Jessica Kriegel, Jubin Dejam, Hanno Durth, Florian Franke, Wolfram Hemkens*

Zur Strafbarkeit von Datenfunden im Darknet

Simulationsstudie für mehr Rechtssicherheit in der Cybersicherheitsforschung

Die Cybersicherheitsforschung in Deutschland ist mit erheblichen rechtlichen Unsicherheiten behaftet, weshalb sich Cybersicherheitsforscher bei ihrer täglichen Arbeit immer wieder in einem rechtlichen Graubereich bewegen müssen. Um diesem Problem entgegenzuwirken, setzen sich Wissenschaftler des Nationalen Forschungszentrums für angewandte Cybersicherheit ATHENE in einer mehrjährigen Simulationsstudie nun dafür ein, dass für die Cybersicherheitsforschung künftig mehr Orientierungspunkte zur Rechtskonformität ihrer Forschungsaktivitäten entwickelt werden.

Dipl. Jur. Jessica Kriegel

ist Rechtswissenschaftlerin am Fraunhofer SIT und in ATHENE.

E-Mail: Jessica.Kriegel@sit.fraunhofer.de

Dr. Jubin Dejam

ist Staatsanwalt in der Staatsanwaltschaft Frankfurt am Main.

Dr. Hanno Durth

ist Rechtsanwalt in der Anwaltskanzlei Kipper Durth Schott PartGmbB in Darmstadt.

Dr. Florian Franke

ist Richter am Amtsgericht Frankfurt am Main.

Wolfram Hemkens

ist Rechtsanwalt in der Anwaltskanzlei HEMKENS in Krefeld.

1 Hintergrund der Simulationsstudie

Cyberangriffe haben in den letzten Jahren sowohl in ihrer Häufigkeit als auch in ihrer Komplexität erheblich zugenommen. Laut einer aktuellen Studie des BSI ist die Zahl der gemeldeten Cybervorfälle in Deutschland im Jahr 2023 um 30 % im Vergleich zum Vorjahr gestiegen.[1] Die Angriffe zielen vermehrt auf politische Institutionen, Wirtschaftsunternehmen und Privatpersonen ab.[2] Vor diesem Hintergrund gewinnt die Forschung zur Abwehr solcher Angriffe immer mehr an Bedeutung, denn um auch künftig effektiv und nachhaltig auf diese Bedrohungen reagieren zu können, ist eine starke Cybersicherheitsforschung unerlässlich. Diese geht jedoch weit über den Einsatz neuartiger und innovativer Technologien hinaus. Regelmäßig umfasst sie auch den Einsatz offensiver Methoden und erfordert, insbesondere bei besonders starker Bedrohung, oftmals sogar eine aktive Abwehr der Cyberangriffe. Cybersicherheitsforscher müssen hierbei häufig dieselben oder sehr ähnliche Werkzeuge und Methoden nutzen, wie sie auch von böswilligen Angreifern genutzt werden – jedoch mit völlig anderem Ziel: Während die Werkzeuge und Methoden von böswilligen Angreifern eingesetzt werden, um IT zu schwächen, setzen Cybersicherheitsforscher diese ein, um neue Angriffe auf IT zu identifizieren und so gut zu verstehen, dass sie

* Dieser Beitrag wurde vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt. Der Beitrag gibt lediglich erste Forschungserkenntnisse wieder und kann eine Rechtsberatung nicht ersetzen.

1 *BSI*, Die Lage der IT-Sicherheit in Deutschland, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html.

2 *Boll*, Ohne Cybersicherheit kein Datenschutz, ohne Datenschutz keine Cybersicherheit?, DuD 2023, 346 (346).

Gegenmaßnahmen gegen die Angriffe ableiten können.[3] Trotz der offensichtlich anderen Zielsetzung können Cybersicherheitsforscher dadurch Strafbarkeitsrisiken ausgesetzt sein.[4] So schaffen die gegenwärtig bestehenden Gesetze, die auf offensive Cybersicherheitsforschung angewendet werden (können), nur wenig Klarheit, da sie ursprünglich nicht dafür ausgelegt waren, speziell den Bereich der offensiven Cybersicherheitsforschung zu regeln.[5] Für Cybersicherheitsforscher stellt sich daher häufig die Frage, ob ihre Forschungsaktivitäten noch legal sind oder bereits strafrechtliche Konsequenzen nach sich ziehen könnten.[6]

Die mangelnde Rechtssicherheit hat nicht nur unmittelbare Auswirkungen auf die Forscher und deren Arbeit, sondern birgt auch ein erhebliches Risiko für die gesamte Gesellschaft. Ohne klare rechtliche Rahmenbedingungen besteht die Gefahr, dass wichtige Forschung gar nicht erst durchgeführt wird, weil Forscher aufgrund bestehender Rechtsunsicherheiten Angst vor (zuvor nicht klar absehbaren) rechtlichen Konsequenzen haben. Dies könnte langfristig die Entwicklung effektiver Cybersicherheitsmaßnahmen hemmen und die Gesellschaft gegenüber Cyberangriffen verwundbarer machen. Klare rechtliche Grundlagen und eine gezielte Unterstützung der Cybersicherheitsforschung sind daher dringend erforderlich, um die Gesellschaft weiterhin und langfristig so gut wie möglich vor den zunehmenden Gefahren im Cyberraum schützen zu können.

