Referentenentwurf

des Bundesministeriums der Justiz

Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Modernisierung des Computerstrafrechts

A. Problem und Ziel

Infolge der fortschreitenden Digitalisierung von Wirtschaft, Staat und Gesellschaft muss der Gesetzgeber darauf achten, dass das Computerstrafrecht an die geänderten technischen Verhältnisse angepasst wird, wenn dies notwendig ist, um den angestrebten Rechtsgüterschutz aufrechtzuerhalten oder auch zu verbessern. Es muss verhindert werden, dass das Strafrecht von Handlungen abschreckt, die im gesellschaftlichen Interesse erfolgen und daher wünschenswert sind. Genau dies droht im Falle des Computerstrafrechts.

Die IT-Sicherheit ist die Achillesferse der Informationsgesellschaft. Die Schließung von Sicherheitslücken hat daher allergrößte Bedeutung für die Abwehr von Cyberangriffen durch Kriminelle und durch fremde Mächte. Daher sind hinsichtlich der Informationstechnologie (IT) die vorhandenen Schwächen in der IT-Infrastruktur in den Blick zu nehmen, die durch die zunehmende Komplexität von IT-Systemen und die teilweise schwachen (Sicherheits-)Standardeinstellungen von IT-Produkten entstehen. Das Aufspüren von Sicherheitslücken in IT-Systemen gehört zu den typischen Tätigkeiten der IT-Sicherheitsforschung. Für ihre Tätigkeit ist nämlich regelmäßig ein Zugriff auf fremde Informationssysteme und Daten notwendig, die sich bereits im praktischen Einsatz befinden. Diese Ausgangslage birgt Strafbarkeitsrisiken, die sich kontraproduktiv auswirken können, weil sie nicht nur von verbotenem, sondern auch von gesellschaftlich erwünschtem Verhalten abschrecken: Die erforderlichen Zugriffshandlungen können jene Straftatbestände erfüllen, die dem Schutz des formellen Datengeheimnisses bzw. der Unversehrtheit von Daten und IT-Systemen dienen (§§ 202a ff., 303a f. des Strafgesetzbuches – StGB). Vor allem ist hier § 202a Absatz 1 StGB in den Blick zu nehmen, der das unbefugte (Sich-)Verschaffen des Zugangs zu Daten unter Strafe stellt, die nicht für den Täter bestimmt und gegen unberechtigten Zugang gesichert sind. Für den Zugang reicht die Möglichkeit der Kenntnisnahme aus, so dass schon ein bloßer Systemzugriff den Tatbestand erfüllen kann.

Eine weitere Kritik am geltenden Recht zielt darauf ab, dass die Strafrahmen die Gefährlichkeit und das hohe Schadenspotential von Computerdelikten teilweise nicht mehr adäquat abbildeten, dies gelte insbesondere bei Angriffen auf kritische Infrastrukturen. Jüngst hat sich die 221. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder vom 19. bis 21. Juni 2024 in Potsdam aus polizeilicher Sicht mit diesem Problem befasst und Reformbedarf auch im Bereich des Strafrechts konstatiert.

Ziel dieses Entwurfs ist die klare gesetzliche Abgrenzung von nicht zu missbilligendem Handeln der IT-Sicherheitsforschung von strafwürdigem Verhalten. Der Gesetzentwurf soll die bestehende Rechtsunsicherheit beseitigen und zudem bei schweren Begehungsformen, bei denen zum Beispiel kritische Infrastrukturen gefährdet oder beeinträchtigt werden, den Strafrahmen erhöhen.

Um bei § 202a StGB (Ausspähen von Daten) sowie § 202b StGB (Abfangen von Daten) alle strafwürdigen Angriffe angemessen ahnden zu können, sollen Regelbeispiele für besonders schwere Fälle eingeführt werden, um eine angemessene Sanktionierung zu ermöglichen.

B. Lösung

Die negative Legaldefinition des Merkmals „unbefugt“ in Artikel 1 StGB-E bewirkt, dass das Aufspüren von Sicherheitslücken in IT-Systemen dann nicht mehr strafbar ist, wenn es im Rahmen der IT-Sicherheitsforschung geschieht. Die Handlung muss dazu in der Absicht erfolgen, eine Sicherheitslücke festzustellen und den Betreiber der Datenverarbeitungsanlage, den Hersteller der betroffenen IT-Anwendung oder das Bundesamt für Sicherheit in der Informationstechnik davon zu unterrichten. Die Handlung muss zudem erforderlich sein, um eine Lücke festzustellen.

Die gleichen Kriterien gelten für die Tathandlungen nach § 202b und § 303a StGB, in denen zukünftig auf § 202a Absatz 3 StGB-E verwiesen werden soll.

Die gewachsene Bedeutung der kritischen Infrastruktur und die Verletzlichkeit, die sich bei schädigenden Zugriffen in der Vergangenheit gezeigt hat, lassen es erforderlich erscheinen, die §§ 202a und 202b StGB so auszugestalten, dass bei Vorliegen eines besonders schweren Falls eine Freiheitsstrafe von drei Monaten bis zu fünf Jahren verwirkt wird.

C. Alternativen

Alternativ könnte der gesetzliche Status quo beibehalten werden. Dieser ist aber zum einen mit Unsicherheiten für die IT-Sicherheitsforschung verbunden und stellt zum anderen keine angemessene Reaktion aufzunehmend schwerere Angriffe dar.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Es werden keine Haushaltsausgaben ohne Erfüllungsaufwand erwartet.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

E.2 Erfüllungsaufwand für die Wirtschaft

Für die Wirtschaft entsteht kein Erfüllungsaufwand.

Davon Bürokratiekosten aus Informationspflichten

Es entstehen keine Informationspflichten.

E.3 Erfüllungsaufwand der Verwaltung

Es entsteht kein Mehraufwand.

F. Weitere Kosten

Für die Justiz entsteht kein Mehraufwand. Weitere Kosten für die Wirtschaft und für soziale Sicherungssysteme werden nicht erwartet, ebenso wenig Auswirkungen auf das Preisniveau, insbesondere auf das Verbraucherpreisniveau.

Referentenentwurf des Bundesministeriums der Justiz

Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Modernisierung des Computerstrafrechts

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des Strafgesetzbuches

Das Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 2 des Gesetzes vom 30. Juli 2024 (BGBl. 2024 I Nr. 255) geändert worden ist, wird wie folgt geändert:

1. Dem § 202a werden die folgenden Absätze 3 und 4 angefügt:

„(3) Die Handlung ist nicht unbefugt im Sinne des Absatzes 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.

(4) In besonders schweren Fällen des Absatzes 1 ist die Strafe Freiheitsstrafe von drei Monaten bis zu fünf Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. einen Vermögensverlust großen Ausmaßes herbeiführt,

2. aus Gewinnsucht oder gewerbsmäßig handelt oder als Mitglied einer Bande, die sich zur fortgesetzten Begehung von solchen Taten verbunden hat oder

3. durch die Tat die Verfügbarkeit, Funktionsfähigkeit, Integrität, Authentizität oder Vertraulichkeit einer kritischen Infrastruktur*) oder die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder beeinträchtigt.“

2. § 202b wird wie folgt geändert:

a) Der Wortlaut wird Absatz 1.

b) Folgender Absatz 2 wird angefügt:

---

*) Der Begriff der „kritischen Infrastrukturen“ in § 2 Abs. 10 BSI-Gesetz wird im NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz durch den Begriff der „kritischen Anlagen“ in § 2 Nummer 22 BSI-Gesetz-E ersetzt! Es muss daher im Laufe des Gesetzgebungsverfahrens geprüft werden, ob gleichwohl hier am Begriff der „kritischen Infrastrukturen“ festgehalten werden kann und sollte.

„(2) § 202a Absatz 3 und 4 gilt entsprechend.“

3. Dem § 303a wird folgender Absatz 4 angefügt:

„(4) § 202a Absatz 3 gilt entsprechend.“

Artikel 2

Inkrafttreten

Dieses Gesetz tritt am … [einsetzen: erster Tag des auf die Verkündung folgenden Quartals] in Kraft.

