Strafbarkeit des Identitätsdiebstahls durch Phishing, Pharming und Spoofing

Von Prof. Dr. Anja Schiemann, Köln/Münster

1 Einleitung

Die bekannteste Form des Identitätsdiebstahls ist das sog. Phishing, das Fischen nach Onlinezugangsdaten.[2] In rechtlicher Hinsicht muss nach vier Stufen differenziert werden. Im ersten Schritt geht es um die Erlangung der relevanten Zugangsdaten und TANs für das Online-Banking. Hierzu locken die Täter vornehmlich Bankkunden durch massenhaft versendete E-Mails auf imitierte Webseites, um sie zur Preisgabe von nutzbaren Daten zu bewegen. Im zweiten Schritt werden, soweit dies erforderlich ist, die so erlangten Daten verändert, bevor sie im dritten Schritt vom Täter zur Durchführung der Transaktion missbraucht werden. Im vierten Schritt werden zur Abwicklung des Geldtransfers sog. Finanzmanager oder Finanzagenten eingesetzt, die das erlangte Geld entgegennehmen und gegen Provision ins Ausland transferieren.[3] Die ersten beiden Schritte sind im Hinblick auf den Identitätsdiebstahl sowie die Datenveränderung relevant. Dagegen soll der vierte Schritt und die Frage nach der Strafbarkeit des Finanzagenten im Rahmen dieses Aufsatzes ausgespart werden, da dies nicht unmittelbar mit dem Phishingvorgang in Verbindung steht.[4]

Soweit in der ersten Phase die Nutzer statt mit einer E-Mail unmittelbar durch Manipulationen an Domain-Name-Servern (DNS) auf gefälschte Web-Seiten umgeleitet werden, spricht man vom sog. Pharming. Das Pharming kommt also ohne die Spam-E-Mail mit dem darin befindlichen Hyperlink aus. Durch die Malware wird vielmehr nicht die Original-Banking-Webseite, sondern die vom Täter manipulierte Webseite aufgerufen.[5]

Beim IP-Spoofing werden falsche IP-Nummern verwendet, um dem angegriffenen Rechner oder System eine falsche Identität vorzutäuschen. Hierbei werden bspw. die IP-Adressen in den Datenpaketen verändert, die an den Eingangs-Port eines Netz-Routers übertragen werden.[6] Insofern sind IP-Spoofing und Pharming stark verwandte Phänomene.

2 Strafbarkeit

2.1 Strafbarkeit hinsichtlich der Datenverschaffung

2.1.1 Nicht in Betracht kommende Straftatbestände

Das Phishing der sensiblen Daten selbst erfüllt nur sehr wenige Straftatbestände. Insbesondere die Straftatbestände Betrug, Computerbetrug oder das Ausspähen oder Abfangen von Daten werden nicht verwirklicht. Warum? Der Straftatbestand des Betrugs gem. § 263 StGB setzt voraus, dass das getäuschte Opfer irrtumsbedingt eine Verfügung über sein Vermögen trifft und sich dadurch selbst schädigt. Die Herausgabe der persönlichen Zugangsdaten als solche wirkt aber nicht unmittelbar vermögensmindernd, sondern schafft vielmehr die Voraussetzungen dafür, dass der Täter durch eine weitere Handlung auf das Konto des Opfers zugreift und erst dadurch einen Vermögensschaden herbeiführt.[7] Auch ein versuchter Computerbetrug wurde vom KG verneint. Denn ein unmittelbares Ansetzen zur Verwirklichung des Straftatbestands i.S.d. § 22 StGB läge erst dann vor, wenn der Täter die erlangten Daten auch verwendet. Dagegen stelle die Einrichtung von Zielkonten, eine fingierte polizeiliche

