Cybercrime im Corona-Deckmantel

Bekannte Phänomene in neuem Gewand

Von PR Martin Hoch M.A., Büchenbeuren[1]

Weltweit führte das *„Coronavirus SARS-CoV-2“* zu massiven Einschränkungen des öffentlichen Lebens. Nahezu alle Aktivitäten der analogen Welt haben sich deshalb verstärkt in den digitalen Raum verlagert: Die Arbeit im Homeoffice, der Kontakt mit Familie und Freunden oder auch der Einkauf von Artikeln des täglichen Bedarfes finden nunmehr verstärkt virtuell statt. Dadurch eröffnet sich auch für Cyberkriminelle ein neuer Angriffsvektor, die sich teils bekannter modi operandi bedienen, um personenbezogene Daten, Zugangsinformationen oder Finanzmittel zu erlangen. Dieser Artikel betrachtet die Abwandlungen bekannter Cybercrime-Phänomene in COVID-19-Zeiten und setzt sich mit den besonderen Faktoren auseinander, die aufgrund der Pandemie eine Viktimisierung ggf. begünstigen.

1 Einleitung: COVID-19 als virtuelle Pandemie

Das seit Anfang 2020[2] weltweit grassierende Virus führte zu bisher nie dagewesenen Herausforderungen auf allen Ebenen von Politik, Wirtschaft und Gesellschaft, die sich – auch nach der Hochphase im 1. Halbjahr – insbesondere in Form von Einschränkungen manifestieren. Die Maßnahmen der Bundesregierung zur Reduzierung der Reproduktionszahl[3] sind hinlänglich bekannt: Schließung von Restaurants, Hotels und öffentlichen Einrichtungen, Reduzierung des Flugbetriebes und des öffentlichen Personennahverkehrs, das Einhalten eines physischen Sicherheitsabstandes von mind. 1,5 bis 2 Metern, Kontaktbeschränkungen und der Erlass von Corona-Landes-Verordnungen zur Regelung bestimmter verbreitungskritischer Verhaltensweisen in der Öffentlichkeit[4]. Sie alle sollten zur Abflachung der exponentiellen Infektionskurve[5] beitragen. Seit Mai 2020 werden die verhängten Maßnahmen zwar gelockert, von einem gesellschaftlichen *„Normalzustand“* kann aber nach wie vor nicht die Rede sein.
Aus kriminologischer Sicht ist insbesondere die Entwicklung der Kriminalität *während* dieser Beschränkung des öffentlichen Lebens von Interesse. Naheliegend ist, dass Straftaten der Straßenkriminalität durch die Verwaisung von Innenstädten und Fußgängerzonen deutlich zurückgehen.[6] Demgegenüber stehen die Entwicklungen im Cybercrime-Sektor. Zeigte Cyberkriminalität in den vergangenen Jahren bekanntermaßen eine kontinuierlich steigende Tendenz[7], so werden virtuelle Delikte durch die genannten Corona-bedingten Entwicklungen noch zusätzlich begünstigt. Denn während das analoge Leben zur Viruseindämmung umfassend beschränkt wird, kann das Leben im virtuellen Raum nach wie vor uneingeschränkt stattfinden: Die berufliche Tätigkeit verlagert sich in das Homeoffice, Familie und Freunde werden per Videochat oder Telefonanruf kontaktiert, der Einkauf erfolgt via Online-Shopping, und E-Mail-Programme ersetzen die ansonsten alltäglichen Gespräche. Natürlich existierten virtuelle Ansteckungsgefahren *(„Computerviren“)* bereits vor der COVID-19-Pandemie. Aber die verstärkte Nutzung von Online-Services in privaten und beruflichen Bereichen eröffnet neue Einfallstore und schafft kritische Schnittstellen, die von Cyberkriminellen noch gezielter und kreativer als bisher ausgenutzt werden können. Insofern ist COVID-19 nicht nur ein ernst zu nehmendes Gesundheitsrisiko in der analogen Welt, sondern auch ein Cyberrisiko, das sowohl Privatpersonen als auch Unternehmen und Behörden tangiert. Es lässt sich sogar konstatieren, dass der Einfluss von COVID-19 auf Cybercrime im Vergleich zur restlichen Kriminalität am auffälligsten und deutlichsten ist[8], da es den Cyberkriminellen bisher sehr schnell gelungen ist, sich den neuen Rahmenbedingungen anzupassen und bestehende Ängste sowie Unsicherheit der Opfer für ihre Zwecke auszunutzen. Sogar die Underground Economy[9] beschreitet in Teilen neue Wege jenseits von Betäubungsmittel- und Waffenhandel, indem COVID-19-bezogene Artikel angeboten werden.[10]

2 Kriminalitätsfaktoren

Um zu erfassen, warum bestimmte Cybercrime-Phänomene gerade in Zeiten der Viruspandemie neue Formen annehmen und die Täter nach wie vor erfolgreich sind, hilft eine Betrachtung der mit COVID-19 verbundenen gesellschaftlichen Auswirkungen weiter. Sie lassen sich als Viktimisierungsfaktoren beschreiben. Kumuliert tragen sie zur Steigerung der personenbezogenen Vulnerabilität bei und können letztlich die Opferwerdung zumindest begünstigen (vgl. Abb. 1).

