# Kommunikation & Recht

K&R

3 | März 2025
28. Jahrgang
Seiten 145 -216





dfv Mediengruppe
Frankfurt am Main

RA Dr. Florian Deusch und Prof. Dr. Tobias Eggendorfer*

# Rechtliche Rahmenbedingungen der IT-Sicherheitsforschung


## Kurz und Knapp

**Der Beitrag befasst sich mit der tatsächlichen und rechtlichen Situation der IT-Sicherheitsforschung sowie Optionen zur Risikovermeidung de lege lata und stellt die Diskussion zu den Reformbestrebungen der Rechtslage dar.**


## I. Einleitung und Problemaufriss

„Softwarefehler, da kann man nichts machen" – so kommentiert regelmäßig sarkastisch-ironisch Felix von Leitner, deutscher IT-Sicherheitsspezialist, auf seinem Blog[1] Sicherheitsvorfälle. Er spielt damit auf die Wahrnehmung an, dass IT-Sicherheitsvorfälle zum Alltag gehören müssten wie Brot und Butter. Denn er teilt wie andere Sicherheitsforscher die Auffassung, dass ordentliche Qualitätssicherung Sicherheitslücken verhindern kann,[2] Softwarehersteller für sie haften[3] (sollten) und tatsächlich eine sichere IT-Welt denkbar ist.

Zu einer besseren/sicheren IT tragen regelmäßig Sicherheitsforscher bei, wenn sie sicherheitsrelevante Programmierfehler entdecken und sodann verantwortungsbewusst den Hersteller auf die Schwachstellen in seinen Produkten hinweisen. Das Verfahren ist in der Community als Verhaltenskodex akzeptiert. Einige Hersteller freuen sich über diese externe Qualitätsprüfung und loben daher eine Bug-Prämie aus,[4] andere dagegen werfen dem Entdecker eine strafbare Ausspähung von Daten vor.[5]

Dass sichere und damit fehlerfreie Systeme einen Beitrag zur Cyber-Sicherheit leisten, auch in Deutschland, ist der Bundesregierung laut ihrer Cybersicherheitsstrategie durchaus bewusst. Gleichzeitig scheint im politischen Raum angekommen zu sein, dass Sicherheitsforscher dazu einen wesentlichen Beitrag leisten, indem sie auf Sicherheitslücken hinweisen. Daher hat das Bundesjustizministerium unter Berufung auf den Koalitionsvertrag der „Ampel" (2021) ein Eckpunktepapier veröffentlicht, wonach das Identifizieren und Melden von Sicherheitslücken „legal durchführbar" werden soll.[6] Das erscheint nicht nur aus technischer Sicht sinnvoll, sondern auch für das Funktionieren des Staates wesentlich, sieht man, dass sogar Kommunen[7] wegen Sicherheitsvorfällen nicht arbeitsfähig sind, auch das Berliner Kammergericht war über Monate sehr eingeschränkt.[8] Angesichts der Tragweite und Bedeutung ihres Handelns entsteht eine Parallele zwischen Whistleblowern und Sicherheitsforschern – erstere genießen durch das HinSchG einen besonderen Schutz. Der Beitrag diskutiert die rechtlichen Rahmenbedingungen für die IT-Sicherheitsforschung de lege lata und stellt sodann den aktuellen Gesetzesentwurf zur Reform des § 202a StGB dar.

## II. Akteure der IT-Sicherheitsforschung

Während der Begriff „IT-Sicherheitsforschung" eine ausschließlich wissenschaftliche Domäne andeutet, findet sich tatsächlich eine bunte Mischung von Handelnden mit unterschiedlichen Motiven. Gemein ist ihnen, dass sie sich systematisch mit IT-Systemen auseinandersetzen, um sie auf Sicherheitslücken zu testen und diese zu explorieren. Früher sprach man von Hackern, die in MacGyver-artiger Kreativität Systeme anders als vom Entwickler gedacht nutzten. Doch der Begriff hat in letzter Zeit medial eine negative Konnotation erfahren,[9] der zunächst eine Unterscheidung in Black-, White- und Grey-Hat-Hacker[10] entgegenwirken sollte: Die einen, die bösartig mit schädigenden Zielen in Systeme einbrechen, die anderen, die als edles Motiv die Identifikation von Sicherheitsproblemen auf ihre Fahnen schreiben. Die „Grey-Hats" liegen irgendwo dazwischen. Doch die Farbcodierung funktioniert nur halb: Die bekannteste Hackerkonferenz „BlackHat"[11] dürfte den Großteil der Teilnehmer aus White-Hats rekrutieren.

Damit bleibt nur, unmittelbar auf die Motivation abzustellen. Neben „soften" Faktoren, wie Anerkennung in der Szene[12] und Spieltrieb, dürften wirtschaftliche Anreize ein Thema sein. Geld durch Hacking lässt sich durch Bug-Bounties, also vom Hersteller ausgelobten Belohnungen für Sicherheitslücken, verdienen oder, am anderen Ende der Skala, z. B. durch Erpressung, Datenhehlerei, den Verkauf der Lücken an andere Straftäter und weitere Straftaten. Teils kann Sicherheitsforschung auch eine Nebenaufgabe des Hauptberufs sein: Penetrationtester oder Software-Entwickler sind Beispiele.

Auch die wissenschaftliche Informatik entdeckt regelmäßig Sicherheitsprobleme, die Sicherheitsforschung kann dabei als eigene Unterdisziplin gelten. Dabei reicht auch hier die Bandbreite der Lücken von „alltäglichen" Softwarefehlern bis hin zu

* Mehr über die Autoren erfahren Sie am Ende des Beitrags. Der Beitrag geht auf einen Vortrag der Autoren bei der DSRI-Herbstakademie 2024 zurück, der veröffentlicht wurde im Tagungsband von *Heinze/Steinrötter* (Hrsg.), KI und Daten: Digitalregulierung auf dem Höhepunkt? 2024, S. 393 ff. Er ist überarbeitet und aktualisiert zum Stand Februar 2025. Alle Links zuletzt abgerufen 1. 2. 2025.

1 http://blog.fefe.org.

2 *Deusch/Eggendorfer*, in: Bernzen et. al., (Hrsg.), Das IT-Recht vor der (europäischen) Zeitenwende, 2023, S. 323 - 339; *Eggendorfer/Andresen*, Using Security Metrics to improve Cyber-Resilience, IARIA Congress 2024, Porto, 2024.

3 *Deusch/Eggendorfer*, in: Taeger (Hrsg.), Internet der Dinge, Digitalisierung von Wirtschaft und Gesellschaft, 2015, S. 833, 846.

4 https://karmainsecurity.com/zip-slip-meets-artifactory-a-bug-bounty-story liefert dafür ein anschaulich erzähltes Beispiel.

5 *Deusch/Eggendorfer*, K&R 2023, 649 - 656; https://netzpolitik.org/2021/cdu-connect-ermittlungsverfahren-gegen-sicherheitsforscherin-lilith-wittmann-eingestellt/.

6 Zur Cybersicherheitspolitik des Bundes, welche sich auf die Cybersicherheitsstrategie der Vorgängerregierung beruft: https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cybersicherheitspolitik/cybersicherheitspolitik-node.html; zum Eckpunktepapier des Bundesjustizministeriums vom 23. 11. 2023, https://kripoz.de/wp-content/uploads/2023/11/1123_Eckpunkte_Modernisierung_Strafrecht.pdf; zum Referentenentwurf siehe unten Abschnitt VI).

7 In einer solchen Aufzählung darf der Kreis Anhalt-Bitterfeld nicht fehlen: https://www.mdr.de/nachrichten/sachsen-anhalt/dessau/anhalt/cyberangriff-kreis-kosten-teurer-als-gedacht-102.html.

8 https://www.heise.de/news/Emotet-Berliner-Kammergericht-bleibt-bis-2020-weitgehend-offline-4569544.html.

9 Zur begrifflichen Vorverurteilung auch *Eggendorfer/Andresen/Gräupner*, „Risiken der digitalen Forensik", in: von Frankenberg/Klein, Polizei und Risiken, 2025.

10 Manche führen sogar noch weitere Farbabstufungen ein: https://sectigostore.com/blog/different-types-of-hackers-hats-explained/.

11 https://www.blackhat.com/.

