Mohamed Bou Sleiman*

Das Corona-Virus – Ein Katalysator für Cyberkriminalität?

Die global zur Eindämmung der Verbreitung des neuartigen Corona-Virus Sars-CoV-2 getroffenen Maßnahmen führen zu einer massiven Einschränkung des öffentlichen Lebens und damit zusammenhängend zu einer Verlagerung sowohl des privaten als auch des beruflichen Alltags in die digitale Welt. Aus der hiermit einhergehenden Verunsicherung der Bevölkerung versuchen (auch) Cyberkriminelle zu profitieren. Der vorliegende Beitrag widmet sich dem coronabegünstigten Cybercrime im engeren Sinne.[1] Dabei zeigt eine Auswertung der in der strafrechtlichen Praxis bekannt gewordenen Fälle, dass sich die Täter in diesem Zusammenhang vor allem des Phishings bedienen, weshalb sich die nachfolgenden Ausführungen hierauf konzentrieren und die im Wesentlichen zur Anwendung kommenden modi operandi sowie deren strafrechtliche Einordnung darstellen.

1 Cybercrime in Zeiten des Corona-Virus

Bereits kurz nach dem Ausrufen der coronabedingten Pandemie stellte das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Zunahme von Cyberangriffen mit Bezug auf das Virus fest.[2] Alleine das Unternehmen Google meldet, dass sein E-Mail-Dienst im Zusammenhang mit COVID-19 täglich mehr als 240 Millionen Spam-Nachrichten registriere sowie weitere 18 Millionen Malware- und Phishing-E-Mails blockiere.[3] Internationale Strafverfolgungsbehörden wie Europol[4] und Interpol[5] warnen eindringlich vor dem erhöhten Risiko coronabedingter Cyberangriffe, die verheerende Folgen hätten; vor allem wenn sie kritische Infrastrukturen im Gesundheitswesen träfen. Dies alles zeigt, wie anpassungsfähig das Repertoire der Cyberkriminellen ist, die vor allem durch Phishing- und Malwareangriffe versuchen, das aktuelle Informationsbedürfnis[6] der Bevölkerung auszunutzen.

1.1 Der grundsätzliche modus operandi des Phishings

Beim Phishing ist zwischen den Tatphasen der Datenbeschaffung und Datenverwendung zu unterscheiden. Im Rahmen der Datenbeschaffung versuchen die Täter, den potenziellen Geschädigten per E-Mail oder auf einer eigens dafür präparierten Internetseite, auf welche sie verlinken, täuschungsbedingt zur Preisgabe sensibler Daten, vor allem Zugangsdaten zum Onlinebanking sowie sonstigen Bezahlsystemen (etwa PayPal), zu bewegen.[7] Da-

* Der Autor ist Staatsanwalt bei der Staatsanwaltschaft Göttingen und ist dort in der Zentralstelle Internet- und Computerkriminalität (Cybercrime), Abteilung für Wirtschafts- und Umweltstrafsachen als Dezernent und Pressesprecher tätig. Der Aufsatz ist nicht in dienstlicher Eigenschaft verfasst und gibt ausschließlich die persönlichen Ansichten des Verfassers wieder.

1 Zur Differenzierung zwischen Cybercrime im engeren und im weiteren Sinne s. nur Wabnitz/Janovsky/Schmitt/*Bär*, HdB Wirtschafts- und SteuerstrafR, 5. Aufl., 2020, 15. Kapitel Rn. 5.

2 BSI-Mitteilung v. 02.04.2020, „Cyber-Kriminelle nutzen Corona-Krise vermehrt aus", abrufbar unter: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/Cyber-Kriminell_02042020.html (zuletzt abgerufen am 18.08.2020).

3 Protecting businesses against cyber threats during COVID-19 and beyond, abrufbar unter: https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond (zuletzt abgerufen am 18.08.2020).