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

1. IT-Sicherheitsforschung ohne Strafbarkeitsrisiken

Die vorgeschlagenen Regelungen greifen die Vereinbarung des Koalitionsvertrags für die 20. Legislaturperiode auf und berücksichtigen Erkenntnisse der im Jahr 2023 durch das Bundesministerium der Justiz durchgeführten Symposien zum Reformbedarf im Computerstrafrecht. „Die Ausübung von IT-Sicherheitsforschung ist, jedenfalls bei wissenschaftstypischer Anwendung sogenannter offensiver Methoden, eine gefahrgeneigte Tätigkeit. Denn nicht nur der als „Hackerparagraph“ fehlbezeichnete § 202c StGB, sondern auch eine Mehrzahl weiterer Straftatbestände des Kern- und Nebenstrafrechts zeigen der IT-Sicherheitsforschung Grenzen auf.“ (Golla/Brodowski, IT-Sicherheitsforschung und IT-Strafrecht, S. 37; vgl. auch Whitepaper zur Rechtslage der IT-Sicherheitsforschung. Reformbedarf aus Sicht der angewandten Sicherheitsforschung). Mit der Einführung eines Tatbestandsausschlusses für IT-Sicherheitsforschende sollen bestehende Konflikte der Strafverfolgung mit Interessen der IT-Sicherheit gelöst werden, ohne dabei den Anspruch zu erheben, sämtliche rechtliche Schwierigkeiten der IT-Sicherheitsforschung auf diese Weise zu beheben. Dabei nutzen die unter diesem Begriff zusammengefasste wissenschaftliche IT-Sicherheitsforschung, die IT-Sicherheitsbranche, aber auch frei tätige Expertinnen und Experten oftmals die gleichen Mittel und Methoden wie Straftäter, um Sicherheitslücken aufzudecken, wenn auch aus gänzlich anderen Motiven.

Die Frage, ob „Hacking“ in der Absicht, Sicherheitslücken aufzufinden und zu schließen, nicht nur straflos bleiben, sondern sogar gefördert werden sollte, stellt sich auch auf europäischer und internationaler Ebene. So wird in der NIS-2-Richtlinie[1)] darauf hingewiesen, dass Schwachstellen häufig von Dritten entdeckt werden, und es wird eine koordinierte Offenlegung von Schwachstellen empfohlen, welche die Koordinierung zwischen der meldenden natürlichen oder juristischen Person und dem Hersteller oder Anbieter der potenziell gefährdeten IKT-Produkte oder -Dienste umfassen sollte (vgl. Erwägungsgründe 58, 60 und 61 sowie die Erwähnung in Artikel 7 Absatz 2c in Verbindung mit Artikel 12 Absatz 1). Einem Gutachten des Wissenschaftlichen Dienstes des Deutschen Bundestages zufolge (WD 7 - 3000 - 104/23) lösen einige Staaten das Problem, indem sie für Hacker, die „guten Glaubens“ handeln, keine Schäden hervorrufen und die von ihnen aufgefundene Sicherheitslücke melden, das Absehen von Strafverfolgung ermöglichen; an der grundsätzlichen Strafbarkeit der Handlung wird jedoch in der Regel festgehalten.[2)] Eine Ausnahme stellen demnach die Regelungen in Österreich dar, bei denen für die Strafbarkeit eine qualifizierte Absicht der Spionage oder der Verwendung der Daten erforderlich ist (§ 118a des Strafgesetzbuches – StGB).

Der Entwurf steht im Kontext der Erreichung der Ziele der Resolution der Generalversammlung der Vereinten Nationen vom 25. September 2015 „Transformation unserer Welt: die UN-Agenda 2030 für nachhaltige Entwicklung“ und trägt insbesondere zur Erreichung des

---

1) Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nummer 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148, vom 27. Dezember 2022, Amtsblatt der Europäischen Union L 333/80.

2) Instruktiv zu den Regelungen in den Niederlanden auch Bao/Zech in Golla/Brodowski a.a.O., S. 168 ff.

Nachhaltigkeitsziels 9 bei, eine widerstandsfähige Infrastruktur aufzubauen, inklusive und nachhaltige Industrialisierung zu fördern und Innovationen zu unterstützen.

§ 202a StGB wurde durch das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität vom 15. Mai 1986 (2. WiKG; BGBl I. S. 721) eingeführt. Der Wortlaut der Vorschrift differenziert nicht zwischen kriminellen und anderen Zielrichtungen der dort unter Strafe gestellten Handlung. Unbeschadet früherer Erwägungen, einfaches „Hacking“ nicht unter Strafe zu stellen (vgl. Beschlussempfehlung und Bericht des Rechtsausschusses, Bundestagsdrucksache 10/5058, S. 28 f.), besteht inzwischen ein erhebliches Risiko, dass aus Sicht der Strafverfolgungsbehörden und Gerichte auch solche „Hacker“ den Tatbestand erfüllen, die sich nur deswegen Zugang zu einem System verschaffen, um dort Sicherheitslücken aufzufinden und auf diese aufmerksam zu machen, ohne sie auszubeuten.

Durch das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG) wurde § 202a Absatz 1 StGB im Jahr 2007 neu gefasst. Die Neufassung des Absatzes 1 diente der Umsetzung von Artikel 2 des Europarats-Übereinkommens über Computerkriminalität (Rechtswidriger Zugang) und Artikel 2 des EU-Rahmenbeschlusses über Angriffe auf Informationssysteme (Rechtswidriger Zugang zu Informationssystemen) in innerstaatliches Recht.

Danach wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe 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 einer Zugangssicherung verschafft. Nach Ansicht des damaligen Gesetzgebers trifft die neue Vorschrift („sich Zugang verschaffen“) mit ihrer vorverlagerten Strafbarkeit das eigentliche Unrecht besser als die vorherige Regelung („sich Daten verschaffen“). Im Wesentlichen hat sie bezüglich der bereits seinerzeit herrschenden Auslegung des früheren § 202a StGB nur eine Klarstellungsfunktion. Die generelle Gefährlichkeit und Schädlichkeit von „Hacking“-Angriffen zeige sich vor allem in jüngster Zeit auch in Deutschland, weshalb an ihrer Strafwürdigkeit und Strafbedürftigkeit keine Zweifel bestehen (Bundestagsdrucksache 16/3656, S. 9).

Die Überwindung einer Zugangssicherung ist, vor allem in der weiten Interpretation, die dieses Tatbestandsmerkmal in der Rechtsprechung gefunden hat, eine typische Handlungsweise bei IT-Sicherheitstests. IT-Sicherheitstests können nämlich nicht immer in einer künstlichen Testumgebung durchgeführt werden, sondern müssen regelmäßig echte, am Markt angebotene Produkte und Systeme einbeziehen (Brodowski, in: Whitepaper zur Rechtslage der IT-Sicherheitsforschung. Reformbedarf aus Sicht der angewandten Sicherheitsforschung, S. 9). Damit hängt es in derartigen Fällen maßgeblich vom Merkmal „unbefugt“ ab, ob sich die Durchführenden strafbar machen. Zu einem nicht tatbestandsmäßigen Handeln führt jedenfalls das Einverständnis derjenigen, die zum Zugriff berechtigt sind. Ein beauftragter Penetrationstest ist damit nicht strafbar. Problematisch ist allerdings, 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. Dem lässt sich entgegenhalten, dass die Vermeidung eines hohen organisatorischen Aufwands noch kein Grund dafür sei, ohne Einverständnis auf fremde IT-Systeme zuzugreifen. Allerdings kann es in einem gewissen Umfang auch wünschenswert sein, in natürlichen Umgebungen Sicherheitslücken aufzuspüren, 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 (Golla/Brodowski a. a. O. S. 10). Viele Unternehmen fordern IT-Sicherheitstester aktiv dazu auf, zu versuchen, ihre Sicherungen zu überwinden und dies dann unter einer bestimmten E-Mail-Adresse zu melden (vgl. z. B. die Internet-Seite der Deutschen Telekom „Hilf uns besser zu werden“). Im Rahmen von sogenannten Bug Bounties werden Sach- oder Geldpreise für die Entdecker von Fehlern in der Software von Unternehmen oder Verbänden ausgelobt.