12 Fn. 4 liefert dafür ein Beispiel.

komplexen Designproblemen in Prozessoren, wie Spectre und Meltdown.[13]

Regelmäßig zeigt sich, dass Sicherheitslücken, die „die Guten" entdecken, schon einige Zeit vorher von unbefugten Personen bzw. Kriminellen genutzt wurden: So fanden sich bei einer Nachsuche in Logfiles für die prominenten Vorfälle „Heartbleed" und „Log4Shell" teils schon Monate vorher Angriffe.[14] Wenn Sicherheitsforscher allerdings aufgrund unsicherer Rechtslage davon absehen, entdeckte Lücken zu kommunizieren, schwächt das die IT-Sicherheit und erhöht die Risiken zu Lasten der Nutzer.[15]

## III. Vorgehen der IT-Sicherheitsforscher und Responsible Disclosure

Sicherheitslücken sind zunächst Programmier- oder Designfehler, die von Anfang an in der Software enthalten sind. Sicherheitsforscher verursachen sie nicht, sie dokumentieren und demonstrieren sie – ähnlich dem TÜV-Mitarbeiter, der bei der Hauptuntersuchung den durchgerosteten Schweller zeigt.[16]

Anders als bei Autos findet bei Software – entgegen jeder technischen Empfehlung[17] – keine regelmäßige Hauptuntersuchung statt, es ist also Sache des Nutzers oder einer zufälligen Verkehrskontrolle, Mängel zu identifizieren. Wie der erfahrene Verkehrspolizist bemerken auch erfahrene Sicherheitsforscher auffälliges Verhalten von Software, sehen auffällige Fehlermeldungen und beginnen entsprechend nachzusuchen.[18]

Alternativ können sich Sicherheitsforscher gezielt Produkte vornehmen und durch diverse Analyse-Verfahren Auffälligkeiten suchen – das Vorgehen ist letztlich einem Penetrationtest gleich.

In beiden Fällen reicht es regelmäßig aus, auffälliges Verhalten zu erzeugen: So ist eine Sicherheitslücke durch einen Buffer Overflow ausreichend nachgewiesen, stürzt das Zielprogramm ab, löst man den Overflow aus; genauso zeigt sich eine erfolgreiche SQL-Injection durch eine Fehlermeldung des Datenbanksystems. Entgegen der gerne – insbesondere von einigen großen Softwarehäusern – vertretenen Auffassung ist es nicht erforderlich, einen sogenannten „Proof of Concept" (PoC) zu schreiben. Der würde beispielhaft zeigen, wie sich die Lücke ausnutzen lässt.

Teils sind die PoCs mit viel Liebe gestaltet, so installierte auf der BlackHat einst ein Hacker ein kleines Rennspiel als Ergebnis eines erfolgreichen Angriffs über eine manipulierte Kreditkarte auf ein Bezahlterminal auf eben dem Terminal, doch auch ohne PoC existiert die Lücke. Teils kann ein kunstvoll gestalteter PoC auch dazu führen, dass die Lücke auf der Schwereskala einen höheren Wert erhält.[19]

Softwarehersteller neigen dazu, eine Lücke ohne PoC zu verneinen oder herunterzuspielen. Das ist für sie statistisch interessant, weil sie so Vorfälle verdecken und medial besser darstellen können. Häufig führt allerdings diese Negation dazu, dass die Forscher die Lücke veröffentlichen, und jemand anderes nun einen PoC schreibt. Wer das ist, ist nicht vorhersagbar – das können auch Angreifer sein. Regelmäßig folgen dann hektische Patch-Aktionen der Hersteller.

Dabei ist das Vorgehen in der Community der Sicherheitsforscher etabliert und gilt als ungeschriebenes Gesetz: Wer eine Sicherheitslücke findet, kontaktiert den Anbieter, erläutert, dass er eine Lücke gefunden hat und bittet um einen geeigneten Ansprechpartner, mit dem er möglichst verschlüsselt E-Mails austauschen kann.[20] Diesem Kontakt erläutert er die Sicherheitslücke, empfiehlt gegebenenfalls sogar, wie sie zu beheben ist, und vereinbart ein Zeitfenster, bis wann der Anbieter sich um die Lücke kümmert.

Gute Softwarehersteller bleiben während der Behebung mit dem Entdecker im Kontakt. Oft bitten sie darum, deren Abhilfemaßnahmen zu prüfen, in jedem Fall unterrichten sie ihn, wenn die Lücke behoben ist. Allerdings gibt es auch hier in Fachkreisen bekannte Anbieter, bei denen regelmäßiges Nachfragen erforderlich ist.

Danach kann (und wird in der Regel) die Lücke auch öffentlich bekannt gegeben. Je nach Ausmaß und Risiko erfolgt diese Publikation einige Tage bis Wochen, nachdem der nötige Patch bereitgestellt wurde, so dass er schon möglichst flächig installiert ist, und Angreifer so keine Gebrauchsanleitung bekommen.

Durch dieses „responsible disclosure" ist sichergestellt, dass sowohl der Sicherheitsforscher für seine Leistung gewürdigt wird, aber auch die Interessen des Softwareherstellers gewahrt sind, ohne übertriebene Eile einen Patch bereitstellen zu können. Dies ist auch im Interesse der Nutzer, weil diese nicht immer sofort die Updates einspielen können.

Einige Hersteller animieren gezielt zu diesem Vorgehen und belohnen entdeckte Sicherheitslücken durch eine Bug-Bounty. Häufig animiert die Bug-Bounty auch zu besonders aufwendigen PoCs, um möglichst einen großen Schweregrad zu dokumentieren und so eine höhere Bounty zu erhalten.

Obwohl dieses Verfahren etabliert ist,[21] finden sich zahllose Negativbeispiele: So gibt es aktuell eine Welle von „durch KI gefundenen" Sicherheitslücken, die teils von der KI zusammenfabuliert sind, teils uralt und nur sehr selten real, für die der vorgebliche Sicherheitsforscher gerne eine Bug-Bounty hätte, faktisch aber den Kommunikationskanal für echte Sicherheitsforscher blockiert. Auf der anderen Seite gibt es Hersteller, die erst auf Presseanfragen reagieren oder direkt den Sicherheitsforscher mit Strafandrohungen überziehen.[22]

Letztlich ist zu fragen, wer den größeren Schaden verursacht: Ein Sicherheitsforscher, der auf eine Lücke hinweist, oder ein

13 https://www.faz.net/pro/d-economy/meltdown-und-spectre-was-hinter-der-chip-luecke-steckt-15373753.html; https://thehackernews.com/2018/11/meltdown-spectre-vulnerabilities.html; https://meltdownattack.com/; https://arxiv.org/pdf/1811.05441.

14 https://www.heise.de/news/Sicherheitsluecke-Log4Shell-Internet-in-Flammen-6304730.html.

15 An die Autoren haben sich bereits Sicherheitsforscher gewandt, die sich aufgrund der Rechtslage unsicher waren, wie sie vorgehen sollen. Auch wenn das nur als anekdotische Evidenz gelten kann, scheint plausibel, dass ein größerer Kreis betroffen ist.

16 Man könnte Rost an Autos, obgleich allmählich entstehend, tatsächlich als Designfehler sehen: Was ordentlich verzinkt, sauber verbunden, und ohne Sicken und Falze für Wasser- und Dreckeinlagerungen hergestellt ist, rostet auch nicht. Daher gibt es fahrzeugtypische Roststellen.

17 *Deusch/Eggendorfer*, K&R 2018, 223 ff.; *Deusch/Eggendorfer*, in: Bernzen et. al. (Fn. 2), S. 323 - 339.

18 So z. B. einer der Autoren, u. a. in: *Eggendorfer*, Linux Magazin 05/2020; *ders.*, Linux Magazin 04/2010, S. 82 ff.; *ders.*, Linux Magazin 12/2010, S. 100 ff.; *ders.*, Linux Magazin 02/2011, S. 108 ff.; *ders./Keller*, Linux Magazin 01/2009, S. 100 ff.; *ders.*, Linux Magazin 12/2008, S. 78 ff.

19 Ein Beispiel dafür ist der PoC zu einer Sicherheitslücke im exim-Mailserver https://bugzilla.suse.com/show_bug.cgi?id=1136587.

20 Erschreckend häufig scheitert es schon am Kontakt zum Anbieter, der einfach nicht reagieren will oder sich taub stellt. Aus eigenem Erleben einer der Autoren ist der „Totstell-Reflex" leider viel zu häufig.

21 Siehe für übergeordnete Beispiele: https://www.cisa.gov/coordinated-vulnerability-disclosure-process; https://www.enisa.europa.eu/news/member-states/WEB_115207_BrochureNCSC_EN_A4.pdf; https://www.hackerone.com/knowledge-center/why-you-need-responsible-disclosure-and-how-get-started; https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html sowie für einzelne Anbieter exemplarisch https://certcc.github.io/CERT-Guide-to-CVD/reference/policy_templates/; https://support.hp.com/us-en/document/c06144280; https://www.usa.philips.com/a-w/security/coordinated-vulnerability-disclosure.html; https://www.etsi.org/standards/coordinated-vulnerability-disclosure sowie ISO/IEC 29141, ISO/IEC 3011 und ISO/IEC TR 5895:2022; a. A. das Bundesjustizministerium im Referentenentwurf zu § 202a StGB (siehe unten Abschnitt VI Ziffer 3).

