekt *Computerprogramm* nicht erfasst.

6.2 Betrachtung der Ergebnisse

Im Mittelpunkt jedes thematisierten objektiven Tatbestandes stehen verschiedene Tatobjekte. Diese werden durch verschiedene Begriffe dargestellt und erläutert. Die nachfolgende Tabelle listet zunächst alle zu betrachtenden Begriffe auf und kennzeichnet, in welcher Norm des StGB diese als Tatobjekt, im Rahmen einer Tathandlung oder anderweitig vorhanden sind.

Tabelle 3 - Vorkommen von Begrifflichkeiten im StGB

	202a	202b	202c	202d	263a	269	271	274	303a	303b
Daten	X	X	X	X	X	X	X	X	X	X
Passwörter und Sicherungscodes			X		X					
Computerprogramme			X		X					
Datenverarbeitungsvorgang					X					X
Datenverarbeitungsanlage		X								
Elektromagnetische Abstrahlung		X								
Datenübermittlung		X								

Aus der Tabelle ist zu entnehmen, dass der Begriff *Daten* die höchste Frequenz aufweist und in alle betrachteten Normen auftritt. Aufgrund dieser Tatsache erfolgt die Betrachtung der einzelnen Sachverhalte in Bezug auf ableitbare Schlussfolgerungen, gruppiert nach dem Datenbegriff. Zunächst taucht der Begriff *Daten* im § 202a auf. Nach Abs. 2 wird der Begriff auf Informationen eingegrenzt, die nicht unmittelbar wahrnehmbar gespeichert oder übermittelt sein müssen. Gemäß der Erläuterung aus Kapitel 2 darf der Inhalt nicht ohne technische Hilfsmittel ersichtlich sein. Diese Erläuterung findet neben dem § 202a auch in anderen Normen Verwendung. Auf diese ausdrücklich verwiesen wird in den §§ 202b, 202c, 202d, 274, 303a sowie 303b. Die §§ 263a, 269 und 271 benutzen zwar den Begriff, verweisen aber nicht explizit auf die Erläuterung aus § 202a Abs. 2.

6.2.1 Daten gemäß den §§ 202a, 202b, 202c, 202d, 303a, 303b

Die folgenden Erläuterungen befassen sich mit § 202a, dem dort enthaltenen Datenbegriff und allen weiteren Normen mit ihren eigenen Begriffen, die auf § 202a Abs. 2 verweisen.

§§ 202a, 202b, 202c - Ausspähen und Abfangen von Daten mit Vorbereitungshandlungen

Gemäß den Erläuterungen der vorherigen Kapitel schließt die Definition des Datenbegriffs jene Handlungen aus den Sachverhalten 1 und 2 aus, da die Informationen im Klartext an die Täterschaft übermittelt werden. Somit werden diese nicht von der Norm geschützt. Dem gegenüber stehen die Informationen, die auf dem Telefon der Geschädigten aus dem dritten Sachverhalt gespeichert sind. Diese fallen unter den Datenbegriff. Neben dem Datenbegriff selbst wird das Tatobjekt *Daten* durch weitere Merkmale eingegrenzt. Zum einen ist der Verfügungswille entscheidend. Dieses Merkmal ist davon abhängig, ob die geschädigte Person von ihrem Geheimhaltungsinteresse gegenüber der vorgetäuschten Identität weiß. Demzufolge hat die Begehungsweise auf dieses Merkmal nur bedingt Einfluss, beispielsweise durch die Wahl der vorgetäuschten Identität. Im dritten Sachverhalt kann davon ausgegangen werden, dass der Verfügungswille die Täterschaft nicht einschließt. Diese Annahme beruht darauf, dass gemäß den Schilderungen aus dem Sachverhalt zu keinem Zeitpunkt wissentlich Daten von der Geschädigten herausgegeben wurden. Dementsprechend kann geschlussfolgert werden, dass bei einem unbemerkten Eindringen in ein elektronisches Gerät der Verfügungswille die Täterschaft ausschließt und die Tatbestandsmerkmale, die daraus abgeleitet werden können, erfüllt sind. In Bezug auf das Merkmal der Zugangssicherung kann festgehalten werden, dass alle Handlungen der Geschädigten auf einer Freiwilligkeit beruhen. In den Sachverhalten 1 und 2 werden Informationen freiwillig preisgegeben, während die Geschädigte freiwillig im dritten Sachverhalt die Schadsoftware installierte. Daraus ergibt sich, dass dieses Merkmal nicht erfüllt wird, wenn ein entscheidender Schritt der Begehungsweise darauf beruht, dass die geschädigte Person freiwillig den Zugang zu Daten in irgendeiner Form gewährleistet und die Täterschaft eine möglicherweise vorhandene Zugangssicherung nicht überwinden muss. Bewegt die Täterschaft die geschädigte Person zu einer entsprechenden

Handlung, wird auch das Benutzen erlangte Informationen nicht von der Norm erfasst, wenn es sich beispielsweise um Passwörter handelt.

Wie erläutert, ist der Datenbegriff auch Bestandteil von § 202b einschließlich des Verfügungswillen. Da alle Sachverhalte bei einer Subsumtion am Tatobjekt scheitern, weil die Kommunikation direkt mit der Täterschaft stattfindet und anderweitig keine elektromagnetische Abstrahlung abgefangen oder eine sonstige nichtöffentliche Datenübermittlung angegriffen wird, lassen sich aus einer Bewertung dieser Norm keine weiteren Erkenntnisse gewinnen, weshalb auf diese Begrifflichkeiten nicht näher eingegangen wird.