Die vorgeschlagenen Regelungen sollen dazu beitragen, die Rechtsunsicherheit zu beseitigen, die im Hinblick auf Zugriff und Auswertung von fremden Daten bei der Sicherheitsforschung im materiellen Strafrecht besteht. Die Neuregelung in § 202a Absatz 3 StGB-E knüpft konsequenterweise an das Tatbestandsmerkmal „unbefugt“ an. So wird gewährleistet, dass nur Handeln mit Schädigungsabsicht unter die Vorschrift fällt, während das Aufspüren von Sicherheitslücken unter den in der Regelung genannten Voraussetzungen straflos bleiben soll.

Der Entwurf verzichtet darauf, über die Absicht im subjektiven Tatbestand hinaus zu verlangen, dass z. B. bestimmte Tatsachen die Annahme rechtfertigen, dass im konkreten Fall eine Sicherheitslücke vorliegen könnte, da eine entsprechende Annahme nicht praktikabel wäre. Die Feststellung der Lücke ist ja gerade das Anliegen der IT-Sicherheitsforschung, auch wenn es dafür (noch) keine konkreten Anhaltspunkte gibt. Die Feststellung der Absicht wird aber immer anhand objektiver Merkmale erfolgen müssen, so dass eine bloße Behauptung, in guter Absicht gehandelt zu haben, das Gericht nicht überzeugen wird, wenn dies nicht auch nach den im Übrigen festgestellten Tatsachen glaubhaft erscheint.

Der Anwendungsbereich der Regelung wird nicht auf die wissenschaftliche Forschung beschränkt. Auch unabhängig von ihrer Qualifizierung tragen sowohl kommerzielle Anbieter als auch die unabhängige IT-Sicherheitsforschung zur IT-Sicherheit maßgeblich bei, indem sie Sicherheitslücken aufspüren und melden. Vor diesem Hintergrund erscheint es nicht zweckmäßig, den Tatbestandsausschluss nur auf Forschung im Sinne von „Wissenschaft“ zu beschränken, sondern auch „Ethical Hackers“ (z.T. auch „Grey Hat Hackers“ genannt) einzubeziehen.

Die IT-Sicherheitsforschung soll nicht verpflichtet werden, einen bestimmten Meldeweg einzuhalten, zumal es dazu noch kein allgemein anerkanntes standardisiertes Verfahren (responsible disclosure) gibt. Es soll aber auch nicht ausreichen, die Sicherheitslücke irgendjemandem mitzuteilen oder sie z. B. auf der eigenen Homepage veröffentlichen zu wollen; die beabsichtigte Meldung muss an einen Verantwortlichen gerichtet sein, der in der Lage ist, die Lücke zu schließen oder dies zu veranlassen. Dabei lehnt die im Entwurf verwendete Formulierung sich an § 15 Absatz 2 des Entwurfs für das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz-E) an[3] und definiert gleichzeitig den Begriff der „Sicherheitslücke“ für die Zwecke des Strafrechts.

Die Maßnahme muss weiterhin erforderlich sein, um eine Sicherheitslücke festzustellen.

Die gleichen Kriterien gelten für die Tathandlungen nach § 202b und § 303a StGB, die zukünftig auf § 202a Absatz 3 StGB-E verweisen. Beide Vorschriften beschreiben Tathandlungen, die häufig aus technischen Gründen verwirklicht werden, wenn ein Datenzugang aus Gründen der IT-Sicherheitsforschung erfolgt (vgl. dazu Golla/Brodowski a. a. O. S. 42 ff).

---

[3]) Artikel 1 des Entwurfs der Bundesregierung eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) (BR-Drs. 380/24): § 15 (2) BSI-Gesetz-E: „Wird durch Abfragen gemäß Absatz 1 eine Schwachstelle oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt, informiert das Bundesamt darüber unverzüglich die für das informationstechnische System Verantwortlichen. Gehört das informationstechnische System zu einer Einrichtung der Bundesverwaltung, sind zugleich die Informationssicherheitsbeauftragten der betroffenen Ein-richtung der Bundesverwaltung nach § 45 und des übergeordneten Ressorts nach § 46 zu informieren. Das Bundesamt soll dabei auf bestehende Möglichkeiten zur Abhilfe des Sicherheitsrisikos hinweisen. Sind dem Bundesamt die Verantwortlichen nicht bekannt oder ist ihre Identifikation nur mit unverhältnismäßigem Aufwand oder über eine Bestandsdatenabfrage nach § 12 möglich, so ist hilfsweise der betreibende Dienstleister des jeweiligen Netzes oder Systems unverzüglich zu benachrichtigen, wenn über-wiegende Sicherheitsinteressen nicht entgegenstehen.“

2. Erhöhung des Strafrahmens für besonders schwere Fälle

§ 202a StGB (Ausspähen von Daten) sowie § 202b StGB (Abfangen von Daten) weisen zudem das Problem auf, dass nicht alle Angriffe mit der angedrohten Höchststrafe von drei Jahren Freiheitsstrafe angemessen geahndet werden können. Dies gilt insbesondere für das immer professionellere Agieren in fremden Datensystemen bei Angriffen auf kritische Infrastrukturen. Die gewachsene Bedeutung der IT-Sicherheit für die kritische Infrastruktur und deren Verletzlichkeit, die sich bei schädigenden Zugriffen in der Vergangenheit gezeigt hat, erfordern es, die §§ 202a und 202b StGB so auszugestalten, dass bei Vorliegen eines besonders schweren Falls eine Freiheitsstrafe von drei Monaten bis zu fünf Jahren verwirkt wird.

3. Keine Änderung von § 202c StGB erforderlich

Keinen Änderungsbedarf sieht der Entwurf bei § 202c StGB, der gelegentlich als „Hackerparagraph“ bezeichnet wird und der das Vorbereiten des Ausspähens und Abfangens von Daten mit Strafe bedroht. Die Änderungen der §§ 202a und 202b StGB werden dazu führen, dass hier für die IT-Sicherheitsforschung keine Strafbarkeitsrisiken mehr bestehen.

Die Vorschrift setzt nämlich voraus, dass das Tatobjekt ein Computerprogramm ist, dessen Zweck die Begehung einer Tat nach § 202a oder § 202b StGB ist. Ferner muss der Täter eine Straftat nach den §§ 202a und 202b StGB vorbereiten.

Jedenfalls an einer dieser Voraussetzungen wird es bei Computerprogrammen mit Bezug zur IT-Sicherheitsforschung fehlen. Das Bundesverfassungsgericht (BVerfG, ZUM 2009, 745) hat klargestellt, dass mit dem „Zweck zur Begehung (…)“ die vom Täter verfolgte Absicht und nicht etwa die objektive Eignung des Computerprogramms zur Begehung von Straftaten gemeint ist. Wenn also jemand ein Hackertool herstellt oder verbreitet und beabsichtigt, dass dieses zu Handlungen eingesetzt wird, die unter den hier vorgeschlagenen Tatbestandsausschluss fallen, bezweckt er keine Begehung von Straftaten. Gleiches gilt auch, wenn er keine Kenntnis davon hat, dass das Computerprogramm zu kriminellen Zwecken verwendet wird oder den Verendungszweck nicht kennt.

Selbst wenn ein „Hackertool“ zu kriminellen Zwecken hergestellt und verbreitet wurde, kann jedermann sich dieses Tool straffrei verschaffen, wenn es zur IT-Sicherheitsforschung benötigt wird. Zwar liegt der Zweck des Computerprogramms darin, eine Tat nach den §§ 202a oder 202b StGB zu begehen. Aber es fehlt an der zweiten relevanten Voraussetzung des § 202c StGB, nämlich an der Handlung zur Vorbereitung einer Tat nach den §§ 202a oder 202b StGB. Denn nach der Rechtsprechung des BVerfG setzt dieses Tatbestandsmerkmal voraus, dass der Handelnde billigend in Kauf nimmt, dass das Tool zur Begehung einer Straftat nach den §§ 202a oder § 202b StGB eingesetzt werde. Wenn er aber Handlungen vornehmen will, die von dem Tatbestandsausschluss umfasst sind, fehlt ihm ein entsprechender Vorsatz.

Für § 303a Abs. 3 StGB i. V m. § 202c StGB gelten diese Überlegungen sinngemäß.

