Neue Strafrechtswissenschaft Heft 3/2024

Kann denn ethisches Hacking strafbar sein?

Brian Valerius, Passau*

ABSTRACT

Kein informationstechnisches System dürfte völlig sicher sein und unerwünschte Zugriffe von außen komplett ausschließen. Daher sollte an sich jede Hilfe erwünscht sein, um Schwachstellen aufzuspüren. So denken jedenfalls nicht wenige Hackerinnen und Hacker, die mitunter auch ohne Zustimmung der Berechtigten nach Sicherheitslücken suchen, um diese zu melden und schließen zu lassen. Häufig wird ein Hacking aus solchen Motiven sogar als „ethisch" bezeichnet. Doch ist es auch rechtlich zulässig?

A. Hacking ist nicht gleich Hacking

Hacking dürfte für viele nach wie vor das Paradebeispiel für Cybercrime darstellen. In der Tat ist Hacking ein notwendiger Bestandteil wesentlicher gegenwärtiger krimineller Aktivitäten gegen informationstechnische Systeme. Zu denken ist nur an Ransomware-Angriffe, die das Bundeskriminalamt als primäre Bedrohung sowohl für Unternehmen als auch für öffentliche Einrichtungen einstuft.[1] Hierbei verschafft sich jemand Zugriff auf die Zielserver, um die betroffenen Systeme oder zumindest die darauf befindlichen Daten mit einer Schadsoftware zu verschlüsseln. Sodann wird für den Entschlüsselungscode und/oder für die Nichtveröffentlichung der Daten ein Lösegeld verlangt.[2] Insbesondere

* Der Verfasser ist Inhaber des Lehrstuhls für Künstliche Intelligenz im Strafrecht an der Universität Passau. Für die anregenden Diskussionen bedanke ich mich herzlich bei meinem wissenschaftlichen Mitarbeiter *Simão Marcante Kruska* und meiner studentischen Mitarbeiterin *Marie Bokeloh*.

[1] BKA (Hrsg.) Bundeslagebild Cybercrime, 2022, S. 1.

[2] Zum Ablauf von Ransomware-Angriffen *Brodowski/Schmid/Scholzen/Zoller* NStZ 2023, 385, 385 f.

https://doi.org/10.61039/29427509-2024-23

der Ukraine-Krieg hat den Blick aber auch auf Hacktivismus-Kampagnen gelenkt, bei denen Hackerinnen und Hacker aus politischen oder sonstigen Gründen versuchen, nicht zuletzt Einrichtungen der sog. Kritischen Infrastruktur (KRITIS) wie etwa der Energieversorgung zum Erliegen zu bringen.[3]

Anders als die aktuellen Beispiele nahelegen, geht mit Hacking jedoch nicht zwingend einher, die Daten auf dem Zielserver herunterzuladen, zu verändern, zu löschen oder sonst hierauf zuzugreifen. Vielmehr erschöpft sich Hacking als solches in der Tätigkeit, sich unbefugt den Zugang zu einem (geschützten) informationstechnischen System zu verschaffen oder auch nur entsprechende Sicherheitslücken zu finden.[4] Schon seit den Anfangszeiten des Hackings wird daher unterschieden. Während das sog. Hacking sich darauf beschränkt, Sicherheitslücken aufzuspüren oder Sicherheitsvorkehrungen zu überwinden, dient beim sog. Cracking der eröffnete Zugang auf das Zielsystem weiterführenden, kriminellen Anliegen.[5]

Mittlerweile ist anstatt von Hacking und Cracking von „White Hat"- und „Black Hat"-Hacking die Rede. Während „Black Hats" zum eigenen Vorteil agieren und z.B. zu Spionage-, terroristischen oder hacktivistischen Zwecken in fremde informationstechnische Systeme eindringen,[6] handeln „White Hats" aus hehren Beweggründen. Sie wollen insbesondere Schwachstellen in Systemen finden, um sie von den Systembetreibenden beheben zu lassen.[7] Die Bezeichnungen sind wie so oft umstritten. Überwiegend wird für das White-Hat-Hacking neben der geschilderten Motivation vorausgesetzt, im Auftrag der Berechtigten und ggf. in näher vorgegebenen Grenzen zu handeln.[8] Fehlt diese Zustimmung ebenso wie die kriminelle Absicht der „Black Hats", wird mitunter auch von Grey-Hat-Hacking gesprochen.[9]

Außerdem fällt in diesem Zusammenhang häufig der Begriff des „ethischen Hackings". Diese Bezeichnung wird zum Teil als Synonym für

---

[3] Hierzu BKA (Hrsg.) Bundeslagebild Cybercrime, 2022, S. 22 ff.

[4] S. nur *Raak-Stilb* CCZ 2023, 190, 190.

[5] *Hilgendorf/Kusche/Valerius*, Computer- und Internetstrafrecht, 3. Aufl. 2022, § 3 Rn. 370.

[6] *Martin* acm Inroads 8 (2017), 33, 34; *Schneider* Kriminalistik 2023, 433, 433.

[7] Zur Implementation von „White Hat"-Hacking, um die Wirksamkeit von Compliance-Management-Systemen zu überprüfen, *Raak-Stilb* CCZ 2023, 190, 192 ff.

[8] *Martin* acm Inroads 8 (2017), 33, 33; *Schneider* Kriminalistik 2023, 433, 433; aA *Klaas* MMR 2022, 187, 187 f.

[9] *Martin* acm Inroads 8 (2017), 33, 34; *Schneider* Kriminalistik 2023, 433, 433.