Innerhalb von § 202c findet durch die repräsentierte Vorbereitungshandlung eine Verknüpfung mit den § 202a und 202b sowie mit dem daran enthaltenen Datenbegriff statt. Als Tatobjekt werden Passwörter oder sonstige Sicherungscodes sowie Computerprogramme genannt. Wie in Kapitel 2 erläutert, können Passwörter und Sicherungscode in visuell wahrnehmbarer Form vorliegen, müssen allerdings zum Zeitpunkt der Tathandlung gültig sein. Innerhalb von Sachverhalt 2 werden Online-Banking-Informationen erlangt, die unteranderem ein Passwort enthalten müssen und Zugang zu Informationen innerhalb des Kontos liefern können. Da allerdings bei einer Benutzung der Informationen keine Zugangssicherung überwunden wird und somit § 202a nicht erfüllt werden kann, scheitert auch die Subsumtion bei § 202c im Rahmen einer möglichen Vorbereitungshandlung. Somit kann festgehalten werden, dass diese Begehungsweise, die auf einer Freiwilligkeit der Geschädigten beruht, sich auch auf eine Erfassung durch § 202c negativ auswirkt. Das zweite Tatobjekt *Computerprogramme* weist die Problematik seiner Zweckbestimmung auf, woraus ein illegaler Zweck erkennbar sein muss. Ebenso ergibt sich die Problematik, was als Programm bewertet wird. Das OLG Rostock hatte festgelegt, dass Programme für Ablaufsteuerungen geeignet sein müssen. Da Websites aufgrund dieser Anforderung nicht als Programm angesehen werden können, erfüllt das Phishing mit einer Website auch nicht das zweite Tatobjekt eines Computerprogramms. Auch anderweitig hat die Begehungsweise Einfluss auf das Tatobjekt *Computerprogramm*. Als beschreibendes Merkmal wird genannt, dass die Software für eine Begehung einer solchen Tat geeignet sein muss. Zwar lässt sich im zweiten und dritten Sachverhalt Software detektieren, allerdings sind diese für eine Tat nach den §§ 202a oder 202b gerade nicht geeignet. Diese können weder Zugangssicherungen überwinden noch Datenübermittlungen oder elektromagnetische Abstrahlungen abfangen.

§ 202d Datenhehlerei

Das Tatobjekt dieser Norm stellen Daten dar, wobei auf die Erläuterungen aus § 202a Abs. 2 verweisen wird. Aus einer Subsumtion der Sachverhalte unter dieser Norm lassen sich keine weiteren Erkenntnisse gewinnen, da mögliche Phishing-Handlungen zunächst die Vortat selbst repräsentieren und anschließend keine Übertragung einer Verfügungskontrolle über Daten in irgendeiner Form stattfindet.

§ 303a Datenveränderung

Diese Norm schützt Daten nach § 202a vor einer Reihe rechtswidriger Eingriffshandlungen. Da in den Sachverhalten 1 und 2 durch das Betreiben der Websites und das Versenden von E-Mail und SMS zunächst keine Daten verändert werden, lassen sich hier keine Erkenntnisse gewinnen. Durch die Initialisierung der TAN wird diese für zukünftige Überweisungen der geschädigten Person unbrauchbar, da jede einmalig verwendet wird. Wie erläutert, wird sie dennoch nicht von der Norm erfasst, da die Bestimmung der TAN in ihrer Verwendung liegt. Entsprechend kann daraus abgeleitet werden, dass die Begehungsweise durchaus die Nichterfüllung dieser Norm beeinflussen kann, wenn die Handlung und Vorgehensweise der Täterschaft entsprechende Informationen beinhaltet. Wie gezeigt erfüllt der dritte Sachverhalt hingegen den objektiven Tatbestand der Norm dadurch, dass Daten auf dem Telefon bereits bei der Installation unbefugt verändert werden. Des Weiteren werden auch beim Versenden von weiteren SMS Daten hinzugefügt, weshalb auch das Benutzen der Schadsoftware den objektiven Tatbestand erfüllt. Innerhalb der Vorbereitungshandlung nach § 202c lassen sich zwei mögliche Handlungen detektieren. Zunächst wird sich durch die Online-Banking-Informationen dem Tatobjekt *Passwörter und Sicherungscodes* verschafft, da mithilfe dieser der Zugang zu Daten innerhalb des Kontos der geschädigten Person ermöglicht wird. Andererseits wird das Tatobjekt *Computerprogramm* durch Sachverhalt 3 erfüllt, da die Schadsoftware, die sich auf dem Telefon der Geschädigten installiert, für eine Datenveränderung geeignet ist. Dementsprechend kann der Umgang mit dieser Software Vorbereitungshandlungen erfüllen, allerdings im Vorfeld möglicher Phishing-Handlungen. Während und nach der Phishing-Phase werden keine weiteren Vorbereitungshandlungen erfüllt. Aus diesen Feststellungen ergibt sich, dass Installieren von Schadsoftware im Rahmen von Phishing beziehungsweise der Sonderform Smishing eine Datenveränderung nach sich zieht und zudem Vorbereitungshandlungen bei entsprechendem Umgang mit dieser erfüllt sein können. Eine größere Varianz in den detektierbaren objektiven Tatbestandsmerkmalen und ein dementsprechender Einfluss der Begehungsweise darauf ergibt sich durch das Phishing mit dem Ziel des Informationsgewinns. Zwar erfüllt weder Sachverhalt 1 noch Sachverhalt 2 den objektiven Tatbestand der Norm selbst, allerdings kann das Erlangen von Passwörtern und Sicherungscodes wie im Rahmen von Sachverhalt 2 eine Vorbereitungshandlung nach § 303a erfüllen.

§ 303b Computersabotage

Innerhalb dieser Norm wird zunächst der Begriff der Datenverarbeitung genannt, worunter gemäß der Erläuterung aus Kapitel 2 jegliche Nutzung von Daten verstanden wird. Da in keiner Begehungsweise ein Datenverarbeitungsvorgang gestört wird, ergibt eine Subsumtion keine neuen Erkenntnisse. Zwar wird, wie auch in § 303a auf eine Vorbereitungshandlung nach § 202c verwiesen, allerdings fehlt es beim Tatobjekt der Computerprogramme, in Form der Schadsoftware aus Sachverhalt 3 und der Hintergrundsoftware aus

Sachverhalt 2 an einer Geeignetheit Computersabotage zu begehen, weshalb sich auch hier keine neuen Erkenntnisse ergeben. Dasselbe gilt für die Online-Banking-Informationen als Tatobjekt der Passwörter und Sicherungscodes, wobei hier die gleiche Varianz detektierbar ist wie in § 303a, eine Subsumtion allerdings an der unbeantwortbaren Frage scheitert, ob dadurch eine Computersabotage vorbereitet werden sollte.