22 Siehe Fn. 5. Auch einer der Autoren kennt die „Bedrohung" aus eigener Erfahrung, siehe https://www.linux-magazin.de/ausgaben/2008/12/botenstoff/.

Hersteller, der sie zu vertuschen sucht und sogar die bedroht, die ihn warnen. Es gibt auch Autoren, die zu dem Schluss kommen, dass solche Rosstäuscher strafbar sein sollten, da sie ein erhebliches Risiko für das Gemeinwohl darstellen.[23]

## IV. Strafrechtliche Rahmenbedingungen

Die Untersuchung von IT-Sicherheitslücken führt für die Forschenden zu Strafbarkeitsrisiken, v. a., wenn die IT-Sicherheitsprüfung außerhalb interner Labore der Institute stattfindet, „in-the-wild" an Systemen, die über das Internet erreichbar sind. Dies erfolgt in der Regel ohne vorherige Information der Systembetreiber.[24]

### 1. § 202a StGB

Gemäß § 202a StGB wird bestraft, wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft.

Problematisch ist für IT-Sicherheitsforscher das Tatbestandsmerkmal der besonderen Zugangssicherung. Diese liegt vor, wenn Vorkehrungen getroffen sind, um den Zugriff auf Daten auszuschließen oder nicht unerheblich zu erschweren.[25] Für die IT-Sicherheitsforschung ist genau dies der Prüfungsgegenstand, nämlich die Feststellung, ob eine geeignete Zugangssicherung vorhanden ist oder nicht. Entscheidend für die Strafbarkeit von IT-Sicherheitsforschern ist deshalb der Meinungsstreit, inwieweit die Sicherung objektiv geeignet sein muss, um den unbefugten Zugang zu verhindern.[26] Aus Sicht der IT-Sicherheit ist sie immer dann objektiv ungeeignet, wenn sie zu umgehen war.

Der Taterfolg des § 202a StGB ist eingetreten, wenn sich der Täter den Zugang zu den betroffenen Daten verschafft hat. Die Überwindung der Zugangssicherung muss dafür ursächlich gewesen sein. Ein tatsächlicher Zugriff auf die Daten (Lesen, Schreiben, Ändern) ist nicht erforderlich.[27] Unklar bleibt aus technischer Sicht, was der Unterschied zwischen einem Überwinden der Zugangssicherung und dem tatsächlichen Zugriff auf die gesicherten Daten sein soll. Das eine ist ohne das andere nicht denkbar: Sind die Daten geschützt, erfordert der Zugriff das Umgehen der Zugangssicherung – die schützt unmittelbar den Zugriff auf die Daten, ein Umgehen ohne Zugriff ist also genauso undenkbar.

Eine Strafbarkeit entfällt, wenn die IT-Sicherheitsprüfung im Einverständnis der Betroffenen stattfindet. Streitig ist dabei, ob die Einwilligung bereits den Tatbestand oder lediglich die Rechtswidrigkeit ausschließt. Entscheidend ist jedoch, dass die Einwilligung aller Personen vorliegen muss, die über die Daten verfügungsbefugt sind. Das sind diejenigen, die den Skripturakt der Daten verantworten.[28] Oftmals treffen die IT-Sicherheitsforscher komplexe Cloud-Systeme an, in denen der Anbieter für zahlreiche Kunden Daten verarbeitet. Verfügungsbefugt ist dabei nicht der Anbieter, sondern jeder einzelne Kunde.

Unter welchen Voraussetzungen das Responsible Disclosure die Rechtswidrigkeit entfallen lässt, erörtert unten Ziffer 6.

### 2. § 202b StGB

Nach § 202b StGB wird bestraft, wer sich oder einem anderen Daten aus einer nicht-öffentlichen Datenübermittlung verschafft, welche nicht für ihn bestimmt sind. Geschützt sind die Daten i. S. d. § 202a Abs 2 StGB während des Übertragungsvorgangs vom Absender an den Empfänger, etwa per Telefon und E-Mail. Zwischenspeicherungen sind hiervon erfasst, wenn der Absender keinen Einfluss darauf hat.[29] Nicht-öffentlich ist eine Übertragung, die sich nicht an die Allgemeinheit richtet, eine Zugangssicherung wie bei § 202a StGB, etwa Verschlüsselung, ist nicht notwendig. Im Gegensatz zu § 202a StGB muss sich der Täter die Daten verschaffen, etwa durch Lesen, Kopieren oder Umleiten, nicht lediglich den Zugang hierzu.[30] § 202b StGB greift nur, wenn die Tat nicht durch andere Strafnormen schärfer sanktioniert wird, z. B. durch § 27 Abs. 1 Nr. 1 TDDDG.

### 3. § 202c StGB

Der sogenannte „Hackerparagraf" stellt bereits die Vorbereitung einer Tat nach den §§ 202a, 202b StGB unter Strafe. Tatbestandsmäßig ist die Herstellung, Verschaffung und Überlassung von Zugangsdaten und Computerprogrammen, deren Zweck das Ausspähen und Abfangen von Daten ist (sogenannte „Hackersoftware").[31] Die Norm war stets großer Kritik ausgesetzt, denn derartige Software wird in der IT-Sicherheitsforschung eingesetzt, aber auch in kommerziellen IT-Sicherheitsunternehmen, allerdings mit dem Ziel, Lücken aufzudecken und diese zu beseitigen. Das BVerfG hat deshalb eine einschränkende Lesart des § 202c StGB vorgegeben. Hiernach darf die Software ausschließlich zum Ausspähen und Abfangen einsetzbar, mithin keine „Dual Use Software" sein.[32] Außerdem muss sie mit der Absicht zur Straftat

23 *Eggendorfer/Andresen*, Using Security Metrics to improve Cyber-Resilience, IARIA Congress 2024, Porto, 2024.

24 Die Anwendbarkeit des deutschen Strafrechts durch den Handlungs- oder Erfolgsort in Deutschland gemäß § 9 StGB wird für diese Untersuchung vorausgesetzt. Weitergehende zivil- und datenschutzrechtliche Betrachtungen müssen einer gesonderten Darstellung vorbehalten bleiben.

25 BGH, 13. 5. 2020 – 5 StR 614/19, Rn. 19 – juris; BT-Drs. 16/3656 S. 10; BGH, 27. 7. 2017 – 1 StR 412/16, K&R 2018, 793 ff. = NStZ 2018, 401, 403; BGH, 21. 7. 2015 – 1 StR 16/15, K&R 2016, 53 = NStZ 2016, 339, 340; BGH, 6. 7. 2010 – 4 StR 555/09, NStZ 2011, 154, jeweils m. w. N.

26 Dafür: *Hilgendorf*, in: Leipziger Kommentar StGB, Band 10, 13. Aufl. 2023, § 202a Rn. 3; *Brodowski*, in: Kipker, Cybersecurity, 2. Aufl. 2023, Kap. 17, Rn. 46; *Deusch/Eggendorfer*, K&R 2023, 649, 553; dagegen: LG Aachen, 27. 7. 2023 – 60 Qs 16/23, K&R 2023, 693 (sich berufend auf BGH, 13. 5. 2020 – 5 StR 614/19), wonach es auf die Dokumentation des Interesses an der Zugangssicherung ankomme und darauf, ob die Sicherung auch durch einen Laien ohne erheblichen technischen und zeitlichen Aufwand möglich sei; im Urteil (LG Aachen, 4. 11. 2024 – 74 NBs 34/24) hielt das LG Aachen an dieser Auffassung fest, siehe https://www.heise.de/news/Modern-Solution-Berufungsgericht-bestaetigt-Schuld-des-Sicherheitsforschers-10007090.html.; *Wagner*, PinG 2020, 66, 69, stellt darauf ab, die Eignung der Zugangssicherung daran zu messen, ob sie für Personen mit durchschnittlichen Informatikkenntnissen überwindbar ist. Ein solcher Durchschnitt ist allerdings schwer zu fassen, fehlt es doch schon an einheitlichen Curricula im Informatikstudium, dazu u. a. *Andresen/Eggendorfer*, Vom Fach, inf.08, 12/2024.

27 *Cornelius*, in: Taeger/Pohle, Computerrechts-Handbuch, 39. Ergänzung, 2024, Kap. 102 Rn. 31 f.

28 *Cornelius*, in: Taeger/Pohle (Fn. 27), Kap. 102 Rn. 20, 33 f.; *Wagner*, PinG 2020, 66, 69; *Deusch/Eggendorfer*, K&R 2023, 649, 653, 655.

29 *Cornelius*, in: Taeger/Pohle (Fn. 27), Kap. 102 Rn. 42, somit wohl auch die Zwischenspeicherung durch die verschiedenen Mailserver, die am Kommunikationsvorgang beteiligt sind.

