IT-Sicherheitsforschung und IT-Strafrecht

Herausgegeben von
SEBASTIAN GOLLA und
DOMINIK BRODOWSKI

Mohr Siebeck

IT-Sicherheitsforschung und IT-Strafrecht

IT-Sicherheitsforschung und IT-Strafrecht

herausgegeben von

Sebastian Golla und
Dominik Brodowski

Mohr Siebeck

Sebastian Golla, geboren 1988; Juniorprofessor für Kriminologie, Strafrecht und Sicherheitsforschung im digitalen Zeitalter an der Ruhr-Universität Bochum.

Dominik Brodowski, geboren 1980; Universitätsprofessor für Strafrecht und Strafprozessrecht an der Universität des Saarlandes, Saarbrücken.
orcid.org/0000-0002-3711-4197

Die Veröffentlichung wurde finanziell gefördert durch das Center for Advanced Internet Studies (CAIS).

CAIS RESEARCH FOR THE DIGITAL AGE

ISBN 978-3-16-162179-6 / eISBN 978-3-16-162184-0
DOI 10.1628/978-3-16-162184-0

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über *https://dnb.de* abrufbar.

Das Buch wurde von Textservice Zink in Schwarzach gesetzt und von Beltz Grafische Betriebe in Bad Langensalza auf alterungsbeständiges Werkdruckpapier gedruckt und gebunden.

Printed in Germany.

Vorwort

Die digitalisierte Gesellschaft wäre ohne IT-Sicherheit nicht funktionsfähig. Die IT-Sicherheit und ihre Erforschung sind daher nicht nur strukturell, technisch und finanziell zu fördern, sondern auch rechtlich zu schützen. Allerdings ist gerade die Forschung in diesem Bereich erheblichen rechtlichen Risiken ausgesetzt, die insbesondere vom scharfen Schwert des Strafrechts ausgehen. Immer wieder werden gegen Forschende, die Sicherheitslücken offenlegen, Strafverfahren eingeleitet.

Der vorliegende Sammelband wirft Schlaglichter auf grundlegende Probleme und aktuelle Konflikte zwischen der IT-Sicherheitsforschung und dem Strafrecht. Er entstand aus einer Arbeitsgemeinschaft, die am *Center for Advanced Internet Studies* (CAIS) durchgeführt und von diesem gefördert wurde. Am 20. und 21. September 2021 fand sich eine Gruppe von Expert*innen aus den (Straf-)Rechtswissenschaften und der Informatik (insbesondere der IT-Sicherheitsforschung) in Bochum zusammen. Die in diesem Rahmen diskutierten Themen wurden in den sieben Beiträgen dieses Bandes aus unterschiedlichen Perspektiven wissenschaftlich ausgearbeitet.

Der einführende Beitrag von *Sebastian Golla* behandelt grundlegende Konflikte zwischen Strafrecht, Strafverfolgung und IT-Sicherheitsforschung. Den verantwortungsvollen Umgang mit Erkenntnissen der IT-Sicherheitsforschung aus Sicht eines Forschenden diskutiert *Felix Freiling*. *Dominik Brodowski* befasst sich aus materiell-strafrechtlicher Perspektive mit dem IT-Strafrecht als Grenze der IT-Sicherheitsforschung. *Liane Wörner* und *Janine Blocher* wenden sich auch mit Blick auf den Allgemeinen Teil des Strafrechts der Frage zu, inwiefern Forschende für Straftaten, die durch Dritte begangen werden, mitverantwortlich gemacht werden können.

Den Implikationen des Urheberrechts für die IT-Sicherheitsforschung, dessen Verletzung auch strafrechtliche Konsequenzen haben kann, widmen sich *Linda Kuschel* und *Darius Rostam*. *Malaika Nolde* behandelt die Konflikte der IT-Sicherheitsforschung mit dem Strafrecht aus der Perspektive einer Praktikerin auf dem Feld der Strafverteidigung in Cybercrime-Fällen. Diese zahlreichen Spannungsfelder und Probleme greifen *Manuela Bao* und *Louisa Zech* auf und erörtern Lösungsansätze auf Ebene des Tatbestands und der Rechtfertigung.