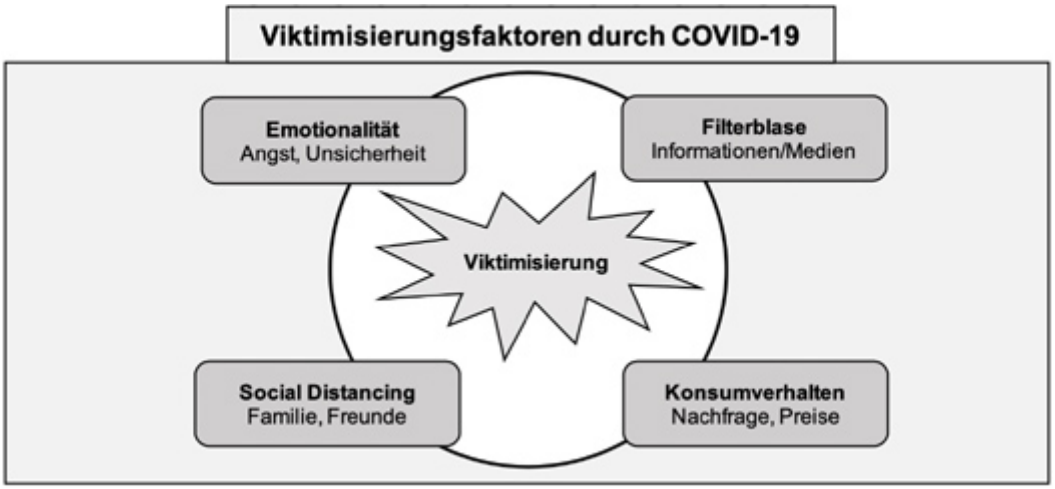

Abb. 1: Viktimisierungsfaktoren für Cybercrime (eigene Visualisierung).

2.1 Konsumverhalten

Der anfängliche rasante Anstieg an Infizierten führte schlagartig zu einer stark erhöhten Nachfrage bspw. an Schutzausstattung und Reinigungsmitteln; nicht nur bei medizinischem Personal, sondern bei allen Teilen der Gesellschaft. Aber auch andere Konsumgüter des täglichen Bedarfes erfuhren eine erhöhte Nachfrage. Besondere Stilblüten entwickelten Hamsterkäufen von Toilettenpapier, Mehl und Nudeln, was teilweise zu leeren Regalen in den Supermärkten führte.[11] Dabei ist der bloße Glaube darüber, dass ein Gut knapp werden könnte, bereits ausreichend, um das Kaufverhalten weiter zu fördern. Im Ergebnis kaufen immer mehr Menschen Waren, deren erhöhte Nachfrage zunächst nicht befriedigt werden kann; der Eindruck der Knappheit verstärkt sich insofern wie eine selbsterfüllende Prophezeiung. Als Nebeneffekt wird aufgrund der großen Nachfrage u.U. der Preis vermeintlich knapper Waren (z.B. Schutzmasken) erhöht.

2.2 Emotionalität

Zu der erhöhten Konsumgüternachfrage tritt aus emotionaler Sicht eine diffuse Angst, die als „Hintergrundrauschen“ bereits sublim Menschen beeinflussen kann. Sie gründet sich auf der Unsicherheit vor einer möglichen Ansteckung mit einem an sich geruchs- und geschmacklosen sowie unsichtbaren Virus und der Ungewissheit der künftigen Entwicklungen. Neben die Infektionsangst tritt eine Verunsicherung über die private oder finanzielle Zukunft hinzu. Der Effekt wird auch deshalb noch verstärkt, weil eine derartige Krise, die als Bedrohung für das eigene Leben (Kurzarbeit, Arbeitslosigkeit, Zusammenbruch des Gesundheitssystems) wahrgenommen werden kann, in den letzten Jahrzehnten einmalig ist. Während die Weltkriegsgenerationen ein gewisses Anpassungsverhalten auf existenzielle Bedrohungen entwickelten, sind derartige Situationen für die heutigen Generationen höchst außergewöhnlich.

2.3 Filterblase

Das Gefühl von Angst und Verunsicherung kann durch die mediale Berichterstattung (Hauptthema: *„Gefahren von Corona“*) und den Austausch mit Familienmitgliedern und Freunden (Hauptthema: *„Einschränkungen durch Corona“*) noch verstärkt werden. Gerade das Prinzip der sozialen Distanz gegenüber anderen Menschen und der Rückzug in den engsten Sozialkreis kann zu einer singulären Wahrnehmung der Realität führen, da der für eine pluralistische Meinungsbildung erforderliche heterogene und konträre Austausch von Argumenten untereinander fehlt. Es besteht insofern die Gefahr, dass Menschen von einer Art *„Filterblase“* umgeben werden, die zu einer Isolation des Einzelnen gegenüber vom eigenen Standpunkt abweichenden anderen Informationen führt.[12] So kann in Form einer Abwärtsspirale dazu beitragen, dass die Realität ausschließlich als schlecht, bedrohlich und düster wahrgenommen wird.

2.4 Social Distancing

Die Einschränkung des öffentlichen Lebens und die auferlegten Kontaktbeschränkungen sollen die Verbreitung von COVID-19 eindämmen, führen aber zwangsläufig auch zu einem Anwachsen des Nährbodens für Cyberkriminelle: Ein Großteil alltäglicher Aktivitäten verlagert sich durch das physische *„Social Distancing"* in die virtuelle Welt. Soziale Kontakte werden intensiv mithilfe von Online-Plattformen gepflegt, Nachrichten vermehrt über E-Mail/Chatprogramme übermittelt und Kontakt mit Familie und Freunde hauptsächlich durch Telefon oder Videocall hergestellt. Hinzu tritt ein verstärktes Online-Konsumverhalten auf Shopping-Plattformen sowie die breite Nutzung von Home-Office-Möglichkeiten. Der analoge Alltag wird quasi digitalisiert. Diese Vielzahl von Nutzungsmöglichkeiten bildet neue Schnittstellen, die gleichermaßen objektive Sicherheitslücken eröffnen, z.B. aufgrund einer fehlenden Anti-Viren-Software, wie subjektive Sicherheitsrisiken formen, z.B. wegen des leichtfertigen Umgangs mit der eigenen digitalen Identität im Internet. Insofern können die Angriffsvektoren von Cyberkriminellen vielfältig sein.