4 Etwa der Europol-Bericht „Catching the virus cybercrime, disinformation and the COVID-19 pandemic" v. 03.04.2020, abrufbar unter: https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know (zuletzt abgerufen am 18.08.2020).

5 Etwa „INTERPOL warns of finanical fraud linked to COVID-19" v. 13.03.2020, abrufbar unter: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraud-linked-to-COVID-19 (zuletzt abgerufen am 18.08.2020).

6 In der gemeinsamen Mitteilung an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Region, Bekämpfung von Desinformation im Zusammenhang mit COVID-19 – Fakten statt Fiktion, JOIN(2020) 8 final v. 10.06.2020, S. 1 ff. spricht die Europäische Kommission in diesem Zusammenhang von einer „Infodemie", welche sich von den elementarsten Ängsten der Menschen nährt.

7 Statt vieler Achenbach/Ransiek/Rönnau/*Kölbel*, HdB WirtschaftsstrafR, 5. Aufl., 2019, 5. Teil, XV. Phishing, Rn. 280.

Dr. Mohamed Bou Sleiman

ist Staatsanwalt bei der Staatsanwaltschaft Göttingen und ist dort in der Zentralstelle Internet- und Computerkriminalität (Cybercrime), Abteilung für Wirtschafts- und Umweltstrafsachen als Dezernent und Pressesprecher tätig.
E-Mail: Mohamed.BouSleiman@justiz.niedersachsen.de

bei geben sie sich regelmäßig als eine vermeintlich seriöse dritte (juristische) Person aus, etwa eine bekannte Bank oder eine Behörde. Die Täter fragen die gewünschten Informationen unter Nennung eines Vorwandes ab, z. B. zur Schließung einer bestehenden Sicherheitslücke oder zur Aktualisierung der vorhandenen Kundendaten, wobei derartige E-Mail-Nachrichten und Internetseiten nicht erst seit dem Ausbruch der aktuellen Pandemie hoch professionell gestaltet sind,[8] sodass sie teils auch bei genauerer Betrachtung den Anschein der Echtheit erwecken. Folgt der Empfänger einer solchen Nachricht dem Ansinnen der Täter und übermittelt ihnen täuschungsbedingt die gewünschten Daten, so werden diese von ihnen in einem weiteren Schritt zur eigenen monetären Bereicherung eingesetzt. Diese kann durch ihren Verkauf, in einem Wareneinkauf auf Kosten des Geschädigten oder – bei Erlangung von Zugangsdaten zum Onlinebanking – durch eine Überweisung vom Bankkonto des Geschädigten auf ein Drittkonto liegen. Um hierbei die eigene Identität zu verschleiern, setzen die Cyberkriminellen zur Erlangung von Barmitteln entweder Finanzagenten[9] ein, die in der Regel als leichtfertige Geldwäscher ihre persönlichen Bankkonten als Empfängerkonten zur Verfügung stellen und hierauf eingehende Zahlungen gegen Abzug einer Provision direkt weiterleiten, oder verwenden Bankkonten, die mit Aliaspersonalien errichtet wurden (sog. Bankdrops).[10] Bei Warenlieferungen wird die Identität der eigentlichen Täter ähnlich verschleiert, um die Strafverfolgung zu erschweren.

Eine leichte Abwandlung der oben dargestellten Phishing-Methode, welche als Reaktion auf die zunehmenden Sicherheitskonzepte der Unternehmen entstanden ist, stellt das Ausspähen oder Abfangen von Daten unter Einsatz von Schadsoftware dar.[11] Zur Infizierung des Heimnetzwerks mit dem maliziösen Programm erhalten die potenziellen Geschädigten in der Regel von vermeintlich seriösen Absendern fingierte E-Mails mit Anhängen,[12] etwa einer Rechnung oder einer Bestellbestätigung. Sobald die angehängte Datei durch ihren Empfänger geöffnet wird, installiert sich im Hintergrund eine Schadsoftware, die – jedenfalls beim Phishing – künftig alle Tätigkeiten am Rechner aufzeichnet und an die Kriminellen weiterleitet.[13]