„White-Hat"-Hacking verwendet.[10] Andere betonen das Attribut „ethisch" und wollen hiermit ein Hacking versehen, das zum Wohle der Gesellschaft die Sicherheit von informationstechnischen Systemen erhöhen will; demzufolge wären darunter sowohl das „White-Hat"- als auch das „Grey-Hat"-Hacking zu fassen.[11] Diese Klassifizierung liegt ebenso den folgenden Ausführungen zugrunde.

Die Wege, sich Zugang zum Zielsystem zu verschaffen, unterscheiden sich beim „Black Hat"- und beim ethischen Hacking grundsätzlich nicht.[12] Zum Teil werden bei der Beauftragung mit Penetrationstests zwar grundlegende technische Informationen über das zu überprüfende System mitgeteilt, damit diese nicht erst beschafft werden müssen. Ansonsten muss das ethische Hacking aber schon deswegen im Wesentlichen mit denselben Mitteln wie seine nicht ethischen Pendants vorgehen, weil gerade Sicherheitslücken für kriminell motivierte Angriffe gefunden werden sollen.[13] Somit ist im Folgenden insbesondere zu untersuchen, ob allein die unterschiedliche Motivation von Bedeutung und ob ein ethisches Hacking auch in rechtlicher Hinsicht unbedenklich ist.

B. Strafbarkeit von Hacking nach geltendem Recht

I. Überblick

Der einschlägige Straftatbestand für das Hacking ist § 202a StGB, der das Ausspähen von Daten unter Strafe stellt. In der IT-Branche wie auch in der öffentlichen Diskussion wird zwar häufig § 202c StGB als „Hackerparagraph" bezeichnet.[14] Allerdings erfasst diese Strafvorschrift nicht das eigentliche Hacking, sondern bereits Vorbereitungshandlungen zum Ausspähen (oder auch Abfangen) von Daten. Die irreführende Titulierung der Norm als „Hackerparagraph" dürfte dem Umstand geschuldet sein, dass der Gesetzgeber hierbei gerade sog. Hacker-Tools im Blick hatte, die schon nach Art und Weise ihres Aufbaus illegalen Zwecken dienen.[15]

[10] *Raak-Stilb* CCZ 2023, 190, 190.
[11] Vgl. *Vettermann* MMR 2023, 827, 828.
[12] *Martin* acm Inroads 8 (2017), 33, 33; *Wagner* DuD 2020, 111, 111.
[13] *Raak-Stilb* CCZ 2023, 190, 190 f.
[14] S. nur *Hilgendorf/Kusche/Valerius* (Fn. 5), § 3 Rn. 384.
[15] BT-Drs. 16/3656, S. 12.

Selbstredend kommen im Zusammenhang mit Hacking auch weitere Straftatbestände in Betracht. Dies gilt insbesondere für das „Black Hat"-Hacking, das dem primär verfolgten kriminellen Anliegen lediglich vorausgeht. Bei Ransomware-Angriffen ist exemplarisch an Datenveränderung (§ 303a StGB) und Computersabotage (§ 303b StGB) sowie an Erpressung (§ 253 StGB) zu denken.[16] Anknüpfend an die Inhalte der verschafften Daten kann zudem unter anderem eine Strafbarkeit nach § 106 I UrhG (bei urheberrechtlich geschützten Inhalten), § 23 I GeschGehG (bei Geschäftsgeheimnissen) oder nach § 42 II BDSG (bei personenbezogenen Daten) im Raum stehen.[17] Das Hacking als solches dürfte hingegen zumeist allenfalls von § 202a StGB erfasst sein.

II. Ausspähen von Daten (§ 202a StGB)

1. Gesetzgebungsgeschichte

§ 202a StGB wurde durch das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG) vom 15. Mai 1986[18] eingefügt. Die Strafvorschrift sollte Daten umfassender als zuvor gegen Spionage schützen, um dem gestiegenen Wert von Informationen auch strafrechtlich Rechnung zu tragen.[19] Allerdings beschränkte sich § 202a StGB in seiner ursprünglichen Fassung darauf, das unbefugte Verschaffen von Daten unter Strafe zu stellen. Hiervon war nach wohl herrschender Meinung aber erst auszugehen, wenn Daten aus dem Zielsystem abgerufen wurden.[20] Sich durch Hacking nur die Möglichkeit hierzu zu verschaffen, genügte nicht.[21] Die Straflosigkeit des Hackings entsprach auch der Vorstellung des Gesetzgebers, der das bloße Eindringen in ein Computersystem lediglich als Vorbereitungshandlung erachtete und zudem der Gefahr einer Überkriminalisierung von Verhaltensweisen vorbeugen wollte.[22]

---

[16] Zur Strafbarkeit von Ransomware-Angriffen *Brodowski/Schmid/Scholzen/Zoller* NStZ 2023, 385, 387.

[17] *Valerius*, in Graf/Jäger/Wittig, Wirtschafts- und Steuerstrafrecht, 3. Aufl. 2024, § 202a Rn. 43; *Kipker/Rockstroh* ZRP 2022, 240, 240.

[18] BGBl. I, S. 721.

[19] BT-Drs. 10/5058, S. 28.

[20] *Hilgendorf/Frank/Valerius*, Computer- und Internetstrafrecht, 1. Aufl. 2005, Rn. 686; vgl. auch BT-Drs. 16/3656, S. 9.

[21] *Hilgendorf/Frank/Valerius* (Fn. 20), Rn. 686 f. m.w.N.; zur Gegenauffassung etwa *Schnabl* wistra 2004, 211, 214 f.

[22] BT-Drs. 10/5058, S. 28.