6.2.2 Daten gemäß den §§ 269, 271 und 274

Im Gegensatz zu den zuvor erläuterten Normen stehen im Mittelpunkt aus § 269 nicht die durch Phishing erlangten Informationen, sondern jene, die die Täterschaft durch ihre Handlungen selbst erzeugt. Diese Konstellation zeigt sich auch durch die Einordnung der Normen im Bereich der Urkundenfälschung.

§ 269 Fälschung Beweiserheblicher Daten

Gemäß den Erläuterungen aus Kapitel 2 ist diese Norm das digitale Äquivalent zur analogen Urkundenfälschung. Beim Datenbegriff wird nicht auf § 202a verweisen, weshalb dieser neu bestimmt werden muss. Unter dem Datenbegriff werden alle Informationen verstanden, dessen Inhalt nicht über menschliche Kommunikationswege erfasst werden können und die in codierter Form vorliegen. Daraus ergibt sich in der Definition des Begriffes, dass die Codierung auch in sichtbarer Form vorliegen kann, beispielsweise durch Strichcodes [22, Rn. 14]. Im Gegensatz dazu werden diese von der Definition nach § 202a Abs. 2 nicht erfasst [17, Rn. 19]. Bei dieser Norm ist zu prüfen, inwieweit eine falsche Datenurkunde in den Sachverhalten vorliegt. E-Mail, SMS sowie die Websites erfüllen sämtliche Eigenschaften einer Datenurkunde. Die entscheidende Handlung der Täterschaft ist das Abgeben einer falschen Erklärung bezüglich der Identität. Dabei kann festgehalten werden, dass der Weg, auf dem diese Erklärung abgegeben wird, unerheblich ist, solange die Informationen vom Begriff Daten erfasst werden. Außerdem erfüllt die Website für sich genommen ebenfalls die Eigenschaften einer Datenurkunde, weshalb für eine Erfassung von Phishing-Handlungen diese nicht zwangsläufig mit E-Mails oder SMS beginnen müssen. Gelangt der Bankkunde auf anderem Wege auf eine solche Website, kann diese dennoch den objektiven Tatbestand erfüllen. Neben E-Mail, SMS und Website wird beim Verwenden der erlangten Informationen ebenso eine falsche Datenurkunde durch das Initialisieren der Überweisung aufseiten der Bank gespeichert. Dementsprechend erfüllt diese Begehungsweise den objektiven Tatbestand der Norm mehrfach. Der dritte Sachverhalt hingegen erfüllt dies zunächst nur durch das Versenden der SMS, da nicht bekannt ist, inwieweit beim Installationsprozess weitere falsche Datenurkunden auftraten. Durch die Funktion der Schadsoftware wird beim Gebrauchen dieser der objektive Tatbestand dennoch erneut und somit ebenso mehrfach erfüllt.

§§ 271 und 274 Mittelbare Falschbeurkundung und Urkundenunterdrückung

Diese Normen sind angelehnt an § 269 und grenzen den Begriff „Beweiserhebliche Daten“ durch zusätzliche Eigenschaften ein. Im Mittelpunkt von § 271 stehen öffentliche Urkunden, wobei von dieser Norm jene Urkunden mit falschem Inhalt erfasst werden. Da solche Urkunden nicht Bestandteil der Sachverhalte sind, liefert eine Subsumtion keine weiteren Erkenntnisse. Innerhalb von § 274 Abs. 1 Nr. 2 wird zwar auf den Datenbegriff nach § 202a Abs. 2 verwiesen, aufgrund des Begriffes der Beweiserheblichkeit, der im Gesetzestext dem Datenbegriff vorangestellt wurde, ergibt sich ebenso eine Anlehnung an § 269. Deshalb ist der Inhalt der Norm ebenso eine Datenurkunde. Da allerdings nur echte Urkunden von der Norm erfasst werden und diese ebenso wenig Bestandteil der Sachverhalte sind wie öffentliche Urkunden, ergeben sich aus einer Subsumtion auch hier keine neuen Erkenntnisse.

6.2.3 Daten gemäß § 263a Computerbetrug

Der Datenbegriff dieser Norm orientiert sich an allgemeinen Auslegungsgrundsätzen und umfasst alle codierten und maschinenlesbaren Informationen. Dabei ist auf einen Verweis auf § 202a bewusst verzichtet wurden damit auch Informationen, die im Rahmen der Tathandlung erst durch eine Eingabe zu Daten werden, erfassbar sind [21, Rn. 22]. Der zweite Begriff *Datenverarbeitungsvorgang* erfasst die Eingabe, die anschließende Verarbeitung dieser und die Ausgabe von Ergebnissen. Dabei ist eine genauere Definition des Begriffes als in § 303b feststellbar. Alle Sachverhalte erfüllen den objektiven Tatbestand der Norm. Innerhalb von Sachverhalt 1 und 2 geschieht dies durch das Initialisieren des Überweisungsauftrags, da durch das Gebrauchen der erlangten Informationen auf das Ergebnis eines Datenverarbeitungsvorgangs mittels unbefugter Verwendung von Daten eingewirkt wird. Dies hat unmittelbar eine Vermögensminderung zur Folge. Der dritte Sachverhalt erfüllt bei einer Verwendung der Schadsoftware ebenso den objektiven Tatbestand. Zunächst wird auf das Ergebnis eines Datenverarbeitungsvorgangs in Form des SMS-Versands unbefugt eingewirkt. Auch dies hat eine Vermögensverschiebung zu Folge, wobei das Vermögensminderung nicht unmittelbar in Form von Geld, sondern durch die verbrauchten Ressourcen der Datenverarbeitung dargestellt wird. Allerdings ändert sich die geschädigte Person, die nicht durch die Telefonbesitzerin, sondern durch den Mobilfunkanbieter dargestellt wird. Somit kann festgehalten werden, dass im Gegensatz zur bloßen Phishing-Phase eine Verwendung entsprechender Informationen den objektiven Tatbestand von § 263a erfüllen kann. Gleiches ist für die Verwendung von Schadsoftware möglich, wenn die Begehungsweise durch eine entsprechende Funktion der Schadsoftware auf einen Computerbetrug abzielt. Im Bereich der Vorbereitungen lassen sich je nach Betrachtungsweise mehrere detektieren. Innerhalb der bloßen Phishing-Phase bzw. beim Installieren der Schadsoftware wird beim zweiten Sachverhalt durch das Erlangen der Online-Bank-Informationen das Verschaffen erfüllt. Bei Sachverhalt 3