Wir hoffen, dass dieses Buch nicht nur zur theoretischen Aufarbeitung der aufgeworfenen Probleme beiträgt, sondern auch das gegenseitige Verständnis von (Straf-)Rechtswissenschaften und Informatik fördert und Anstöße für die praktische Anwendung und Fortbildung des Rechts liefert. Um einen breiten Austausch zu ermöglichen, wird der vorliegende Band in Open Access veröffentlicht. Ohne die großzügige Förderung des *CAIS* wäre dies nicht möglich gewesen. Wir bedanken uns herzlich beim *CAIS* und allen an der Arbeitsgemeinschaft sowie dem Sammelband beteiligten Personen.

Sebastian Golla
Dominik Brodowski

Inhaltsverzeichnis

Problemaufriss

Die Rolle des Strafrechts beim Schutz der IT-Sicherheit – Dissonanzen, Defizite und Perspektiven

Sebastian Golla

Diverse strafrechtliche Regelungen sollen einen Beitrag zum Schutz von informationstechnischen Systemen leisten. Zugleich geraten sie sowie Interessen an der Strafverfolgung allerdings in Konflikt mit Interessen der IT-Sicherheit. Das zeigt sich exemplarisch auf dem Feld der IT-Sicherheitsforschung. Der Beitrag untersucht bestehende Konflikte, Defizite der geltenden Regelungen und mögliche Perspektiven des IT-Strafrechts.

I. IT-Sicherheit, Forschung und Strafrecht

Die IT-Sicherheit ist Grundbedingung für die Funktionsfähigkeit der digitalen Gesellschaft und für den Schutz vieler anderer Güter. Damit sie gewährleistet werden kann, bedarf es wissenschaftlicher und technischer Anstrengungen. Aber auch Politik und Recht müssen die IT-Sicherheit als Priorität behandeln und die Rahmenbedingungen für ihre bestmögliche Gewährleistung schaffen. Jüngst hat etwa der Koalitionsvertrag 2021–2025 die staatliche Pflicht zur Förderung der IT-Sicherheit prominent betont. Dabei wurde auch die IT-Sicherheitsforschung erwähnt und gefordert, dass „[d]as Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren, z.B. in der IT-Sicherheitsforschung, […] legal durchführbar sein" solle.[1] Wie ein verantwortungsvoller Umgang mit IT-Sicherheitslücken rechtlich im Einzelnen geregelt werden könnte, wird an anderer Stelle zu thematisieren sein.[2]

Im Zentrum des Interesses dieses Sammelbandes steht die IT-Sicherheitsforschung. Aus Sicht des Strafrechts und verwandter Rechtsgebiete wird den Fragen nachgegangen, welchen Risiken Forschende ausgesetzt

[1] *SPD, Bündnis 90/Die Grünen, FDP*, Koalitionsvertrag 2021–2025: „Mehr Fortschritt wagen. Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit", S. 16 f., https://cms.gruene.de/uploads/documents/Koalitionsvertrag-SPD-GRUENE-FDP-2021–2025.pdf (zuletzt abgerufen am 31.10.2022).

[2] Siehe hierzu *Bao/Zech* (in diesem Band) S. 131, 166 ff.

sind und wie sich diese bei der Anwendung und Fortbildung des Rechts handhaben bzw. abmildern lassen. Diese Thematik hat zuletzt in der IT-Sicherheitsforschung selbst sowie in der breiten Öffentlichkeit für Diskussionen gesorgt. Auslöser hierfür waren Fälle wie jener der IT-Sicherheitsexpertin Lilith Wittmann. Nachdem Wittmann eine Sicherheitslücke in der Wahlkampf-App CDU-Connect entdeckt und in einem hierfür anerkannten Verfahren offengelegt hatte (responsible disclosure), wurde gegen sie Anzeige erstattet und ein Ermittlungsverfahren eingeleitet, das mittlerweile wieder eingestellt wurde.[3] Derartige Fälle zeigen das öffentliche Interesse daran auf, dass IT-Sicherheitslücken aufgedeckt und Erkenntnisse hierüber verantwortungsvoll behandelt werden. Sie zeigen aber auch, dass es im Auge des Betrachters liegt, ob ein bestimmter Umgang mit einer Sicherheitslücke wünschenswert ist und welche Tätigkeiten sich noch dem Bereich der Forschung zuordnen lassen. Für Letzteres dürfte jedenfalls ein gewisses methodisches Vorgehen mit dem Ziel der Gewinnung neuartiger Erkenntnisse notwendig sein. Die Grenzen zwischen politischem Aktivismus, privater Neugier und wissenschaftlicher Forschung verlaufen in der Realität allerdings mitunter fließend.