Das Bild vom Hacking änderte sich aber mit der Zeit. In Anbetracht der generellen Gefährlichkeit und Schädlichkeit von Hacking-Angriffen, der auch das Übereinkommen des Europarates über Computerkriminalität vom 23. November 2001[23] sowie der Rahmenbeschluss über Angriffe auf Informationssysteme vom 24. Februar 2005[24] Rechnung trugen, sollte daher auch das Hacking als solches unter Strafe gestellt werden.[25] Durch das Einundvierzigste Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG) vom 7. August 2007[26] wurde § 202a StGB daher dergestalt geändert, dass seitdem nicht erst das Verschaffen von Daten, sondern bereits das Verschaffen des Zugangs zu Daten strafbar ist.

2. Tatbestandsverwirklichung durch Hacking

a) Tatobjekt

(1) Keine inhaltlichen Anforderungen

Unberührt von der Gesetzesänderung blieb das Tatobjekt des § 202a StGB. Das Ausspähen muss Daten betreffen, die nicht für den Täter bestimmt sowie gegen unberechtigten Zugang besonders gesichert sind. Als Daten sind kodierte Informationen jeder Art anzusehen,[27] angefangen von Mediendateien bis hin zu Zugangsdaten wie Passwörtern, Bank- und Kreditkartendaten, Geschäftsgeheimnissen und sensiblen persönlichen Informationen. Inhaltliche Anforderungen werden somit nicht gestellt, schützt § 202a StGB doch das formelle Geheimhaltungsinteresse der Verfügungsberechtigten.[28] Einschränkend sieht Abs. 2 lediglich vor, dass unter Daten im Sinne des § 202a I StGB nur solche zu verstehen sind, „die [...] nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden“. Für das Hacking ist diese Begrenzung indessen nicht von Bedeutung.

[23] SEV Nr. 185.
[24] ABl. EU vom 16.3.2005 Nr. L 69, S. 67.
[25] BT-Drs. 16/3656, S. 9.
[26] BGBl. I, S. 1786.
[27] *Hilgendorf*, in Leipziger Kommentar StGB, Bd. 10, 13. Aufl. 2023, § 202a Rn. 7.
[28] BGH NStZ 2018, 401, 403; NStZ-RR 2020, 278, 280.

(2) Nicht für den Täter bestimmt

Relevant kann aber die Voraussetzung sein, dass die Daten nicht für den Täter bestimmt sind. Durch diese Einschränkung wird die Befugnis der Verfügungsberechtigten betont, über den Zugang zu den geschützten Daten zu bestimmen. Als verfügungsberechtigt wird gewöhnlich angesehen, wem die Speicherung des Datums rechtlich zuzurechnen ist.[29] Auch insoweit sind die Inhalte der Daten nicht von Bedeutung; so ist ein (z.B. personenbezogenes) Datum nicht allein deswegen für jemanden bestimmt, weil er hiervon betroffen ist.[30] Ebenso wenig vermag daher eine auch noch so verständliche Motivation dazu führen, dass die durch Hacking zugänglichen Daten für den Täter bestimmt sind. Maßgeblich bleibt ausschließlich der Wille der (formal) Verfügungsberechtigten.

Nicht für den Täter bestimmt sind Daten, die ihm nach dem Willen der Verfügungsberechtigten zum Zeitpunkt der Tathandlung nicht zur Verfügung stehen sollen.[31] Liegt eine solche Zustimmung vor, erweist sie sich als tatbestandsausschließendes Einverständnis.[32] Reine Nutzungsbeschränkungen lassen die Bestimmung der Daten (auch) für den Täter nicht entfallen; allein eine zweckwidrige Verwendung von Daten verwirklicht folglich nicht den Tatbestand des § 202a I StGB.[33]

(3) Gegen unberechtigten Zugang besonders gesichert

Dass der Wille der Verfügungsberechtigten im Vordergrund steht, verdeutlicht auch die zweite Einschränkung, wonach nur Daten geschützt sind, die gegen unberechtigten Zugang besonders gesichert sind. Von einer *besonderen* Sicherung kann lediglich gesprochen werden, wenn die (technischen, mechanischen, baulichen oder sonstigen) Sicherheitsvorkehrungen geeignet sind, den Zugriff Unbefugter auszuschließen oder zumindest erheblich zu erschweren.[34] Die Rechtsprechung verlangt insoweit einen typischerweise, d.h. unabhängig von den spezifischen Möglichkeiten oder Kenntnissen des konkreten Täters, nicht unerheblichen

---

[29] Statt vieler *Hilgendorf*, in LK StGB (Fn. 27), § 202a Rn. 26.

[30] *Eisele*, in Schönke/Schröder StGB, 30. Aufl. 2019, § 202a Rn. 10; *Hilgendorf/Kusche/Valerius* (Fn. 5), § 3 Rn. 352.

[31] *Eisele*, in Schönke/Schröder (Fn. 30), § 202a Rn. 8; *Hilgendorf/Kusche/Valerius* (Fn. 5), § 3 Rn. 350.

[32] *Hilgendorf*, in LK StGB (Fn. 27), § 202a Rn. 20.

[33] BayObLG NJW 1999, 1727, 1727 f.; *Graf*, in Münchener Kommentar StGB, Bd. 4, 4. Aufl. 2021, § 202a Rn. 24.

[34] BGH NJW 2015, 3463, 3464; NStZ-RR 2020, 278, 280.