3 Angriffsvektoren

Kriminelle nutzen die besondere Situation aus, um die modi operandi bereits bekannter Cybercrime-Phänomene im Zusammenhang mit der COVID-19-Pandemie in ein neues Gewand zu kleiden, so dass ein aktueller thematischer Bezug entsteht und gezielt die genannten Viktimisierungsfaktoren adressiert werden (vgl. Abb. 2).

3.1 Enkeltrick

So wird der polizeilich bekannte *„Enkeltrick",* bei dem organisierte Täter die Notlage eines vermeintlichen Enkels (oder anderen Verwandten) vortäuschen und das Opfer dazu bringen, hohe Bargeldbeträge oder Schmuckgegenstände an einen *„Freund"* des Enkels zu übergeben, Corona-bezogen abgewandelt.
Eine naheliegende (und genutzte) Abwandlung besteht darin, dass die Täter mitteilen, ein Familienmitglied habe sich mit Corona infiziert und benötige nun schnellstmöglich Bargeld für ein experimentelles Medikament. Aber die Täter geben sich mitunter auch als Mitarbeiter staatlicher Institutionen (Polizei oder Gesundheitsamt) aus und täuschen das Erfordernis der Durchführung eines Corona-Schnelltestes durch des Opfers vor, dessen Kosten zwischen 5.000 bis 7.000 Ä liegen.[13] Es sind auch Fälle bekannt, in denen die Täter in Schutzanzügen unmittelbar an der Haustür des Opfers klingeln und vortäuschen, das Haus wegen eines Infektionsverdachtes mit einem teuren Desinfektionsmittel reinigen zu müssen. In anderen Fällen wird der Vorwand genutzt, das Haus wegen COVID-19 überprüfen zu müssen, wobei Wertsachen entwendet werden.[14]
Im Pandemiekontext werden durch die Täter also gezielt die Faktoren Angst und Verunsicherung, insbesondere älterer Menschen, ausgenutzt. Ergänzt wird das Verhalten der Täter durch das Vorspiegeln einer zeitlichen Dringlichkeit, den Aufbau von Druck und ein sehr selbstbewusstes Auftreten. Als Straftatbestände kommen auch in diesen neuen Sachverhaltskonstellationen der Betrug nach § 263 StGB (insbesondere kann ein strafschärfender gewerbsmäßiger Bandenbetrug nach Absatz 5 vorliegen) und/oder die Amtsanmaßung nach § 132 StGB in Betracht.
Während der abgewandelte Enkeltrick unter Ausnutzung digitaler Technik begangen wird, aber nach wie vor einen wichtigen Tatanteil durch die Täter in der physischen Welt umfasst, beziehen sich die folgenden Cybercrime-Delikte auf die *digitale* Identität[15] eines Opfers.

3.2 Phishing

Eine in COVID-19-Zeiten besonders verbreitete Vorgehensweise ist aufgrund des vergleichsweise geringen technischen Aufwandes[16], der Vielzahl potenzieller Opfer und der hohen Aussichten auf Taterfolg das Phishing[17]. So blockt derzeit beispielsweise der Freemail-Anbieter Google täglich 18 Mio. E-Mails mit Phishing-Relevanz[18], das Bundesamt für Sicherheit in der Informationstechnik warnt offiziell vor diesem Cyber-Phänomen[19] und Europol erwartet, dass Phishing in Art und Umfang perspektivisch weiter zunehmen wird.[20]
Das neue Gewand von Phishing zeichnet sich durch eine Bezugnahme auf COVID-19 aus und greift verschiedene Einzelaspekte der Krankheit auf: den Virusschutz, die Informationsweitergabe oder das Offerieren finanzieller Hilfe. Dabei sind die Täter kreativ und beschreiben beispielsweise, dass virusbedingt Bankfilialen schließen müssen und deshalb die Eingabe der Zugangsdaten für die Nutzung des Online-Bankings erforderlich sei.[21] Eine andere Vorgehensweise ist die Tarnung als Behördennachricht unter Bezugnahme auf eine beantragte Corona-Soforthilfe für Unternehmen, die durch die Angabe weiterer persönlicher Daten bestätigt werden soll. Aber auch mit Fake-Shops wird geworben. Hierzu fälschen die Täter professionell Webseiten, auf denen Desinfektionsmittel oder Schutzkleidung angeboten werden. Über eine – teilweise im Namen real existierender Unternehmen verschickte – Phishing-Mail werden die Opfer dazu animiert, ihre persönlichen Daten für eine vermeintliche Bestellung einzugeben. Tatsächlich wird die Bestellung jedoch nie versandt – den Tätern kommt es nur auf das Erlangen persönlicher Daten oder den unbemerkten Download von Malware (siehe Punkt 3.4) an.