können verschiedenen Handlungsmöglichkeiten durch den Umgang mit der Schadsoftware aufseiten der Täterschaft unterschieden werden, allerdings wieder im Vorfeld des Phishings. Demnach kann geschlussfolgert werden, dass auch auf die Erfüllung von Vorbereitungshandlungen die Begehungsweise Einfluss hat.

6.3 Phishing als Cyberstraftat

In Kapitel 3 wurde unabhängig von denen in der Einleitung genannten Zielstellungen die Frage aufgeworfen, ob die Bewertung von Phishing als Cybercrime im engeren Sinn korrekt ist und inwieweit die beiden Definitionen miteinander harmonieren. Wird die Definition von Manfred Wernert betrachtet, wonach für eine Straftat die Tatbestandsmerkmale der dazugehörigen Rechtsnorm des StGB auschlaggebend für eine Bewertung sind, kann seiner Erläuterung zugestimmt werden. Nach dieser Definition handelt es bei einer Straftat nach § 269 StGB um Cybercrime im engeren Sinn, da eine Datenurkunde als Bestandteil einer elektronischen Datenverarbeitung betrachtet werden kann. Da alle Phishing-Handlungen erfolgreich unter diesen Paragrafen subsumiert werden konnten, können diese auch als Cybercrime im engeren Sinn betrachtet werden. Gemäß der Einleitung definierte das Bundeskriminalamt den engeren Sinn als alle Straftaten, die sich gegen Datenverarbeitende Systeme, deren Daten selbst oder das Internet richten. Im dritten Sachverhalt wird durch die Sonderform des Phishings – dem Smishing – Schadsoftware verbreitet. Bereits bei deren Installation werden Daten auf dem Telefon der Geschädigten verändert und somit angegriffen. Deshalb kann die Phishing-Handlung des dritten Sachverhaltes auch nach der Definition des BKA als Cybercrime im engeren Sinn bezeichnet werden. Als entscheidende strafbare Handlung des ersten und zweiten Sachverhaltes lässt sich innerhalb der Phishing-Phase das Fälschen beweiserheblicher Daten bestimmen. Hierbei stellt sich nun die Frage, inwieweit durch diese Handlung nach der Definition des BKA ein Datenverarbeitendes System, deren Daten oder das Internet angegriffen werden. Da durch die Erstellung einer falschen Datenurkunde im Rahmen einer Phishing-Handlung ein solcher Angriff nicht zweifelsfrei bestätigt werden kann, kann eine solche Phishing-Handlung nach der Definition des BKA nicht als Cybercrime im engeren Sinn bezeichnet werden. Da darüber hinaus die erlangten Informationen der Phishing-Handlung zu keinem Zeitpunkt als Daten innerhalb einer Norm geschützt werden, kann das Erlangen dieser auch nicht als Angriff auf Daten bewertet werden. Wird der Blickwinkel hingegen auf die gesamten Sachverhalte ausgeweitet, wird von beiden der objektive Tatbestand des § 263a erfüllt. Da das Ergebnis einer Datenverarbeitung beeinflusst wird, kann das Phishing mit anschließender Benutzung der Informationen in den Fällen dieser beiden Sachverhalte als Angriff auf Daten bezeichnet werden. Demzufolge kann geschlussfolgert werden, dass die Phishing-Handlungen der Sachverhalte 1 und 2 lediglich in Verbindung mit einer anschließenden Verwendung der erlangten Informationen in der Lage sind, die Definition des BKA zu erfüllen und als Cybercrime im engeren Sinn eingestuft zu werden.

7 Fazit

Im Bereich der Begrifflichkeiten kann abschließend festgehalten werden, dass es innerhalb des StGB keine einheitliche Definition des Begriffes *Daten* gibt. Insgesamt lassen sich drei verschiedenen Auslegungen finden. Die erste Gruppe umfasst die §§ 202a bis 202d sowie 303a und 303b. Zwar stehen im Mittelpunkt dieser Normen Informationen potenziell geschädigter Personen, allerdings werden diese nicht zwangsläufig erfasst und geschützt. Phishing-Handlungen scheitern bereits am Datenbegriff von § 202a, wenn die Informationen im Klartext übermittelt werden, weshalb diese Begehungsweise einer Erfassung durch diese Norm umgehen kann. Weiterhin scheitert die Erfassung bei einer freiwilligen Herausgabe der Informationen an der notwendigen Zugangssicherung. Auch hier hat die Begehungsweise eine Möglichkeit, § 202a aus dem Weg zu gehen. Diese Freiwilligkeit wirkt sich auch auf § 202c und mögliche Vorbereitungshandlungen aus, da aufgrund dessen auch eine Verwendung der Informationen nicht von § 202a erfasst werden kann. Allerdings hat die Begehungsweise nicht auf alle Merkmale den gleichen Einfluss. Der Verfügungswille richtet sich nach dem Kenntnisstand der geschädigten Person bezüglich des Geheimhaltungsinteresses der Informationen gegenüber der vorgetäuschten Identität. Eine Kontrolle dieses Merkmals seitens der Täterschaft ist somit nur bedingt möglich. Auch das unbemerkte Eindringen in Geräte mittels Schadsoftware wird aufgrund einer fehlenden Überwindung einer Zugangssicherung nicht erfasst, wenn die geschädigte Person diese freiwillig installiert, wohingegen beim Verfügungswillen davon ausgegangen werden kann, dass dieser bei einem Eindringen nicht vorliegt. Abschließend kann festgehalten werden, dass die Täterschaft die Erfassung einer Begehungsweise nach 202a sowie 202c dadurch steuern kann, indem sie die geschädigte Person zu einer freiwilligen Ermöglichung des Zugangs zu Daten bewegt. Auch die §§ 303a und 303b beziehen sich auf den Datenbegriff nach § 202a Abs. 2. Hier hat die Begehungsweise ebenfalls Einfluss auf detektierbare objektive Tatbestandsmerkmale. Wie erläutert werden keine Informationen vor der Handlung des Unbrauchbarmachens geschützt, wenn deren Zweckbestimmung die Verwendung ist, wie es bei der TAN aus den Sachverhalten 1 und 2 der Fall ist. Dagegen wird das Installieren von Schadsoftware prinzipiell erfasst, da bei dieser Handlung Daten auf dem jeweiligen Gerät hinzugefügt werden müssen. Auf die Erfassung als Vorbereitungshandlung hat die Begehungsweise Einfluss. Je nach Art der erlangten Informationen kann dies eine Vorbereitung einer Datenveränderung erfüllen, wenn die Informationen Zugang zu entsprechenden Daten gewährleisten, wie beispielsweise in Sachverhalt 2. Ebenso kann der Umgang mit Schadsoftware eine Vorbereitungshandlung im Sinne des Tatobjektes *Computerprogramm* erfüllen, wenn diese Software entsprechende Funktionen aufweist und aufgrund dessen zur Datenveränderung geeignet ist. An dieser Stelle ist darauf hinzuweisen, dass einer Erfüllung dieser Vorbereitungshandlungen von der Betrachtungsweise abhängig ist. Die bloße Phishing-Handlung, in der Schadsoftware