Aufwand, um die Zugangssicherung zu überwinden.[35] Sollte jeder interessierte Mensch die Sicherungsmaßnahmen ohne Weiteres überwinden können, liegt keine besondere Sicherung vor.[36] Nahezu unstreitig dürften hierfür einerseits bloße organisatorische Maßnahmen oder Registrierungspflichten nicht genügen[37] und andererseits standardisierte Verschlüsselungen (z.B. in einem WLAN) ausreichen.[38] Ansonsten kann über die Abgrenzung nicht nur im Einzelfall vortrefflich gestritten werden.

Die Motivation für das Hacking bleibt jedoch abermals unerheblich. Zum einen kommt auch in dem Merkmal der Zugangssicherung das formale Geheimhaltungsinteresse der Verfügungsberechtigten zum Ausdruck. Zum anderen gilt für die Anforderungen an die besondere Sicherung ein objektiver Maßstab; wie dargelegt unterscheiden sich Black-Hat- und White-Hat-Hacking aber in ihrer äußeren Vorgehensweise grundsätzlich nicht.

b) Tathandlung

Die Tathandlung des § 202a StGB besteht darin, sich oder einem anderen den Zugang zu den vorstehend näher beschriebenen Daten zu verschaffen. Seit der Erweiterung der Norm durch das 41. StrÄndG (siehe II. 1.) ist es nicht mehr erforderlich, sich die geschützten Daten selbst zu verschaffen. Somit sind auch Erscheinungsformen des Hackings erfasst, wenngleich bei dem bloßen Aufspüren von Sicherheitslücken die Reichweite des Straftatbestandes durchaus umstritten ist. Dies gilt unter anderem für das sog. Portscanning, das sich darauf beschränkt, beim Zielsystem offene Ausgänge als mögliche Angriffspunkte zu suchen.[39] Nicht nur wegen des Hintergrunds der Gesetzesänderung empfiehlt es sich aber jedenfalls, „Zugang" in diesem Sinne weit und technikoffen zu interpretieren.[40] Es ist daher etwa ohne Belang, auf welchem Speichermedium (z.B. auf einem Computer im Intranet oder auf einem Cloudserver)

[35] BGH NStZ-RR 2020, 278, 280.

[36] *Hilgendorf*, in LK StGB (Fn. 27), § 202a Rn. 32; enger wohl BGH NStZ-RR 2020, 278, 280: „jedermann".

[37] BT-Drs. 16/3656, S. 10; *Hilgendorf/Kusche/Valerius* (Fn. 5), § 3 Rn. 360.

[38] *Eisele*, in Schönke/Schröder (Fn. 30), § 202a Rn. 16; *Hilgendorf/Kusche/Valerius* (Fn. 5), § 3 Rn. 361.

[39] Eine Strafbarkeit bejahend etwa *Hilgendorf/Kusche/Valerius* (Fn. 5), § 3 Rn. 371; *Weidemann*, in Beck'scher Online-Kommentar StGB, 60. Ed. 1.2.2024, § 202a Rn. 17.4; a.A. *Böken*, in Cybersecurity, 2. Aufl. 2023, Kap. 19 Rn. 72.

[40] *Graf*, in MüKo StGB (Fn. 33), § 202a Rn. 37.

sich die betreffenden Daten befinden und in welcher Weise hierauf (z.B. drahtlos oder leitungsgebunden) ein Zugriff eröffnet wird.[41]

Den Zugang muss sich der Täter „unter Überwindung der Zugangssicherung" verschaffen. Diese Passage wurde ebenfalls durch das 41. StrÄndG neu eingefügt, benennt aber lediglich ausdrücklich eine Voraussetzung, über die zuvor schon Einigkeit bestand.[42] Das Merkmal soll verdeutlichen, dass sich spiegelbildlich neben der Dokumentation des Geheimhaltungsinteresses der Verfügungsberechtigten auch die kriminelle Energie des Täters in der Tat manifestieren muss.[43] Auch bei der Tathandlung wird somit an die (äußere) Missachtung des Geheimhaltungsinteresses angeknüpft und kann daher die Motivation des Täters nicht berücksichtigt werden.

c) Unbefugt

Bei dem Merkmal „unbefugt" ist – wie so häufig bei den §§ 201 ff. StGB[44] – umstritten, ob es sich lediglich um ein allgemeines Deliktsmerkmal der Rechtswidrigkeit[45] oder um ein Merkmal mit Doppelfunktion handelt, so dass die Zustimmung der Verfügungsberechtigten bereits die Tatbestandsmäßigkeit entfallen ließe.[46] Unstreitig ist der Tatbestand des § 202a StGB aber jedenfalls ausgeschlossen, wenn die tatgegenständlichen Daten für den Täter bestimmt sind (siehe schon II. 2. a).

d) Motivation der Hackenden

Zusammenfassend lässt sich festhalten, dass zumindest bestimmte Erscheinungsformen des Hackings grundsätzlich den Tatbestand des § 202a I StGB verwirklichen. Dies ist nicht sonderlich überraschend, wollte der Gesetzgeber des 41. StrÄndG durch die Ausweitung der Norm doch gerade das Hacking als solches erfassen. Auch dieses Anliegen streitet dafür, dass die Motivation für das Hacking zumindest auf Tatbestandsebene unerheblich bleibt. Die einzelnen Tatbestandsmerkmale

---

[41] *Valerius*, in GJW (Fn. 17), § 202a Rn. 30; vgl. auch BT-Drs. 16/7218, S. 62.

[42] BGH NStZ 2011, 154, 154; *Weidemann*, in BeckOK StGB (Fn. 39), § 202a Rn. 19; s.a. BT-Drs. 16/3656, S. 10.

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

[44] Hierzu etwa *Popp*, in Handbuch des Strafrechts, Bd. 4, 2019, § 15 Rn. 57.