30 *Hassemer*, in: Schneider, Handbuch EDV-Recht, 5. Aufl. 2017, Kap. E Rn. 114, 115.

31 Beachtenswert ist in der Bezeichnung „Hackerparagraph", „Hackertools" und „Hackersoftware" bereits die Kriminalisierung des ursprünglich positiv besetzten Begriffes „Hacker". Ebenso eindrucksvoll ist, dass diese Norm eine der wenige Normen ist, die bereits den Besitz potentieller Tatmittel unter Strafe stellt: Der Erwerb einer Axt mit dem Ziel durch Mord die Scheidungskosten einzusparen und stattdessen die Lebensversicherung zu kassieren, ist – solange der Täter von seinem Tatplan zurücktritt – eine straffreie Vorbereitungshandlung. Sogar das „ab-phishen" von Nutzername und Passwort soll keine strafbare Vorbereitung z. B. eines Online-Betrugs sein, so z. B. https://www.hrr-strafrecht.de/hrr/archiv/10-02/index.php?sz=7, die nur die Möglichkeit einer Strafbarkeit wegen des Fälschens beweiserheblicher Daten (§ 269 StGB) und ggf. nach UrhG in Betracht ziehen.

32 Eine solche „Single-Use"-Software existiert allerdings nur in der Theorie – kaum jemand verkauft ein Messer ausschließlich als Mordwaffe, sogar solche, die waffenrechtlich erfasst sind, wie z. B. Einhandmesser, die als Rescue-Tool, Outdoor-Survival-Messer o. ä. auch einen (sinnvollen) Nutzen finden. Gleiches gilt für Software. Siehe insoweit auch die Diskussion

entwickelt worden sein, welche sich objektiv manifestiert haben muss, etwa in der Vertriebspolitik des Herstellers.[33] Ob diese Einschränkungen geeignet sind, um die redliche IT-Sicherheitsforschung von kriminellen Vorbereitungen abzugrenzen, mag zweifelhaft erscheinen. Zu empfehlen ist der IT-Sicherheitsforschung jedenfalls, durch organisatorische Maßnahmen für den Einsatz derartiger Software ihre redlichen Absichten zu dokumentieren, etwa durch interne Richtlinien/Anweisungen zur Verwendung der Software. Derartige Maßnahmen sprechen jedenfalls gegen einen Tatvorsatz.

### 4. §§ 303a, 303b StGB

Die §§ 303a, 303b StGB stellen es unter Strafe, fremde Daten zu manipulieren (§ 303a StGB) und in eine Datenverarbeitung von wesentlicher Bedeutung einzugreifen (Computersabotage gemäß § 303b StGB). Für die IT-Sicherheitsforschung sind diese Tatbestände relevant, wenn durch das Ausnutzen einer Lücke Zugang zu einem IT-System besteht. Bereits bei der Überwindung der Zugangssicherung gemäß § 202a StGB können Daten auf dem betroffenen IT-System geschädigt werden. Wenn der IT-Sicherheitsforscher weitere Ermittlungen unternimmt, um die Reichweite der Lücke zu prüfen, können ebenfalls Eingriffe in die Datenverarbeitung und Datenveränderungen stattfinden bis hin zum Systemausfall. Diese sind zwar vom Zweck der IT-Sicherheitsforschung nicht erfasst. Für eine Strafbarkeit reicht jedoch bedingter Vorsatz aus; die Absicht, Nachteil zuzufügen, wird nur für den Sondertatbestand § 303b Abs. 1 Nr. 2 StGB relevant, und zwar wenn Daten eingegeben oder an Dritte übermittelt werden.[34]

### 5. Weitere einschlägige Strafnormen

Weiter kann eine Untersuchung durch IT-Sicherheitsforschende zur Fälschung beweiserheblicher Daten führen (§ 269 StGB) oder es kann eine Sachbeschädigung (§ 303 StGB) vorliegen, wenn IT-Hardware oder Waren in Produktionsprozessen zerstört werden. Für eine Tatbestandsverwirklichung reicht bedingter Vorsatz aus.[35]

Ebenso können Forschende auf Geschäftsgeheimnisse und personenbezogene Daten auf untersuchten IT-Systemen von Unternehmen stoßen. Ein Zugriff auf diese Daten kann unter die §§ 23 Abs. 1 Nr. 1 GeschGehG und 42 Abs. 2 BDSG fallen; beide Normen setzen aber Schädigungs- bzw. Bereicherungsabsicht voraus, die bei den hier dargestellten Forschungen fehlen.

### 6. Rechtfertigung durch Responsible Disclosure?

Soweit Hersteller im *Responsible Disclosure* die Lücke binnen angemessener Frist nicht beseitigt haben, veröffentlicht der Sicherheitsforscher die entdeckte Lücke, um die Öffentlichkeit und die betroffenen Nutzer zu warnen und ihnen die Möglichkeit zu verschaffen, ihre Daten anderweitig in Sicherheit zu bringen.[36]

#### a) Rechtfertigender Notstand

Eine Sicherheitslücke stellt eine gegenwärtige Gefahr für die Sicherheit der betroffenen IT-Systeme und ihrer Nutzer dar. Denn sie kann durch Kriminelle jederzeit ausgenutzt werden, um die IT-Systeme zu infiltrieren, zu schädigen und zu weiteren Straftaten zu missbrauchen.[37] Maßnahmen der IT-Sicherheitsforschung, die Straftatbestände gemäß Ziffern 1 bis 5 (oben) erfüllen, können daher gemäß § 34 StGB gerechtfertigt sein, allerdings nur, wenn die Notstandshandlungen zur Gefahrenbeseitigung geeignet, erforderlich und angemessen sind. Das Vorgehen gemäß den Grundsätzen des Responsible Disclosure kann eine solche Notstandshandlung sein.[38] Für eine Straffreiheit muss jede einzelne Maßnahme, beginnend von der Untersuchung eines fremden IT-Systems bis hin zur Veröffentlichung der Lücke diesem Prüfungsmaßstab standhalten. Alle Maßnahmen müssen von einem Nothilfewillen des Sicherheitsforschers getragen sein. Der rechtfertigende Notstand ist kein Persilschein, um willkürlich in fremde IT-Systeme einzudringen. Es müssen zumindest Anhaltspunkte für einen Anfangsverdacht einer Sicherheitslücke für das betroffene IT-System vorliegen.[39] Allerdings kann die Beurteilung eines solchen Verdachts im Einzelfall schwierig sein: So gibt es Lücken, die auf typische Denk- und Logikfehler in der Programmierung hindeuten, und daher oft mit anderen Lücken gemeinsam auftreten. Reicht dieser Erfahrungssatz zur Begründung des Verdachts? Reicht die Erfahrung aus, dass Produkte bestimmter Hersteller, wie es der bereits zitierte Fefe so nett formuliert, „stabil liefern", und zwar Sicherheitslücken anstelle eines mangelfreien Produkts?[40] Forschern ist daher zu raten, ihre Verdachtsmomente nachzuweisen, die eine nähere Untersuchung veranlasst haben.

Liegt ein solcher Anfangsverdacht vor, so kann z. B. das Überwinden einer Zugangssicherung geeignet sein, um die Gefahr zu beseitigen. Denn zur Beseitigung der Gefahr gehört es, diese zu benennen und nachzuweisen. Ob es hiernach zur Prüfung der Kritikalität einer Lücke sogar erforderlich sein kann, eine Datenveränderung oder die Störung einer Datenverarbeitung (§§ 303a, 303b StGB) in Kauf zu nehmen, hängt vom Einzelfall ab, insbesondere von der Abwägung der betroffenen Interessen bei der Angemessenheit der Notstandshandlung. Entscheidend in dieser Forschungsphase ist eine fachliche Risikobewertung, welche Schäden bei der Untersuchung des betroffenen Systems mit welcher Wahrscheinlichkeit eintreten können und in welchem Verhältnis sie zu den gefährdeten Rechtsgütern stehen, die durch die Notstandshandlung zu schützen sind. Stets sind der aktuelle Stand von Wissenschaft und Technik zu beachten, um Datenverluste, Soft- und (äußerst unwahrscheinliche) Hardwareschäden des Prüfobjekts zu vermeiden.[41]

Auch die Veröffentlichung der Lücke hat diese Anforderungen zu erfüllen. Ein erforderliches, weil milderes Mittel einer Lücke ist es daher, im Responsible-Disclosure-Verfahren den System-

zur Encrochat-Rechtsprechung, z. B. bei *Deusch/Eggendorfer*, in: Pfeffer, Policing Crime Chat Networks, Lessons from the EnchroChat Operation, Göttingen 2024, S. 37 - 51.