Aufgrund dessen haben es sich Rechtswissenschaftler des Nationalen Forschungszentrums für angewandte Cybersicherheitsforschung ATHENE zur Aufgabe gemacht, die rechtlichen Rahmenbedingungen genauer zu untersuchen, mögliche Rechtsunsicherheiten aufzuzeigen und zu adressieren. Hierfür haben sie eine auf mehrere Jahre angelegte Simulationsstudie ins Leben gerufen, im Rahmen derer in regelmäßigen Abständen simulierte Gerichtsverhandlungen mit echten Strafrichtern, Staatsanwälten, Strafverteidigern und Sachverständigen durchgeführt werden, um für verschiedene aktuelle Forschungsaktivitäten aus der Cybersicherheitsforschung Entscheidungen des Simulationsgerichts zur Rechtskonformität dieser Aktivitäten zu erwirken. Angesichts der oft unklaren rechtlichen Rahmenbedingungen soll die Simulationsstudie künftig ein erster, wichtiger Wegweiser für Cybersicherheitsforscher darstellen, der diesen hilft, einzuschätzen, ob ihre Forschungsaktivität potenziell (straf-)rechtliche Risiken birgt oder aber sich voraussichtlich in einem rechtlich sicheren Rahmen bewegt.

2 Die erste simulierte Gerichtsverhandlung im Überblick

Ziel der ersten simulierten Gerichtsverhandlung, welche am 17. September 2024 in den Räumlichkeiten des Fraunhofer-Instituts für Sichere Informationstechnologie SIT in Darmstadt durchgeführt wurde, war es, mehr Klarheit und Rechtssicherheit für Cybersicherheitsforscher im Hinblick auf zulässige Reaktionen auf Datenfunde im Darknet zu schaffen. Im Rahmen der Simulationsstudie diskutierten ein Richter, ein Staatsanwalt und zwei Strafverteidiger (unter weiterer Beteiligung eines IT-Sachverständigen sowie vier Statisten als Angeklagte und weitere Zeugen) über die rechtliche Zulässigkeit einer fiktiven, aber realistischen Cybersicherheitsaktivität im Darknet.

2.1 Ablauf der simulierten Verhandlung

Um eine bestmögliche Vorbereitung der Teilnehmer und ein möglichst realistisches Szenario zu gewährleisten, wurde den Teilnehmern der Simulationsstudie der zu verhandelnde Sachverhalt sowie alle relevanten Beweismittel vorab zur Verfügung gestellt. In einem vorbereitenden Abstimmungstermin wurden organisatorische und erste inhaltliche Fragen geklärt. Die Gerichtsverhandlung selbst folgte einem realitätsgetreuen Ablauf. Der Vorsitzende Richter eröffnete die Sitzung, stellte die Parteien vor, erläuterte kurz den Sachverhalt und leitete die Verhandlung ein. Anschließend verlas der Staatsanwalt die Anklageschriften. Danach erfolgte die Befragung der Angeklagten zur Person sowie ihre Einlassungen zur Sache. Die Parteien präsentierten ihre Argumente, es wurden Zeugen befragt, Beweismittel vorgelegt und die zentralen Aspekte des Falls wurden ausführlich erörtert. Besondere Aufmerksamkeit galt den rechtlichen Grenzen der Cybersicherheitsforschung, der verantwortungsvollen Offenlegung von Sicherheitslücken sowie den (ethischen und gesetzlichen) Pflichten der Cybersicherheitsforscher, insbesondere den Dokumentationspflichten und Grenzen der Zuständigkeit für die Weiterverfolgung von im Rahmen der Forschung identifizierter Auffälligkeiten. Nach der Verhandlung des Simulationsgerichts wurde die Entscheidung des Gerichts verkündet. Im Anschluss hatte das Publikum die Möglichkeit, mit dem Simulationsgericht in Austausch zu treten und gemeinsam über die Ergebnisse zu diskutieren.

Ziel der Simulationsstudie war es, die Straffreiheit oder Strafbarkeit der fiktiven Angeklagten A und B nach dem StGB zu bestimmen.[7] Die beiden Angeklagten agierten in dem fiktiven Fall bewusst unterschiedlich und teilweise auch absichtlich abweichend von den Standards verantwortungsvoller Cybersicherheitsforscher. Diese Herangehensweise ermöglichte es, einen möglichst umfassenden Überblick über die „Dos" and „Don´ts" der Cybersicherheitsforschung im Rahmen der Simulationsstudie zu erhalten. Vor diesem Hintergrund wurde das Simulationsgericht auch gebeten, auf alle aufgeworfenen Rechtsfragen und Probleme einzugehen.

3 *Selzer/Spiecker gen. Döhmann*, Rechtsrahmen der offensiven Cybersicherheitsforschung, Tagesspiegel, 2022, https://background.tagesspiegel.de/it-und-cybersicherheit/briefing/warum-es-einen-rechtsrahmen-fuer-die-offensive-cybersicherheitsforschung-braucht.

4 *Schlindwein/Kriegel*, Der Einsatz von Open Source Intelligence im Darknet – Eine strafrechtliche Bewertung, GI-Informatik (in print).

5 *Selzer/Spiecker gen. Döhmann*, Rechtsrahmen der offensiven Cybersicherheitsforschung, Tagesspiegel, 2022, https://background.tagesspiegel.de/it-und-cybersicherheit/briefing/warum-es-einen-rechtsrahmen-fuer-die-offensive-cybersicherheitsforschung-braucht.