4. Keine Tatbestandsausnahme für Computersabotage

Für den Straftatbestand des § 303b StGB (Computersabotage) wird kein Tatbestandsausschluss vorgesehen. Vorsätzlich eine derart gravierende Störung zu verursachen, kann auch im Interesse der IT-Sicherheit nicht straflos bleiben.

5. Weitere relevante Vorschriften ohne Änderungsbedarf

a) Sachbeschädigung

Die Sachbeschädigung nach § 303 StGB kann bei Zugriffen auf fremde Informationssysteme erfüllt werden, etwa wenn das betroffene IT-Gerät über einen nicht unerheblichen Zeitraum nicht eingesetzt werden kann. Ist dieser Tatbestand neben § 303b StGB erfüllt, wird § 303 StGB verdrängt (das Konkurrenzverhältnis zwischen § 303 und § 303b StGB ist umstritten, vgl. Goeckenjan, in: Leipziger Kommentar zum StGB, 13. Auflage 2023, § 303b, Rn. 41: § 303b StGB konsumiert § 303 StGB; Hecker, in: Schönke/Schröder, StGB, 30. Auflage 2019, § 303b, Rn. 23: Tateinheit).

§ 303 StGB erlangt daher nur Bedeutung, wenn der Tatbestand des § 303b StGB nicht erfüllt ist. Das ist vor allem dann relevant, wenn zwar die Funktionsfähigkeit einer fremden Sache beeinträchtigt wird, dies aber keine erhebliche Störung einer Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, zur Folge hat. Ein Tatbestandsausschluss wird hier nicht vorgesehen, weil die Sachbeschädigung, die vorsätzlich erfolgen muss, hier vergleichbar mit anderen Begehungsformen bleibt.

b) Gesetz zum Schutz von Geschäftsgeheimnissen

Im Zuge der IT-Sicherheitsforschung können auch Geschäftsgeheimnisse erlangt und im Disclosure-Prozess offengelegt werden. Ob hier eine Strafbarkeit nach § 23 des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) droht, hängt vor allem davon ab, ob der Täter zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht handelt, dem Inhaber eines Unternehmens Schaden zuzufügen. Denkbar ist ein Handeln mit Schädigungsabsicht, doch werden diese Voraussetzungen eher selten vorliegen. Relevanter wird ein Handeln aus Eigennutz sein. Um ein Strafbarkeitsrisiko der IT-Sicherheitsforschung gemäß § 23 GeschGehG auszuschließen, ist es geboten, in diesen Fällen einen Gleichlauf zwischen § 202a Absatz 3 StGB-E und § 23 GeschGehG herzustellen. Um dem – unionsrechtlich in vielen Bereichen vollharmonisierten – Schutz des Geschäftsgeheimnisses in ausreichendem Maße Rechnung zu tragen, ist es erforderlich, einen angemessenen Ausgleich zwischen Geschäftsgeheimnisschutz und im öffentlichen Interesse liegender Sicherheitsforschung zu schaffen. Gerichte werden bei der Prüfung dieser Frage zukünftig zu berücksichtigen haben, dass die IT-Sicherheitsforschung unter den Voraussetzungen des § 202a Absatz 3 StGB-E regelmäßig ein sonstiges legitimes Interesse im Sinne des § 5 GeschGehG darstellt, sofern der Zugang allein darauf beschränkt bleibt und auch im Übrigen ein angemessener Schutz des Geschäftsgeheimnisses durch entsprechende Beschränkung des Handlungszwecks im Einzelfall, insbesondere durch angemessene Geheimhaltungsmaßnahmen, gesichert ist.

Eine gesondert zu betrachtende Konstellation liegt vor, wenn Sicherheitslücken im Wege des Reverse Engineering ermittelt werden sollen. Dieser Begriff bezeichnet eine Produktanalyse, in der ein existentes Produkt untersucht wird, um dessen Bestandteile, Funktionsweisen und auch den Herstellungsprozess nachvollziehen zu können. Es handelt sich also um einen gedachten umgekehrten Herstellungsprozess. Er vollzieht sich nicht von der Idee zum Produkt, sondern vom Produkt zur Idee. Für das Erlangen von Geschäftsgeheimnissen durch Reverse Engineering enthält das GeschGehG zwar eine Regelung in § 3 Abs. 1 Nr. 2. Diese Vorschrift erlaubt Reverse Engineering aber nur dann, wenn der Testgegenstand öffentlich verfügbar gemacht wurde oder sich im rechtmäßigen Besitz des Beobachtenden, Untersuchenden, Rückbauenden oder Testenden befindet und dieser keiner Pflicht zur Beschränkung der Erlangung des Geschäftsgeheimnisses unterliegt. Diese Voraussetzungen werden in der IT-Sicherheitsforschung meistens fehlen. Das Nichtvorliegen der Tatbestandsvoraussetzungen des § 3 Abs. 1 Nr. 2 GeschGehG bedeutet aber nicht, dass das Verhalten nicht dennoch als sonstiges legitimes Interesse gewertet werden und trotz Vorliegens einer unerlaubten Handlung ausnahmsweise gerechtfertigt sein kann. Denn anderenfalls würde § 5 GeschGehG regelmäßig leerlaufen. Erforderlich ist hier stets eine Einzelfallabwägung. Innerhalb der Prüfung von § 5 GeschGehG muss dann abgewogen werden, ob ein so starkes legitimes Interesse vorliegt, dass dies den Eingriff in das Geschäftsgeheimnis rechtfertigt. Die Gesetzesbegründung (Bundestagsdrucksache 19/4724, 28) zu § 5 GeschGehG führt dabei aus, dass es sich bei den berechtigten Interessen auch um

wirtschaftliche Interessen handeln kann, so dass ein vollständig altruistisches Handeln nicht notwendig ist.

c) Urheberrecht

Wird Software auf Fehler untersucht, kann es in einigen Fällen erforderlich sein, den Quellcode zu vervielfältigen, zu übersetzen oder auf sonstige Weise zu bearbeiten. Insbesondere kann eine Dekompilierung des Objektcodes in einen „Quellcode“ erforderlich werden. Wird zum Zwecke der IT-Sicherheitsforschung eine solche urheberrechtlich relevante Handlung vorgenommen, ohne dass diese durch eine vertragliche Erlaubnis des Rechtsinhabers (Lizenz) oder eine gesetzliche Erlaubnis („Schranke“) abgedeckt ist, liegt ein Urheberrechtsverstoß vor, der über die §§ 106 ff. des Urheberrechtsgesetzes (UrhG) strafbewehrt ist.

Es ist jeweils im Einzelfall zu prüfen, ob die Lizenzbedingungen des Computerprogramms die beabsichtigte Nutzung des Quellcodes zulassen. Zum Teil stellen Rechtsinhaber Programme gezielt zur Fehlersuche bereit (z. B. als sog. „Bug Bounty Programm“) und definieren hierfür gesonderte Lizenzbedingungen. Die Lizenzbedingungen für die „Bug Bounty“ können die allgemeinen Lizenzbedingungen des Computerprogramms ergänzen oder modifizieren, indem sie etwa erlauben, dass ein Programm von registrierten Nutzenden, in einem bestimmten Zeitraum und zum Zweck der Sicherheitsforschung dekompiliert werden darf.

Die gesetzlich erlaubten Nutzungen von Computerprogrammen ergeben sich aus § 69d und § 69e UrhG. Die §§ 69a ff. UrhG setzen die Vorgaben der Richtlinie 91/250/EWG um (ersetzt durch die konsolidierte Fassung als Richtlinie 2009/24/EG – „Software-RL“).

Die derzeitigen Vorgaben des Unionsrechts lassen keinen Spielraum dafür, explizit gesetzliche Nutzungserlaubnisse für die IT-Sicherheitsforschung im UrhG zu schaffen. Die Software-RL sieht keine Möglichkeit für die Mitgliedstaaten vor, für die IT-Sicherheitsforschung eine Beschränkung des urheberrechtlichen Schutzes von Computerprogrammen im nationalen Recht einzuführen.