1.2 Pandemiebedingte Anpassung

Charakteristisch für die dargestellte Art des Phishings ist – gleich ob dabei Malware zum Einsatz kommt oder nicht –, dass die Täter versuchen, menschliche Eigenschaften wie Vertrauen, Neugier, Respekt vor Autorität oder auch aktuelle Ängste und Sorgen auszunutzen, um die Empfänger der Nachrichten dazu zu veranlassen, etwaige Schutzmechanismen zu ignorieren (sog. Social Engineering).[14] Daher ist es keinesfalls verwunderlich, dass Cyberkriminelle die derzeitige globale Herausforderung[15] als thematische Grundlage ihrer Angriffe nutzen. So konnte etwa das Landeskriminalamt Niedersachsen mit Blick auf die pandemiebedingten Existenzängste vieler Unternehmen beobachten, wie Cyberkriminelle sich im Zusammenhang mit den durch den Bund gewährten Corona-Soforthilfen als angebliche Mitarbeiter der Agentur für Arbeit bei Gewerbetreibenden meldeten und ihnen unaufgefordert Hilfe zur Beantragung von Kurzarbeitergeld zwecks Erstattung von Lohnausgaben anboten. Hierzu forderten sie die Empfänger der Nachrichten auf, näher konkretisierte Daten an eine täterseitig kontrollierte E-Mail-Adresse zu übermitteln.[16]
Malware kommt in ähnlicher Weise zum Einsatz. So werden etwa im Namen der NBank, die in Niedersachsen die Anträge auf Gewährung von Corona-Soforthilfen für Kleinstunternehmen und Soloselbstständige bearbeitet, E-Mail-Nachrichten versandt, in denen die jeweiligen Empfänger darüber informiert werden, dass die gewährte Corona-Soforthilfe als zu versteuerndes Einkommen dem Finanzamt mitzuteilen und dazu ein sich im Anhang befindendes, mit einer Schadsoftware ausgestattetes Dokument zu verwenden ist.[17]

Auch das allgemeine Informationsbedürfnis der Bevölkerung in Bezug auf den Stand der Infektionsrate verstehen digital agierende Täter für sich zu nutzen, indem sie etwa die IT-Systeme der Nutzer durch sog. „Corona-Virus Karten"[18], die in Echtzeit den aktuellen Infektionsverlauf von COVID-19 darstellen sollen, mit Schadsoftware infiltrierten. Anschließend werden – je nach Programmierung der Malware – entweder sensible Daten des Ge-

8 Eine Darstellung der Entwicklung des Phishings zu finden bei *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl., 2018, Rn. 1416 ff.; auch die Spezialisierung der Täter dürfte zur gesteigerten Professionalität beigetragen haben, s. zu dem unter dem Schlagwort „Crime-as-a-Service" behandelten Phänomen nur *Manske*, Kriminalistik 2020, 235 ff.

9 Zur Strafbarkeit der Finanzagenten s. *Sanli*, ZWH 2018, 205, 211 f.

10 *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl., 2018, Rn. 1422.

11 *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl., 2018, Rn. 1418 f., welcher auf Rn. 772 zudem die verschiedenen Formen der Schadsoftware darstellt.

12 Wobei mittlerweile die Infektion des Systems zunehmend durch das Ausnutzen einer Schwachstelle des verwendeten Browsers ohne weiteres Zutun des Betroffenen beim bloßen Aufrufen entsprechend präparierter Internetseiten erfolgt (sog. Drive-by-Infection), s. auch *Angerer*, DRiZ 2019, 428, 429, nach dem der Befall eines Rechners dadurch kaum noch zu verhindern ist.