[45] So u.a. *Eisele*, in Schönke/Schröder StGB (Fn. 30), § 202a Rn. 24; *Kargl*, in NomosKommentar StGB, 6. Aufl. 2023, § 202a Rn. 46.

[46] So etwa *Graf*, in MüKo StGB (Fn. 33), § 202a Rn. 65; *Kipker/Rockstroh* ZRP 2022, 240, 241.

geben aber ohnehin keinen Raum, um Beweggründe, Ziele oder sonstige Kriterien in der Person des Täters zu berücksichtigen. Vielmehr ist eine deutliche Ausrichtung an dem Rechtsgut der formalen Geheimsphäre erkennbar, die den Willen der Verfügungsberechtigten als solchen schützen will und daher etwa auch den Inhalt der Daten, namentlich deren Geheimbedürftigkeit oder Personenbezogenheit außer Acht lässt.

III. Besonderheiten des Grey- und White-Hat-Hackings

1. Zustimmung der Verfügungsberechtigten

Für das Black-Hat-Hacking endet mit den vorstehenden Ausführungen die strafrechtliche Betrachtung. Bei dem Grey-Hat- bzw. White-Hat-Hacking treten jedoch – je nach Begriffsverständnis – bis zu zwei wesentliche Eigenarten hinzu. Hierzu zählt zum einen die ehrenwerte Motivation des Täters. Darüber hinaus kann zum anderen das Hacking mit Zustimmung der Verfügungsberechtigten geschehen.

Sollten – wie bei der wohl überwiegenden Definition des White-Hat-Hackings (siehe A.) – die Sicherheitslücken eines informationstechnischen Systems mit Zustimmung der Betroffenen ermittelt werden, scheint bereits der Tatbestand zu entfallen.[47] Schließlich stellt es ein tatbestandliches Einverständnis dar, wenn die zugangsgeschützten Daten für den Täter bestimmt sind. Dadurch würde aber die Differenzierung zwischen Zugang zu und Zugriff auf Daten, die sich schon der Gesetzgebungsgeschichte des § 202a StGB entnehmen lässt, vernachlässigt werden. Auch wenn ein Unternehmen jemanden damit beauftragt, Schwachstellen in seinem informationstechnischen System aufzuspüren, dürfte hiermit nicht zugleich erklärt werden, dass den Beauftragten auch die im System gespeicherten Daten zur Verfügung stehen, z.B. Dateien mit personenbezogenen Informationen geöffnet oder heruntergeladen werden dürfen. Die Zustimmung der Berechtigten, die Sicherheit des Systems zu überprüfen, lässt die gesicherten Daten somit noch nicht als bestimmt für die Beauftragten erscheinen, sondern stellt „lediglich“ eine rechtfertigende Einwilligung dar.[48]

---

[47] So etwa *Kipker/Rockstroh* ZRP 2022, 240, 241, jedoch auch aufgrund einer dem Merkmal „unbefugt“ zugeschriebenen doppelfunktionellen Bedeutung (hierzu B. II. 2. c)).

[48] *Valerius*, in GJW (Fn. 17), § 202a Rn. 36.

Im Ergebnis dürfte aber Einigkeit darüber bestehen, dass einverständliches Hacking und somit das White-Hat-Hacking im Sinne der obigen Definition als solches straflos bleibt. Dies ist aber nicht der besonderen Motivation der Handelnden, sondern allein dem Umstand geschuldet, dass die Verfügungsberechtigten durch ihre Zustimmung die formale Geheimsphäre gerade erweitern bzw. insoweit aufgeben. Wie diese Zustimmung erteilt wird, d.h. durch eine individuelle Beauftragung oder infolge einer öffentlichen Auslobung von Preisgeldern oder sonstigen Belohnungen für das Aufspüren und die Meldung von Schwachstellen (sog. Bug Bounties), ist unerheblich.

Die Zustimmung der Verfügungsberechtigten muss jedoch zum Zeitpunkt der Tat vorliegen. Nachträgliche Genehmigungen sind im Strafrecht unbeachtlich.[49] In der Regel dürfte in diesen Fällen aber kein Strafantrag gestellt werden, der für die Verfolgung des Antragsdelikts des § 202a StGB nach § 205 I 2 StGB grundsätzlich notwendig ist.[50] Zwar könnten die Strafverfolgungsbehörden den fehlenden Strafantrag überwinden, indem sie ein besonderes öffentliches Interesse an der Strafverfolgung bejahen; gegen ein solches Einschreiten von Amts wegen dürfte aber nicht zuletzt die ehrenhafte Motivation beim Grey-Hat-Hacking sprechen.

2. Motivation des Täters

a) Einwilligung und mutmaßliche Einwilligung

Fehlt die Zustimmung der Verfügungsberechtigten, kann auf deren Einwilligung nicht verwiesen werden. Ebenso scheidet eine mutmaßliche Einwilligung aus, die nur dann eine rechtfertigende Wirkung zu entfalten vermag, wenn die Zustimmung der Betroffenen nicht (rechtzeitig) vor der Tat eingeholt werden kann.[51] Das betroffene Unternehmen vor Maßnahmen wie Penetrationstests zu befragen, ist aber in der Regel durchaus möglich.[52]

---

[49] *Klaas* MMR 2022, 187, 189; allg. hierzu BGHSt 17, 359, 360.

[50] Zur (wohl eher geringen) Häufigkeit von Strafanträgen beim sog. Grey-Hat-Hacking *Schneider* Kriminalistik 2023, 433, 437.

[51] BGHSt 16, 309, 312; *Rönnau*, in Leipziger Kommentar StGB, Bd. 3, 13. Aufl. 2019, Vor §§ 32 ff. Rn. 222.