Der EuGH hat jedoch die Vorgaben der Richtlinie und damit auch der §§ 69a ff. UrhG im Hinblick auf Dekompilierungen zur Fehlerbehebung konkretisiert. In seinem Urteil vom 6. Oktober 2021 hat er sich eingehend zu der Frage geäußert, inwieweit eine Dekompilierung zur Fehlerbehebung auf Artikel 5 Absatz 1 Software-RL gestützt werden kann: Nach Artikel 5 Absatz 1 Software-RL bedarf es keiner Zustimmung des Rechtsinhabers zu urheberrechtlich relevanten Handlungen, wenn diese „für eine bestimmungsgemäße Benutzung des Computerprogramms einschließlich der Fehlerberichtigung durch den rechtmäßigen Erwerber notwendig sind“. Nach dem EuGH ist Artikel 5 Absatz 1 der Software-RL dahin auszulegen, dass der rechtmäßige Erwerber eines Computerprogramms berechtigt ist, dieses ganz oder teilweise zu dekompilieren, um Fehler, die das Funktionieren dieses Programms beeinträchtigen, zu berichtigen, einschließlich des Falles, dass die Berichtigung darin besteht, eine Funktion zu deaktivieren, die das ordnungsgemäße Funktionieren der Anwendung, zu der dieses Programm gehört, beeinträchtigt. Der Begriff „Fehler“ sei dabei nach seinem üblichen Sinn im gewöhnlichen Sprachgebrauch auszulegen, wobei der Zusammenhang, in den er sich einfügt, und die Ziele zu berücksichtigen sind, die mit der Regelung verfolgt werden. Im Bereich der Informatik bezeichne ein Fehler im Allgemeinen einen Defekt in einem Computerprogramm, der zu dessen Fehlfunktion führt. Ein solcher Defekt, der einen Fehler im Sinne dieser Bestimmung darstellt, müsse die Möglichkeit beeinträchtigen, das betreffende Programm bestimmungsgemäß zu benutzen. Vervielfältigungen dürften – so betont der EuGH – zum einen nur in dem für die Berichtigung notwendigen Ausmaß erfolgen. Die Berichtigung von Fehlern, welche die bestimmungsgemäße Benutzung eines Programms beeinträchtigten, bringe nach dem EuGH in den meisten Fällen eine Änderung des Codes dieses Programms mit sich und erfordere für die Durchführung dieser Berichtigung den Zugriff auf den Quellcode oder zumindest auf den Quasi-Quellcode dieses Programms. Wenn der Quellcode dem Erwerber des betreffenden Programms rechtlich oder

vertraglich zugänglich ist, kann jedoch nicht davon ausgegangen werden, dass eine Dekompilierung dieses Programms „notwendig“ ist. Zum anderen hat der EuGH zu Artikel 5 Absatz 1 Software-RL auch klargestellt, dass die Lizenzbedingungen für Computerprogramme grundsätzlich Grenzen für urheberrechtlich relevante Handlungen setzen können. Durch die Lizenzbedingungen dürfe aber vertraglich nicht jede Möglichkeit einer Berichtigung für die Berechtigten ausgeschlossen werden (EuGH, Urteil vom 6. Oktober 2021 – C-13/20). Die Vorgaben des Artikels 5 Absatz 1 Software-RL sind in § 69d Absatz 1 UrhG weitgehend wortgleich umgesetzt (Bundestagsdrucksache 12/4022, S. 12). Entscheidend ist damit auch unter § 69d Absatz 1 UrhG, dass im Einzelfall, z. B. dem Fall, dass zur Suche und Identifizierung eines Fehlers eine Software dekompiliert werden soll, zu prüfen ist, ob die Dekompilierung zur Berichtigung des Fehlers erforderlich ist bzw. von den Lizenzbedingungen abgedeckt ist.

In Deutschland wird die unerlaubte Nutzung urheberrechtlich geschützter Inhalte umfassend strafrechtlich sanktioniert (§§ 106 ff. UrhG). Für den Bereich der Computerkriminalität ist Deutschland auch nach Artikel 10 des Übereinkommens des Europarats vom 23. November 2001 über Computerkriminalität (Budapest Konvention, ETS-Nummer 185) dazu verpflichtet, Urheberrechtsverletzungen, die vorsätzlich, in gewerbsmäßigem Umfang und mittels eines Computersystems begangen werden, strafrechtlich zu sanktionieren. Das Kriterium des „gewerbsmäßigen Umfangs“ in Artikel 10 Absatz 1 dieses Übereinkommens dient zur Angleichung an die Vorgaben in Artikel 61 des Übereinkommens über handelsbezogene Aspekte der Rechte des geistigen Eigentums (TRIPS) (Explanatory Report to the Convention on Cybercrime, ETS-Nummer 185, S. 18). Der „gewerbsmäßige Umfang“ nach Artikel 61 TRIPS ist erfüllt bei einer auf Dauer angelegten, grundsätzlich nicht lediglich im Einzelfall erfolgten Tatbegehung, mittels derer die Lebensführung vor dem Hintergrund einer gewissen Ertragskraft finanziert werden soll. Nicht umfasst sind daher Verstöße, die lediglich im privaten Bereich und ohne nennenswerte finanzielle Bereicherungsabsicht begangen werden (vgl. Vander/Steigüber, in: Busche/Stoll/Wiebe, TRIPS, 2. Auflage 2013, Artikel 61, Rn. 7). Für die Ermittlung der Ertragskraft ist eine produkt- und marktspezifische Untersuchung vorzunehmen (vgl. Vander/Steigüber a. a. O., Artikel 61, Rn. 9). Die Vorgaben von Artikel 10 der Budapest Konvention werden durch die §§ 106 und 108a UrhG umgesetzt (Bundestagsdrucksache16/7218, S. 46). Zwar sind demnach auch nicht-gewerbsmäßige Urheberrechtsverletzungen strafbar. Hieran soll jedoch im Sinne eines einheitlichen und umfassenden Schutzes urheberrechtlich geschützter Inhalte durch das Strafrecht festgehalten werden. Bagatellfällen mit geringem Unrechtsgehalt kann, wie auch im Übrigen bei § 106 UrhG, mit strafprozessualen Möglichkeiten begegnet werden (vgl. Bundestagsdrucksache 16/1828, S. 18).

6. Strafbarkeit bei späterer Absichtsänderung

Wer eine Lücke in einem Sicherheitssystem in guter Absicht identifiziert, die Sicherheitslücke aber im Anschluss daran nicht meldet oder offenlegt, sondern missbräuchlich verwendet, macht sich zukünftig nicht mehr nach § 202a Absatz 1, § 202b Absatz 1 oder § 303a Absatz 1 StGB strafbar. Man mag zwar einwenden, dass sich dieses Problem aus praktischer Sicht nicht allzu oft stellen wird. Denn man wird dem Beschuldigten selten glauben, dass er zunächst eine schützenswerte Absicht hatte, wenn er die Daten im Anschluss verkauft oder erhebliche Schäden verursacht. Wie oben bereits erläutert wurde, ist die Absicht – wie auch sonst der subjektive Tatbestand – anhand der objektiven Umstände des Falles zu ermitteln, zu denen auch das Nachtatverhalten gehört.

Aber auch in den Fällen, in denen davon ausgegangen werden muss, dass tatsächlich bei der Begehung der Tat in guter Absicht gehandelt wurde, entstehen keine unvertretbaren Strafbarkeitsdefizite.