13 Graf/Jäger/Wittig/*Bär*, Wirtschafts- und Steuerstrafrecht, 2. Aufl., 2017, § 269 Rn. 15.

14 *MünchKommBGB/Jungmann*, 8. Aufl., 2020, § 675l Rn. 39; zum Social Engineering im Zusammenhang mit dem Home-Office im Zeitalter der Corona-Pandemie s. *Fischer/Schmidt*, CB 2020, 200 ff.

15 Die Corona-Pandemie ist von der Bundeskanzlerin als größte Herausforderung seit dem zweiten Weltkrieg bezeichnet worden, s. die Fernsehansprache der Bundeskanzlerin *Merkel* v. 18.03.2020, abrufbar unter https://www.bundesregierung.de/breg-de/themen/coronavirus/ansprache-der-kanzlerin-1732108 (zuletzt abgerufen am 18.08.2020).

16 Mitteilung des LKA Niedersachsen v. 02.04.2020, „Aktuelle Corona-Info: Phishingmail der angeblichen Arbeitsagentur bietet Hilfe bzgl. Kurzarbeitergeld", abrufbar unter: https://www.polizei-praevention.de/aktuelles/aktuelle-corona-info-phishingmail-der-angeblichen-arbeitsagentur-bietet-hilfe-bzgl-kurzarbeitergeld.html (zuletzt abgerufen am 18.08.2020). Zur Veranschaulichung der in diesem Zusammenhang versandten Phishing-Mails wurde eine entsprechend (anonymisierte) Nachricht auf diese Website hochgeladen. Die Täter setzen auch beim Vishing (Voice Phishing, bei dem die Kontaktaufnahme telefonisch erfolgt) und Smishing (SMS Phishing, bei dem die Kontaktaufnahme per SMS erfolgt) die Corona-Pandemie als Aufhänger des jeweiligen Angriffs ein, wobei beide Varianten sowohl in tatsächlicher, mit Ausnahme der Art der Kontaktaufnahme, als auch in rechtlicher Hinsicht analog zum hier dargestellten Phishing laufen.

17 Mitteilung des LKA Niedersachsen v. 05.05.2020, „Aktuelle Corona-Info: Angebliche Mails der NBank im Umlauf", abrufbar unter: https://www.polizei-praevention.de/aktuelles/aktuelle-corona-info-angebliche-mails-der-nbank-im-umlauf.html (zuletzt abgerufen am 18.08.2020). Zur Veranschaulichung der in diesem Zusammenhang versandten Nachrichten wurde eine Beispielsmail auf der genannten Website hinterlegt.

18 Das BKA warnte bereits im April vor derartigen Karten, s. Mitteilung des BKA v. 03.04.2020, „Achtung: Kriminalität im Internet im Zusammenhang mit dem Coronavirus", abrufbar unter: https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Warnhinweise/200403_CoronaInternet.html (zuletzt abgerufen am 18.08.2020).

schädigten ausgelesen[19] oder aber das infizierte System gesperrt und Lösegelder zu dessen Entsperrung verlangt[20].

An einen Man-in-the-Middle-Angriff[21], bei dem sich der Phishing-Täter mittels einer Schadsoftware zwischen zwei Kommunikationspartner schaltet und die Transaktionsdaten nach Belieben manipulieren kann, erinnert die Tatbegehung von Cyberkriminellen in Nordrhein-Westfalen. Die Täter kamen hier allerdings ohne den Einsatz von Malware auf den IT-Systemen der Betroffenen aus, indem sie sich schlicht deren Existenzängste zu eigen machten. Hierzu kopierten sie nahezu den gesamten Webauftritt des nordrhein-westfälischen Wirtschaftsministeriums mit dem Ziel, Antragsformulare für coronabedingte Subventionen über diese ausfüllen zu lassen. Sobald die Hilfesuchenden die geforderten Daten in das zur Verfügung gestellte Formular eingetragen hatten, wurde die Bankverbindung des jeweiligen Antragsstellers zu Gunsten der Kriminellen abgeändert und der Antrag an die tatsächlich für die Subventionsgewährung zuständige Stelle weitergeleitet.[22] Nach ersten Erkenntnissen sind die Täter auf diese Weise an 3.500 bis 4.000 Unternehmensdaten gelangt und haben diese, nach Änderung des begünstigten Bankkontos zu ihrem Vorteil, an die tatsächlich für die Gewährung der jeweiligen Subvention zuständige Stelle weitergeleitet. Im Falle der erfolgten Auszahlung der beantragten Subventionen könnte dies rechnerisch zu einem Schaden im mittleren zweistelligen Millionenbereich führen.[23]