[52] *Graf*, in MüKo StGB (Fn. 33), § 202a Rn. 71; *Hilgendorf*, in LK StGB (Fn. 27), § 202a Rn. 38.

b) Notwehr (§ 32 StGB) und rechtfertigender Notstand (§ 34 StGB)

Nicht nur in Anbetracht der derzeit in anderem Zusammenhang geführten Debatte, mit welchen Mitteln ehrenwerte Ziele legal verfolgt werden dürfen,[53] könnte aber erwogen werden, das (immerhin) ethische Hacking nach allgemeinen Erlaubnistatbeständen als gerechtfertigt anzusehen.[54] Ein Notwehrrecht dürfte indessen in der Regel bereits daran scheitern, dass es an einem Angriff im Sinne des § 32 II StGB und somit an einer Notwehrlage fehlt. Auf ein drohendes Verhalten Dritter (etwa durch ein befürchtetes Black-Hat-Hacking) kann von vornherein nicht verwiesen werden, weil sich die Verteidigung (in Gestalt des Grey-Hat-Hackings) gegen die Verfügungsberechtigten wendet; Notwehrhandlungen müssen sich aber stets gegen den Angreifer richten, beruht § 32 StGB doch auf dem Gedanken der Rechtsbewährung, dass das Recht dem Unrecht nicht zu weichen braucht.[55] Von Seiten der Verfügungsberechtigten könnten als Angriff allenfalls mangelhafte Sicherheitsvorkehrungen angesehen werden. Diese Untätigkeit dürfte aber in der Regel keinen gegenwärtigen, d.h. keinen zumindest unmittelbar bevorstehenden[56] Angriff auf zudem grundsätzlich allein als notwehrfähig anerkannte Individualrechtsgüter[57] darstellen.

Der rechtfertigende Notstand gestattet hingegen anders als § 32 StGB die Verteidigung jedes durch die Rechtsordnung geschützten Rechtsguts und somit ebenso von Universalrechtsgütern.[58] Zwar sind die Ziele beim ethischen Hacking nicht homogen, weil die überprüften informationstechnischen Systeme unterschiedlichen Anliegen dienen. Es müsste demzufolge stets im Einzelfall ermittelt werden, welches Rechtsgut es durch das Hacking zu schützen gilt. Sollten aber Sicherheitslücken z.B. den Zugriff auf personenbezogene Daten ermöglichen, steht eine Gefahr für das Recht auf informationelle Selbstbestimmung im Raum.[59] Nicht zuletzt bei informationstechnischen Systemen der Kritischen Infrastruktur könnte auch auf die Sicherheit in der Informationstechnik als

---

[53] Zu Aktionen der sog. letzten Generation *Erb* NStZ 2023, 577, 580 ff.; *Preuß* NZV 2023, 60, 72; *Zimmermann/Griesar* JuS 2023, 401, 403 ff.

[54] S. vor allem *Klaas* MMR 2022, 187, 189 ff. zu § 34 StGB.

[55] *Erb*, in Münchener Kommentar StGB, Bd. 1, 4. Aufl. 2020, § 32 Rn. 122; *Perron/Eisele*, in Schönke/Schröder (Fn. 30), § 32 Rn. 31.

[56] S. nur *Erb*, in MüKo StGB (Fn. 55), § 32 Rn. 104.

[57] BGHSt 5, 245, 247; BGH NJW 2013, 2133, 2136.

[58] *Erb*, in MüKo StGB (Fn. 55), § 34 Rn. 65, 72; *Zieschang*, in LK StGB (Fn. 51), § 34 Rn. 48.

[59] Zu möglichen Notstandslagen *Klaas* MMR 2022, 187, 189; *Schneider* Kriminalistik 2023, 433, 434.

Interesse der Allgemeinheit verwiesen werden, das etwa das gleichnamige Bundesamt für Sicherheit in der Informationstechnik (BSI) gemäß § 3 I 1 BSIG zu fördern hat und das in § 2 II 4 BSIG legaldefiniert wird.

Wiederum abweichend von § 32 StGB wird zudem der Begriff „gegenwärtig" weiter verstanden und umfasst auch sog. Dauergefahren, die sich jederzeit, d.h. ggf. sogar alsbald in einen Schaden realisieren können, selbst wenn der Schadenseintritt ebenso noch einige Zeit auf sich warten lassen kann.[60] Bei informationstechnischen Systemen der Kritischen Infrastruktur könnte daher argumentiert werden, dass jederzeit Black-Hat-Hackingattacken möglich und deshalb schon jetzt Abwehrmaßnahmen erforderlich seien, damit die Gefahr bei natürlicher Weiterentwicklung der Dinge nicht in einen Schaden umschlage bzw. ein bereits eingetretener Schaden sich nicht intensiviere.[61] Um eine Gefahr im Sinne des § 34 StGB annehmen zu können, die (ausnahmsweise) ein Eingriffsrecht begründet und spiegelbildlich eine Duldungspflicht desjenigen auslöst, gegen den sich die Notstandshandlung richtet, bedarf es jedoch tatsächlicher Umstände, die einen Schadenseintritt nach der Erfahrung als naheliegend erscheinen lassen.[62] Insbesondere das allgemeine Risiko, dass informationstechnische Systeme wie viele technische Errungenschaften zum Gegenstand krimineller Handlungen werden können, reicht deshalb nicht aus, um eine Notstandslage zu begründen. Ohne einen Anlass ein informationstechnisches System auf Sicherheitslücken zu überprüfen, ist somit nicht von § 34 StGB gestattet.[63]

Sollten tatsächliche Umstände (wie z.B. aufgedeckte Fehler in von Unternehmen bekanntlich verwendeter Software) auf eine Sicherheitslücke hinweisen, müsste zudem die Gefahr nicht anders als durch das Hacking abwendbar sein. Dies setzt nicht zuletzt die Erforderlichkeit der Notstandshandlung voraus, d.h. das Hacking müsste sich als das relativ mildeste Mittel erweisen.[64] Vorrangig sind (hoheitliche oder private) Maßnahmen Dritter, welche die Gefahrenlage ohne Eingriff in fremde Rechtsgüter abwenden können.[65] Zu denken wäre somit auch an Bemühungen

[60] Vgl. BGH NJW 1979, 2053, 2054; BGHSt 48, 255, 259, jeweils zu § 35 StGB.