Es sind verschiedene Konstellationen denkbar:

Wenn die Daten Geschäftsgeheimnisse enthalten, kommt eine Strafbarkeit nach den bereits oben erörterten Vorschriften des GeschGehG in Betracht. Die Nutzung oder das Offenlegen (schon die Eröffnung eines Geschäftsgeheimnisses gegenüber einer einzigen Person, vgl. Keller, in: Keller/Schönknecht/Glinke, GeschGehG, 1. Auflage 2021, § 4 Rn. 63) von Geschäftsgeheimnissen wird nach § 23 Absatz 1 Nummer 2 GeschGehG bestraft, wenn damit ein bestimmter Zweck verfolgt wird, namentlich die Förderung des eigenen oder fremden Wettbewerbs, Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen, und die Handlung gegen § 4 Absatz 2 Nummer 1 Buchstabe a GeschGehG verstößt. § 4 Absatz 2 Nummer 1 Buchstabe a GeschGehG verbietet die Nutzung oder Offenlegung von Geschäftsgeheimnissen, wenn diese durch eine Handlung nach § 4 Absatz 1 Nummer 1 GeschGehG erlangt wurden. § 4 Absatz 1 Nummer 1 GeschGehG erfasst die unbefugte Erlangung. Eine solche liegt auch dann vor, wenn nach § 202a Absatz 3 StGB-E beim Datenzugang keine unbefugte Handlung im Sinne von § 202a Absatz 1 StGB vorlag. Wie oben dargelegt wurde, führt diese Tatsache zwar gegebenenfalls zur Annahme eines legitimen Interesses nach § 5 GeschGehG, führt aber nicht dazu, dass der Handelnde das Geschäftsgeheimnis ursprünglich – rückwirkend – rechtmäßig erlangt hat. Das Erlangen dürfte rechtswidrig bleiben, das Handeln zu den Zwecken des § 202a Absatz 3 StGB-E ist aber ausnahmsweise gerechtfertigt. Geht der IT-Sicherheitsforscher darüber hinaus, bleibt es dabei, dass er das Geschäftsgeheimnis grundsätzlich unerlaubt erlangt hat und Handlungen, die nicht gemäß § 5 GeschGehG gerechtfertigt sind, nach § 23 GeschGehG strafbar bleiben.

Eine weitere „Strafbarkeitslücke“ könnte auf Seiten des Empfängers des Geschäftsgeheimnisses bestehen. § 23 Absatz 2 GeschGehG enthält eine Strafnorm für den Fall, dass jemand einen bestimmten Zweck verfolgt und ein Geschäftsgeheimnis, das er durch eine fremde Handlung nach Absatz 1 Nummer 2 oder 3 GeschGehG erlangt hat, nutzt oder offenlegt. Ein Fall des Erlangens nach § 23 Absatz 1 Nummer 2 oder 3 GeschGehG liegt bei der IT-Sicherheitsforschung aber nicht vor. Die Geschäftsgeheimnishehlerei ist also nur bei bestimmten Vortaten nach dem Geschäftsgeheimnisgesetz strafbar. Dennoch besteht hier keine Lücke, weil es sich jedenfalls um einen Fall der Geldwäsche (§ 261 Absatz 1 Nummer 3 Variante 2 StGB) handeln könnte. Entscheidend dürfte sein, ob es sich bei Geschäftsgeheimnissen um einen Gegenstand im Sinne des § 261 Absatz 1 StGB handelt und durch welche Vortat es erlangt wurde. Dabei ist zu berücksichtigen, dass Geschäftsgeheimnisse nicht zwingend kodiert und deshalb Daten sein müssen; sie können auch als bloße Information übertragen werden (etwa indem der Handelnde einer anderen Person von dem Geschäftsgeheimnis erzählt). Ob Daten oder gar bloße Informationen von dem Gegenstandsbegriff in § 261 StGB erfasst werden, wird in der Literatur nicht einheitlich beantwortet (bejahend für einen Paysafe-Code BGH, NStZ-RR 2019, 112 (113), generell bejahend („jede bestimmbare, einer Person zuordenbare und übertragbare Position, die einen wirtschaftlichen Wert hat“) Altenhain, in: Nomos Kommentar zum StGB, 6. Auflage 2023, § 261, Rn. 11; ablehnend (Daten kein Gegenstand im Sinne des § 261 StGB) Neuheuser, in: Münchener Kommentar zum StGB, 4. Auflage 2021, § 261, Rn. 36).

Bei Daten, die keine Geschäftsgeheimnisse darstellen, bleibt es bei der Strafbarkeit, wenn es sich um personenbezogene Daten handelt. Hier kann der Täter regelmäßig nach § 42 Absatz 1 Nummer 1 oder Absatz 2 Nummer 1 BDSG bestraft werden. Hinsichtlich des Empfängers der Daten kommt eine Strafbarkeit nach § 42 Absatz 2 Nummer 1 BDSG in Betracht.

Nur wenn es sich nicht um personenbezogene, sondern nur um „gewöhnliche“ Daten handelt, kommt für den Täter kein Straftatbestand in Betracht, und für den Erwerber der Daten wird § 202d StGB dadurch gesperrt, dass mangels rechtswidriger Vortat eine Datenhehlerei ausscheidet. Dies kann aber hingenommen werden, denn die Situation unterscheidet sich nicht von der im geltenden Recht, wenn jemand berechtigten Zugriff auf Daten hat und diesen dann missbraucht. Vom Unwertvorwurf her besteht kein wesentlicher Unterschied zwischen einer dann vorliegenden Datenuntreue und einem IT-Sicherheitsforscher, der seine Absicht ändert und nun den rechtmäßig erlangten Zugriff missbraucht.

II. Alternativen

Alternativ könnte der gesetzlichen Status quo beibehalten werden. Dieser ist aber zum einen mit Unsicherheiten für die IT-Sicherheitsforschung verbunden und wird zum anderen zunehmend schwereren Angriffen nicht mehr ausreichend gerecht.

III. Exekutiver Fußabdruck

Der Gesetzentwurf nimmt teilweise Anregungen auf, die durch Expertinnen und Experten des Bundes und der Länder sowie Interessenvertreter aus Forschung und Wissenschaft sowie der IT-Sicherheitsbranche u.a. auf zwei vom Bundesministerium der Justiz veranstalteten Symposien vorgetragen wurden. Daneben wurde ein Gespräch mit dem Verband der Automobilindustrie geführt, dessen Papier „Cybersecurity-Tests“ im Lobbyregister hochgeladen wurde.

IV. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes folgt aus Artikel 74 Absatz 1 Nummer 1 des Grundgesetzes (Strafrecht).

V. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Der Gesetzentwurf ist mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland abgeschlossen hat, vereinbar.

Durch das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG) vom 7. August 2007 (BGBl. I S. 1786) wurde § 202a Absatz 1 StGB neu gefasst. Die Neufassung des Absatzes 1 diente der Umsetzung von Artikel 2 des Übereinkommens des Europarates über Computerkriminalität (Budapest Konvention) und von Artikel 2 des Rahmenbeschlusses 2005/222/JI des Rates, der durch Artikel 3 der Richtlinie 2013/40/EU der Europäischen Parlamentes und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates (ABl. L 218 vom 14.8.2013, S. 8 bis 14) ersetzt wurde, in innerstaatliches Recht.

Die vorgeschlagenen Änderungen berühren die vollständige Umsetzung dieser Rechtsakte nicht. In der NIS-2-Richtlinie[4)] wird ausdrücklich darauf hingewiesen, dass Schwachstellen häufig von Dritten entdeckt werden, und es wird empfohlen, Regelungen für die koordinierte Offenlegung von Schwachstellen zu treffen (vgl. Erwägungsgründen 58, 60 und 61 sowie die Erwähnung in Artikel 7 Absatz 2c in Verbindung mit Artikel 12 Absatz 1).

VI. Gesetzesfolgen

Ziel des Entwurfs ist die Schaffung von Rechtsklarheit für die Normenadressaten. Sicherheitsforschung im Interesse der Öffentlichkeit, insbesondere im Bereich der vulnerablen kritischen Infrastrukturen wird – sofern sie verantwortungsvoll durchgeführt wird – entkriminalisiert. Gleichzeitig wird die Bedeutung des verantwortungsvollen Umgangs mit Daten hervorgehoben und die Bestrafung in Fällen von besonderer Schwere erhöht, um die Widerstandsfähigkeit im Sinne einer nachhaltigen Entwicklung zu erhalten. Die Neureglungen werden zu einer Entlastung der Gerichte führen, weil den gegebenen Kriminalitätsphänomenen mit der neuen Rechtslage effektiv und effizient begegnet wird.