Die Strafbarkeit der Täter richtet sich dabei nach der jeweiligen Tatphase. Während bei der Erstellung gefälschter E-Mails oder Webseiten eine Strafbarkeit der Fälschung beweiserheblicher Daten nach § 269 Abs. 1 StGB (mit Strafschärfungsmöglichkeiten nach § 269 Abs. 3 i.V.m. § 263 Abs. 3, 4 StGB, z.B. bei bandenmäßiger Begehung oder Herbeiführung eines Vermögensverlustes großen Ausmaßes[22]) in Betracht kommt, scheitert sie bei § 202a StGB bei dem Merkmal der Überwindung einer *„besonderen“* Zugangssicherung, da die Daten *„aus der Hand des Opfers“* weitergegeben werden.[23]§ 202b StGB kommt in Ermangelung einer laufenden Datenübermittlung, aus der die Daten durch die Täter tatbestandlich abgefangen (*„durch Einklinken“*) werden müssen, ebenso nicht in Betracht.[24]
Sobald die Cyberkriminellen die Daten erlangt haben, kann sich die weitere Strafbarkeit aus § 202a Abs. 1 StGB ergeben, da bei der Datenverwendung – selbst unter Eingabe zuvor gephishten und damit erwartungsgemäß korrekten Daten – eine Zugangssicherung (z.B. Login-Oberfläche) überwunden wird. § 202b Abs. 1 StGB ist hingegen nicht einschlägig, da von vornherein ein Datenaustausch zwischen den Computern der Täter und dem Zielserver (z.B. der Online-Shopping-Webseite) erfolgt. Gleichwohl kommt eine weitere Strafbarkeit nach § 263a Abs. 1 StGB in Betracht, da die erlangten Daten unbefugt verwendet werden und dadurch das Ergebnis der serverseitigen Datenverarbeitung beeinflusst wird.

3.3 Social Engineering

In Zeiten von COVID-19 nutzen Kriminelle auch zunehmend das Instrument des *„Social Engineering“*[25]. Der Begriff beschreibt die Durchführung sozialer Manipulation, basierend auf der Annahme, dass der Mensch grds. das schwächste Glied in einer IT-Sicherheitskette darstellt. Das Ziel besteht darin, das Opfer (meist Mitarbeiter eines Unternehmens) durch geschickte zwischenmenschliche Interaktionen und damit verbundene Täuschung über Identität und Absicht des Täters zu einem bestimmten Verhalten zu veranlassen, so dass geltende Sicherheitsrichtlinien (z.B. Vier-Augen-Prinzip, Rücksprache mit Vorgesetzten) missachtet und vertrauliche Unternehmensinformationen preisgegeben werden. Hierzu betreiben die Täter einen vergleichsweise hohen Aufwand, da eine genaue Kenntnis der Unternehmensstruktur, wichtiger Akteure und der Betriebsabläufe entscheidend für die Tatausführung in Form von Betrugshandlungen ist. Social Engineering dient insofern als Vorbereitung auf folgende Cybercrime-Handlungen.
So werden oftmals in einem ersten Schritt Mitarbeiter und ggf. erforderliche Zugangsberechtigungen zum Unternehmen ausgespäht[26], das Corporate Design offizieller Unternehmensdokumente gefälscht[27] und durch scheinbar unverbindliche Telefonanrufe/E-Mail-Korrespondenz die Unternehmensstruktur, namentlich beschäftigte Mitarbeiter sowie der intern genutzte Sprachgebrauch ausgeforscht. In einem zweiten Schritt werden sodann gezielt Phishing-Mails an zuvor festgelegte Mitarbeiter/Abteilungen versandt[28] oder telefonisch Kontakt aufgenommen, um durch eloquentes Auftreten gepaart mit Wissen um interne Abläufe bestimmte Handlungen, wie die Veranlassung von Geldzahlungen oder Preisgabe interner sensibler Informationen, auszulösen. Dabei geben sich die Täter in Corona-Zeiten als Angehörige der Personalabteilung des Opfer-Arbeitgebers aus, die vorsorglich die Aktualität personenbezogener Daten erheben müssen, falls es im Unternehmen zu Corona-Erkrankungen kommen sollte. Aber auch die Legende, ein Großlieferant zu sein, der das Unternehmen mit Masken/Schutzausstattung versorgt hat und noch auf die Begleichung hoher Rechnungsbeträge wartet, oder das Verschicken von E-Mails im Unternehmensdesign mit angehängten angeblichen internen Handlungsanweisungen (tatsächlich ist ein Schadprogramm angehängt) für einen Corona-Verdachtsfall, sind mögliche Abwandlungen.
Die Strafbarkeit ergibt sich aus den konkreten Anschlusshandlungen. Regelmäßig dürfte ein Betrug i.S.d. § 263 Abs. 1 StGB vorliegen. Je nach vorbereitender Handlung kommen diverse Straftatbestände in Betracht, wie z.B. das unbefugte Betreten des Unternehmensgeländes zur Auskundschaftung (Hausfriedensbruch i.S.d. § 123 StGB) oder der Diebstahl i.S.d. § 242 Abs. 1 StGB von Firmendokumenten (auch entsorgte Dokumente in Zusammenhang mit dem *„Dumpster Diving“*).

3.4 Malware/Ransomware

Das aus den Wörtern *„malicious“* und *„software“* zusammengesetzte Kunstwort bezeichnet als Oberbegriff solche Computerprogramme, die von Kriminellen mit dem Ziel entwickelt und verbreitet werden, unerwünschte und meistens schädliche Funktionen auf dem Zielrechner auszuführen. Ein solches Schadprogramm kann verschiedene Erscheinungsformen annehmen, z.B. als Virus (benötigt ein Wirtsprogramm, um Schadcode auszuführen) oder Trojaner (Tarnung als vermeintlich nützliche Software/Datei).[29] Malware kann auf ebenso unterschiedlichen Wegen auf ein IT-System gelangen, z.B. als getarnter Anhang in einer E-Mail, durch das Klicken auf Links oder das Anzeigen präparierter Webseiten, die bestimmte Sicherheitslücken im Browser ausnutzen, um Programmcode auszuführen[30]. In diesem Zusammenhang stellt auch das Bundesamt für Sicherheit in der Informationstechnik fest, dass vermehrt Domains auf Begriffe wie *„Corona“* oder *„Covid“* registriert werden.[31] Teilweise nutzen Kriminelle diese vermeintlich offiziell wirkenden Domainnamen aus, um auf den professionell gestalteten Webseiten entweder personenbezogene Daten abzuphishen (siehe Punkt 3.2) oder Schadcode in der Webseite zu verstecken. Beispiele dafür sind manipulierte Online-Angebote wie eine interaktive COVID-19-Infektionskarte[32], falsche Informationswebseiten zum Virus oder gefälschte Infektions-Tracking-Apps[33].
Eine in Corona-Zeiten besonders relevante Malware ist Ransomware. Der Begriff beschreibt eine Variante von Schadsoftware, bei der das Programm die auf dem Zielsystem gespeicherten Daten als *„Geisel“* nimmt und die Festplatte verschlüsselt. Das