Dieser Beitrag widmet sich zur Einführung in die Thematik zunächst den grundlegenden Spannungen, die zwischen einigen Regelungen des Strafrechts und der Gewährleistung der IT-Sicherheit bestehen. Das Strafrecht spielt beim rechtlichen Schutz der IT-Sicherheit traditionell eine wichtige Rolle. Lange bevor weitgehende Kodifikationen zum Schutz der IT-Sicherheit außerhalb des Strafrechts in Sicht waren, wurden in §§ 202a, 303a, 303b StGB durch das zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität vom 15. Mai 1986[4] Delikte zum Schutz der Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen eingeführt. Die Regelungen wurden später unter anderem auf Grundlage der Cybercrime Convention des Europarates vom 23. November 2001[5] ergänzt.[6]

Heute wird das IT-Sicherheitsrecht als Querschnittsmaterie über das Strafrecht hinaus immer wichtiger und bewegt sich auf eine weitere Kodi-

[3] *Zeit Online* vom 5.8.2021, https://www.zeit.de/digital/datenschutz/2021–08/cdu-connect-app-it-sicherheit-lilith-wittmann-forscherin-klage/komplettansicht (zuletzt abgerufen am 31.10.2022).

[4] BGBl. 1986 I, S. 721.

[5] BGBl. 2008 II, S. 1242.

[6] Vgl. zur Entwicklung des Regelungsbereichs insgesamt *Singelnstein/Zech*, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2020, § 20 Rn. 25 ff.

fizierung zu.[7] Auf nationaler Ebene lieferte hierfür das IT-Sicherheitsgesetz von 2015[8] einen wichtigen Impuls.[9] Die Entwicklung fand ihre Fortsetzung zuletzt in dem im April 2021 verabschiedeten IT-Sicherheitsgesetz 2.0[10], durch das unter anderem das Bundesamt für Sicherheit in der Informationstechnik (BSI) noch einmal gestärkt wurde.[11] Der erste Referentenentwurf des IT-Sicherheitsgesetzes 2.0 von März 2019[12] hatte dazu noch zahlreiche Änderungen des Straf- und Strafverfahrensrechts vorgesehen; unter anderem sollten neue Straftatbestände des Zugänglichmachens von Leistungen zur Begehung von Straftaten (§ 126a StGB-E) und der unbefugten Nutzung informationstechnischer Systeme (§ 202e StGB-E) eingeführt sowie der Strafrahmen für mehrere Delikte erhöht werden.[13] Ein zweiter Referentenentwurf von Mai 2020[14] nahm schließlich Abstand von sämtlichen Änderungen des Straf- und Strafverfahrensrechts.

Das Strafrecht ist heute im Gesamtsystem der rechtlichen Unterstützung der IT-Sicherheit weniger zentral als früher, aber eine nicht zu vernachlässigende Komponente. Jedoch steht das Strafrecht stellenweise im Konflikt mit dem Schutz der IT-Sicherheit. Sowohl im materiellen Strafrecht als auch im Strafverfahrensrecht gibt es Regelungen, die in der Lage sind, unerwünschte Nebeneffekte für den Schutz der IT-Sicherheit auszulösen. Dieser Beitrag wird zunächst aktuelle Dissonanzen zwischen dem Strafrecht und dem Schutz der IT-Sicherheit untersuchen (II.). Dabei legt er ein besonderes Augenmerk auf Tätigkeiten der IT-Sicherheitsforschung wie das Aufdecken von und den weiteren Umgang mit Sicherheitslücken. Darauf aufbauend wird der Beitrag Vorschläge unterbreiten, um die bestehenden Dissonanzen aufzulösen und das derzeit belastete Verhältnis von IT-Sicherheit und Strafrecht neu zu kalibrieren (III.).

---

[7] Vgl. *Klett/Amann* CR 2014, 93, 95; *Wischmeyer* Die Verwaltung 50 (2017), 155, 156.

[8] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17.7.2015; BGBl. 2015 I, S. 1324.

[9] Vgl. *Schallbruch* CR 2017, 648.

[10] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18.5.2021; BGBl. 2021 I, S. 1122.

[11] Siehe im Einzelnen *Hornung* NJW 2021, 1985 ff.

[12] Vgl. hierzu *Kipker/Scholz* MMR 2019, 431 ff.