6 Ebenda.

7 Gegenstand der Simulationsverhandlung war die Strafbarkeit nach dem deutschen Strafgesetzbuch. Ggfs. auftretende datenschutzrechtliche Fragen, insbesondere zur DSGVO, blieben unberücksichtigt und waren kein Gegenstand der Simulationsverhandlung.

2.2 Der fiktive Fall[8]

Folgender fiktiver Fall war Gegenstand der Simulationsverhandlung: A und B, zwei angesehene Cybersicherheitsforscherinnen mit langjähriger Erfahrung, die an zwei unterschiedlichen Forschungseinrichtungen tätig sind, haben sich im Rahmen eines gemeinsamen Forschungsprojekts zum Ziel gesetzt, Schwachstellen in IT-Systemen zu identifizieren und ggf. durch die Entwicklung von Gegenmaßnahmen potenzielle Schäden für Betroffene zu verhindern. Um während der Projektlaufzeit immer auf dem neusten Stand der Bedrohungslage zu bleiben, recherchieren sie regelmäßig im Darknet nach den neusten Angriffsszenarien, -methoden und -tools. A dokumentiert jeden ihrer Verfahrensschritte. Die Dokumentationen enthalten die Namen anderer, eventuell beteiligter Forscher sowie die jeweiligen Gründe, weshalb einzelne Recherchetätigkeiten unternommen wurden. Die Dokumentationen sind mittels elektronischer Signaturen im Nachhinein nicht mehr veränderbar. Dies macht sie aus dem Grund, dass die Forschungseinrichtung, für die A tätig ist, der Ansicht ist, dass sich ein sozialadäquates Verhalten nur so dokumentieren und nachweisen lässt. B dokumentiert ihre Arbeiten im Rahmen des Forschungsprojekts dagegen nicht.

Am 25. März 2024 stoßen A und B bei einer gemeinsamen Recherche im Darknet auf einem Darknet-Marktplatz auf eine Datei, die als „Angebot-zur-Übernahme-von-Cyberangriffen-im-Auftrag.pdf" benannt ist. A und B entscheiden sich, dass sie beide die Datei herunterladen, um sich darüber zu informieren, welche Cyberangriffe im Auftrag angeboten werden und ob neue Angriffsszenarien, -methoden oder -tools beschrieben werden, gegen die sie Abhilfemaßnahmen entwickeln könnten. Die Darknet-Recherche inkl. des Funds und Downloads hält A zusammen mit der Skizzierung des Forschungszwecks in ihrer Dokumentation fest. B unterlässt diesen Schritt. Nach dem Runterladen der Datei bemerken A und B, dass die Datei kein Angebot zur Übernahme von Cyberangriffen beinhaltet, sondern dass die Datei eine Liste mit 5.000 gestohlenen Zugangsdaten (bestehend aus E-Mail-Adressen und Passwörtern) von Kunden eines deutschen Onlineshops Y sowie 4.000 gestohlenen Zugangsdaten (bestehend aus Nutzernamen und Passwörtern) von Mitarbeitern einer großen deutschen Versicherungsgesellschaft Z für eine über das Internet erreichbare betriebsinterne Mitarbeiterplattform zum Projektmanagement enthält. Den Datensatz haben die Cyberangreifer als eine Art „Arbeitsprobe" in der Datei mitveröffentlicht. A und B sind sich darüber einig, dass sie diesen Fund nicht ignorieren können, sprechen sich aber für das weitere Vorgehen rund um den Fund nur insofern ab, dass A sich um die Mitarbeiter der Versicherungsgesellschaft Z und B sich um die Kunden des Onlineshops Y kümmern soll.

A entscheidet sich dazu, zunächst zu überprüfen, ob es sich bei den gefundenen Zugangsdaten der Mitarbeiter der Versicherungsgesellschaft Z überhaupt um aktuelle Passwörter handelt. Daher entscheidet sich A dazu, anhand von drei zufällig ausgewählten Einträgen zu überprüfen, ob die Passwörter (noch) gültig sind. Durch das Austesten von Nutzername und Passwort erhält sie Zugriff auf einen der drei Mitarbeiteraccounts, loggt sich jedoch unmittelbar wieder aus. Da mit zwei von drei der ausprobierten Passwörter ein Zugriff auf die Mitarbeiteraccounts nicht möglich war, entscheidet sich A gegen weitere Schritte und informiert die Versicherungsgesellschaft Z weder über den Darknet-Fund noch über den (versuchten) Accountzugriff. B verzichtet hingegen auf ein Überprüfen der Aktualität der Passwörter und entscheidet sich dazu, den Onlineshop Y über die auf der Webseite als Kontaktmöglichkeit angegebene E-Mail-Adresse zu kontaktieren, informiert diesen über ihren Fund sowie die Fundstelle und bittet darum, den Sachverhalt zu prüfen. B empfiehlt dem Onlineshop Y zusätzlich, seine Kunden zu informieren und zu bitten, ihre Passwörter schnellstmöglich zurückzusetzen.