Anmeldung und das Abfangen von Kontounterlagen noch keinen versuchten Computerbetrug dar.[8]
Eine Strafbarkeit in Form der Vorbereitung eines Computerbetrugs gem. § 263a Abs. 3 StGB wird ebenfalls in der Regel nicht verwirklicht, weil hierzu ein Computerprogramm gegeben sein muss, dessen Zweck auf die Begehung einer Tat nach Abs. 1 gerichtet ist.[9] Das Verfassen einer sog. Phishing-E-Mail ist aber keine solche Vorbereitungshandlung, weil als Programm nur eine Befehlsfolge an einen Computer bezeichnet werden kann, die selbsttätig abläuft und ein eigenes Arbeitsergebnis produziert. Auch soweit mit entsprechender Intention eine Internet-Seite erstellt wird, die als Programm gewertet werden kann, fehlt es am erforderlichen Unmittelbarkeitszusammenhang, da nicht dieses Programm, sondern erst die darüber erlangten Daten für den späteren Computerbetrug verwendet werden.[10]Auch sofern seit Inkrafttreten des 61. StrÄndG v. 10.3.2021[11]am 18.3.2021 gem. Nr. 2 Passwörter oder sonstige Sicherungscodes als Tatobjekte erfasst werden, kommt eine Strafbarkeit nicht in Betracht.[12]
Auch der Straftatbestand des Ausspähens von Daten gem. § 202a StGB ist nicht einschlägig. Aufgrund der weiten Auslegung des Datenbegriffs können PIN und TAN als Kontozugangs- und Transaktionsinformationen zwar hierunter subsumiert werden.[13]Allerdings veranlasst der Täter das Opfer selbst dazu, die fraglichen Daten an seinen Rechner zu übersenden. Insofern muss der Täter keine Sicherung gegen den unberechtigten Zugang überwinden, vielmehr sind die Daten für ihn bestimmt.[14]
Strafbar gem. § 202a StGB ist dagegen das IP-Spoofing. Denn soweit das Opfer die vorgespiegelte Adresse für vertrauenswürdig hält, gibt es den Zugang zu seinem Netzwerk und damit zu den dort vorhandenen Daten frei. Da hier mit dem Netzwerk-Rechner Daten ausgetauscht werden und zusätzlich die Adresse eines weiteren Rechners benutzt wird, werden Geheimhaltungs- und Sicherungsmaßnahmen des Verfügungsberechtigten ausschaltet.[15] Einschränkend ist aber erforderlich, dass ein Zugangsschutz überwunden wurde.[16]
Der Straftatbestand des Abfangens von Daten gem. § 202b StGB ist in keiner Konstellation erfüllt. Voraussetzung ist nämlich, dass der Täter Daten aus einer nichtöffentlichen Datenübermittlung oder einer elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage abfängt. Hierfür müsste sich der Täter in die Datenübermittlung zwischen Bankkunden und Bank schalten. Dies ist aber beim Versenden von Phishing-E-Mails und dem Aufbau von Phishing-Websites ersichtlich nicht der Fall, weil die Datenübermittlung von Anfang an nur zwischen Täter und Opfer stattfindet.[17]
Ebenfalls nicht verwirklicht sind die Straftatbestände der Datenveränderung gem. § 303a Abs. 1 StGB und der Computersabotage gem. § 303b Abs. 1 StGB. Weder verursachen Phishing-Mails oder Phishing-Websites ein Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von nach § 303a StGB geschützten Daten, noch liegt eine Störung der Datenverarbeitung i.S.v. § 303b Abs. 1 StGB vor.