---

4) Siehe Fußnote 1

1. Nachhaltigkeitsaspekte

Der Entwurf steht im Einklang mit der deutschen Nachhaltigkeitsstrategie. Mit der Agenda 2030 werden fünf Kernbotschaften und 17 Nachhaltigkeitsziele benannt (Mensch, Planet, Wohlstand, Frieden und Partnerschaft). Die beabsichtigte Klarstellung dient der Verwirklichung des Ziels 9, das eine widerstandsfähige Infrastruktur aufbauen will und inklusive und nachhaltige Industrialisierung fördern und Innovationen unterstützen soll. Die IT-Sicherheit ist zur Erreichung dieses Ziel unabdingbar. Die Erhöhung des Strafrahmens dient der Umsetzung von Ziel 16. Dieses Nachhaltigkeitsziel verlangt, friedliche und inklusive Gesellschaften für eine nachhaltige Entwicklung zu fördern, allen Menschen Zugang zur Justiz zu ermöglichen und leistungsfähige, rechenschaftspflichtige und inklusive Institutionen auf allen Ebenen aufzubauen. Zu den Unterzielen von Ziel 16 zählen auch die Bekämpfung illegaler Finanz- und Waffenströme sowie der organisierten Kriminalität (Ziel 16.4), die sich auch durch Computerstraftaten bereichert. Nur so können andere Nachhaltigkeitsziele der Agenda 2030 wie die nachhaltige Armutsbekämpfung (Ziel 1), Gesundheit (Ziel 3), Bildung (Ziel 4), die Gleichstellung der Geschlechter (Ziel 5) oder die Erhaltung der natürlichen Lebensgrundlagen (Ziel 13 bis 15) auf globaler Ebene erreicht werden.

2. Haushaltsausgaben ohne Erfüllungsaufwand

Es entstehen keine Haushaltsausgaben ohne Erfüllungsaufwand.

3. Erfüllungsaufwand

Es entsteht kein Erfüllungsaufwand.

4. Weitere Kosten

Für die Justiz entsteht kein Mehraufwand. Die bestehende Rechtsunklarheit ist vor allem deswegen zu beheben, weil sie geeignet ist, gesellschaftlich relevante und nützliche IT-Sicherheitsforschung zu verhindern. Die geringe praktische Relevanz des gegenwärtigen Rechts wird auch in der Literatur beschrieben (bei Golla/Brodowski, IT-Sicherheitsforschung und IT-Strafrecht, S. 14 ff.). Im Jahr 2022 verzeichnete die Polizeilichen Kriminalstatistik für das „Ausspähen, Abfangen von Daten einschließlich Vorbereitungshandlungen und Datenhehlerei“ 13 206 Fälle, für „Datenveränderung und Computersabotage“ 3 351 Fälle; die Strafverfolgungsstatistik weist für das gleiche Jahr für § 202a StGB aber nur 43 Verurteilte aus, für § 202b StGB fünf und für § 303a StGB 16. Wie viele dieser Verfahren die IT-Sicherheitsforschung betrafen, ist aus den Statistiken nicht ersichtlich; soweit über Medienveröffentlichungen bekannt, liegt die Zahl der Verfahren im einstelligen Bereich. Im Fall der „echten“ Kriminalität führt die bloße Einführung eines besonders schweren Falles nicht zu Mehraufwand bei den Strafverfolgungsbehörden und Gerichten.

Es entstehen keine sonstigen direkten oder indirekten Kosten für die Wirtschaft, insbesondere für mittelständische Unternehmen. Auswirkungen auf die Einzelpreise und das Preisniveau sind nicht zu erwarten.

5. Weitere Gesetzesfolgen

Der Entwurf hat Auswirkungen für Verbraucherinnen und Verbraucher insofern, als er einen Beitrag zu einer erhöhten Sicherheit von IT-Produkten leisten will. Gleichstellungspolitische und demografische Auswirkungen und Auswirkungen auf die Wahrung und Förderung gleichwertiger Lebensverhältnisse sind nicht zu erwarten.

VII. Befristung; Evaluierung

Es ist keine Evaluierung und auch keine Befristung vorgesehen.

B. Besonderer Teil

Zu Artikel 1 (Änderung des Strafgesetzbuches)

Zu Nummer 1

Das Aufspüren von Sicherheitslücken in IT-Systemen gehört zu den typischen Tätigkeiten der IT-Sicherheitsforschung. Hierfür ist regelmäßig ein Zugriff auf fremde Informationssysteme und Daten notwendig, die sich im praktischen Einsatz befinden. Die Suche nach Sicherheitslücken und Sicherheitstests können nicht allein in „Laborumgebungen“ durchgeführt werden und geschehen auch nicht immer im Auftrag der Berechtigten. Dieses Vorgehen wird auch als „offensive IT-Sicherheitsforschung“ bezeichnet. Die notwendigen Zugriffshandlungen können jene Straftatbestände erfüllen, die dem Schutz des formellen Datengeheimnisses bzw. der Unversehrtheit von Daten und IT-Systemen dienen (§§ 202a ff., 303a f. StGB). Dies gilt vor allem für § 202a Absatz 1 StGB, der bereits den unbefugten Zugang zu Daten unter Strafe stellt, wenn sie nicht für den Täter bestimmt und gegen unberechtigten Zugang gesichert sind. Für das Tatbestandsmerkmal des Zugangs reicht die Möglichkeit der Kenntnisnahme aus, so dass ein bloßer Systemzugriff bereits den Tatbestand erfüllen kann. Um dieses Problem zu lösen, soll eine Regelung geschaffen werden, die an das Tatbestandsmerkmal „unbefugt“ anknüpft und das Handeln der IT-Sicherheitsforschung so vom Tatbestand ausnimmt.

Der Begriff „unbefugt“ wird im StGB mehrfach verwendet und je nach Straftatbestand dogmatisch unterschiedlich beurteilt: In § 132a StGB (Missbrauch von Titeln) ist die Einordnung umstritten (Hohmann, in: Münchener Kommentar zum StGB, 4. Auflage 2021, § 132a, Rn. 33, einerseits – Tatbestandsmerkmal – und andererseits wohl Lackner/Kühl/Heger, StGB, 30. Auflage 2023, § 132a, Rn.10 – Rechtfertigungsgrund). In den §§ 324 Absatz 1, 326 Absatz 1 StGB (Straftaten gegen die Umwelt) wird „unbefugt“ als Bezeichnung dafür verwendet, dass die Tathandlung rechtswidrig sein muss. In § 238 StGB (Nachstellung) wird „unbefugt“ als Tatbestandsmerkmal angesehen, um „sozialadäquate Verhaltensweisen“ von der Strafbarkeit von vornherein auszuschließen (Lackner/Kühl/Heger, StGB, 30. Auflage 2023, § 238, Rn. 6). In § 201 StGB (Verletzung der Vertraulichkeit des Wortes) wird der Begriff als tatbestandsausschließend betrachtet, in § 201a StGB als „Hinweis auf Rechtfertigungsgründe“ (Lackner/Kühl/Heger, StGB, 30. Auflage 2023, vor § 201, Rn. 2, § 201a, Rn. 9).

Für § 202a StGB wird bislang – fast einhellig – angenommen, dass das Merkmal „unbefugt“ zum gesetzlichen Tatbestand gehört und sein Fehlen den Tatbestand ausschließt hat (Weidemann, in: Beck’scher Online-Kommentar zum StGB, 62. Edition, § 202a, Rn. 20). Das ist offenbar auch die Auffassung des BVerfG (Beschluss vom 18. Mai 2009, 2 BvR 2233/07, BeckRS 2009, 35232).

Zu § 202a Absatz 3

Nach **§ 202a** Absatz 3 Nummer 1 **StGB-E** ist die in § 202a Absatz 1 StGB beschriebene Handlung dann nicht unbefugt, wenn sie in der Absicht erfolgt, eine Schwachstelle oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems (Sicherheitslücke) festzustellen und den für das informationstechnische System Verantwortlichen, den Betreiber der Datenverarbeitungsanlage, den Hersteller der betroffenen IT-Anwendung oder das Bundesamt für Sicherheit in der Informationstechnik davon zu unterrichten.

Um festzustellen, ob das subjektive Element der Absicht vorliegt, sind, wie auch sonst im Strafrecht üblich, neben den Einlassungen des Betroffenen die Tatumstände im Übrigen zu würdigen. Die Absicht muss sich darauf beziehen, eine Sicherheitslücke „festzustellen“ und zu schließen. Abzugrenzen ist dies vom mutwilligen Ausprobieren, ob sich Systeme „knacken“ lassen oder einem Hacking aus rein persönlichen Motiven.