Nachdem B den Onlineshop Y über die gefundenen gestohlenen Zugangsdaten informiert hat, nimmt Letzterer die Angelegenheit sehr ernst. Der IT-Sicherheitsbeauftragte des Onlineshops überprüft die von B erhaltenen Informationen und bestätigt, dass es sich um aktuelle, gestohlene Zugangsdaten ihrer Kunden handelt. Der Onlineshop Y informiert daraufhin die betroffenen Kunden und schaltet zusätzlich die Polizei ein, um den Ursprung und die Verbreitung der gestohlenen Zugangsdaten zu ermitteln.

Durch die Ermittlungen der Polizei und durch Aussagen von B wird bekannt, dass B den Fund zusammen mit A gemacht hat. Im Rahmen einer Aussage von A legt diese der Polizei die Dokumentation ihrer Darknet-Recherche vor, weil sie davon überzeugt ist, keine Fehler gemacht zu haben. Die Polizei und die Staatsanwaltschaft überprüfen die Handlungen von A und B im Detail. Während aufgrund fehlender Dokumentation unklar ist, wie B an die Passwörter gelangt ist, finden sich bei A Hinweise, dass sie selbst Zugangsdaten getestet und sich kurzzeitig in ein fremdes Konto eingeloggt hat. A und B werden daraufhin von der Polizei vernommen. Beide versuchen, ihre Handlungen als notwendige Prüfmaßnahmen im Rahmen der Cybersicherheitsforschung darzustellen. Jedoch handelten beide ohne Zustimmung der betroffenen Parteien. Aufgrund des von der Versicherungsgesellschaft Z gestellten Strafantrags und aufgrund der Ermittlungen entscheidet die Staatsanwaltschaft deshalb, Anklage gegen A wegen Vorbereiten des Ausspähens von Daten gemäß § 202c Abs. 1 Nr. 1 StGB und Ausspähens von Daten gemäß § 202a StGB sowie gegen B wegen Vorbereitens des Ausspähens von Daten gemäß § 202c Abs. 1 Nr. 1 StGB zu erheben.

3 Die simulierte Entscheidung[9]

Das Gericht hat Forscherin A aufgrund des probeweisen Logins in einen Account gemäß § 202a StGB schuldig gesprochen, sie verwarnt und die Verurteilung zu einer Strafe von 20 Tagessätzen in Höhe von je 100 EUR vorbehalten. Zudem erteilte das Gericht A die Auflage, 4000 Euro an eine gemeinnützige Organisation zu zahlen. In dem weiteren Anklagepunkt wurde Forscherin A freigesprochen, Forscherin B wurde vollständig freigesprochen.

In seiner Entscheidung ging das Simulationsgericht auf folgende Fragen ein:

8 Dieser Sachverhalt sowie die darin vorkommenden Personen sind frei erfunden. Er dient ausschließlich der Veranschaulichung der Herausforderungen, denen sich Cybersicherheitsforscher in ihrer Arbeit gegenübersehen, und dessen Entscheidung durch das simulierte Simulationsgericht soll eine erste, vorsichtige Einschätzung zur Rechtskonformität der beschriebenen Forschungsaktivitäten ermöglichen.

9 Bei der vorliegenden Entscheidung handelt es sich um eine simulierte Gerichtsentscheidung. Eine endgültige Beurteilung ist einzelfallabhängig ist und kann zudem nur durch die zuständigen Gerichte erfolgen.

1. Wie ist es zu bewerten, wenn beim Herunterladen einer Datei aus dem Internet, insbesondere dem Darknet, versehentlich Zugangsdaten (Nutzername und Passwort) entdeckt, diese Daten anschließend für eine erfolgreiche Anmeldung auf der Internet-Plattform eines Unternehmens genutzt werden und dadurch Zugriff u.a. auf personenbezogene Daten ermöglicht wird? Kann bei der Bewertung einer Strafbarkeit nach § 202a StGB das Tatbestandsmerkmal „Überwinden einer besonderen Zugangssicherung" dadurch entfallen, dass dem Forscher die Zugangsdaten durch den Zufallsfund bereits bekannt sind, für sich genommen die Daten also nicht mehr besonders geschützt sind?
2. Kann von einem Verbotsirrtum gem. § 17 StGB ausgegangen werden, wenn Forscher in der Annahme handeln, ihr Verhalten sei aufgrund des wissenschaftlichen Zwecks oder der Förderung der Cybersicherheit nicht strafbar?
3. Kann unter Berücksichtigung des Nutzens von Forschungsaktivitäten für die Allgemeinheit sowie der möglicherweise vorgenommenen umfangreichen Dokumentation von einer Sozialadäquanz des Verhaltens von Forschern ausgegangen werden, sodass ihr Handeln unter bestimmten Umständen gerechtfertigt sein könnte? Welche Voraussetzungen sind an ein sozialadäquates Verhalten zu stellen?
4. Wie wirkt sich eine umfangreiche Dokumentation durch einen Forscher auf dessen Vorsatz aus?
5. Unter welchen Umständen könnte das Handeln eines Cybersicherheitsforschers aufgrund eines rechtfertigenden Notstands gemäß § 34 StGB gerechtfertigt sein?
6. Kann ein Forscher strafrechtlich belangt werden, wenn er Betroffene nicht über den Fund von Zugangsdaten im Darknet und einen eventuell erfolgten (versuchten) Zugriff auf deren Accounts informiert?
7. Machen sich Forscher durch das Herunterladen von Passwörtern gemäß § 202c Abs. 1 Nr. 1 Alt. 1 StGB strafbar? Bei der Prüfung des § 202c Abs. 1 Nr. 1 Alt. 1 StGB wurde sowohl die Strafbarkeit der A als auch die der B hinsichtlich der Frage untersucht, wie fehlender Vorsatz oder andere subjektive Elemente nachgewiesen werden können. Besonderer Beachtung galt dabei den Unterschieden im Verhalten von A und B sowie den möglicherweise daraus resultierenden unterschiedlichen strafrechtlichen Bewertungen. Zudem wurden die Voraussetzungen des subjektiven Tatbestands des § 202c StGB diskutiert, denn während es sich nach dem Willen des Gesetzgebers bei § 202c StGB um ein abstraktes Gefährdungsdelikt handeln soll (BT-Drs. 16/3656), wonach ein vorsätzliches Handeln nur bzgl. der Tathandlung, nicht jedoch hinsichtlich der Begehung einer Computerstraftat erforderlich ist,[10] wird dagegen in der Literatur[11] und vom Bundesverfassungsgericht des Weiteren vorausgesetzt, dass neben dem vorsätzlichen Handeln bzgl. der Tathandlung auch eine Computerstraftat in Aussicht genommen wurde und Eventualvorsatz hinsichtlich der Begehung einer Computerstraftat besteht, ohne dass eine konkrete Vorstellung erforderlich ist.