2.1.2 Fälschung beweiserheblicher Daten

Zentrale Vorschrift, um dem ersten Schritt des Phishings, nämlich der Datenbeschaffung, strafrechtlich zu begegnen, ist § 269 Abs. 1 StGB. Allerdings sollte die „Schlagkraft“ dieser Vorschrift nicht überschätzt werden.[18] Die Prüfung der Strafbarkeit nach § 269 StGB erfordert eine „urkundengerechte“ Umsetzung der Datenverarbeitungsvorgänge.[19] Daher gelten für die Bestimmung des Ausstellerbegriffs und der Echtheit die Regeln zur Urkundenechtheit analog.[20]
Der wirkliche oder scheinbare Aussteller einer Erklärung per E-Mail kann also auch aus der E-Mail-Adresse oder einem Firmenlogo des Absenders hervorgehen. Deshalb ist eine sog. Phishing-Mail, mit der unter falscher Absenderangabe, z.B. einer Bank, persönliche Daten und sensible Informationen abgefragt werden, eine unechte Datenurkunde. Denn hier werden rechtlich erhebliche Gedankenerklärungen unter falscher Identität gemacht, so dass über den wahren erkennbaren Aussteller getäuscht wird.[21]
Auch die Einrichtung einer Homepage mit falschen Angaben zur Identität des Betreibers (Pharming) ist nach § 269 StGB strafbar, wenn diese scheinbar eine rechtserhebliche Erklärung der wahrheitswidrig genannten Person enthält. Hierfür ist weder die Verwendung einer gefälschten elektronischen Signatur, noch der Einsatz einer gefälschten IP-Adresse erforderlich. Denn die rechtserhebliche Erklärung wird in erster Linie durch den Text verkörpert, an dem sich das Täuschungsopfer im Rechtsverkehr orientiert.[22]
Auch bei IP-Spoofing ist eine Strafbarkeit nach § 269 StGB gegeben. Denn beim echten IP-Spoofing werden falsche IP-Nummern verwendet, um eine falsche Identität vorzuspiegeln. Insofern werden falsche Absenderkennungen verschickt.[23]Durch das Verändern der Daten wird eine echte Urkunde verfälscht.[24] Doch auch beim unechten IP-Spoofing[25] ist § 269 StGB in Form des Gebrauchs gespeicherter oder veränderter Daten verwirklicht.[26]

2.1.3 Weitere Vorschriften

Für eine Strafbarkeit in Betracht kommen darüber hinaus auch weniger bekannte Vorschriften aus dem Nebenstrafrecht. Soweit Elemente des Corporate Designs einer Bank oder ähnlicher benutzter Adressaten markenrechtlich oder urheberrechtlich geschützt sind, verwirklicht der Täter durch die Benutzung von Logos, geschäftlichen Bezeichnungen und ähnlichem die

Straftatbestände der §§ 143 Abs. 1, 143a Abs. 1 MarkenG sowie der §§ 106 ff. UrhG.[27]
Daneben ist eine Strafbarkeit in Form der unzulässigen Datenverarbeitung personenbezogener Daten gem. Art. 84 Abs. 1 DSGVO i.V.m. § 42 Abs. 2 Nr. 1 BDSG denkbar, da PIN und TAN zweifellos personenbezogene Daten nach Art. 4 Nr. 1 DSGVO darstellen. Die für die Datenverarbeitung erforderliche Einwilligung oder ein gesetzlicher Erlaubnistatbestand sind nicht gegeben, so dass die Datenverarbeitung unzulässig ist. Wird vorsätzlich und mit Bereicherungsabsicht gehandelt, ist der Straftatbestand erfüllt.[28]