installiert wird, erfüllt keine Vorbereitungshandlung im Rahmen von § 303a, da dies im Vorfeld und somit außerhalb der Phishing-Handlung geschieht.

Die zweite Gruppe, die sich aufgrund der verschiedenen Auslegungen des Datenbegriffes ergibt, umfasst die §§ 269, 271 sowie 274. Dabei kann aufgrund der unterschiedlichen Informationen unterschieden werden, dass beispielsweise Strichcodes zwar nicht von § 202a als Daten erfasst werden, allerdings von der Auslegung nach § 269. Im Mittelpunkt dieser Normen steht die Datenurkunde. Daraus ergibt sich eine neue Betrachtung der Sachverhalte, da nun nicht die erlangten Informationen subsumiert werden müssen, sondern jene, die durch die Täterschaft erzeugt werden. Phishing-Handlungen werden vom § 269 erfasst, da SMS, E-Mail und Website falsche Datenurkunden darstellen. Gleiches kann auch für solche Begehungsweisen festgehalten werden, in denen SMS verschickt werden, die Zugang zu Schadsoftware verbreiten möchten. Werden beim Phishing Online-Banking-Informationen erlangt, erfüllen diese die Norm zusätzlich, wobei es darauf ankommt, dass durch die Benutzung der Daten erneut eine falsche Datenurkunde gespeichert wird. Auch eine Begehungsweise bei Benutzung der Schadsoftware kann, wie in Sachverhalt 3 gezeigt, den objektiven Tatbestand bei einer entsprechenden Funktion der Schadsoftware erneut erfüllen. Auf die Nichterfüllung des objektiven Tatbestandes wie bei § 202a hat die Begehungsweise keinen Einfluss, da bereits das Versenden einer E-Mail oder SMS diesen erfüllt. Weitere Handlungen können sich lediglich auf eine mehrfache Erfüllung auswirken.

Die dritte Gruppe beinhaltet lediglich eine Norm, den § 263a. Wie erläutert, wurde dort bewusst auf einen Verweis auf die Erläuterung nach § 202a verzichtet. Im Mittelpunkt dieser Norm steht weder der Schutz von Daten selbst, wie beispielsweise in § 202a, noch eine Datenurkunde und daraus resultierende Entscheidungen wie bei § 269. Diese Norm möchte, wie in Kapitel 2 erläutert, das Vermögen von Personen schützen. Nach der Definition von Phishing und der Unterform des Smishings ist das Erlangen von Informationen bzw. das Installieren von Schadsoftware nicht in der Lage, einen Computerbetrug nach § 263a zu begehen. Werden hingegen die gesamten Sachverhalte einschließlich einer Verwendung der Informationen betrachtet, erfüllen alle den objektiven Tatbestand. Dabei wurde festgestellt, dass die Vermögensminderung nicht nur direkt in Form von Geld geschehen muss. Ebenso muss es sich bei der geschädigten Person nicht um jene handeln, bei der die Phishing-Handlung begann.

Wie gezeigt wurde, ist lediglich § 269 in der Lage, dass Erlangen von Informationen und das Installieren von Schadsoftware auf Geräten als Phänomen Phishing zu erfassen, wobei dies nicht aufgrund eines Schutzes der potenziellen gefährdeten Informationen, sondern auf dem Fälschen einer Datenurkunde beruht. Eine Unterscheidung ist dennoch zwischen dem Erlangen der Informationen und dem Installieren der Schadsoftware möglich, da letzterer Vorgang auch von § 303a erfasst wird. Je nach Begehungsweise können zudem verschiedene Vorbereitungshandlungen erfüllt werden. Im gezeigten Beispiel betraf dies solche nach § 303a. Hier bleibt anzumerken, dass die einzeln betrachtete Phishing-Phase je nach konkreter Begehungsweise selbst in der Lage ist,