3.1 Entscheidung zu Frage 1

Das Austesten von gefundenen Passwörtern erfüllt nach Auffassung des Simulationsgerichts den Straftatbestand des § 202a Abs. 1 StGB und ist somit strafbar.

Zur Begründung: Der Straftatbestand des Ausspähens von Daten gemäß § 202a StGB schützt nach der herrschenden Meinung das formelle Datengeheimnis desjenigen, der aufgrund seines Rechts an dem gedanklichen Inhalt über eine Weitergabe oder Übermittlung der Daten entscheidet, jedoch nur dann, wenn diese gegen unbefugten Zugriff besonders gesichert sind.[12] In dem fiktiven Fall stellte sich die Frage, ob das zufällige Auffinden von Zugangsdaten, hier im Darknet, und deren anschließende Nutzung zur Anmeldung auf einer fremden Plattform die Tatbestandsmerkmale des § 202a StGB erfüllt. Insbesondere war zu prüfen, ob der Tatbestand des „Überwindens einer besonderen Zugangssicherung" auch dann gegeben ist, wenn dem Täter die Zugangsdaten bereits durch Zufall bekannt sind. Eine Zugangssicherung im Sinne des § 202a Abs. 1 StGB liegt vor, wenn die Daten durch technische Maßnahmen gegen den Zugriff unbefugter Personen geschützt sind. Dies können etwa Passwörter, Verschlüsselungen oder andere Formen technischer Sicherheitsvorkehrungen sein.[13] Im vorliegenden Fall handelte es sich um Passwörter, die im Darknet gefunden wurden. Die maßgebliche Frage war, ob diese Passwörter nach ihrer Veröffentlichung im Darknet noch als Zugangssicherung im Sinne des § 202a StGB angesehen werden können. Der bloße Umstand, dass Zugangsdaten durch Dritte öffentlich zugänglich gemacht werden, hebt die Zugangssicherung jedoch nicht auf.[14] Selbst wenn ein Passwort im Darknet veröffentlicht wird, bleibt es als technische Zugangssicherung im Sinne des § 202a StGB bestehen, da es weiterhin dem Schutz der Daten dient. Dies gilt insbesondere, weil die Sicherheitsvorkehrungen für den rechtmäßigen Nutzer fortbestehen. Der Schutz eines Passwortes entfällt nicht durch die unbefugte Veröffentlichung, sondern bleibt im Verhältnis zu den eigentlichen Nutzungsberechtigten bestehen.

Der Begriff des „Überwindens" ist in § 202a StGB dahingehend zu verstehen, dass der Täter die Zugangssicherung überwindet, indem er eine technische Schutzvorrichtung, die dazu dient, den Zugang zu den Daten auf berechtigte Personen zu beschränken, umgeht oder benutzt. In dem vorliegenden Fall hat die Forscherin A die Zugangsdaten, die sie zufällig im Darknet gefunden hat, genutzt, um sich in das System einer Versicherungsgesellschaft einzuloggen. Hierbei stellte sich die Frage, ob die Nutzung der zufällig aufgefundenen Passwörter ein Überwinden der Zugangssicherung darstellt. Das „Überwinden" liegt nicht erst dann vor, wenn der Täter die Zugangssicherung durch technische Manipulationen umgeht. Vielmehr genügt es, wenn der Täter, wie im vorliegenden Fall, durch den Gebrauch von unrechtmäßig erlangten Passwörtern eine technische Sicherung überwindet, die dazu dient, den Zugang zu den Daten auf einen bestimmten Personenkreis zu beschränken. Dass die Passwörter im Darknet gefunden wurden, ändert an dieser Bewertung nichts. Die Passwörter dienten weiterhin dazu, den Zugang zu den Daten nur berechtigten Personen zu ermöglichen, und durch ihre Nutzung wurde die Zu-

10 *Höfinger*, Anmerkung zu BVerfG, Beschluss vom 18. Mai 2009 – 2 BvR 2233/07, ZUM 2009, 751 (753).