2.2 Strafbarkeit hinsichtlich der Datenverwendung

Der zweite Schritt des Phishings, nämlich die Nutzung der erlangten Zugangsdaten für eine Onlineüberweisung zulasten des Kontos des Getäuschten, erfüllt dann mehr Straftatbestände als der erste Schritt. Zunächst steht eine Strafbarkeit gem. § 202a StGB im Raum. Mit PIN und TAN verschafft sich der Täter Zugang zu den Konto- oder Depotinformationen des Opfers, die eigentlich ausschließlich für den Kontoinhaber bestimmt und durch die vorgeschaltete Abfrage der Zugangsdaten besonders gesichert sind. Da es dem Täter gerade um die Erlangung der Informationen geht, handelt er auch vorsätzlich.[29]
§ 202b StGB ist dagegen auch im Rahmen der Datenverwendung nicht verwirklicht, da es auch hier zu keinem Datenaustausch zwischen dem Bankkunden und der Bank kommt.
Verwirklicht ist dagegen der Straftatbestand des Computerbetrugs in der Tatalternative des unbefugten Verwendens von Daten gem. § 263a Abs. 1 Var. 3 StGB. Durch die betrugsspezifische Auslegung des Tatbestandsmerkmals der unbefugten Datenverwendung, wird eine täuschungsäquivalente Handlung des Phishers vorausgesetzt. Der Täter gibt gegenüber der Bank vor, der berechtigte Bankkunde zu sein. Auch wenn die Preisgabe von PIN und TAN durch das Opfer bewusst erfolgte, so erstreckt sich dies jedoch nicht auf die zweckfremde Nutzung der Daten, so dass die Datenverwendung durch den Täter unbefugt ist. Indem der Phisher die Passwörter beim kontoführenden Institut einsetzt und sich ins System einloggt, beeinflusst er zudem das Ergebnis eines automatisierten Datenverarbeitungsvorgangs. Dieser Datenverarbeitungsvorgang wirkt sich unmittelbar vermögensmindernd aus, da hierfür die Freigabe eines vermögensrelevanten Zugangs ausreicht. Durch die Überweisung des Geldbetrags durch den Täter auf das Zielkonto tritt ein Vermögensschaden ein.[30] Auch die Bereicherungsabsicht ist gegeben, da es dem Täter, auch wenn er das Geld zunächst auf ein Konto eines Finanzkuriers transferiert, darum geht, sich selbst zu bereichern. Hat man wegen der Stoffgleichheit aufgrund der Tatsache, dass in den Fällen, in denen ein Finanzkurier beteiligt ist, zunächst eine Bereicherung beim Finanzkurier eintritt, Zweifel, so ist zu bedenken, dass es ausreicht, wenn der rechtswidrige Vermögensvorteil für einen Dritten erlangt werden soll.[31]
Auch der Straftatbestand der Fälschung beweiserheblicher Daten ist gegeben. Der Phisher stellt durch die Eingabe der Zugangsdaten des Opfers auf der Bankwebsite und die Tätigung einer Onlineüberweisung einen Datensatz her, den die Bank speichert. Erklärungsinhalt ist der Überweisungsauftrag. Durch die Verwendung von PIN und TAN erklärt der Täter, Verfügungsberechtigter über das Konto zu sein. Damit werden beweiserhebliche Daten so gespeichert, dass bei ihrer Wahrnehmung eine unechte Urkunde vorliegen würde. Da der Täter infolge des automatisierten Vorgangs keinen Menschen im Rechtsverkehr täuscht, muss ein Rückgriff auf § 270 StGB erfolgen, nach dem die fälschliche Beeinflussung einer Datenverarbeitung der Täuschung im Rechtsverkehr gleichsteht.[32]

2.3 Strafbarkeit hinsichtlich des Anwerbens eines Finanzkuriers

Dagegen ist das reine Anwerben eines Finanzkuriers durch den Phisher nicht strafbar. In Betracht käme allein eine Strafbarkeit wegen Betrugs gem. § 263 StGB. Die Spam-Mail des Täters stellt dabei zweifellos eine Täuschungshandlung dar, weil die beschriebene Aufgabe des Kuriers eine andere ist, als seine tatsächlich vorgesehene Rolle. Der Finanzkurier geht nämlich davon aus, eine legale Arbeitsleistung zu erbringen. Sieht man mit der herrschenden Meinung Arbeitsleistungen generell als Bestandteil des rechtlich geschützten Vermögens an, so ist auch eine irrtumsbedingte Vermögensverfügung in Form der vom Finanzkurier erbrachten Dienstleistung gegeben.[33] Auch ein Vermögensschaden kann bejaht werden, da der Finanzagent der Bank des Kontoinhabers gegenüber bereicherungsrechtlichen Haftungsansprüchen ausgesetzt ist. Letztlich scheitert eine Betrugsstrafbarkeit jedoch an der fehlenden Stoffgleichheit. Nach dem Gesichtspunkt der Stoffgleichheit muss sich die Bereicherungsabsicht des Täters auf einen Vorteil beziehen, der unmittelbar aus dem Vermögen des Opfers stammt.[34] Der Bereicherungsanspruch der Bank führt aber zu einem Schaden des Finanzkuriers und beruht daher nicht auf der Überweisung und insofern nicht auf einer Verfügung des Täters.[35]