Vorbereitungshandlungen zu erfüllen, es allerdings auch möglich ist, dass Vorbereitungshandlungen nicht durch diese selbst, sondern im Vorfeld erfüllt werden. Damit bleibt festzuhalten, dass eine entsprechende Erfüllung dieser zum einen von der Betrachtungsweise des Sachverhaltes und zum anderen von dem Sachverhalt selbst abhängig ist. Werden Daten über das bloße Phishing hinaus verwendet, können weitere Normen erfüllt werden, am Beispiel dieser Arbeit der § 263a. Abschließend kann festgehalten werden, dass die Subsumtion der Sachverhalte innerhalb des Erlangens von Daten und der Installation der Schadsoftware zwar lediglich bei § 269 erfolgreich durchgeführt werden kann bzw. bei Letzterem auch bei § 303a, dennoch wurde gezeigt, dass bei verschiedenen Begehungsweisen auch unterschiedliche objektive Tatbestandsmerkmale detektierbar sind, sowohl in der Vorbereitung als auch in der eigentlichen Ausführung. Ebenso lässt sich die Erkenntnis gewinnen, dass nicht auf alle Merkmale die Begehungsweise den gleichen Einfluss hat. In Bezug auf den zentralen Datenbegriff lässt sich zudem festhalten, dass keine einheitliche Definition existiert. Aufgrund verschiedener Anwendungen des Begriffes ergibt sich allerdings diese Notwendigkeit der unterschiedlichen Auslegung. In Bezug auf die Unterordnung des Phänomens Phishing unter den Begriff Cybercrime lassen sich abschließend zwei Erkenntnisse festhalten. Zunächst existieren unterschiedliche Definitionen der Begriffe Cybercrime im engeren und weiteren Sinn. Zum anderen ist die Einordnung von Phishing sowohl von der genutzten Definition als auch von der konkreten Begehungsweise abhängig. Wird sich nach Manfred Wernert am StGB orientiert, ist eine Zuordnung von Phishing unabhängig der Begehungsweise unter Cybercrime im engeren Sinn möglich. Bei der Definition nach dem BKA hingegen hängt diese Zuordnung von der konkreten Ausgestaltung des Sachverhaltes ab, ob durch das Phishing, beispielsweise bei der Installation von Schadsoftware Datenverarbeitendes System, deren Daten oder das Internet konkret gefährdet wurden und inwieweit lediglich das Erlangen von Informationen durch Phishing oder auch eine anschließende Verwendung der Informationen betrachtet wird. Das bloße Erlangen von Informationen kann nach der Definition des BKA nicht zweifelsfrei als Cybercrime im engeren Sinn bezeichnet werden. Anschließend an diese Arbeit können weitere Cybercrime-Phänomene nach dem gleichen Prinzip betrachtet werden. Außerdem ist eine intensivere Beschäftigung mit dem Thema Phishing denkbar. So können im Rahmen weiterer Arbeiten die Fragen beantwortet werden, ob ein eigenständiger Schutz der durch Phishing erlangten Informationen außerhalb von § 269 sinnvoll ist. Zudem kann untersucht werden, welches Entwicklungspotenzial das Thema Phishing in Bezug auf technische Neuerungen hat und ob neben der Unterkategorie Smishing zukünftig weiter Kategorien auftreten können. Auch dabei ist eine strafrechtliche Betrachtung sinnvoll.

Literatur

[1] Bundeskriminalamt, *Cybercrime Bundeslagebild 2021*. Wiesbaden, 2022. [Online]. Verfügbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.pdf;jsessionid=D2C4F13E2A9F792264705446B34EDAC8.live601?__blob=publicationFile&v=5

[2] Bundeskriminalamt, *Cybercrime.* [Online]. Verfügbar unter: https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html (Zugriff am: 15. Juli 2022).

[3] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, *Straf- & Sicherheitsrecht - Die Cybercrime-Konvention.* [Online]. Verfügbar unter: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Polizei-Strafjustiz/Cybercrime.html (Zugriff am: 15. Juli 2022).

[4] *Übereinkommen über Computerkriminalität*, 185, Council of Europe, Nov. 2001. [Online]. Verfügbar unter: https://rm.coe.int/168008157a

[5] M. Wernert, *Internetkriminalität: Grundlagenwissen, erste Maßnahmen und polizeiliche Ermittlungen,* 4. Aufl. Stuttgart, München, Hannover, Berlin, Weimar, Dresden: Boorberg, 2021. [Online]. Verfügbar unter: www.boorberg.de

[6] Bundesamt für Sicherheit in der Informationstechnik, *Identitätsdiebstahl durch Datenleaks und Doxing.* [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Identitaetsdiebstahl/identitaetsdiebstahl_node.html (Zugriff am: 17. August 2022).

[7] L. I. Savić, C. Momsen und M. Schmidl, „Phishing“ in *Compliance von A-Z*, T. Grützner und A. Jakob, Hg., 2 Aufl. München: Beck, 2015.

[8] M. Büchel und P. Hirsch, *Internetkriminalität: Phänomene - Ermittlungshilfen - Prävention,* 2. Aufl. Heidelberg: Kriminalistik, 2020.

[9] Bundesamt für Sicherheit in der Informationstechnik, *Alle Meldungen News - "Smishing" - SMS-Phishing im Herbst 2021 mit neuen Betrugsmaschen.* [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Smishing_SMS-Phishing_141021.html (Zugriff am: 26. Juni 2022).

[10] Anti Phishing Working Groupe, *About the APWG.* [Online]. Verfügbar unter: https://apwg.org/about-us/ (Zugriff am: 18. August 2022).

[11] Anti Phishing Working Groupe, *PHISHING ACTIVITY TRENDS REPORT: Activity January-March2022*, 2022. [Online]. Verfügbar unter: https://docs.apwg.org/reports/apwg_trends_report_q1_2022.pdf?_gl=1*v3tgzd*_ga*MjEzOTM1NTI4LjE2NjA3NTIxNjQ.*_ga_55RF0RHXSR*MTY2MDgwMzc0NC4yLjEuMTY2MDgwNDIzMS4wLjAuMA.&_ga=2.35015329.1686835535.1660752164-213935528.1660752164

[12] J. Knupfer, „Phishing for Money“, *Multimedia und Recht*, Jg. 7, Nr. 10, 2004.

[13] H. Roll, „Begehungsweise“ in *EBL-Schweitzer*, v.20, *Kriminalistik-Lexikon*, I. Wirth et al., Hg., 4 Aufl. Heidelberg, s.l.: Verlagsgruppe Hüthig Jehle Rehm GmbH, 2013.