11 *Cornelius*, in: Taeger/Pohle, Computerrechts-Handbuch, 39. Auflage 2024, Teil 10, 102, Rn. 68; MüKoStGB/Graf, 4. Aufl. 2021, StGB § 202c Rn. 30; *Mansdörfer*, in: Borges/Hilber, BeckOK IT-Recht, 15. Auflage 2024, § 202c Rn. 1-15.

12 MüKoStGB/Graf, 4. Aufl. 2021, StGB § 202a Rn. 2.

13 BGH 21.7.2015 – 1 StR 16/15, NJW 2015, 3463.

14 MüKoStGB/Graf, 4. Aufl. 2021, StGB § 202a Rn. 21, 38.

gangssicherung überwunden. Ein „Überwinden" liegt demnach vor, und der Tatbestand des § 202a StGB ist erfüllt.

3.2 Entscheidung zu Frage 2

Ein Verbotsirrtum gemäß § 17 StGB liegt bei A nach Auffassung des Simulationsgerichts nicht vor.

Zur Begründung: Ein Verbotsirrtum hätte gemäß § 17 StGB die Strafbarkeit der A mindern oder sogar ausschließen können, sofern er unvermeidbar gewesen wäre. Hierbei ist zwischen einem direkten und einem indirekten Verbotsirrtum zu unterscheiden. Ein direkter Verbotsirrtum liegt vor, wenn der Täter die Existenz eines Verbots überhaupt nicht erkennt. Im vorliegenden Fall kommt jedoch eher ein indirekter Verbotsirrtum in Betracht, da A möglicherweise die Rechtswidrigkeit ihres Verhaltens kannte, jedoch irrte, weil sie davon ausging, dass ihre Handlung durch einen rechtfertigenden Grund – hier die Förderung der Cybersicherheit – gedeckt sei. Hier ist jedoch zu beachten, dass eine bestimmte Absicht, die verschafften Zugangsdaten oder in der Folge auch die dadurch erst erlangten „Inhaltsdaten" zu verwerten, nicht erforderlich ist.[15] Nach § 17 StGB entfällt die Schuld nur dann, wenn der Verbotsirrtum unvermeidbar war. Nach der Rechtsprechung gilt ein Irrtum als vermeidbar, wenn der Täter das Unrecht seiner Handlung „bei einer ihm zumutbaren Gewissensanspannung" hätte erkennen können.[16] Ist der Täter geschäftlich tätig, gelten für ihn besondere Erkundigungspflichten.[17]

Zunächst galt es zu klären, ob für A die tatsächliche Möglichkeit bestand, die Rechtswidrigkeit ihres Verhaltens zu erkennen. Anschließend war zu untersuchen, ob A einen konkreten Anlass hatte, über die rechtliche Zulässigkeit ihres Handelns nachzudenken. Schließlich musste geprüft werden, ob es der A zuzumuten war, die vorhandene Möglichkeit zur Erkenntnis der Rechtswidrigkeit zu nutzen. Dies bedeutet, dass A sich in ihrer konkreten Situation ausreichend hätte informieren müssen, um den Irrtum zu vermeiden. Bei Forschern, die im Bereich der Cybersicherheit tätig sind, ist davon auszugehen, dass sie über entsprechende rechtliche Kenntnisse verfügen oder sich zumindest darüber informieren müssen, welche gesetzlichen Grenzen für ihre Forschung gelten. Der Zugriff auf fremde, besonders gesicherte Daten ohne Einwilligung der Betroffenen ist nach § 202a StGB eindeutig strafbar. Von erfahrenen Forschern im Bereich der IT-Sicherheit wird erwartet, dass sie diese Grundsätze kennen. Ein Verbotsirrtum könnte in Ausnahmefällen unvermeidbar sein, wenn die Rechtslage unklar oder widersprüchlich ist. In diesem Fall ist die Rechtslage jedoch klar: Der unbefugte Zugriff auf gesicherte Daten stellt eine Straftat dar, selbst wenn die Zugangsdaten durch Zufall entdeckt werden. Somit wäre der Irrtum vermeidbar – und der Verbotsirrtum kann die Strafbarkeit nicht ausschließen.

3.3 Entscheidung zu Frage 3

Das Simulationsgericht folgte nicht der Argumentation der A, dass ihr Verhalten aus Gründen der Sozialadäquanz straflos sei, auch wenn das Einloggen in die Accounts nur zu dem Zwecke geschah, die Anmeldedaten zu testen.

Zur Begründung: Der Grundgedanke der Rechtsfigur der Sozialadäquanz sei es, dass Handlungen, die sich „innerhalb der geschichtlich gewordenen sozialethischen Ordnung des Gemeinschaftslebens bewegen", also sozialadäquat seien, niemals strafbar seien, auch wenn sie dem Wortlaut der Strafnorm unterfielen.[18]

Der Zweck heiligt hier jedoch nicht die Mittel: Der unbefugte Zugriff auf persönliche Informationen bleibt unrechtmäßig, selbst bei guter Absicht der Cybersicherheitsforscher oder Dokumentation des Vorgehens. Es existiert keine gesellschaftliche Norm, die es erlaubt, fremde Zugangsdaten zu nutzen, selbst für legitime Zwecke. Das Simulationsgericht verglich den Fall mit einem gefundenen Hausschlüssel: Auch hier wäre die eigenmächtige Nutzung, um den Zugang zu dem Haus zu prüfen, sozial inakzeptabel und invasiv. Die adäquate Vorgehensweise wäre, den Schlüssel zurückzugeben. Die geringe Eingriffsintensität und gute Absicht der Angeklagten sei eine Frage der Strafzumessung, nicht der Tatbestandsmäßigkeit.