[13] Vgl. zu den straf- und strafverfahrensrechtlichen Regelungen in dem Entwurf insgesamt *Selzer* KriPoZ 2019, 221 ff.

[14] Vgl. hierzu *Kipker* MMR-Aktuell 2020, 429348.

II. Dissonanzen zwischen strafrechtlichen Regelungen und dem Schutz der IT-Sicherheit

Zwischen Interessen an der Strafverfolgung, dem materiellen Strafrecht und der Gewährleistung der IT-Sicherheit bestehen stellenweise Dissonanzen, die im Folgenden näher herauszuarbeiten sind (1.). Ein besonderes Augenmerk ist auf Strafbarkeitsrisiken zu legen, die beim Aufdecken von Lücken in der IT-Sicherheit durch Forschende bestehen (2.).

1. Konflikte zwischen Strafrecht und IT-Sicherheit

Zunächst können Interessen an der Strafverfolgung in Konflikt mit dem Schutz der IT-Sicherheit geraten. Zuletzt wurde vermehrt die Konstellation diskutiert, dass Strafverfolgungs- und Sicherheitsbehörden sich Kenntnisse über IT-Sicherheitslücken verschaffen und diese gegenüber der Öffentlichkeit zurückhalten könnten, um Ermittlungsmaßnahmen durchzuführen.[15] Entsprechende Sicherheitslücken könnten ausgenutzt werden, um Quellen-Telekommunikationsüberwachungen (§ 100a Abs. 1 Satz 2 StPO) und „Online-Durchsuchungen" (§ 100b StPO) durchzuführen. Der damit verbundene Anreiz, Sicherheitslücken nicht zu melden und zu beheben, ist angesichts des verfassungsrechtlich gebotenen Schutzes der IT-Sicherheit problematisch. Eine IT-Sicherheitslücke kann ähnlich wie ein defektes Türschloss nicht nur von Strafverfolgungsbehörden, sondern genauso von Kriminellen ausgenutzt werden. Vor diesem Hintergrund hat das Bundesverfassungsgericht im Juni 2021 zurecht eine Verpflichtung des Gesetzgebers angenommen, den Umgang von Polizeibehörden mit Sicherheitslücken, die den Herstellern nicht bekannt sind, zu regeln.[16] Eine entsprechende Regelung ist bisher allerdings noch nicht erfolgt.

Auch Regelungen des materiellen Strafrechts stehen mitunter in einem schwierigen Verhältnis zum Schutz der IT-Sicherheit. So können beispielsweise das Ausfiltern (mutmaßlich) mit Schadsoftware infizierter E-Mails[17] oder die Weitergabe von IP-Adressen zum Zwecke des Austauschs über

[15] Vgl. *Blechschmitt* MMR 2018, 361, 365; *Derin/Golla* NJW 2019, 1111 ff.; *Heim* NJW-Spezial 2018, 120.

[16] BVerfG, Beschluss v. 8.6.2021 – 1 BvR 2771/18 Rn. 41 ff. Die konkrete Verfassungsbeschwerde wies das Gericht jedoch als unzulässig zurück, da die Beschwerdeführenden nicht hinreichend dargelegt hätten, dass die grundrechtliche Schutzpflicht verletzt sein könnte.

[17] Vgl. OLG Karlsruhe MMR 2005, 178.

Sicherheitsrisiken[18] den Straftatbestand der Verletzung des Fernmeldegeheimnisses (§ 206 StGB) erfüllen. Dies kann etwa die Arbeit von Computer Emergency Response Teams (CERTs) behindern, die eine wichtige Funktion für den Schutz der IT-Sicherheit in Behörden und Unternehmen erfüllen, indem sie Vorsorge zum Schutz der IT-Sicherheit treffen und bei Sicherheitsvorfällen schützend eingreifen.[19]

Ein besonderes Paradoxon ist zu beobachten, wenn Regelungen, die grundsätzlich zum Schutz von IT-Systemen und Daten dienen, gleichzeitig problematische Folgen für die IT-Sicherheit mit sich bringen. Dies ist bei den §§ 202a ff., §§ 303a f. StGB der Fall, sofern sie für die IT-Sicherheit nützliche Handlungen unter Strafe stellen. Dies gilt namentlich für die IT-Sicherheitsforschung. In diesem Bereich besteht grundsätzlich das Problem, dass die Handlungen von Forschenden sich unter Umständen objektiv wenig von Handlungen unterscheiden, die Hacker mit kriminellen Motiven vornehmen. Ob ein Zugriff auf ein IT-System aus einem legitimen Forschungsinteresse heraus erfolgt oder ob dadurch Straftaten vorbereitet werden sollen, ist von außen kaum zu erkennen.