Opfer wird erpresst, indem erst durch Zahlung eines *„Lösegeldes“* (engl. *„Ransom“*), meistens auf ein Bitcoin-Konto, die Verschlüsselung (angeblich) deaktiviert und der Zugriff auf die Daten wieder ermöglicht wird. Ransomware kann in unterschiedlichen Formen (Datenverschlüsselung, -löschung oder -veränderung) auftreten und wird aufgrund der kontinuierlichen Anpassung durch die Täter oftmals nicht schnell genug von Antivirenprogrammen erkannt. In Zeiten von COVID-19 entwickeln Kriminelle *„Lockscreens“*, die jegliche Benutzerinteraktionen mit dem System unmöglich machen oder Programme, die den Namen *„Corona“* tragen und das System mit *„Krankheitssymptomen“* (Veränderung von Symbolen, Verschieben von Dateien, Auslösen randomisierter Funktionen) überziehen. Darüber hinaus verleitet der Schock, plötzlich nicht mehr auf seine privaten oder beruflichen Dokumente, Videos, Fotos und sonstige Dateien zugreifen zu können, die Opfer zur schnellen Zahlung der erpressten Geldbeträge.
Die Strafbarkeit richtet sich dabei nach der konkreten Funktionsweise der Software und dem jeweiligen Tatstadium. Bei der durch die Software hervorgerufene Datenveränderung auf dem Zielsystem dürfte regelmäßig eine Tatbestandsalternative von § 303a Abs. 1 StGB in Form der Datenunterdrückung[34], -löschung, -unbrauchbarmachung oder -veränderung vorliegen. Wenn die Daten zudem eine wesentliche Bedeutung für das Opfer haben oder ein Unternehmen/eine Behörde betroffen ist, sind Qualifikationen i.S.d. § 303b Abs. 1, 2 StGB denkbar. U.a. bei einem durch die Tat entstehenden großen finanziellen Schaden, gewerbs- oder bandenmäßiger Begehung oder einer kritischen Infrastruktur als Angriffsobjekt können strafverschärfende Regelbeispiele i.S.d. § 303b Abs. 4 StGB hinzutreten.

Der Gesetzgeber stellt zudem bereits Vorbereitungshandlungen, wie das Entwickeln von Malware, das Anbieten oder den Ankauf von Schadsoftware im Darknet (z.B. durch *„Gelegenheitskriminelle“,* die sich die benötigte Software i.S.v. *„crime-as-a-service“* in der Underground Economy in Form von Baukästen zusammenstellen) über § 202c StGB i.V.m. §§ 303a Abs. 3, 303b Abs. 5 StGB unter Strafe, sofern das Programm gezielt illegalen Zwecken dient. Maßgeblich ist dabei, ob das Programm wenigstens *auch* dafür hergestellt wurde, eine solche Tat zu begehen. Wird ein nicht für die Straftat bestimmtes Programm zur Tatbegehung *„zweckentfremdet“,* ist nach h.M. der Tatbestand nicht erfüllt, insbesondere bei *„dual use tools“* (legal und illegal nutzbare Software) ist die bloße Eignung unzureichend. Bei der strafrechtlichen Bewertung kommt es insofern auf die Feststellung der konkreten objektiven Funktionsweise des Programmes und den subjektiven Tatbestand des Täters an.