3.4 Entscheidung zu Frage 4

Eine umfangreiche Dokumentation des Forschers kann nach Auffassung des Simulationsgerichts zwar als Nachweis für die Ziele des Forschers hilfreich sein, lässt jedoch nicht zwingend den Vorsatz entfallen und führt somit nicht automatisch zur Straflosigkeit eines Forschers.

Zur Begründung: Der bloße Besitz der Passwörter könnte grundsätzlich dafür sprechen, dass diese auch vorsätzlich verschafft wurden. Das Simulationsgericht würdigte in diesem Zusammenhang die umfangreiche Dokumentation durch A im Rahmen der Beweisaufnahme. Es konnte nachvollziehen, dass A die Dateien im Darknet zufällig und nicht unrechtmäßig erlangte, was für die Strafbarkeit nach § 202c StGB relevant war. Der Irrtum über den Inhalt der Dateien ließ den Vorsatz entfallen. Das Simulationsgericht betonte, dass vorsätzliches Handeln jedenfalls nachgewiesen werden müsse. Bei Zweifeln gelte der Grundsatz „in dubio pro reo". Da der Vorsatz eine innere Tatsache sei, könne er nur aus Indizien abgeleitet werden, was eine Gesamtschau aller objektiven und subjektiven Umstände erfordere.

Obwohl B keine Dokumentation über die Durchführung der Forschungsaktivität angefertigt hat, war laut Simulationsgericht hinsichtlich B auch der Umstand zu würdigen, dass sie letztlich den Berechtigten auf die gestohlenen Passwörter aufmerksam machte. Dies spräche laut Simulationsgericht dagegen,, dass sie sie ursprünglich für schädliche Zwecke erlangt hatte und somit – auch ohne Dokumentation – gegen ein vorsätzliches Handeln.

3.5 Entscheidung zu Frage 5

Eine Straflosigkeit aus dem Blickwinkel des rechtfertigenden Notstandes nach § 34 StGB ist nach Auffassung des Simulationsgerichts durchaus naheliegend, scheidet im vorliegenden Fall jedoch aus.

Zur Begründung: Ein frei abrufbarer (zutreffender) Datensatz verschafft einer unüberschaubaren Zahl von Personen die Möglichkeit, sich mittels ihrer Nutzung Zugang zu den Accounts der Betroffenen zu verschaffen, diese ggf. zu übernehmen und miss-

15 MüKoStGB/Graf, 4. Aufl. 2021, StGB § 202a Rn. 80, 81.

16 BGH 18.3.1952 – GSSt 2/51, BGHSt 2, 194 (209); 20.3.1956 – 1 StR 498/55, BGHSt 9, 164 (172); 27.1.1966 – KRB 2/65, BGHSt 21, 18 (20) = NJW 1966, 842; 18.7.2018 – 2 StR 416/16, NJW 2018, 3467 Rn. 11.

17 BGH 18.11.2020 – 2 StR 246/20, NStZ 2022, 30 Rn. 11.

18 Vgl. Roxin, Strafrecht Allgemeiner Teil, Band 1, 4. Auflage, München 2006, der wiederum auf den Entwickler der Theorie, *Welzel* in ZstW 58 (1939), 514 ff. verweist.

bräuchlich zur Begehung von weiteren Straftaten (Betrug etc.) zu verwenden. Solange diese Daten abrufbar sind, besteht die naheliegende Möglichkeit ihrer missbräuchlichen Verwendung gleichsam als Dauerzustand: Wegen der Dezentralität und Anonymität der Darknet-Nutzung sowie insbesondere angesichts des ggf. deliktsgeneigten Personenkreises im Darknet liegt eine gegenwärtige Dauergefahr vor. Niemand weiß, wann, wo und wie genau sie sich realisieren wird, gleichwohl besteht bei einer wertenden Gesamtbetrachtung der konkreten Tatumstände im vorliegenden Fall eine hinreichende, jederzeitige und über ein bloßes Risiko hinausreichende Realisierungswahrscheinlichkeit.

Dass sich Cybersicherheitsforscher in einer solchen Situation über die Eingabe/Abfrage der heruntergeladenen Kennungen probeweise Zugang zu den bei den verantwortlichen Stellen geführten Benutzerkonten verschaffen, kann – bei in Prognosekonstellationen notwendiger großzügiger Bewertung – als geeignete Abwehrmaßnahme für die vorgezeichnete Gefahr angenommen werden: Manche Gefahren erfordern eine mehraktige Abwehr.

Eine derartige „Zwischenabfrage", wie sie die Angeklagte A vorgenommen hat, dürfte insbesondere in Antizipation einer durch eine falsch positive Meldung ggf. ausgelösten Meldekette des betroffenen Unternehmens nach Art. 33 DS-GVO als vorherige „Vergewisserung" bezüglich des tatsächlichen Vorliegens (echter) personenbezogener (gestohlener/abgeflossener Daten) zweckmäßig sein.