33 BVerfG, 18. 5. 2009 – 2 BvR 2233/07, K&R 2009, 632 ff.; *Hassemer*, in: Schneider (Fn. 30), Kap. E Rn. 133.

34 *Cornelius*, in: Taeger/Pohle (Fn. 27), Kap. 102 Rn. 201; *Böken*, in: Kipker (Fn. 26), Kap. 19 Rn. 68, 69.

35 *Brodowski*, in: Kipker (Fn. 26), Kap. 17 Rn. 39, 40, 44.

36 Siehe dazu Fn. 5; *Böken*, in: Kipker (Fn. 26), Kap. 19 Rn. 55; *Vonderau/Wagner*, in: Taeger (Hrsg.), Den Wandel begleiten, 2020, S. 525, 535, mit weiteren Differenzierungen nach „Limited und Full Disclosure"; *Deusch/Eggendorfer*, K&R 2023, 649, 652; teils auch als „Coordinated Vulnerability Disclosure" (https://www.enisa.europa.eu/topics/vulnerability-disclosure) bezeichnet, im Detail unterscheidet sich die Vorgehen zur endgültigen Publikation, der Vorgang an sich ist allerdings identisch.

37 Dass diese Gefahr nicht nur abstrakt besteht, dokumentieren z. B. Heartbleed und Log4Shell, s. o. Fn. 14.

38 *Wagner*, PinG 2020, 66, 73; *Klaas*, MMR 2022, 187, 189; *Schneider*, Kriminalistik 2023, 433, 434; *Hillert*, jurisPR-ITR 23/2023 Anm. 3; *Deusch/Eggendorfer*, K&R 2023, 649, 655; a. A. (die „gegenwärtige Gefahr" ablehnend) Stellungnahme WD 7 – 3000 – 104/23 des wissenschaftlichen Dienstes des Deutschen Bundestags vom 23. 4. 2024 (S. 17; https://www.bundestag.de/resource/blob/1005444/ed435cb1a5311bb688385a81f295c8a3/WD-7-104-23-pdf.pdf).

39 *Wagner*, PinG 2020, 66, 74; *Schneider*, Kriminalistik 2023, 433, 435, der auf Verdachtsmomente aus Forenbeiträgen zum betroffenen IT-System abstellt.

40 Z. B. https://blog.fefe.de/?ts=99890345.

41 Dazu unter zivilrechtlichen Aspekten: *Böken*, in: Kipker (Fn. 26), Kap. 19 Rn. 39 - 45.

hersteller/Betreiber vertraulich zu informieren und Gelegenheit zur Fehlerbeseitigung zu geben, bevor die Lücke veröffentlicht wird. Dabei wird es auch für zulässig gehalten, die Erteilung des Hinweises unter die Bedingung zu stellen, keinen Strafantrag zu stellen und einer anschließenden Veröffentlichung zuzustimmen.[42]

Die Frist für den Produktverantwortlichen zur Fehlerbehebung muss angemessen sein. Dabei sind die Komplexität des Fehlers sowie der notwendigen Beseitigungsmaßnahmen und die Gefahren und möglichen Folgen eines Exploits abzuwägen. Ob die dazu diskutierten Fristen von 30 bis 120 Tagen passend sind, ist insbesondere fraglich, wenn bereits Exploits zur Lücke bekannt sind: Dann ist die zeitnahe Beseitigung nötig.[43]

Teilweise wird angeführt, die Meldung einer Lücke an das BSI gemäß § 4b BSIG sei einer Veröffentlichung vorzuziehen, da eine Veröffentlichung der Lücke auch durch Kriminelle genutzt werden könne, um sie auszunutzen.[44] Einzuräumen ist, dass die Veröffentlichung einer Lücke, wenn sie vom Hersteller nicht zuvor beseitigt ist, nur teilweise geeignet ist, die betroffenen Nutzer zu schützen. Denn nur die interessierte Fachwelt verfolgt derartige Veröffentlichungen[45] und kaum ein IT-Nutzer wird in der Lage sein, die notwendigen Maßnahmen selbst einzuleiten, um die Gefahr für seine Daten zu beseitigen. Aus Sicht des Sicherheitsforschers, der die Lücke gemeldet hat, ist jedoch fraglich, ob eine Meldung an das BSI geeignet zur Gefahrenbeseitigung i. S. d. § 34 StGB ist. Denn er hat keinerlei Möglichkeiten zu prüfen, ob und wie das BSI auf seine Eingabe reagiert. Die Veröffentlichung der Lücke kann er jedoch selbst vornehmen. Wenn der betreffende Hersteller/Betreiber die Beseitigung der Lücke ablehnt oder innerhalb der – angemessenen – Frist nicht behebt, ist sie für den Forscher die einzige Möglichkeit, zu einer Reduzierung der Gefahr beizutragen. Denn sie verschafft den Nutzern immerhin die Option, die betreffende IT-Lösung zu meiden, deren Verwendung zu stoppen oder sonstige Maßnahmen („Work-Around“) zu treffen (sofern erforderlich mit fachlicher Hilfe).

#### b) Hinweisgeberschutzgesetz

Das HinSchG schafft keine Rechtsgrundlage für die IT-Sicherheitsforschung. Der Anwendungsbereich ist zwar eröffnet, da Schwachstellen in Software die Produktsicherheit gemäß § 2 Abs. 1 Nr. 3b HinSchG betreffen. Der Hinweisgeber ist allerdings nicht geschützt, sofern die Beschaffung der Information als solche oder der Zugriff hierauf eine eigenständige Straftat ist (§ 35 Abs. 1 HinSchG). Der Gesetzgeber hat damit den Informationszugriff gemäß den §§ 202a, 202b StGB vom Hinweisgeberschutz ausgenommen.[46]

### 7. Keine Strafbarkeit durch Unterlassen

Bei der Untersuchung von IT-Anwendungen erhalten die Forschenden das Wissen und durch das Responsible Disclosure die Möglichkeit, die Gefahr aus erkannten Sicherheitslücken zu beenden oder zu reduzieren. Gleichwohl sind sie de lege lata nicht verpflichtet, eine Lücke zu melden oder zu veröffentlichen.[47] Es besteht auch keine Garantenpflicht aus § 13 StGB, durch das Responsible Disclosure zu verhindern, dass kriminelle Dritte die Lücke ausnutzen, um Straftaten zu begehen.

Als sogenannter Beschützergarant übernimmt der Täter Schutzpflichten gegenüber dem Opfer. Dies muss aber für das Opfer erkennbar sein und es dazu veranlasst haben, dem Verpflichteten besondere Schutzpflichten zu überantworten.[48] Bei der hier behandelten IT-Sicherheitsforschung ist aber weder dem IT-Hersteller/-Anbieter noch dem Nutzer die Tätigkeit des Forschers bekannt. Auch eine Strafbarkeit als Überwachergarant ist nicht einschlägig. Denn als solcher müsste der IT-Sicherheitsforscher für eine Gefahrenquelle verantwortlich sein, die von ihm beherrscht wird. Dies wird z. B. angenommen, wenn der Täter durch pflichtwidriges Vorverhalten eine Gefahrenquelle geschaffen hat.[49] Auch dieser Fall liegt nicht vor. Zwar besteht die Gefahr, dass die Forschenden bei ihren Untersuchung Straftatbestände verwirklichen (siehe oben Ziffer 1 bis 5); diese sind aber nicht ursächlich für die Gefahrenquelle. Die Gefahr ist in der Sicherheitslücke begründet; sie besteht unabhängig von der Untersuchung der Forschenden.

## V. Rahmenbedingungen im Urheberrecht

Wenn Computerprogramme Gegenstand der IT-Sicherheitsforschung sind, sind die Rechtspositionen des Softwareherstellers gemäß den §§ 69a ff. UrhG betroffen. Das Kopieren einer Software, um den Code in einer spezifischen Umgebung zu untersuchen, das Disassemblieren eines Maschinencodes und das Dekompilieren sind Maßnahmen, die die Zustimmung bzw. Lizenz des Nutzungsinhabers voraussetzen. Diese liegt bei IT-Sicherheitsforschungen „in the wild“ selten vor.[50]

In Bug-Bounty-Programmen loben Softwarehersteller Prämien für die Information über Sicherheitslücken aus. Diese Zusage kann nicht anders verstanden werden, als die Zustimmung des Herstellers, alle urheberrechtlich relevanten Handlungen vorzunehmen, die für eine Untersuchung der Software nötig sind.[51] Oftmals bleiben aber die Bug-Bounty-Bedingungen auslegungsbedürftig und die Reichweite der Zustimmung unklar, so dass erhebliche Rechtsunsicherheiten zu Lasten der IT-Sicherheitsforschung bestehen. Eine gesetzliche Nutzungsbefugnis fehlt ebenso.[52]

Eingriffe in das Urheberrecht können aber durch den zivilrechtlichen Notstand gemäß § 228 BGB gerechtfertigt sein; insofern wird auf Abschnitt IV Ziffer 6 oben verwiesen.[53]

42 *Klaas*, MMR 2022, 187, 189.