[14] R. R. Zahn, „Praktikumsbericht: Praktikum bei der Kriminalpolizeiinspektion der Polizeidirektion Görlitz“, Angewandte Computer- und Biowissenschaften, Allgemeine und digitale Forensik, Hochschule Mittweida, Mittweida, 2022.

[15] R. Rengier, *Strafrecht Allgemeiner Teil,* 13. Aufl. München: C.H. Beck, 2021.

[16] *StGB, Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 2 des Gesetzes vom 22. November 2021 geändert worden ist.*

[17] J. P. Graf, „§ 202a“ in *§§ 185-262*, Bd. 4, *Münchener Kommentar zum Strafgesetzbuch*, G. M. Sander, Hg., 4 Aufl. München: C.H. Beck, 2021.

[18] J. P. Graf, „§ 202b“ in *§§ 185-262*, Bd. 4, *Münchener Kommentar zum Strafgesetzbuch*, G. M. Sander, Hg., 4 Aufl. München: C.H. Beck, 2021.

[19] J. P. Graf, „§ 202c“ in *§§ 185-262*, Bd. 4, *Münchener Kommentar zum Strafgesetzbuch*, G. M. Sander, Hg., 4 Aufl. München: C.H. Beck, 2021.

[20] J. P. Graf, „§ 202d“ in *§§ 185-262*, Bd. 4, *Münchener Kommentar zum Strafgesetzbuch*, G. M. Sander, Hg., 4 Aufl. München: C.H. Beck, 2021.

[21] R. Hefendehl und M. Noll, „§ 263a“ in *§§ 263-297*, Bd. 5, *Münchener Kommentar zum Strafgesetzbuch*, R. Hefendehl, Hg., 4 Aufl. München: C.H. Beck, 2022.

[22] V. Erb, „§ 269“ in *§§ 263-297*, Bd. 5, *Münchener Kommentar zum Strafgesetzbuch*, R. Hefendehl, Hg., 4 Aufl. München: C.H. Beck, 2022.

[23] V. Erb, „§ 270“ in *§§ 263-297*, Bd. 5, *Münchener Kommentar zum Strafgesetzbuch*, R. Hefendehl, Hg., 4 Aufl. München: C.H. Beck, 2022.

[24] V. Erb, „§ 271“ in *§§ 263-297*, Bd. 5, *Münchener Kommentar zum Strafgesetzbuch*, R. Hefendehl, Hg., 4 Aufl. München: C.H. Beck, 2022.

[25] V. Erb, „§ 274“ in *§§ 263-297*, Bd. 5, *Münchener Kommentar zum Strafgesetzbuch*, R. Hefendehl, Hg., 4 Aufl. München: C.H. Beck, 2022.

[26] B. Wieck-Noodt, „§ 303a“ in *§§ 263-358*, Bd. 5, *Münchener Kommentar zum Strafgesetzbuch*, R. Hefendehl, Hg., 3 Aufl. München: C.H. Beck, 2019.

[27] B. Wieck-Noodt, „§ 303b“ in *§§ 263-358*, Bd. 5, *Münchener Kommentar zum Strafgesetzbuch*, R. Hefendehl, Hg., 3 Aufl. München: C.H. Beck, 2019.

[28] Norton, *Was ist Spear Phishing und wie funktioniert es?* [Online]. Verfügbar unter: https://de.norton.com/norton-blog/2016/11/was_ist_spear_phishi.html (Zugriff am: 18. August 2022).

[29] Bundesamt für Sicherheit in der Informationstechnik, *Social Engineering – der Mensch als Schwachstelle.* [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html (Zugriff am: 16. Juni 2022).

[30] C. Hadnagy, *Die Kunst des Human Hacking: Social Engineering - Deutsche Ausgabe,* 2. Aufl. mitp Verlags GmbH & Co. KG, 2011. [Online]. Verfügbar unter: http://ebooks.ciando.com/book/index.cfm/bok_id/1618066

[31] Bundeskriminalamt, *Cybercrime Bundeslagebild 2018*. Wiesbaden, 2019. [Online]. Verfügbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2018.html?nn=28110

[32] Bundeskriminalamt, *Cybercrime Bundeslagebild 2019*. Wiesbaden, 2020. [Online]. Verfügbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2019.html?nn=28110

[33] Bundeskriminalamt, *Meldungen - Hacker-Sammlung gefunden: 500 Mio. E-Mail-Adressen und Passwörter betroffen.* [Online]. Verfügbar unter: https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/170705_HackerSammlung.html (Zugriff am: 19. August 2022).

[34] Hasso-Plattner-Institut, *Identity Leak Checker.* [Online]. Verfügbar unter: https://sec.hpi.de/ilc/ (Zugriff am: 18. August 2022).

[35] Bundesamt für Sicherheit in der Informationstechnik, *Phishing – Bankbetrug im* Posteingang*.* [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Wie-geht-Internet/E-

Mail-Phishing-Bankbetrug/email-phishing-bankbetrug_node.html (Zugriff am: 19. August 2022).

[36] Münchener Bank, *Phishing-Warnungen.* [Online]. Verfügbar unter: https://www.muenchner-bank.de/online-filiale/sicherheit/phishing-warnungen.html (Zugriff am: 19. August 2022).

[37] A. Popp, „„Phishing", „Pharming" und das Strafrecht", *MMR*, Jg. 9, Nr. 2, S. 84–85, 2006.

[38] A. Popp, „Von „Datendieben" und „Betrügern" - Zur Strafbarkeit des so genannten „phishing" zur Fussnote *", *Neue Juristische Wochenschrift*, Jg. 57, Nr. 49, S. 3517–3518, 2004.

[39] OLG Rostock, *Beschluss*, *Medien Internet und Recht*, Jg. 3. Verfügbar unter: http://www.medien-internet-und-recht.de/volltext.php?mir_dok_id=1290. Zugriff am: 5. Juli 2022.

[40] C.-F. Stuckenberg, „Zur Strafbarkeit von „Phishing"", *Zeitschrift für die Gesamte Strafrechtswissenschaft*, Jg. 118, Nr. 4, S. 878–912, 2007, doi: 10.1515/ZSTW.2006.032.