[61] Vgl. etwa *Deusch/Eggendorfer* K&R 2023, 649, 655; *Klaas* MMR 2022, 187, 189; *Schneider* Kriminalistik 2023, 433, 434; *Wagner* DuD 2020, 111, 116.

[62] *Erb*, in MüKo StGB (Fn. 55), § 34 Rn. 85; *Zieschang*, in LK StGB (Fn. 51), § 34 Rn. 59; vgl. auch BGHSt 26, 176, 179 zur Gefahr i.S.d. § 315b I StGB.

[63] *Deusch/Eggendorfer* K&R 2023, 649, 655.

[64] S. nur *Erb*, in MüKo StGB (Fn. 55), § 34 Rn. 104; *Zieschang*, in LK StGB (Fn. 51), § 34 Rn. 90.

[65] *Erb*, in MüKo StGB (Fn. 55), § 34 Rn. 115.

der Verfügungsberechtigten selbst, ließe sich dadurch die zu rechtfertigende Verletzung des Geheimhaltungsinteresses doch von vornherein vermeiden. Hiergegen kann auch nicht vorgetragen werden, dass die Gefahr aus der Sphäre der Verfügungsberechtigten stammt, deren Systeme Sicherheitslücken offenbaren. Wer die Gefahr verursacht, ist nach der Wertung des in § 228 BGB normierten Defensivnotstandes zwar für die den Notstand prägende Interessenabwägung von Bedeutung, nicht aber für die vorgelagerte Frage, ob mildere Mittel für die Gefahrenabwehr existieren. § 34 StGB dient schließlich – anders als § 32 StGB – gerade nicht dem Rechtsbewährungsprinzip, sondern beruht auf dem Solidaritätsprinzip und vermag daher selbst in den Fällen des Defensivnotstandes nur das schonendste Mittel zu rechtfertigen.[66] Dieses Mittel würde bei der Kenntnis von Umständen, die auf Sicherheitslücken hinweisen, aber grundsätzlich darin bestehen, die Betroffenen zu informieren und dadurch in die Lage zu versetzen, die Schwachstelle selbst zu schließen. In Anlehnung an eine jüngere Entscheidung zu einem zur Dokumentation von Verstößen gegen das Tierschutzgesetz begangenen Hausfriedensbruch könnte eine private Eigeninitiative nur dann als gerechtfertigt erwogen werden, wenn eine Einschaltung der Betroffenen von vornherein aussichtslos wäre.[67]

Diese Grundsätze gelten im Übrigen unabhängig davon, wie bei aufgefundenen Schwachstellen weiter verfahren wird. Häufig wird etwa beim Grey-Hat-Hacking dem betroffenen Unternehmen eine Frist gesetzt, um die Schwachstelle zu beseitigen, und nach deren Ablauf die Sicherheitslücke offengelegt. Dies kann verantwortlich (sog. responsible disclosure) geschehen, indem die Lücke erst bekannt gegeben wird, nachdem sie geschlossen wurde, oder auch vor Beseitigung der Schwachstelle erfolgen (sog. full disclosure), verbunden mit der Gefahr, dass die Lücke dann für kriminelle Zwecke ausgenutzt wird.[68] Abgesehen davon, wie die Veröffentlichung als solche strafrechtlich zu bewerten ist, hat sie jedenfalls keinen Einfluss auf die Rechtfertigung des vorangegangenen Hackings. Mit anderen Worten vermag ein verantwortungsvoller Umgang mit der gefundenen Sicherheitslücke eine bereits eingetretene Strafbarkeit wegen des Hackings nicht zu beseitigen.[69]

---

[66] *Neumann*, in NK StGB (Fn. 45), § 34 Rn. 58; *Zieschang*, in LK StGB (Fn. 51), § 34 Rn. 94.

[67] OLG Naumburg NStZ 2018, 472, 474.

[68] Zur Unterscheidung von responsible und full disclosure *Schneider* Kriminalistik 2023, 433, 433.

[69] *Deusch/Eggendorfer* K&R 2023, 649, 655 f.

c) Strafzumessung

Allein das ehrenhafte Anliegen schließt die Strafbarkeit des Grey-Hat-Hackings somit nicht aus. Die hehren Motive sind lediglich auf der Strafzumessungsebene zu berücksichtigen, zählen die Beweggründe des Täters doch zu den ausdrücklich in § 46 II 2 StGB genannten Strafzumessungsfaktoren und handelt es sich hierbei um ein wesentliches Kriterium, um die Täterpersönlichkeit sowie die Verwerflichkeit der Tat zu beurteilen.[70] Insoweit sind auch sozialethische Maßstäbe anzulegen und können demzufolge nachvollziehbare Motive zugunsten des Täters berücksichtigt werden.[71] Mit dem Aufdecken von Schwachstellen in informationstechnischen Systemen zu deren Sicherheit, nicht zuletzt bei Systemen der Kritischen Infrastruktur beizutragen, und dadurch mittelbar auch Gefahren für die Rechtsgüter Einzelner sowie ggf. der Allgemeinheit zu minimieren, dürfte sich in der Regel strafmildernd auswirken.