Eine coronabedingte Zunahme von Cyberangriffen auf Kritische Infrastrukturen i.S.v. § 2 Abs. 10 BSIG, d.h. insbesondere auch auf Einrichtungen des Gesundheitswesens, sollen laut der Zentralen Meldestelle für IT-Sicherheit Kritischer Infrastrukturen – jedenfalls in Deutschland – bislang nicht festgestellt worden sein.[24]

1.3 Rechtliche Einordnung

Trotz der täuschungsbedingten Preisgabe der Daten durch den Geschädigten ist die Datenbeschaffung rechtlich nicht als Betrug einzustufen. Alleine die Preisgabe der Daten hat keine unmittelbare Vermögensminderung zur Folge. Eine solche folgt erst in dem nachgelagerten Schritt der Datenverwendung.[25] Aus diesem Grund ist für die Einordnung der Strafbarkeit des Phishings zwischen den unterschiedlichen Tatphasen der Datenbeschaffung und der Datenverwendung zu differenzieren.

1.3.1 Phishing-Mail

Im Falle des Einsatzes von Phishing-Mails ist die Datenbeschaffung regelmäßig als ein Sich-Verschaffen von Passwörtern und sonstigen Sicherungscodes i.S.v. § 202c Abs. 1 Nr. 1 StGB zu qualifizieren.[26] Sofern im Rahmen der Phishing-Mail der Eindruck erweckt wird, die entsprechende Nachricht stamme vermeintlich von einer tatsächlich existierenden dritten Person, was die Regel sein dürfte, so unterfällt die Angabe zum Absender dem Datenbegriff des § 269 StGB und ist zudem beweiserheblich, sodass eine Strafbarkeit wegen Fälschung beweiserheblicher Daten anzunehmen ist.[27] Tateinheitlich kommt im Falle der Verwendung urheberrechtlich geschützter Zeichen – etwa eines Logos einer Bank – darüber hinaus auch eine Strafbarkeit nach §§ 143 Abs. 1, 143a Abs. 1 MarkenG sowie §§ 106 ff. UrhG in Betracht.[28]

Werden die ausgespähten Daten sodann im zweiten Schritt verwendet, etwa um im Onlinebanking eine Kontoverfügung vorzunehmen, ist der Tatbestand des Computerbetruges gem. § 263a Abs. 1 Var. 2 StGB in Tateinheit mit § 269 Abs. 1 StGB erfüllt.[29] Tateinheitlich liegt ferner eine Strafbarkeit nach § 42 Abs. 2 Nr. 1 BDSG vor, da jeder vom Täter kausal und objektiv zurechenbar verursachte Umgang mit den erlangten, nicht allgemein zugänglichen personenbezogenen Daten ein unzulässiges Verarbeiten im Sinne der Norm darstellt.[30] Des Weiteren kommt bei einer gewerbs- und bandenmäßigen Begehung die Qualifikation des § 263a Abs. 2 i.V.m. § 263 Abs. 5 und § 269 Abs. 3 i.V.m. § 267 Abs. 4 StGB in Betracht. Sofern mit den abgefangenen Daten Corona-Soforthilfeleistungen beantragt werden, wird der Computerbetrug vom Subventionsbetrug gem. § 264 StGB verdrängt.[31]