Cybercrime-Phänomene in neuem Gewand

Phänomen	Modus Operandi	Corona-Abwandlung
Enkeltrick/ Gesundheitstrick	Die Täter geben sich als Verwandte, behördliche Mitarbeiter oder Ärzte aus. Sie täuschen vor, dass eine Notlage besteht oder die Wohnung aus Infektionsschutzgründen betreten werden muss. Dadurch wird das Objekt/die Person ausgekundschaftet und durch Druckausübung/Vertrauensschaffung zur Übergabe von Bargeld an die Täter bewegt.	▸ Behördenmitarbeiter, teils mit Schutzanzügen verkleidet, müssen die Wohnung für einen Corona-Test betreten ▸ Mitarbeiter einer Reinigungsfirma müssen die Wohnung desinfizieren ▸ Familienangehörige haben sich mit Corona infiziert und benötigen Bargeld für eine Behandlung
Phishing	Inhalte von E-Mails oder Webseiten werden mit Corona-Bezug erstellt. Die Täter konstruieren realistische Situationen (finanzielle Nöte, Bedarf an Schutzausstattung, Filialschließung), die das Opfer überzeugen sollen, auf einen Link zu klicken. Über die Internetverknüpfung werden personenbezogene Daten, wie Personalien, Kennwörter oder Login-Kennungen erfragt.	▸ Teilnahme an einer Studie für einen Corona-Impfstoff zu suchen / Anbieten finanzieller Unterstützung in der Krise ▸ Fake-Shop für Schutzausstattung mit Bestelloberfläche ▸ E-Mail einer Gesundheitsbehörde mit Dateneingabe ▸ Schließung von Bankfilialen wegen Corona und Verifizierung personenbezogener Daten ▸ E-Mail von einer angeblichen Förderbank mit auszufüllenden und einem beigefügten Corona-Fragebogen[35]
Social Engineering	Social Engineering beschreibt grds. die Einflussnahme auf Menschen in Form manipulativen Vorgehens. Durch umfassendes Ausspähen von bspw. Unternehmensstrukturen, Zuständigkeiten und Gepflogenheiten, bauen Kriminelle Vertrauen zu den Opfern auf, um es zu bestimmten Handlungen zu bewegen. Gerade in COVID-19-Zeiten sind die potenziellen Opfer aufgrund der Viktimisierungsfaktoren anfälliger für betrügerisch-manipulatives Handeln.	▸ Mitarbeiter der Personalabteilung muss für etwaige Corona-Erkrankungen die personenbezogenen Daten aktualisieren ▸ Behördlicher Mitarbeiter muss die COVID-19-Maßnahmen im Unternehmen überprüfen und erfragt bestimmte persönliche Daten. ▸ Eine gefakte Unternehmens-E-Mail wird mit einer internen Handlungsanleitung zum Umgang mit Corona versandt; tatsächlich ist Malware angehängt.
Malware/ Ransomware	Ransomware ist eine Form von Malware, die ein Computersystem verschlüsselt. Zur Entschlüsselung ist die Zahlung eines Geldbetrages erforderlich. Die Corona-Pandemie führt zu neuen Verbreitungswegen dieser Schadprogramme, indem gezielt die Interessen/Ängste der Bevölkerung adressiert werden.	▸ Inoffizielle Online-Corona-Karte (Browser-Exploit) ▸ E-Mail mit E-Book der WHO mit Corona-Informationen (Trojaner) ▸ E-Mail einer Gesundheitsbehörde mit Anhang *„Krankschreibung“* (Virus) ▸ Corona-Virus-Tracking-App (Trojaner)

Abb. 2: Cybercrime-Phänomene in neuem Gewand (eigene Visualisierung).

4 Herausforderungen für die Sicherheitsbehörden

Die deliktischen Cybercrime-Ausprägungen lassen drei zentrale Herausforderungen für die Sicherheitsbehörden erkennen. Hierzu zählt als vorbeugende und damit zentrale straftatenverhindernde Maßnahme die Aufklärung über Phänomenologie, modi operandi und Präventionsmöglichkeiten für Privatpersonen und Unternehmen. Insofern sind besonders die zuständigen Organisationseinheiten für Presse- und Öffentlichkeitsarbeit sowie Kriminalprävention gefordert, proaktiv und crossmedial über Gefahren und Risiken in Zusammenhang mit der COVID-19-Situation zu informieren, die Vorgehensweisen auch für technische Laien nachvollziehbar zu erläutern und konkrete Verhaltensweisen zu empfehlen.
Weiterhin lassen die steigenden Fallzahlen eine Zunahme des diesbezüglichen Strafanzeigenaufkommens erwarten, wobei ein erheblicher Teil der Delikte nach wie vor im Dunkelfeld liegen und der Polizei erst gar nicht bekannt gegeben werden dürfte[35]. Neben den besonderen Anforderungen, die COVID-19 ohnehin schon an den täglichen Dienst stellt (z.B. neues Schichtsystem oder zeitversetzte Dienstverrichtung in festen Gruppen), müssen die vermehrten Strafanzeigen professionell, übergreifend und zeitnah abgearbeitet werden. Da sich Cybercrime dynamisch entwickelt, verändern sich Täterstrukturen und Vorgehensweisen ebenso schnell. Umso wichtiger ist der personaladäquate Einsatz, der durch Fortbildung insbesondere bei erkannten neuen Phänomenausprägungen gewährleistet werden muss.

5 Zusammenfassung und Ausblick

Die COVID-19-Pandemie ist ein Ereignis von gesamtgesellschaftlicher Bedeutung und hat durch die damit verbundene verstärkte Verlagerung von Alltagstätigkeiten aus der analogen Welt in den digitalen Raum deutliche Auswirkungen auf die Entwicklung von Cybercrime. Cyberkriminelle verkleiden bekannte Deliktsphänomene mit einem neuen Gewand und passen Sie im Kontext der Infektionskrankheit an. Dabei entwickeln sie bekannte Cybercrime-Phänomene weiter, indem sie kreative Virus bezogene Szenarien erstellen. Die der Corona-Krise immanenten besonderen Viktimisierungsfaktoren begünstigen zusätzlich die Opferwerdung in Zeiten von sozialer Distanz, emotionaler Unsicherheit und der Hortung von Konsumgütern.
So wird der bekannte *„Enkeltrick“* unter Ausnutzung von Hilfsbereitschaft und Angst älterer Menschen zum *„Gesundheitstrick“*, Malware durch Adressierung der Interessen/Sorgen der Bevölkerung über neue Kanäle, wie gefälschte Webseiten oder Apps, verbreitet und ein auf Corona gemünztes Social Engineering als Methode eingesetzt, um Phishing-E-Mails noch zielgerichteter verbreiten und sensible Daten erlangen zu können. Die Herausforderungen für Sicherheitsbehörden bestehen darin, diese neuen Abwandlungen bekannter Phänomene frühzeitig zu erkennen, die Öffentlichkeit rechtzeitig zu warnen und effektive Ermittlungsarbeit in diesem komplexen Themenfeld zu gewährleisten.
Die von Cybercrime ausgehende Bedrohung für die Cybersicherheit von Privatpersonen und Unternehmen zeigt sich während der COVID-19-Krise dynamisch und vielfältig. Das Virus wird die Öffentlichkeit noch mindestens solange beschäftigen, bis ein Impfstoff oder ein Medikament gefunden ist – aufgrund der besonderen gesellschaftlichen Auswirkungen wohl eher noch darüber hinaus. Cyberkriminelle werden deshalb auch weiterhin ihre modi operandi proaktiv anpassen und modifizieren, was steigende Deliktszahlen erwarten lässt. Es bedarf deshalb umso mehr einer professionellen und zielgerichteten polizeilichen Auseinandersetzung mit diesen Kriminalitätsphänomenen, damit der *„Corona-Effekt“* nicht zu einem neuen Treiber für Cybercrime wird.