3 Fazit

Der Phishingtäter erfüllt durch sein Verhalten einen bunten Strauß von Straftatbeständen, wobei zwischen den Handlungen der Datenbeschaffung und anschließenden Datenverwendung differenziert werden muss. Bereits durch die Datenbeschaffung durch das Verschicken der Phishing-E-Mail oder das Erstellen der Phishing-Webseite macht er sich nach § 269 StGB strafbar. Sofern die Variante des IP-Spoofing gegeben ist, wird ggf. noch § 202a StGB verwirklicht. Darüber hinaus verwirklicht der Phishing-,

Pharming- oder Spoofing-Täter im Nebenstrafrecht die Strafnormen der §§ 143, 143a MarkenG sowie §§ 106 ff. UrhG, sofern er markenrechtlich oder urheberrechtlich geschützte Kennzeichen oder Bezeichnungen verwendet. Auch eine Strafbarkeit nach datenschutzrechtlichen Vorschriften steht im Raum.
Durch die anschließende Datenverwendung verwirklicht der Phisher § 202a StGB, indem er sich durch die abgefischten Daten Zugang zu den Kontoinformationen des Opfers verschafft. Durch die Verwendung der Daten im Rahmen der Onlineüberweisung ist darüber hinaus eine Strafbarkeit gemäß § 263a und §§ 269, 270 StGB gegeben.
Diese kurze rechtliche Würdigung macht deutlich, dass das geltende Strafrecht ausreichend Schutz gegen das Phishing und seine Sonderformen insgesamt bietet. Dennoch sollte der Gesetzgeber auch neuere Formen und Tatmodalitäten stets im Blick haben, um hier mit einer Nachjustierung der strafrechtlichen Vorschriften angemessen auf die fortschreitende Digitalisierung auch kriminellen Verhaltens reagieren zu können.

Anmerkungen

1. Die Verfasserin war bis Ende März 2022 Leiterin des Fachgebiets Strafrecht, Strafprozessrecht und Kriminalpolitik an der Deutschen Hochschule der Polizei (DHPol) in Münster. Zum 1. April 2022 ist die Universitätsprofessorin auf den Lehrstuhl für Strafrecht und Strafprozessrecht an der Universität zu Köln gewechselt. Der DHPol bleibt sie über eine Gastprofessur verbunden.
2. So Bär, in: Graf/Jäger/Wittig, Wirtschafts- und Steuerstrafrecht, 2. Aufl. (2017), § 269 Rn. 15.
3. Vgl. Bär, in: Graf/Jäger/Wittig, § 263a Rn. 27; Sanli, ZWH 2018, 205.
4. Vgl. hierzu ausführlich Sanli, ZWH 2018, 205 (211 f.); Seidl/Fuchs, HRRS 2010, 85 (90 f.).
5. S. Borges, NJW 2005, 3313 (3314); Popp, MMR 2006, 84.
6. S. Weidemann, in: BeckOK-StGB, Computerkriminalität, 51. Ed. (1.11.2021), Rn. 8; Metz, JR 2019, 492 (498 f.).
7. Vgl. ausf. Popp, MMR 2006, 84 (85 f.); Popp, NJW 2004, 3517 (3518); Sanli, ZWH 2018, 205 (208).
8. So KG, MMR 2012, 845.
9. S. Fischer, StGB, 68. Aufl. (2021), § 263a Rn. 30.
10. Vgl. hierzu Mühlbauer, in: MK-StGB, Bd. 5, 3. Aufl. (2019), § 263a Rn. 115; Sanli, ZWH 2018, 205 (209); Waßmer, in: Leitner/Rosenau, Wirtschafts- und Steuerstrafrecht, 1. Aufl. (2017), § 263a Rn. 108.
11. BGBl. 2021 I, 333.
12. Nach Auffassung des Gesetzgebers sollten hierdurch primär Skimming-Fälle erfasst werden, vgl. BT-Drs. 19/25631, S. 23.
13. So Stuckenberg, ZStW 118 (2006), 878 (884); Goerckenjahn, wistra 2009, 47 (52); zweifelnd Popp, MMR 2006, 84 (85).
14. S. Popp, MMR 2006, 84 (85); Fischer, § 202a Rn. 9a; Kargl, in: NK-StGB, 5. Aufl. (2017), § 202a Rn. 10.
15. So Graf, in: MK-StGB, Bd. 4, 4. Aufl. (2021), § 202a Rn. 92.
16. S. Böken, in: Kipker, Cybersecurity, 1. Auf. (2020), Kap. 15 Rn. 76; Graf, in: MK-StGB, § 202a Rn. 92.
17. Hierzu Sanli, ZWH 2018, 205 (208); Bär, in: Wabnitz/Janovsky/Schmitt, Hdb. Wirtschafts- und Steuerstrafrecht, 5. Aufl. (2020), Kap. 15 Rn. 88.
18. So Popp, MMR 2006, 84 (85).
19. Fischer, § 269 Rn. 3.
20. Vgl. Heger, in: Lackner/Kühl, StGB, 29. Aufl. (2018), § 269 Rn. 2; ausf. Buggisch, NJW 2004, 3519 (3520 f.).
21. Vgl. Bär, in: Graf/Jäger/Wittig, Wirtschafts- und Steuerstrafrecht, 2. Aufl. (2017), § 269 Rn. 15; Erb, in: MK-StGB, Bd. 5, 3. Aufl. (2019), § 269 Rn. 33; Stuckenberg, ZStW 118 (2006), 878 (890).
22. S. Erb, in: MK-StGB, § 269 Rn. 34; Sanli, ZWH 2018, 205 (209).
23. Vgl. Rinker, MMR 2002, 663.
24. S. Rinker, MMR 2002, 663 (664); Marberth-Kubicki, Computer- und Internetstrafrecht, 2. Aufl. (2020), Rn. 178.
25. Hier wird vom Hacker der Rechner eines Dritten benutzt, um davon gezielt Datenpakete an den Dritten zu schicken. Die Daten stammen also von dem Rechner, der als Absender bezeichnet wird. Allerdings bleib der Hacker anonym und das Opfer hält den infiltrierten Computer für den Absender bzw. Angreifer, vgl. Rinker, MMR 2002, 663.