[41] Bundeskriminalamt, *Warnmeldung der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin): Warnung vor Tätigkeit als Finanzagent.* [Online]. Verfügbar unter: https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Warnhinweise/050517_Finanzagent.html (Zugriff am: 23. Juli 2022).

[42] A. Seidl und K. Fuchs, „Die Strafbarkeit des Phishing nach Inkrafttreten des 41. Strafrechtsänderungsgesetzes", *Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht*, Jg. 11, Nr. 2, 2010. [Online]. Verfügbar unter: https://www.hrr-strafrecht.de/hrr/archiv/10-02/hrrs-2-10.pdf

[43] Bundesamt für Sicherheit in der Informationstechnik, *Denial-of-Service (DoS) und Distributed Denial-of-Service (DDoS).* [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/DoS-Denial-of-Service/dos-denial-of-service_node.html (Zugriff am: 10. August 2022).

Anlagen

Sachverhalt 1 – Smishing mit Telefonat

„Herr Müller erhielt von einer unbekannten Rufnummer eine SMS mit dem Inhalt: „Sehr geehrte Herr Thomas Müller, ihr sofortiges Handeln ist erforderlich (Gesetzesverstoß): https://vr-id-45r334.de/123456789 Ihre Volksbank eG.“ auf sein Mobiltelefon. Herr Müller folgte dem Link und wurde auf eine Seite der Volksbank weitergeleitet, auf welcher er ein Formular ausfüllen sollte. Er müsse das Formular innerhalb von 14 Tagen ausfüllen, da sonst sein Konto gesperrt werden würde. Er kam dieser Aufforderung nach und gab seine EC-Kartennummer, das Gültigkeitsdatum, seine Handynummer sowie E-Mail-Adresse an. Noch am selben Tag erhielt Herr Müller eine E-Mail mit einem weiteren Link, welchem er allerdings nicht folgte. Zwei Tage später, erhielt Herr Müller einen Anruf eines vermeintlichen Bankmitarbeiters. Die Person stellte mit dem Namen eines bekannten Bankmitarbeiters vor. Zunächst ist Herr Müller gefragt wurden, ob er eine Überweisung autorisieren möchte, was er verneinte. Als Nächstes wurde sich erkundigt, ob er einen Mann namens Gustav Schmidt kenne. Dies verneinte er ebenfalls. Anschließend habe der Bankmitarbeiter vorgeschlagen, dass Herr Müller eine TAN mündlich durchgebe, welche er gleich per SMS erhalten würde. Er stimmte zunächst zu, beendete aber anschließend den Anruf, ohne die TAN durchzugeben. Der SMS ist zu entnehmen, dass ein Betrag in Höhe von 5000,00 Euro auf ein deutsches Konto überwiesen werden sollte. Der tatsächliche Bankmitarbeiter hielt Rücksprache mit Herrn Müller und gab an, dass er diesen nicht angerufen habe. Später konnte festgestellt werden, dass die Links zu einer Domäne gehörten, welche auf eine falsche Identität registriert wurde. Eine damit verknüpfte E-Mail-Adresse wurde ebenfalls auf eine falsche Identität registriert. Der letzte Log-in erfolgte über einen ausländischen Provider. Beim Kontoinhaber handelte sich um eine reale Person.“ [14, S. 9-10]

Sachverhalt 2 – Phishing

„Frau Lehmann erhielt eine E-Mail, welche den Anschein erweckte, von der Volksbank zu sein, bei welcher Frau Lehmann ein Konto besitzt. In dieser wurde Frau Lehmann angewiesen, einem Link zu folgen, wodurch das Secure-Go Verfahren aktiviert werden kann. Nachdem Frau Lehmann dieser Aufforderung nachkam, gelangte sie auf eine Website, welche den Eindruck vermittelte, von der Volksbank zu sein. Die Website forderte Frau Lehmann auf, zunächst ihre Bankdaten und später eine TAN, welche in ihrer Banking App angezeigt wurde, einzugeben. Nach der Aufforderung zur Eingabe einer weiteren TAN, welcher Frau Lehmann ebenfalls nachkam, brach sie den Vorgang ab. Durch die Eingabe wurden zwei Überweisungen autorisiert, wobei mangels Kontodeckung nur eine Überweisung im vierstelligen Bereich auf ein französisches Bankkonto ausgeführt werden konnte. Das Bankkonto wurde per Online-Authentifizierungsverfahren eröffnet. Der Ausweis, welcher für das Verfahren genutzt wurde, ist nicht als gestohlen oder verloren gemeldet. Eine

Person mit Namen und weiteren Daten konnte an einer anderen Adresse verifiziert werden. Weitere Ermittlungen diesbezüglich konnten aufgrund des fehlenden Meldewesens in Frankreich nicht durchgeführt werden.“ [14, S. 11]

Sachverhalt 3 – Smishing

„Frau Schäfer empfing eine SMS einer unbekannten Rufnummer, welche über einen Paketversand informierte. In dieser war ein Link enthalten, der den Anschein erweckte, vom Paketdienstleisters FedEx zu stammen. Nachdem Frau Schäfer dem Link folgte, installierte sich eine Schadsoftware auf ihrem Mobiltelefon, welche ohne ihr Zutun das Versenden einer Vielzahl gleichartiger SMS an diverse Telefonnummern veranlasste. Durch den Mobilfunkanbieter wurden Kosten von 529 Euro für die versendeten Nachrichten in Rechnung gestellt. Weitere Funktionen der Schadsoftware, z. B. Keylogger-Funktionen, sind nicht bekannt. Erkenntnisse zu der unbekannten Rufnummer liegen nicht vor.“ [14, S. 12-13].

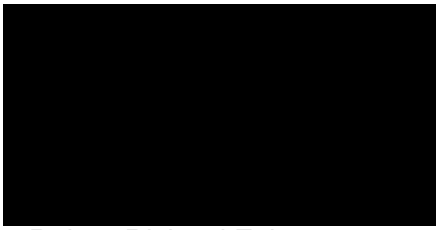
Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Bautzen, den 25.08.2022



Robert Richard Zahn