Anmerkungen

1. Der Autor ist Dozent an der Hochschule der Polizei Rheinland-Pfalz, Fachgebiet IX – Cybercrime und digitale Ermittlungen. Erreichbarkeit: martin.hoch@polizei.rlp.de.
2. COVID-19 brach im Dezember 2019 in der chinesischen Stadt Wuhan aus und entwickelte seit Anfang 2020 eine weltweite Relevanz. Das Virus erreichte Deutschland offiziell ab Ende Januar 2020.
3. Die Reproduktionszahl (R) gibt an, wie viele Menschen ein Infizierter durchschnittlich ansteckt; liegt der R-Wert bei 1,0 wird durchschnittlich eine weitere Person angesteckt; vgl. Robert-Koch-Institut: Täglicher Lagebericht zur Coronavirus-Krankheit-2019 (COVID-19), Stand: 29.4.2020, S. 6.
4. Die Bezeichnungen variieren je nach Bundesland; in Rheinland-Pfalz wird die *„Bezeichnung Corona-Bekämpfungsverordnung“* genutzt, in Berlin ist *„SARS-CoV-2-Eindämmungsmaßnahmenverordnung“* gebräuchlich.
5. Unter dem Motto *„Flatten the curve“* wird insbesondere medial dazu aufgerufen, die von der Bundesregierung

verhängten Beschränkungen und Verhaltensregelungen zur Reduzierung der COVID-19-Infektionskurve einzuhalten.

6. Vgl. Ministerium des Innern und für Sport Rheinland-Pfalz (2020): Polizei beobachtet rückläufige Kriminalitätsentwicklung. Pressemeldung vom 8.4.2020; ähnliche Pressemeldungen haben die Innenministerien anderer Bundesländer veröffentlicht.
7. Bundesweit ist in dem aktuellen Bundeslagebild zu Cybercrime (berücksichtigt das Jahr 2018) erneut ein Anstieg um 1,3% auf 87.106 Fälle von Cybercrime im engeren Sinne im Vergleich zum Vorjahr (2017: 85.960 Fälle) zu verzeichnen; vgl. Bundeskriminalamt (2019): Cybercrime. Bundeslagebild 2018, S. 8.
8. Vgl. Europol (2020a): Catching the virus cybercrime, disinformation and the COVID-19 pandemic, S. 4.
9. Der Begriff *„Underground Economy“* ist eine Oberbezeichnung für alle wirtschaftlichen Aktivitäten Cyberkrimineller in Zusammenhang mit dem Kauf und Verkauf illegaler Waren, wie Betäubungsmit-teln, Waffen, Schadsoftware, insbesondere im Dark Web, oftmals unter Nutzung digitaler Han-delsplattformen.
10. Vgl. Europol (2020a), S. 10f.
11. Vgl. Statistisches Bundesamt (2020): Corona-Krise: Experimentelle Daten zeigen Kaufverhalten im Einzelhandel. Pressemitteilung Nr. 112 vom 25.3.2020. Abrufbar unter: www.destatis.de/DE/Presse/Pressemitteilungen/2020/03/PD20_112_61.html, zuletzt geprüft am 1.6.2020.
12. Der aus den Medienwissenschaften stammende Begriff der *„Filterblase“* beschreibt ursprünglich den Umstand, dass insbesondere Social Media-Seiten dem Nutzer durch algorithmische Berechnungen nahezu ausschließlich Informationen und Meinungen anzeigen, die mit seinen bisherigen Interessen (erfasst durch Kommentare, Likes oder Shares) übereinstimmen. Der Grundgedanke lässt sich allerdings über den digitalen Raum in die reale Welt abstrahieren.
13. Vgl. SWR-Aktuell (2020): Polizei warnt vor Corona-Betrügern. Pressemitteilung vom 4.4.2020. Abrufbar unter: www.swr.de/swraktuell/rheinland-pfalz/koblenz/meldung-46136.html, zuletzt geprüft am 1.6.2020.
14. Vgl. Zeit-Online (2020): Abzocke im Corona-Schutzanzug. Artikel vom 20.4.2020. Abrufbar unter: www.zeit.de/gesellschaft/zeitgeschehen/2020-04/kriminaelitaet-coronavirus-enkeltrick-betrueger-mafia-haeusliche-gewalt, zuletzt geprüft am 29.5.2020.
15. Die digitale Identität einer Person lässt sich als die Gesamtheit aller Möglichkeiten und Rechte sowie der mit ihr verbundenen personenbezogenen Daten und Aktivitäten in der Gesamtstruktur der digitalen Welt beschreiben. Insofern ist sie also ein Abbild der physischen Gestalt als digitale Entität.
16. Selbst Laien ohne technisches Knowhow können *„phishen“*, indem Sie sich insbesondere im Darknet Baukastenelemente (manipulierte Webseite, gefakte E-Mail, Software zum Mailversand) wie in einem legalen Online-Shop gegen Bezahlung bei einem Dienstleister bestellen können (sog. *„crime-as-a-service“*).
17. Phishing ist ein aus den englischen Begriffen *„password“*, *„harvesting“* und *„fishing“* zusammengesetzter Begriff zur Beschreibung einer Handlung, bei der die Täter meist in mehreren Phasen vorgehen, um personenbezogene Daten (i.d.R. Zugangsdaten zu Bank- oder Online-Shopping-Accounts) unter Täuschung des Opfers zu erhalten, das nach dem Klick auf einen Link in einer manipulierten Internetmaske vertrauliche Daten eingeben soll; vgl. BGH, Urteil vom 24.4.2012, Az. XI ZR 96/11.
18. Vgl. Digital Pioneers (2020): Phishing mit Corona: Google stoppt täglich 18 Millionen betrügerische Mails. Presseartikel vom 20.4.2020. Abrufbar unter: t3n.de/news/phishing-corona-google-stoppt-18-1271466/, zuletzt geprüft am 4.6.2020.
19. Vgl. Bundesamt für Sicherheit in der Informationstechnik (2020): Update: Cyberkriminelle nutzen Corona aus. Abrufbar unter: www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/corona-falschmeldungen.html, zuletzt geprüft am 22.5.2020.
20. Vgl. Europol (2020a), S. 4.
21. Vgl. Bundesamt für Sicherheit in der Informationstechnik (2020), a.a.O.
22. Die Formulierung ist analog zu § 263 Abs. 3 Nr. 2 StGB zu sehen, wonach eine objektive Wertgrenze von mind. 50.000 Ä anzusetzen ist.
23. Vgl. Popp, Andreas (2006): *„Phishing“*, *„Pharming“* und das Strafrecht. In: MMR. 9(2), 84f.
24. Vgl. Seidl, Alexander/Fuchs, Katharina (2010): Die Strafbarkeit des Phishing nach Inkrafttreten des 41. Strafrechtsänderungsgesetzes. In: HRRS 11(2), S. 86.
25. Vgl. Europol (2020b): Pandemic profiteering, how criminals exploit the COVID-19 crisis, S. 4.
26. Sog. *„Badge Surveillance“*, bei der die Täter ausspionieren, welche Ausweisdokumente oder Zutrittskarten von Mitarbeitern unterschiedlicher Entscheidungsebene beim Betreten des Unternehmensgebäudes genutzt werden.