43 *Goerke/Obermaier/Schink/Schuster/Wagner*, in: Balaban et al., Whitepaper zur Rechtslage der IT-Sicherheitsforschung S. 32 (https://sec4research.de/assets/Whitepaper.pdf).

44 *Schneider*, Kriminalistik 2023, 433, 434.

45 Dabei gibt es eine Vielzahl von Quellen, von Mailinglisten wie Full-Disclosure bis hin zu https://cve.mitre.org und den daraus kondensierten Meldungen z. B. des BSI.

46 *Bruns*, NJW 2023, 1609, 1615; a. A. *Wagner*, PinG 2020, 66, 72, wonach die Privilegierung des Whistleblowers gemäß § 5 GeschGehG auch auf die Rechtfertigung zu den §§ 202a, 202b StGB durchschlagen müsse. Einen anderen Weg hat z. B. Belgien eingeschlagen, siehe unten Abschnitt VI Ziffer 2.

47 Zum Zivilrecht: *Dickmann*, in: Balaban et al., Whitepaper zur Rechtslage der IT-Sicherheitsforschung S. 20 (https://sec4research.de/assets/Whitepaper.pdf).

48 BGH, 17. 7. 2009 – 5 StR 394/08, NJW 2009, 3173, 3174; BGH, 11. 9. 2019 – 2 StR 563/18, NJW-Spezial 2020, 121.

49 Sog. *Ingerenz*, BGH, 3. 7. 2019 – 5 StR 132/19, NJW 2019, 3092, 3094; BGH, 17. 7. 2009 – 5 StR 394/08, NJW 2009, 3173.

50 *Vonderau/Wagner*, in: Taeger (Fn. 36), 525, 526; *Wagner/Tran/Franzen*, in: Balaban et al., Whitepaper zur Rechtslage der IT-Sicherheitsforschung S. 13 (https://sec4research.de/assets/Whitepaper.pdf); welche durch EuGH, 6. 10. 2021 – C-13/20, K&R 2021, 785 ff., die Tür für IT-Sicherheitstests „einen Spalt breit geöffnet“ sehen; allerdings war es im EuGH-Fall der Lizenznehmer, der die Software zur Fehlersuche disassembliert hat; bei der IT-Sicherheitsforschung geht es um Konstellationen, in denen Forschende keine Lizenzen haben.

51 Beispiel für Bug Bounty: https://bughunters.google.com/; https://www.mozilla.org/en-US/security/bug-bounty/; zum Urheberrecht *Halder*, jurisPR-ITR 6/2022 Anm. 3.

52 *Balaban* et al., Whitepaper zur Rechtslage der IT-Sicherheitsforschung S. 13 (https://sec4research.de/assets/Whitepaper.pdf).

53 Zu § 228 BGB im Urheberrecht *Dreier/Schulze*, UrhG, § 97 UrhG, Kommentar, 7. Aufl. 2022, Rn. 15; zur Auswirkung des strafrechtlichen Notstands (§ 34 StGB) auf § 228 BGB *Ellenberger*, in: Grüneberg, Kommentar zum BGB, 85. Aufl. 2025, § 228 BGB Rn. 2.

## VI. Lösungsansätze de lege ferenda

Politische Reformbemühungen zugunsten der IT-Sicherheitsforschung konzentrieren sich auf § 202a StGB. Um den entsprechenden Referentenentwurf aus dem Bundesjustizministerium zu bewerten, werden zunächst die internationalen Rahmenbedingungen sowie die Lösungsansätze anderer Staaten dargestellt.

### 1. Internationale Rahmenbedingungen

Für die Bundesrepublik Deutschland gibt es eine doppelte internationale Verpflichtung, den unbefugten Zugang zu Computersystemen als Straftat zu ahnden:

#### a) Cybercrime Convention

Die Cybercrime Convention vom 23. 11. 2001 ist ein völkerrechtlicher Vertrag, dem alle Parteien des Europarats beigetreten sind (Budapest Convention). In Deutschland ist der Vertragstext gemäß Art. 59 Abs. 2 GG im Rang eines Bundesgesetzes ratifiziert.[54]

Art. 2 der Cybercrime Convention verpflichtet die Vertragsstaaten, den vorsätzlichen unbefugten Zugang zu Computersystemen unter Strafe zu stellen. Dabei ist es zulässig, die Tat nur zu bestrafen, wenn der Täter beabsichtigte, durch die Tat Computerdaten zu erlangen oder sonst in unredlicher Absicht handelte.

Die Cybercrime Convention des Europarats ist zu unterscheiden von den Bestrebungen der Vereinten Nationen (UN), ihrerseits ein Abkommen zur Verfolgung von Computerstraftaten zu verabschieden („United Nations Convention Against Cybercrime“). Dieses Abkommen befindet sich zum Zeitpunkt des Redaktionsschlusses im Entwurfsstadium, d. h. die hierfür eingesetzte UN-Ad-hoc-Gruppe[55] hat der UN-Generalversammlung einen Text zum Beschluss einer UN-Resolution vorgeschlagen. Der Europarat hat die Ad-hoc-Gruppe bei der Ausarbeitung des Entwurfs begleitet, um auf dessen Konsistenz der bereits bestehenden Budapest Convention hinzuwirken (ebenfalls als „Cybercrime Convention“ bezeichnet). Die „Budapest Convention“ besteht somit losgelöst von der Verabschiedung einer UN-Cybercrime Convention.[56]

#### b) Cybercrime-Richtlinie der EU

Art. 3 der Cybercrime-Richtlinie (RL 2013/40/EU)[57] lautet: „(…) verpflichtet die EU-Mitgliedstaaten, den vorsätzlichen unbefugten Zugang zu IT-Systemen, der unter Verletzung von Sicherheitsmaßnahmen erfolgt, unter Strafe zu stellen, wenn kein leichter Fall vorliegt“.

Nach ErwG 11 der Richtlinie kann ein Fall als „leicht“ eingestuft werden, wenn der durch die Straftat verursachte Schaden und/oder die Gefahr für öffentliche oder private Interessen, wie etwa die Integrität eines Computersystems oder von Computerdaten oder die Integrität, die Rechte oder andere Interessen einer Person geringfügig oder so geartet ist, dass die Verhängung einer Strafe innerhalb der gesetzlichen Grenzen oder die Begründung einer strafrechtlichen Verantwortung nicht erforderlich ist.

Die Richtlinie ist gemäß Art. 288 AEUV für alle EU-Mitgliedstaaten verbindlich und verpflichtet diese zum Erlass entsprechender nationaler Gesetze.

#### c) EU- und völkerrechtlich verpflichtende Tatbestandsmerkmale

Die EU- und völkerrechtlichen Rahmenbedingungen verpflichten somit dazu, Verhaltensweisen mit folgenden Tatbestandsmerkmalen unter Strafe zu stellen:

- Zugang zu einem Computer- bzw. Informationssystem ohne Befugnis
- unter Verletzung von Sicherheitsmaßnahmen
- Option, „leichte Fälle“ auszunehmen.

#### d) Vorgaben aus dem IT-Sicherheitsrecht der EU

Ein geordneter Rechtsrahmen zur Meldung von Sicherheitslücken ist kein „nice-to-have“ für einige „Nerds“ aus der IT-Sicherheitsforschung. Im Gegenteil: Das IT-Sicherheitsrecht der EU gibt an verschiedenen Stellen Vorgaben für einen koordinierten Umgang mit entdeckten Lücken vor,[58] z. B.:

- Der Cyber Security Act (VO (EU) 2019/881) stellt in ErwG 30 klar, dass die Aufdeckung und die Behebung von Sicherheitslücken eine wichtige Rolle bei der Verringerung der Gesamtrisiken im Bereich der Cybersicherheit spielen. Gefordert ist eine Koordinierung zwischen demjenigen, der die Sicherheitslücke aufgespürt hat, und der Organisation im Hinblick auf die Veröffentlichung jener Sicherheitslücke. Dementsprechend sieht Art. 54 des Cyber Security Act die Schaffung eines Schemas zur Cybersicherheitszertifizierung vor, das auch Vorschriften für die Meldung und Behandlung bislang nicht erkannter Cybersicherheitslücken enthält.
- Art. 7 Abs. 2 der NIS 2 Richtlinie (RL (EU) 2022/2555) verpflichtet die EU-Mitgliedstaaten zu nationalen Cybersicherheitsstrategien mit einem koordinierten Vorgehen zur Offenlegung von Schwachstellen. Gemäß Art. 12 Abs. 1 NIS-2-RL soll der nationale Koordinator für die Offenlegung von Schwachstellen ein Verfahren einrichten, das natürlichen Personen die anonyme Meldung von Schwachstellen ermöglicht.
- Gemäß Art. 14 und Anlage II des Cyber Resilience Act (VO (EU) 2024/2847) sind die Hersteller von IKT-Produkten zur Vorhaltung eines koordinierten Verfahrens für den Umgang mit Informationen über Schwachstellen verpflichtet.