Die erforderliche Güter- und Interessenabwägung ist ebenfalls erfolgt: Durch eine stichprobenartige Abfrage weniger Datensätze – d.h. durch einen niederschwelligen Eingriff in das Recht auf informationelle Selbstbestimmung weniger – könnten die entsprechenden Grundrechte einer Vielzahl von Betroffenen sowie mögliche weitergehende Übergriffe in deren Grundrechte auf Eigentum und Vermögen verhütet werden.

Allerdings setzt ein Rückgriff auf § 34 StGB voraus, dass – über die Kenntnis der Notstandslage hinausreichend – auch ein entsprechender subjektiver Rettungswille bezüglich der bedrohten Rechtsgüter und Interessen vorhanden ist. Hieran fehlt es jedenfalls bezüglich der Angeklagten A. Die abstrakte Eigenschaft als „Cybersicherheitsforscher" reicht nicht. Vielmehr muss glaubhaft dargelegt werden, dass die Abfrage einen notwendigen Zwischenschritt in der Gefahrenabwendung bildet, welche für eine unbeteiligte beobachtende Person – wenn überhaupt – mit einer etwaigen Meldung an die verantwortliche Stelle tatsächlich geleistet würde. Zumindest in diesem fiktiven Fall ist ohne eine solche spätere Meldung ein ursprünglich mit Rettungswillen erfolgendes Handeln nicht plausibel und im strafrechtlichen Sinne nicht zu rechtfertigen.

3.6 Entscheidung zu Frage 6

Das Unterlassen der Meldung eines Datenfundes im Darknet bei einer zuständigen Behörde oder bei den Betroffenen selbst ist nach Auffassung des Simulationsgerichts nicht strafbar.

Zur Begründung: Ein Unterlassen ist nur dann strafbar, wenn eine Pflicht zum Handeln besteht. Eine solche Pflicht kann sich etwa ergeben, wenn diese gesetzlich vorgeschrieben ist oder die Gefahr selbst geschaffen wurde. Das ist vorliegend jedoch nicht der Fall. Die Datei war im Darknet für alle frei verfügbar und wurde auch nicht von der Angeklagten A ins Darknet gestellt. Die Angeklagte hat somit nicht die Gefahr selbst geschaffen. Auch eine einschlägige gesetzliche Pflicht zur Meldung besteht derzeit nicht. Die Nicht-Meldung führt folglich auch nicht zu einer Strafbarkeit der A.

3.7 Entscheidung zu Frage 7

Das im Rahmen der Erforschung von neuen, bisher unbekannten Angriffswerkzeugen im Bereich der Cybersicherheit unbeabsichtigte Herunterladen von Passwörtern aus dem Darknet stellt nach Auffassung des Simulationsgerichts keine Straftat im Sinne des § 202c Abs 1 Nr. 1 Alt 1 StGB dar.

Zur Begründung: Nach § 202c StGB macht sich strafbar, wer eine Straftat nach § 202a oder § 202b StGB vorbereitet, indem er Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten ermöglichen, oder Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht. Durch das Herunterladen der Datei hatten A und B aber gerade nicht vor, sich Passwörter oder sonstigen Sicherungscodes zu verschaffen, daher mangelt es schon am Vorsatz. Die ggf. vorliegende fahrlässige Tatbegehung ist nicht strafbar. Zum Zeitpunkt der Verschaffung der Datei haben A und B weder gewusst noch billigend in Kauf genommen, sich eine Liste mit Daten (Passwörtern) zu verschaffen.

Auch müsste für eine Strafbarkeit nach § 202c StGB die Absicht zur Vorbereitung einer anderen Computerstraftat bestanden haben. Dies ist vorliegend weder bei A noch bei B der Fall. A und B hatten keinerlei Plan, eine Straftat zu begehen. Dies haben sie schlüssig vor Gericht vorgetragen. Vor diesem Hintergrund wäre eine Strafbarkeit nach § 202c Abs. 1 Nr. 1 StGB ebenfalls ausgeschlossen, wenn A und B bewusst Passwortlisten aus dem Darknet heruntergeladen hätten, solange sie glaubhaft machen können, diese ausschließlich zu Forschungszwecken (z.B. statistische Auswertungen zu Angriffszielen) – und gerade nicht zur Vorbereitung und/oder Durchführung einer Computerstraftat nach § 202a oder § 202b StGB – zu verwenden.

4 Fazit

Im Rahmen der (offensiven) Cybersicherheitsforschung besteht ein hohes Maß an Rechtsunsicherheit, dem es zu begegnen gilt. Simulationsstudien können die Rechtssicherheit erhöhen, indem sie realistische Forschungsaktivitäten durch ein Simulationsgericht mit Richtern, Staatsanwälten und Strafverteidigern rechtlich bewerten lassen und somit eine erste Einschätzung zur rechtlichen Zulässigkeit dieser Forschungsaktivitäten ermöglichen. Im Rahmen der Simulationsstudie des Nationalen Forschungszentrums für angewandte Cybersicherheit ATHENE werden in den kommenden Jahren unter Anwendung derselben Methodik weitere Forschungsaktivitäten einer ersten rechtlichen Bewertung zugeführt. Cybersicherheitsforscher sind eingeladen, der Erstautorin des vorliegenden Beitrags – nach entsprechender Freigabe ihrer übergeordneten Forschungseinrichtung – Vorschläge über zu verhandelnde Cybersicherheitsaktivitäten zu unterbreiten.