Aus der objektiven Gleichartigkeit bestimmter Handlungen von Cyberkriminellen und IT-Sicherheitsforschern resultieren Strafbarkeitsrisiken, die Forschende davon abhalten können, Maßnahmen zu ergreifen, die im Sinne des Schutzes der IT-Sicherheit sind. Dass das Risiko einer Strafverfolgung von Forschenden oder ethischen Hackerinnen und Hackern durchaus real ist, zeigt der bereits erwähnte Fall von Lilith Wittmann. Auch in der kriminalistischen Betrachtung schlägt sich die Gleichartigkeit der Handlungen von Forschenden und potentiell feindseligen Hackern für die Forschenden ungünstig nieder. So ordnete etwa eine Studie des Bundeskriminalamts aus dem Jahr 2015 „Cyberforscher" auf einer Stufe mit Terroristen und Cybervandalen als Bedrohung für die IT-Sicherheit ein.[20] Selbst unter Berücksichtigung der Motivlage der Akteure ist nicht stets eindeutig zu bestimmen, wer forschend auf IT-Systeme zugreift und wer hierbei kriminelle Absichten verfolgt. Neugier bzw. Wissbegier gelten auch als verbreitete Motive bei Hackern, die nicht der institutionalisierten IT-Sicherheitsforschung zuzuordnen sind.[21]

---

[18] *Ruhmann/Bernhardt* DuD 2017, 34, 35 f.; *Singelnstein/Zech,* in: Hornung/Schallbruch (Fn. 6), § 20 Rn. 25 ff.

[19] *Ruhmann/Bernhardt* DuD 2017, 34, 35 f.

[20] *Bundeskriminalamt,* Täter im Bereich Cybercrime, 2015, S. 37. Diese Einordnung wurde dabei aus dem jährlich vom niederländischen National Cyber Security Centre veröffentlichten Cyber Security Assessment Netherlands übernommen.

[21] *Bundeskriminalamt* (Fn. 20), S. 17 f.

Die Problematik einer möglichen Strafbarkeit von IT-Sicherheitsforschern wurde besonders nach der Einführung von § 202c StGB durch das 41. Strafrechtsänderungsgesetz im Jahr 2007[22] im Zusammenhang mit Herstellung und Vertrieb von „Dual Use-Tools" diskutiert. Hier zeigten sich Forschende besorgt, dass der Umgang mit derartigen Computerprogrammen, die sowohl für die Begehung von Straftaten als auch für sozial wünschenswerte Handlungen geeignet sind, von § 202c Abs. 1 Nr. 2 StGB umfasst sein könnte.[23] Das Bundesverfassungsgericht sah ein Risiko strafrechtlicher Verfolgung der Hersteller und Nutzer von Dual Use-Tools aufgrund fehlender Tatbestandsmäßigkeit und jedenfalls fehlenden Vorsatzes nicht gegeben und nahm eine Verfassungsbeschwerde gegen § 202c StGB wegen fehlender Beschwerdebefugnis nicht zur Entscheidung an.[24] Maßgeblich hierfür führte das Gericht an, dass § 202c Abs. 1 Nr. 2 StGB voraussetze, dass der Zweck eines Computerprogramms die Begehung von Straftaten nach §§ 202a, 202b StGB sein müsse, eine bloße Eignung hierfür aber nicht ausreichend sei. Ein Programm müsse mit der Absicht „entwickelt oder modifiziert worden sein, es zur Begehung der genannten Straftaten einzusetzen."[25] Diese Absicht müsse sich ferner objektiv manifestiert haben.[26]

Zwar hat das Bundesverfassungsgericht hiermit Unsicherheiten bei der Auslegung des Zweckbegriffs in § 202c StGB[27] beseitigt, allerdings treten mittlerweile Strafbarkeitsrisiken im Zusammenhang mit anderen Verhaltensweisen in den Vordergrund. Heute steht unter anderem die Erforschung und Schließung von Sicherheitslücken im Fokus der IT-Sicherheitsforschung. So zeigte beispielsweise der Fall WannaCry[28], dass das Ausnutzen derartiger Sicherheitslücken schwerwiegende Folgen haben kann. Daher ist es wünschenswert, wenn sie aufgespürt und geschlossen werden, bevor Kriminelle sie nutzen können.