C. Fazit und Ausblick

Ob ethisches Hacking strafbar ist, ist wie so häufig eine Frage der Definition. Wird für die Bezeichnung als „ethisch“ die Zustimmung der Verfügungsberechtigten als unerheblich angesehen, kann auch ethisches Hacking strafbar sein. Allein die ehrenhafte Motivation vermag eine Strafbarkeit nach § 202a StGB nicht auszuschließen. Demzufolge ist nur das White-Hat-Hacking straflos, weil es mit der Zustimmung der Verfügungsberechtigten geschieht. Das Grey-Hat-Hacking ist hingegen grundsätzlich ebenso zu behandeln wie das Black-Hat-Hacking.

Die derzeitige Rechtslage wird allerdings häufig als nicht befriedigend erachtet, da die betroffenen Systembetreibenden und die zuständigen Behörden allein kaum die angestrebte Sicherheit in der Informationstechnik gewährleisten können und demzufolge auch die Mithilfe Privater benötigen.[72] Daher wird verschiedentlich angedacht, das ethische Hacking straffrei zu belassen. So hinterfragt die sog. „NIS 2.0“-Richtlinie[73] in ihrem Erwägungsgrund 60 die straf- (und zivil-)rechtliche Haftung von

[70] *Kinzig*, in Schönke/Schröder (Fn. 30), § 46 Rn. 12.

[71] *Kinzig*, in Schönke/Schröder (Fn. 30), § 46 Rn. 13; *Schneider*, in Leipziger Kommentar StGB, Bd. 4, 13. Aufl. 2020, § 46 Rn. 76 und Rn. 85.

[72] S. nur *Klaas* MMR 2022, 187, 187 f.

[73] Richtlinie (EU) 2022/2555 vom 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union […]; ABl. EU vom 27.12.2022 Nr. L 333, S. 80.

Forschenden im Bereich der IT-Sicherheit, die sich mit Schwachstellen befassen und deren Tätigkeit sich folglich auch als ethisches Hacking begreifen lässt.[74] Auch der Koalitionsvertrag der derzeitigen Bundesregierung gibt als Ziel aus, dass das „Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren, z.B. in der IT-Sicherheitsforschung, […] legal durchführbar sein" soll.[75] Konkrete Bemühungen, dieses Ziel umzusetzen, sind bislang jedoch nicht zu verzeichnen.[76] Weder in dem Referentenentwurf des Bundesministeriums des Innern und für Heimat eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen vom 21. Dezember 2023, mit dem das sog. KRITIS-Dachgesetz eingeführt werden soll, noch in einem Diskussionspapier aus demselben Ministerium über wirtschaftsbezogene Regelungen zur Umsetzung der genannten NIS 2.0-Richtlinie in Deutschland vom 27. September 2023 finden sich Überlegungen zum Umgang mit ethischem Hacking. Immerhin greifen die aus dem November 2023 stammenden Eckpunkte des Bundesministeriums der Justiz zur Modernisierung des Strafgesetzbuchs die genannte Passage im Koalitionsvertrag auf und kündigen für die erste Jahreshälfte 2024 einen Gesetzentwurf an, in den auch die Erkenntnisse aus Symposien mit Expertinnen und Experten einfließen sollen.

Es wäre in der Tat wünschenswert, wenn bei den einschlägigen legislativen Bemühungen auch das ethische Hacking ausdrücklich aufgegriffen und normiert wird, ob und ggf. unter welchen Voraussetzungen es zulässig ist.[77] Vorschläge wurden insoweit im Schrifttum schon unterbreitet, angefangen von der klareren Normierung des Meldesystems für Sicherheitslücken[78] über die Einführung eines Tatbestandsausschlusses in Anlehnung an § 7a I BSIG[79] bis hin zum Erlangen von Straffreiheit bei Meldung einer Sicherheitslücke nach der responsible disclosure.[80] Dass auf eine Selbstregulierung durch die Praxis (und etwa ausbleibende Strafanträge bei gefundenen Sicherheitslücken) nicht vertraut werden kann,

[74] *Vettermann* MMR 2023, 827, 827 f.

[75] Koalitionsvertrag „Mehr Fortschritt wagen. Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit", S. 16.

[76] Kritisch *Vettermann* MMR 2023, 827, 831 f.

[77] S. schon *Deusch/Eggendorfer* K&R 2023, 649, 654; *Wagner* DuD 2020, 111, 119.

[78] *Vettermann* MMR 2023, 827, 829.

[79] *Kipker/Rockstroh* ZRP 2022, 240, 243.

[80] *Schneider* Kriminalistik 2023, 433, 437.

zeigen eingeleitete Strafverfahren in Fällen ethischen Hackings.[81] Bislang bedeutet somit beim ethischen Hacking selbst ein noch so hehres Anliegen keinen strafrechtlichen Freifahrtschein, heiligt also auch hier der Zweck nicht die Mittel.

[81] S. etwa https://www.heise.de/news/Modern-Solution-Jetzt-doch-Hackerparagraf-Verfahren-gegen-Sicherheitsforscher-9246117.html (letztmals abgerufen am 28.3.2024) zu LG Aachen MMR 2023, 866 mit krit. Anm. *Kipker/Rockstroh* und mit krit. Bespr. *Deusch/Eggendorfer* K&R 2023, 649.