### 2. Regelungen anderer Staaten

Alle EU-Mitgliedstaaten haben die Cybercrime-Richtlinie umgesetzt und den unbefugten Zugang zu Informationssystemen bei Strafe verboten. Nur sechs Mitgliedstaaten und das United Kingdom (UK) sehen Ausnahmeregelungen für die IT-Sicherheitsforschung vor:[59]

- In Frankreich untersagt Art. 323-1 des Code pénal (Strafgesetzbuch), sich in betrügerischer Absicht Zugang zu einem IT-System zu verschaffen. Die Tat wird nach der

54 BGBl. 2008-II, 1242, dazu *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 27), Kap. 50.1 Rn. 360. Russland ist dem Abkommen seinerzeit als einziges Mitglied des Europarats nicht beigetreten, ist jedoch ohnehin seit 16. 3. 2022 vom Europarat ausgeschlossen (https://www.coe.int/de/web/portal/-/the-russian-federation-is-excluded-from-the-council-of-europe). Cybercrime Convention UN (Entwurf): https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_reconvened_concluding_session/main.

55 Die Ad-hoc-Gruppe wurde eingesetzt durch UN-Resolution 74/247, dazu *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 27), Kap. 50.1 Rn. 357.

56 Zum Text und Entwurfsstadium der UN-Cybercrime Convention siehe das Dokument A/78/986 auf der UN-Webseite https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_reconvened_concluding_session/main; zur Begleitung durch den Europarat https://www.coe.int/en/web/cybercrime/-/united-nations-treaty-on-cybercrime-agreed-by-the-ad-hoc-committee (insofern *falsch*: becklink 2031801 vom 10. 9. 2024, wo das „Budapester Übereinkommen“ des Europarats als „UN-Übereinkommen über Computerkriminalität“ bezeichnet wird).

57 Dazu *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 27), Kap. 50.1 Rn. 294.

58 Jenseits der rechtlichen Vorgaben ist eine aktive Sicherheitsforschung ein wichtiger Beitrag zur Cyberresilienz der EU und Deutschlands, dazu u. a. *Eggendorfer/Andresen* (Fn. 2).

59 Eine gut sortierte Übersicht liefern *Burghard Piltz* und *Carlo Piltz* unter https://www.piltz.legal/news-blog/strafbarkeit-von-white-hat-hacking-in-europa.

dortigen Strafprozessordnung (Art. L2321-4 des „Code de la défense“[60]) aber nicht verfolgt, wenn der Täter im guten Glauben gehandelt und die Schwachstelle der nationalen Agentur für die Sicherheit von Informationssystemen gemeldet hat (Agence nationale de la sécurité des systèmes d'information).[61]

- Belgien hat das „ethische Hacking“ im Klokkenluiderswet (Hinweisgeberschutzgesetz) in Umsetzung der „Whistleblower-Richtline“ (RL (EU) 2019/1937) geregelt. Hiernach ist die Forschung nach Sicherheitslücken in (fremden) IT-Systemen erlaubt, wenn der Täter keine Vergütung für die Meldung der Lücke verlangt, die Ausforschung auf das Notwendige begrenzt und die Lücke der nationalen Cybersicherheitsbehörde und der untersuchten Einrichtung meldet. Außerdem darf der Täter die Lücke nur mit Zustimmung der Cybersicherheitsbehörde veröffentlichen.[62]
- Lettland stellt das Eindringen in fremde IT-Systeme nur dann unter Strafe, wenn ein wesentlicher Schaden (derzeit: ab € 2500,00) entstanden ist.[63]
- Litauen hat den Umgang mit der Entdeckung von IT-Sicherheitslücken seit Juni 2021 ausdrücklich geregelt.[64] Der anderslautende Bericht des wissenschaftlichen Dienstes des Bundestags vom 23. 4. 2024 („In Litauen existieren keine gesonderten Reglungen in Bezug auf das ‚gewollte‘ Aufdecken von Sicherheitslücken“)[65] ist daher nachweislich falsch. Dieser Fehler ist relevant, weil der Referentenentwurf zur Novellierung des § 202a StGB (unten Ziffer 3) mehrfach auf diesen Bericht Bezug nimmt.[66]
  Nach der litauischen Regelung müssen IT-Sicherheitsforschende die Integrität des untersuchten IT-Systems wahren (z. B keine Unterbrechung von Datenverarbeitungsvorgängen) und die Lücke der untersuchten Einrichtung und der nationalen Cybersicherheitsbehörde melden. Die Veröffentlichung der Lücke ist nur zulässig, wenn die untersuchte Einrichtung ausreichend (bis zu 90 Tagen) Gelegenheit hatte, die Meldung des Forschenden auszuwerten.[67]
- Die Niederlande, Spanien und das UK sehen ebenfalls davon ab, das Eindringen in fremde IT-Systeme zu bestrafen, wenn die Lücke an die nationale Cybersicherheitsbehörde gemeldet wird und die behördlichen Vorgaben zum Umgang mit der Lücke („Disclosure Policies“) beachtet werden.[68]
- § 118a des österreichischen StGB bestraft ebenfalls den unautorisierten Zugang zu einem fremden IT-System, jedoch nur, wenn der Täter in der Absicht handelt, sich Kenntnis von den dortigen Daten zu verschaffen. Diese Absicht hat nicht, „wer bloß ausprobieren möchte, ob er den Einstieg in das Computersystem schafft.“[69]

## 3. Referentenentwurf

Am 4. 11. 2024 hat das Bundesjustizministerium einen Referentenentwurf zur Reform des § 202a StGB vorgelegt, der im Koalitionsvertrag angekündigt war.[70] Obwohl die sogenannte „Ampelkoalition“ bereits zwei Tage später beendet war,[71] lohnt sich eine Untersuchung des Entwurfs aus wissenschaftlicher Sicht, um Fehler bei einer späteren Novellierung zu vermeiden.

### a) Text des Referentenentwurfs

Der Referentenentwurf sah vor, dem § 202a StGB die folgenden Absätze (3) und (4) anzufügen:

„(3) Die Handlung ist nicht unbefugt im Sinne des Abs. 1, wenn 1. sie in der Absicht erfolgt, eine Schwachstelle oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems (Sicherheitslücke) festzustellen und die für das informationstechnische System Verantwortlichen, den betreibenden Dienstleister des jeweiligen Systems, den Hersteller der betroffenen IT-Anwendung oder das Bundesamt für Sicherheit in der Informationstechnik über die festgestellte Sicherheitslücke zu unterrichten und 2. sie zur Feststellung der Sicherheitslücke erforderlich ist.“

Zudem soll ein neuer Absatz (4) schwere Fälle erfassen, die mit einem höheren Strafmaß versehen sind.

Die Regelungen sollten für den §§ 202a und 303a StGB entsprechend gelten.

### b) Auswirkungen des Referentenentwurfs

Der Referentenentwurf würde die IT-Sicherheitsforschung (nur) dann straffrei stellen, wenn die Tathandlung in der Absicht erfolgt, eine Schwachstelle oder ein anderes Sicherheitsrisiko festzustellen und dem für das System Verantwortlichen, dem betreibenden Dienstleister, dem Hersteller oder dem BSI zu melden. Laut Seite 6 des Referentenentwurfs werde „eine bloße Behauptung, in guter Absicht gehandelt zu haben, das Gericht nicht überzeugen.“ Damit obliegt dem Beschuldigten der Nachweis seiner redlichen Absicht. Dies steht im Widerspruch zur verfassungsrechtlichen Unschuldsvermutung gemäß Art. 20 Abs. 3 GG. Hiernach gilt: Bis zum Nachweis der Schuld wird die Unschuld des Beschuldigten vermutet.[72] Kein anderer EU-Staat verlangt von seinen IT-Sicherheitsforschenden den Nachweis, sich nach der Verwirklichung eines Straftatbestands zu entlasten. Im Gegenteil: § 118a des österreichischen StGB verlangt von der Strafverfolgungsbehörde den Nachweis, dass der Täter in das IT-System des Opfers mit der qualifizierten Absicht der Schädigung eingedrungen ist, was bei der redlichen IT-Sicherheitsforschung ausgeschlossen wird (siehe oben Ziffer 1).