---

[22] BGBl. I, S. 1786.

[23] Vgl. *Böhlke/Yilmaz* CR 2008, 261 ff.; *Gröseling/Höfinger* MMR 2007, 626, 628 f.; *Popp* GA 2008, 375, 388 f.; *Stuckenberg* wistra 2010, 41 f. m.w.N.

[24] BVerfG ZUM 2009, 745.

[25] BVerfG ZUM 2009, 745, 749.

[26] BVerfG ZUM 2009, 745, 749.

[27] Dazu ausführlich *Popp* GA 2008, 375, 379 ff.

[28] Im Mai 2017 verursachte das Schadprogramm WannaCry weltweit erhebliche Schäden. In Deutschland traf es unter anderem die Deutsche Bahn, in Großbritannien zahlreiche Gesundheitseinrichtungen; vgl. *Zeit Online* v. 15.5.2017, https://www.zeit.de/digital/internet/2017–05/wannacry-microsoft-nsa-hackerangriff-usa-regierung (zuletzt abgerufen am 31.10.2022).

2. Aufdecken von Sicherheitslücken

Das Aufspüren von Sicherheitslücken in IT-Systemen gehört zu den typischen Tätigkeiten von IT-Sicherheitsforschern. Hierfür ist regelmäßig ein Zugriff auf fremde Informationssysteme und Daten notwendig, die sich im praktischen Einsatz befinden. Die Suche nach Sicherheitslücken und Sicherheitstests kann nicht allein in „Laborumgebungen" durchgeführt werden. Die notwendigen Zugriffshandlungen[29] können jene Straftatbestände erfüllen, die dem Schutz des formellen Datengeheimnisses[30] bzw. der Unversehrtheit von Daten und IT-Systemen dienen (§§ 202a f., 303a f. StGB).[31] Hierbei kommt vor allem § 202a Abs. 1 StGB in Betracht, der das unbefugte Verschaffen des Zugangs zu Daten, die nicht für den Täter bestimmt und gegen unberechtigten Zugang gesichert sind, unter Strafe stellt. Für den Zugang reicht die Möglichkeit der Kenntnisnahme aus, so dass ein bloßer Systemzugriff bereits tatbestandlich ist.[32]

Anders als in § 202c Abs. 1 Nr. 2 StGB, der auf den Zweck eines Programmes abstellt, sind in § 202a Abs. 1 StGB keine objektiven Tatbestandsmerkmale enthalten, die nach einer Zweckrichtung der Handlungen differenzieren.[33] Auch die Voraussetzung der Überwindung einer Zugangssicherung ist im Fall von Tätigkeiten der IT-Sicherheitsforschung nicht geeignet, ein besonders strafwürdiges Unrecht zu umschreiben. Sie mag in vielen Fällen ein Indiz für die kriminelle Energie von Tä-

---

[29] Neben dem Zugriff auf IT-Systeme könnte auch die Weitergabe von hierbei erlangten Informationen über Sicherheitslücken durch Forschende als Datenhehlerei (§ 202d Abs. 1 StGB) oder Verletzung von Geschäftsgeheimnissen (§ 23 Abs. 1 Nr. 2 GeschGehG) strafbar sein. Hierfür wird es aber in der Regel an den notwendigen subjektiven Merkmalen fehlen. Wird ein solche Information zu Forschungszwecken weitergegeben, wird es an einer Bereicherungs- oder Schädigungsabsicht im Sinne von § 202d Abs. 1 StGB fehlen. Ein wissenschaftliches Interesse fällt auch nicht unter das Merkmal „aus Eigennutz" in § 23 Abs. 1 Nr. 2 GeschGehG; *Joecks/Miebach,* in: MüKo-StGB, 3. Aufl. 2019, § 23 GeschGehG Rn. 56.

[30] Zur Systematisierung des IT-Strafrechts nach formellem und inhaltsbezogenem Schutz *Singelnstein/Zech,* in: Hornung/Schallbruch (Fn. 6), § 20 Rn. 37 ff.

[31] Der Beitrag konzentriert sich dabei auf die Risiken des Kernstrafrechts. Daneben kann etwa die unerlaubte Dekompilierung von Softwareprogrammen § 106 UrhG erfüllen; vgl. zu den urheberrechtlichen Aspekten des „Reverse Engineering" *Wagner* DuD 2020, 111 f.