1.3.2 Phishing-Webseiten

Auch bei den zum Abfangen von Daten entsprechend präparierten Internetseiten, wie etwa bei dem durch Cyberkriminelle kopierten Webauftritt des nordrhein-westfälischen Wirtschaftsministeriums, ist zwischen den Tatphasen der Datenbeschaffung und der Datenverwendung zu differenzieren. Im Rahmen der Datenbeschaffung werden die Besucher der jeweiligen Domain über die Identität des Webseitenbetreibers getäuscht, sodass in dieser Tatphase eine Strafbarkeit nach § 269 Abs. 1 StGB (Fälschung beweiserheblicher Daten) anzunehmen ist.[32] Da der

19 Mitteilung des BKA v. 03.04.2020, „Achtung: Kriminalität im Internet im Zusammenhang mit dem Coronavirus", abrufbar unter: https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Warnhinweise/200403_CoronaInternet.html (zuletzt abgerufen am 18.08.2020).

20 Mitteilung des LKA Niedersachsen v. 14.04.2020, „Aktuelle Corona-Info: Gefährliche Mail im Namen des Bundesministeriums für Gesundheit", abrufbar unter: https://www.polizei-praevention.de/aktuelles/aktuelle-corona-info-gefaehrliche-mail-im-namen-des-bundesministeriums-fuer-gesundheit.html (zuletzt abgerufen am 18.08.2020).

21 Hierzu *Sanli*, ZWH 2018, 205, 207; *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl., 2018, Rn. 282 spricht in diesem Zusammenhang zutreffender vom „Man-in-the-*System*".

22 Redaktion beck-aktuell v. 14.04.2020, becklink 2016019.

23 *Willmroth*, Kriminelle kopieren Webseite des NRW-Wirtschaftsministeriums, in der Süddeutschen Zeitung v. 12.04.2020, abrufbar unter: https://www.sueddeutsche.de/politik/nrw-corona-soforthilfe-webseite-betrug-1.4874750 (zuletzt abgerufen am 18.08.2020).

24 BT-Drucks. 19/19676, S.10 Ziff. 11.

25 Achenbach/Ransiek/Rönnau/*Kölbel*, HdB WirtschaftsstrafR, 5. Aufl., 2019, 5. Teil, XV. Phishing, Rn. 280 f.; ausführlich hierzu auch *Sanli*, ZWH 2018, 205, 208 f.; aA *Ceffinato*, NZWiSt 2016, 464, 465 f., der den ausgespähten Daten jedenfalls dann einen Vermögenswert einräumt und von einem Gefährdungsschaden ausgeht, wenn der Täter durch diese in die Lage versetzt wird unmittelbar auf tatsächlich vorhandenes und zu verfügendes Vermögen zuzugreifen.

26 *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl., 2018, Rn. 1441.

27 MünchKomm StGB/*Erb*, 3. Aufl., 2019, § 269 Rn. 33; Graf/Jäger/Wittig/*Bär*, Wirtschafts- und Steuerstrafrecht, 2. Aufl., 2017, § 269 Rn. 15 mwN, s. auch *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl., 2018, Rn. 1441, nach dem § 269 StGB den § 202c Abs. 1 Nr. 1 StGB verdrängen würde, wobei nach hiesiger Auffassung die Taten im Verhältnis der Tateinheit zueinander stehen dürften.

28 So auch *Sanli*, ZWH 2018, 205, 210.

29 *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl., 2018, Rn. 1443.

30 BeckOK DatenschutzR/*Brodowski/Nowak*, 32. Ed., Stand: 01.05.2020, § 42 BDSG Rn. 45; *Sanli*, ZWH 2018, 205, 211.

31 Zur Strafbarkeit des Subventionsbetruges im Zusammenhang mit den Corona-Soforthilfen s. *Rau/Bou Sleiman*, NZWiSt 2020 373.