Die europarechtlich vorgegebenen Ziele, das Entdecken und Beseitigen von Sicherheitslücken zu fördern und dabei anonyme Meldungen zu ermöglichen, wird durch den Referentenentwurf ebenso verfehlt. Kaum ein IT-Sicherheitsforschender wird es goutieren, sich in einer behördlichen Datenbank des BSI wiederzufinden mit der Information, man habe den Tatbestand des § 202a StGB verwirklicht, sei aber in diesem Fall aufgrund seiner Absicht zur Meldung straffrei.[73]

60 https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033206854.
61 WD 7 – 3000 – 104/23 (Fn. 38), S. 22.
62 *Somers/Vrankaert/Drechsler*, Belgium legalises ethical hacking: a threat or an opportunity for cybersecurity (https://www.law.kuleuven.be/citip/blog/belgium-legalises-ethical-hacking-a-threat-or-an-opportunity-for-cybersecurity/).
63 https://www.piltz.legal/news-blog/strafbarkeit-von-white-hat-hacking-in-europa.
64 So ausdrücklich S. 11 des Berichts des litauischen Verteidigungsministeriums zum Cybersecurity Status 2021-Q 1-2022 (https://www.nksc.lt/doc/en/Key-trends-and-statistics-2021-q1-2022.pdf).
65 WD 7 – 3000 – 104/23 (Fn. 38), S. 24.
66 https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/RefE/RefE_ComputerStrafR.pdf?__blob=publicationFile&v=3 (dort z. B. auf S. 6).
67 https://www.tgsbaltic.com/en/publications/ethical-hacking-in-the-baltics-comparative-legal-map/.
68 https://www.piltz.legal/news-blog/strafbarkeit-von-white-hat-hacking-in-europa.
69 *Reindl-Krauskopf*, in: Höfel/Ratz (Hrsg.), Wiener Kommentar zum StGB, 2. Aufl., Stand 1. 3. 2022, § 118a StGB Rn. 35.
70 https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/2024_ComputerStrafR.html.
71 https://www.tagesschau.de/inland/ampel-aus-100.html; https://de.wikipedia.org/wiki/Bruch_der_Ampelkoalition_in_Deutschland_2024.
72 BVerfGE 35, 311, 320 = NJW 1974, 26; BVerfGE 74, 358, 371 = NJW 1987, 2427. Siehe hierzu auch die Kritik an § 202c in Fn. 31 und 32, die ein in ähnlicher Weise belastendes Denken des Gesetzgebers gegenüber Sicherheitsforschenden zu erkennen gibt. Auch *Marnau*, CR 2024, 839, 842 erkennt eine „überschießende Innentendenz“ in § 202a Abs. (3) des Referentenentwurfs, die der Rechtssicherheit entgegensteht.
73 Ähnlich die Kritik der AG KRITIS: https://ag.kritis.info/2024/10/24/hackerparagraph-stellungnahme-referentenentwurf-computerstrafrecht/?trk=feed_main-feed-card_feed-article-content.

Realitätsfremd wirkt die Annahme auf Seite 8 des Referentenentwurfs, es gebe „noch kein allgemein anerkanntes standardisiertes Verfahren (responsible disclosure) zur Meldung von Sicherheitslücken." Die Darstellungen oben in Abschnitt II und III widerlegen dies. Zudem setzt der EU-rechtliche Rahmen (oben Ziffer 1 d) voraus, dass es ein jedenfalls in der Praxis anerkanntes Verfahren zur Erforschung und Meldung von Sicherheitslücken gibt.

Schließlich beansprucht der Referentenentwurf zu Unrecht für sich, mit dem Entwurf des BSI-Gesetzes konsistent zu sein, z. B. indem der Begriff „Sicherheitslücke" legaldefiniert wird. Das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz ersetzt den Begriff der „Sicherheitslücke" vielmehr durch „Schwachstelle".[74]

## VII. Zusammenfassung und Fazit

Die aktuelle Rechtslage birgt für die IT-Sicherheitsforschung gravierende straf- und zivilrechtliche Risiken. Sie ist nicht geeignet, die IT-Sicherheit zu verbessern und daher zu reformieren. Der Referentenentwurf zur Neuregelung des § 202a StGB hat dazu einen ersten Anlauf unternommen, ist aber leider nicht geeignet, die Rechtslage zu verbessern.

Technisch ist stets zu beachten: Die Sicherheitslücke ist vom Hersteller verursacht, sie haftet dem Softwareprodukt von Anfang an, der Sicherheitsforscher ist nur ihr Entdecker. Es stellt sich damit die Frage, ob die Entdecker der Lücken die falschen Adressaten etwaiger Strafdrohungen sind,[75] und vielmehr durch geeignete Maßnahmen, wie Sanktionen und Haftungsbestimmungen, wie z. B. durch den Cyber Resilience Act Softwarehersteller in die Pflicht genommen werden müssen, z. B. durch eine Verpflichtung, gemeldete Lücken innerhalb einer bestimmten Frist zu beheben.

Bei der Neuregelung des § 202a StGB scheint ein sorgfältiger Blick in die EU-Nachbarländer sinnvoll,[76] die entsprechende Regelungen bereits umgesetzt haben, insbesondere nach Litauen und Belgien. Dort sind Regelungen in Übereinstimmung mit den Vorgaben der Cybercrime Convention und der Cybercrime-Richtlinie eingerichtet, die die IT-Sicherheitsforschung unter Anwendung der Responsible-Disclosure-Grundsätze legalisiert haben.

Dreh- und Angelpunkt für die Legalisierung dürfte die Intention der Sicherheitsforschenden sein: Sie verfolgen das Ziel, durch Identifikation von Sicherheitslücken größeren Schaden zu vermeiden. Gehen sie dabei technisch korrekt und verantwortungsvoll vor, so verhindert dies Schäden, auch für das betroffene System. Wenn Beschädigungen des betroffenen IT-Systems dennoch nicht vermeidbar sind, sind sie in der Regel durch eine geringe Schadenshöhe gekennzeichnet. Dementsprechend haben die IT-Sicherheitsforschenden keine Schädigungsabsicht. Alle genannten Kriterien sind indiziert, wenn die Forschenden nach den Grundsätzen des Responsible Disclosure vorgehen. Angezeigt ist somit eine gesetzliche Regelung des Responsible Disclosure, die den Forschenden Rechtssicherheit verschafft, ohne dass sie sich von einem Strafvorwurf (etwa im Rahmen eines Rechtfertigungsgrunds) entlasten müssen. Denn die Sicherheitslücken sind Probleme, die der Softwareanbieter zu verantworten hat. Anstelle des Verursachers den Entdecker zu bestrafen, erscheint widersinnig.

**Dr. Florian Deusch**
ist Rechtsanwalt und Fachanwalt für Informationstechnologierecht in der Anwaltskanzlei Dr. Gretter in Ravensburg. Er ist zudem als Datenschutzbeauftragter tätig.

**Prof. Dr. Tobias Eggendorfer**
ist Professor für Sicherheit in verteilten Anwendungen an der TH Ingolstadt, davor war er als Abteilungsleiter „Sichere Systeme" an der Agentur für Innovation in der Cybersicherheit für die Weiterentwicklung der Forschung im Bereich der IT-Sicherheit zuständig. Er ist zudem als IT-Berater und Datenschutzbeauftragter tätig.

74 BT-Drs. 20/1384, https://dserver.bundestag.de/btd/20/131/2013184.pdf, dort S. 133. Allerdings ist auch dieser Gesetzesentwurf nicht konsequent, siehe § 65 Abs. 4 Nr. 2 BSIG-E, S. 62 des Entwurfs, der den Begriff „Sicherheitslücke" im Rahmen einer Ordnungswidrigkeit verwendet.

75 https://ris.utwente.nl/ws/portalfiles/portal/73653760/s40163_018_0090_8.pdf.

76 Anders als das fehlerhafte Gutachten des wissenschaftlichen Dienstes insbesondere zu Litauen, siehe oben Abschnitt VI 1 d).

RAin Dr. Laura Marie Münster*

# Aktuelle Rechtsfragen zur Zulässigkeit von Drohnenaufnahmen

## Kurz und Knapp

**Bei der Herstellung und Verwertung von Drohnenaufnahmen müssen das Recht auf Privatsphäre, das Recht am eigenen Bild, Datenschutzrechte sowie Eigentums- und Urheberrechte berücksichtigt werden. Erst kürzlich hat der BGH zu der Frage entschieden, ob die Panoramafreiheit des UrhG auch für Drohnenaufnahmen gilt. Ein weiteres BGH-Urteil verdeutlicht die Kriterien für die Abwägung von Pressefreiheit und Persönlichkeitsrecht bei der Frage nach der Zulässigkeit von Drohnenaufnahmen.**

* Mehr über die Autorin erfahren Sie am Ende des Beitrags.