27. Die Täter schreiben Unternehmen mit einer scheinbar unbedeutenden E-Mail an und nutzen das Design der Antwort-E-Mail, um das Layout nachzubilden oder sie nutzen *„Dumpster Diving“*, indem sie in Abfallbehältern nachsehen, ob sie dort entsorgte Unternehmensdokumente zur Nachbildung des Corporate Designs finden.

28. Sog. *„Spear Phishing“*, bei dem im Gegensatz zum regulären *„Phishing“* nicht an beliebig viele E-Mail-Empfänger Nachrichten mit dem Ziel der Datenerlangung versandt, sondern gezielt bestimmte Personen adressiert werden. Insofern handelt es sich um eine personalisierte Form des Phishings, da die enthaltenen Informationen auf das Unternehmen bzw. die Zielperson(en) zugeschnitten sind.

29. Vgl. Bundesamt für Sicherheit in der Informationstechnik (2020): Glossar zum IT Grundschutz. Abrufbar unter: www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html, zuletzt geprüft am 4.6.2020.

30. Bei sog. *„drive-by-downloads“* reicht der bloße Besuch einer Webseite aus, um von dem Opfer unbemerkt Schadsoftware im Hintergrund auf das Zielsystem herunterzuladen. Dabei werden in der Regel Sicherheitslücken im Browser *(„Exploits“)* ausgenutzt.

31. Bundesamt für Sicherheit in der Informationstechnik (2020): Cyber-Kriminelle nutzen Corona-Krise vermehrt aus. Pressemeldung vom 2.4.2020. Abrufbar unter: www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/Cyber-Kriminell_02042020.html, zuletzt geprüft am 4.6.2020.

32. So existiert ein Corona Infection Kit, das von Kriminellen als Baukasten genutzt werden kann, um anhand einer Java-basierten COVID-19-Livekarte die Malware *„AZORult“* (spioniert Zahlungs- und Zugangsdaten aus) auf dem Zielrechner zu installieren; vgl. Reason Blog (2020): COVID-19, Info Stealer & the Map of Threats – Threat Analysis Report. Stand: 9.3.2020. Abrufbar unter: blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/, zuletzt geprüft am 4.6.2020.

33. Vgl. Domaintools (2020): CovidLock: Mobile Coronavirus Tracking App Coughs Up Ransomware. Abrufbar unter: www.domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware, zuletzt geprüft am 4.6.2020.

34. Die Datenunterdrückung ist tatbestandlich erfüllt, wenn der Zugriff auf die Daten dauerhaft, d.h. zeitlich nicht unerheblich, nicht mehr möglich ist. Ein Anwendungsfall ist die Datenverschlüsselung durch das Schadprogramm.

35. Bundeskriminalamt (2020): Achtung: Bundesweite Phishing-Welle in Zusammenhang mit der COVID-19 Pandemie. Pressemeldung vom 9.5.2020. Abrufbar unter: www.bka.de/SharedDocs/Kurzmeldungen/DE/Warnhinweise/200507_Coronaphishing.html, zuletzt geprüft am 10.5.2020

36. Laut niedersächsischer Dunkelfeldstudie werden nur rund 10% aller Cybercrimedelikte durch die Betroffenen angezeigt werden; vgl. Landeskriminalamt Niedersachen (2015): Befragung zu Sicherheit und Kriminalität in Niedersachsen. Abschlussbericht zur ersten Befragung im Frühjahr 2013. Hannover.