32 MünchKomm StGB/*Erb*, 3. Aufl., 2019, § 269 Rn. 34; *Sanli*, ZWH 2018, 205, 209; im Allgemeinen auch Spindler/Schuster/*Gercke*, Recht der elektronischen Medien, 4. Aufl., 2019, § 269 Rn. 5.

Tatbestand des § 269 Abs. 1 StGB hier bereits infolge der Einrichtung der Internetseite vollendet wird, ist bei der späteren Erlangung von Passwörtern und Sicherungscodes aufgrund ihrer täuschungsbedingten Eingabe auf der vom Täter betriebenen Seite in Tatmehrheit eine Strafbarkeit der Verantwortlichen nach § 202c Abs. 1 Nr. 1 StGB anzunehmen.[33]

Die obigen Ausführungen hinsichtlich der Strafbarkeit im Rahmen der Datenverwendung gelten an dieser Stelle entsprechend.

1.3.3 Einsatz von Malware

Beim Einsatz von Malware ist zwischen zwei strafrechtlich relevanten Phasen zu differenzieren, nämlich der Anlieferung des Schadprogramms bis hin zu dessen Installation und der Phase, in welcher das installierte Programm ausgeführt wird. Während sich die Täter bis zur Installation der Malware wegen Computersabotage gem. § 303b Abs. 1 Nr. 2 StGB strafbar machen, hängt die Strafbarkeit nach der Installation der maliziösen Software davon ab, welche Funktion ihr zukommt. Ist sie dazu programmiert worden, das infizierte System zu sperren, um unter Androhung eines empfindlichen Übels, etwa des Löschens sämtlicher Daten, ein Lösegeld zu fordern (Ransomware[34]), erfüllt dies den Tatbestand des § 303a Abs. 1 Var. 2 StGB[35] (Datenveränderung) in Tateinheit mit Erpressung gem. § 253 Abs. 1 StGB.[36] Dient die Malware dazu, Daten auszuspähen, ist eine Strafbarkeit gem. § 202a Abs. 1 StGB anzunehmen.[37] Ist Letzteres der Fall, kommt eine weitere Phase der Tatbegehung hinzu, nämlich die der Datenverwendung. Bei dieser gibt es hinsichtlich der Strafbarkeit keine Besonderheiten im Vergleich zur Datenverwendung nach deren Erlangung durch das Mail- oder Webseiten-Phishing.

2 Fazit

Bereits vor der Corona-Krise berichtete das BSI über die im Cyberbereich anhaltend hoch einzustufende Bedrohungslage,[38] woran sich nichts geändert hat. Die in der Praxis bekannt gewordenen Fälle zeigen in beeindruckender, aber auch erschreckender Weise, wie schnell die kriminellen Akteure der digitalen Welt unter Beibehaltung ihres bekannten Werkzeugkastens ihr Vorgehen den jeweiligen gesellschaftlichen Gegebenheiten anpassen können. Sie nutzen altbekannte Methoden des Cyberangriffs und kombinieren diese mit einer für die Bevölkerung neuen, emotional sowie wirtschaftlich belastenden Thematik, die zum Teil bis hin zur Existenzgefährdung geht.[39] Aufgrund der mit COVID-19 verbundenen Sorgen und der dadurch begünstigten stärkeren Digitalisierung des privaten sowie beruflichen Alltags ist die Angriffsfläche für Cyberkriminelle breiter geworden. Dies führt insbesondere im Bereich des Phishings zu einer gestiegenen Anzahl von Attacken[40], denen auch eine höhere Erfolgschance beizumessen ist, sodass das Corona-Virus die Cyberkriminalität tatsächlich katalysiert haben dürfte.