[32] Vgl. BT-Drs. 16/3656, S. 9; *Eisele,* in: Schönke/Schröder (Hrsg.), StGB, 30. Aufl. 2019, § 202a Rn. 18; *Kubiciel/Großmann* NJW 2019, 1050, 1052 f.; *Goeckenjan* wistra 2009, 47, 49; *Puschke,* in: Brunhöber (Hrsg.), Strafrecht im Präventionsstaat, 2014, S. 113.

[33] Kritisch hierzu *Kubiciel/Großmann* NJW 2019, 1050, 1053. Dieser Mangel wirkt sich auch auf § 202c Abs. 1 Nr. 2 StGB aus, der auf den Zweck der Begehung von Straftaten nach § 202a f. StGB verweist.

tern sein,[34] dies gilt aber nicht in der IT-Sicherheitsforschung. Sicherheits- bzw. Penetrationstests müssen gerade darauf zielen, Zugangssicherungen zu überwinden, um wirksam zu sein.

Damit hängt es in derartigen Fällen maßgeblich von Merkmal „unbefugt" ab, ob IT-Sicherheitsforscher sich strafbar machen. Zu einem befugten und damit nicht-tatbestandsmäßigen[35] Handeln führt jedenfalls das Einverständnis derjenigen, die zum Zugriff berechtigt sind. Ein beauftragter Penetrationstest wäre damit nicht strafbar.[36] Problematisch ist hieran, dass die Verhältnisse der Berechtigung an IT-Systemen komplex sind. Diese Verhältnisse eindeutig zu klären und die notwendigen Einverständnisse einzuholen, gestaltet sich für die Forschenden aufwändig.[37] Dem lässt sich entgegenhalten, dass die Vermeidung eines hohen organisatorischen Aufwands noch kein Grund dafür ist, ohne Einverständnis auf fremde IT-Systeme zuzugreifen. Allerdings kann es in einem gewissen Umfang auch wünschenswert sein, dass IT-Sicherheitsforscher in natürlichen Umgebungen Sicherheitslücken aufspüren, ohne zuvor ein Einverständnis sämtlicher potentiell Berechtigter einzuholen. Für die Erforschung von IT-Sicherheitslücken ist ein tentatives Vorgehen charakteristisch, das sich selten auf die zuvor gesteckten Grenzen eines einzelnen Systems beschränken lässt.

Unter diesem Gesichtspunkt könnte IT-Sicherheitsforschung, die sich für das Aufdecken von Sicherheitslücken als notwendig erweist und selbstauferlegten, anerkannten ethischen Standards genügt, unter Umständen als sozialadäquat und damit als nicht „unbefugt" betrachtet werden.[38] Es erscheint allerdings schwer zu bestimmen, welche Formen des Systemzugriffs durch IT-Sicherheitsforscher als von der Allgemeinheit gebilligt und damit im Rahmen der sozialen Handlungsfreiheit liegend[39]

[34] Vgl. BT-Drs. 16/3656, S. 10.

[35] Dafür, das Merkmal „unbefugt" im objektiven Tatbestand zu verorten, spricht eine funktional-wertende Betrachtung. Der Eingriff in ein informationstechnisches System erhält erst dadurch seinen spezifischen Unrechtsgehalt, dass er gegen oder ohne den Willen des Betroffenen erfolgt; so im Ergebnis auch *Brodowski* ZIS 2019, 49, 55; *Popp* NJW 2004, 3517, 3518; *Graf*, in: MüKo-StGB, 4. Aufl. 2021, § 202a Rn. 65; anders *Kargl*, in: NK-StGB, 5. Aufl. 2017, § 202a Rn. 16.

[36] BT-Drs. 16/3656, S. 10; *Singelnstein/Zech,* in: Hornung/Schallbruch (Fn. 6), § 20 Rn. 42.

[37] Siehe hierzu *Brodowski* (in diesem Band) S. 37, 40 ff.

[38] In diese Richtung auch *Kubiciel/Großmann* NJW 2019, 1050, 1053. In derartigen Fällen wäre das Tatbestandsmerkmal „unbefugt" unter dem Gesichtspunkt der Sozialadäquanz einschränkend auszulegen.

[39] Vgl. zu diesen Kriterien der Sozialadäquanz BGHSt 23, 226, 228; *Zipf* ZStW 82 (1970), 633 ff.