26. Ausf. Rinker, MMR 2002, 663 (664); Marberth-Kubicki, Rn. 111.
27. S. Sanli, ZWH 2018, 205 (210); Ingerl/Rohnke, Markengesetz, 3. Aufl. (2010), § 143 Rn. 10; ausf. Beck/Dornis, CR 2007, 642; Marberth-Kubicki, Rn. 73; Seidl/Fuchs, HRRS 2010, 85 (87 f.).
28. S. Sanli, ZWH 2018, 205 (210); zur alten Rechtslage Heghmanns, wistra 2007, 167.
29. Vgl. Seidl/Fuchs, HRRS 2010, 85 (88); Sanli, ZWH 2018, 205 (210); a.A. Graf, NStZ 2007, 129 (131).
30. Wo genau dieser Vermögensschaden eintritt, kann im Einzelfall problematisch sein und richtet sich nach § 675u und § 675v BGB und soll hier nicht weiter vertieft werden. Ausf. hierzu aber Seidl/Fuchs, HRRS 2010, 85 (89).
31. Vgl. Fischer, § 263 Rn. 186; zu den Fallkonstellationen Sanli, ZWH 2018, 205 (209).
32. So auch Sanli, ZWH 2018, 205 (210); Seidl/Fuchs, HRRS 2010, 85 (89); Stuckenberg, ZStZ 118 (2006), 878 (906).
33. Diese Auffassung ist aber durchaus umstritten, s. dazu ausf. Heinrich, GA 1997, 24; Saliger, in: Matt/Renzikowski, StGB, 2. Aufl. (2020), § 263 Rn. 169.
34. Vgl. Fischer, § 263 Rn. 187; Lackner/Kühl, § 263 Rn. 59.
35. Insg. hierzu Sanli, ZWH 2018, 205 (211); Seidl/Fuchs, HRRS 2010, 85 (90); Goeckenjan, wistra 2008, 128 (132 f.).