Literatur

[1] Achenbach/Ransiek/Rönnau, Handbuch Wirtschaftsstrafrecht, 5. Auflage, 2019.
[2] Angerer, Kampf gegen Cybercrime – Phänomene und Ermittlungsprobleme, DRiZ 2019, 428-431.
[3] Brink/Wolff, BeckOK Datenschutzrecht, 32. Edition, Stand: 01.05.2020.
[4] Ceffinato, Vermögensstraftaten im und über das Internet, NZWiSt 2016, 464-467.
[5] Fischer/Schmidt, Social Engineering im Zeitalter von COVID-19 und Home-Office, CB 2020, 200-204.
[6] Graf/Jäger/Wittig, Wirtschafts- und Steuerstrafrecht, 2. Auflage, 2017.
[7] Hefendehl/Hohmann, Münchner Kommentar zum Strafgesetzbuch, Band 5, §§ 263-358 StGB, 3. Auflage, 2019.
[8] Henssler, Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 6, §§ 631-704 BGB, 8. Auflage, 2020.
[9] Kochheim, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Auflage, 2018.
[10] Manske, Crime-as-a-Service, Die Neun Säulen – Eine Phänomenbeschreibung, Kriminalistik 2020, 235-239.
[11] Meier, „Digitale Erpressung", Kriminalistik 2016, 361-365.
[12] Rau/Bou Sleiman, Subventionsbetrug im Zusammenhang mit Corona-Soforthilfen für Kleinstunternehmen und Soloselbstständige, NZWiSt 2020, 373-377.
[13] Sander, Münchner Kommentar zum Strafgesetzbuch, Band 4, §§ 185-262 StGB, 3. Auflage, 2017.
[14] Sanli, Die Strafbarkeit des Phishings unter Berücksichtigung neuer Phishing-Formen, ZWH 2018, 205-213.
[15] Schmidt, COVID-19, Rechtsfragen zur Corona-Krise, 2. Auflage, 2020.
[16] Spindler/Schuster, Recht der elektronischen Medien, 4. Auflage, 2019.
[17] Vogelgesang/Möllers, Ransomware als moderne Piraterie – Erpressung in Zeiten digitaler Kriminalität, jM 2016, 381-387.
[18] Wabnitz/Janovsky/Schmitt, Handbuch des Wirtschafts- und Steuerstrafrechts, 5. Auflage, 2020.

33 *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl., 2018, Rn. 1464, 1466.

34 Zur Ransomware s. *Vogelgesang/Möllers* jM 2016, 381 ff.

35 Etwa Graf/Jäger/Wittig/*Bär*, Wirtschafts- und Steuerstrafrecht, 2. Aufl., 2017, § 303a Rn. 18.

36 MünchKomm StGB/*Sander*, 3. Aufl., 2017, § 253 Rn. 11; zur „Digitalen Erpressung" s. auch *Meier*, Kriminalistik 2016, 361 ff.

37 Ausführlich hierzu *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl., 2018, Rn. 828 ff., 1473 ff.

38 BSI, Die Lage der IT-Sicherheit in Deutschland 2019, S. 7, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=7 (zuletzt abgerufen am 18.08.2020).

39 Insoweit weist *Rau* in: Schmidt, COVID-19, Rechtsfragen zur Corona-Krise, 2. Aufl., 2020, § 19 Rn. 2 zu Recht darauf hin, dass die „eigentliche Masche" der Täter unverändert ist und die alten Tricks lediglich auf „Corona getrimmt" werden.

40 S. die Bedrohungsübersicht des CERT-EU für das zweite Quartal 2020, wonach die Anzahl der Phishing-Angriffe innerhalb Europas insgesamt zugenommen habe und hierbei thematisch vor allem an die derzeitige Pandemie angeknüpft werde, abrufbar unter: https://media.cert.europa.eu/static/MEMO/2020/TLP-WHITE-2020Q2-Threat_Landscape_Report-Executive-Summary-v1.0.pdf (zuletzt abgerufen am 18.08.2020).