Mit der Formulierung „in der Absicht erfolgt, (…) 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“ sollen die Handelnden zwar nicht verpflichtet werden, einen bestimmten Meldeweg einzuhalten, zumal es dazu noch kein anerkanntes, standardisiertes Verfahren (responsible disclosure) gibt. Nutzt der Handelnde einen entsprechenden Meldeweg, den der Verantwortliche anbietet, kann dieses Nachtatverhalten ein sehr starker Beleg für seine Absicht sein, eine Sicherheitslücke schließen zu wollen. Es soll aber auch nicht ausreichen, die Sicherheitslücke irgendjemandem mitteilen oder sie z. B. nur auf der eigenen Homepage zu veröffentlichen zu wollen, ohne den Verantwortlichen oder das BSI zu informieren. Die beabsichtigte Meldung muss an einen Verantwortlichen gerichtet sein, der in der Lage ist, die Lücke zu schließen oder dies zu veranlassen. Dabei lehnt sich die Formulierung an § 15 Absatz 2 BSI-Gesetz-E an.

Die Handlung erfüllt auch in solchen Fällen den Tatbestand nicht, in denen der Handelnde zwar zunächst mit Unterrichtungsabsicht tätig wird, es letztlich aber – aus welchen Gründen auch immer – nicht zu einer Meldung der Lücke kommt. Dies mag unbefriedigend erscheinen, weil so bei nicht gemeldeten Lücken die Schutzbehauptung zur Straflosigkeit führen könnte, man habe dies noch vorgehabt, wobei es letztlich eine Frage der gerichtlichen Würdigung sämtlicher Umstände des Einzelfalles ist, ob der Beschuldigte mit dieser Behauptung Gehör findet. Die Ausgestaltung ist aber erforderlich, um bereits zum Zeitpunkt der Tathandlung bestimmen zu können, ob diese strafbar war oder nicht; es soll kein Schwebezustand eintreten.

Der Entwurf entscheidet sich bewusst nicht für eine bloße Rechtfertigungsmöglichkeit der IT-Sicherheitsforschung oder die Einführung eines Strafaufhebungsgrundes, um in Unternehmen angestellten IT-Sicherheitsforschern genau wie der wissenschaftlichen Forschung nicht zuzumuten, zunächst tatbestandsmäßig handeln zu müssen und lediglich auf eine spätere Rechtfertigung bzw. Strafaufhebung vertrauen zu können. Damit würde der bewusste Verstoß gegen Compliance-Regelungen ebenso in Kauf genommen wie gegen die Bedingungen beispielsweise der Drittmittelvergabe.

Nach **§ 202a** Absatz 3 Nummer 2 **StGB-E** ist eine weitere Voraussetzung, dass die Handlung zur Feststellung der Sicherheitslücke erforderlich gewesen sein muss. Durch die Aufnahme dieses Kriteriums wird sichergestellt, dass diejenigen weiter den Tatbestand verwirklichen, die auf mehr oder andere Daten zugreifen, als dies für die Feststellung der Sicherheitslücke notwendig ist. Die Maßnahme muss auch geeignet sein, um eine Sicherheitslücke festzustellen, denn eine ungeeignete Maßnahme kann nicht erforderlich sein. Auch ist die Erforderlichkeit nur zu bejahen, wenn es kein gleich wirksames Mittel zur Feststellung einer Sicherheitslücke gibt, das milder ist, z. B. indem man die Erlaubnis des Betroffenen einholt. Die Erforderlichkeit der Handlung wird nicht dadurch ausgeschlossen, dass der Zugriff in entsprechender Absicht und in dem für die Feststellung erforderlichen Umfang erfolgte, eine Sicherheitslücke dann aber nicht aufgefunden wird, z. B. weil sie schon geschlossen wurde.

Zu § 202a Absatz 4

Um der erhöhten Bedeutung der Informationstechnik für Wirtschaft und Gesellschaft und den zunehmenden Gefahren für die IT-Sicherheit Rechnung zu tragen, sollen besonders schwere Fälle mit einer höheren Strafandrohung eingeführt werden. Damit wird auch dem Anliegen der Länder Rechnung getragen, wie es z. B. in den Gesetzesanträgen der Länder Bayern (vom 19. April 2019, Bundesratsdrucksache 168/19) und Nordrhein-Westfalen (vom 28. Mai 2019, Bundesratsdrucksache 248/19) zum Ausdruck kommt. Auch die Innenministerkonferenz hat sich in ihrer Frühjahrsitzung im Jahr 2024 mit dem Thema befasst.

Drei dieser besonders schweren Fälle (Vermögensverlust großen Ausmaßes, Gewerbsmäßigkeit und bandenmäßiges Handeln) wurden aus § 303b Absatz 4 Nummer 1, 2 StGB

übernommen. Ferner wurden als Regelbeispiele das Handeln aus Gewinnsucht sowie die Beeinträchtigung der Verfügbarkeit, Funktionsfähigkeit, Integrität, Authentizität oder Vertraulichkeit einer kritischen Infrastruktur oder der Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder eingefügt.

§ 303b Absatz 4 Nummer 3 StGB (Beeinträchtigung der Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder der Sicherheit der Bundesrepublik Deutschland) wurde hingegen nicht in § 202a Absatz 4 StGB-E übernommen. Dieses Regelbeispiel erscheint bei den §§ 202a und 202b StGB nicht passend, weil es sich dabei nicht um Delikte handelt, die auf die Zerstörung oder Beeinträchtigung anderer gerichtet sind.

Der Vorschlag spricht in **Nummer 1** von einem „Vermögensverlust großen Ausmaßes“. Denkbar wäre insoweit auch, generell „erheblich Nachteile“ genügen zu lassen, wie dies Sieber in seinem Gutachten für den 69. Deutschen Juristentag im Jahr 2012 vorgeschlagen hatte (C 87, 89). Insofern wäre eine Orientierung an dem Nachteilsbegriff in § 274 StGB denkbar. Freilich würde es erhebliche Rechtsunsicherheit hervorrufen zu bestimmen, wann ein „erheblicher“ Nachteil vorläge. Hingegen sind die Maßstäbe zur Bestimmung eines Vermögensverlustes großen Ausmaßes durch die Rechtsprechung schon recht klar konturiert (so schon im Gesetzentwurf der Bundesregierung aus dem Jahr 2006, Bundestagsdrucksache 16/3655, S. 14). Dass die Strafschärfung hier an die Verletzung eines anderen als des von den §§ 202a, 202b StGB geschützten Rechtsguts anknüpft, ist nicht ungewöhnlich (vgl. § 267 Absatz 3 Nummer 2 StGB).

Das Regelbeispiel erfasst bestimmte Sachverhalte nicht, bei denen eine höhere Strafandrohung durchaus auch angemessen erscheinen könnte. Das gilt insbesondere für Fälle, in denen zwar ein erheblicher Vermögensschaden entsteht, dieser jedoch nicht bei einem einzelnen Geschädigten, sondern erst in der Summe bei einer Vielzahl Betroffener. Die Rechtsprechung geht hier davon aus, dass die Voraussetzungen des Regelbeispiels nicht vorliegen (BGH, NJW 2011, 1825, 1827; NStZ 2012, 213 f.). Sie begründet das damit, dass derartige Regelbeispiele opferbezogen seien. Das besondere Unrecht wird also in der Beeinträchtigung einer Einzelperson und nicht darin gesehen, dass gesamtgesellschaftlich erhebliche Nachteile eingetreten sind. Diese den Individualschutz betonende Rechtsprechung erscheint unpassend, wenn bei großangelegten Hackerangriffen eine Vielzahl von Personen zu Schaden kommt und damit gleichzeitig für die Gesellschaft nachteiligen Folgen eintreten. Für Fälle dieser Art muss aber kein besonderes Regelbeispiel vorgesehen werden, hier kommt ein unbenannter besonders schwerer Fall in Betracht.

Auch die Regelbeispiele in **Nummer 2** der banden- bzw. gewerbsmäßigen Begehung wurden von der Rechtsprechung schon klar konturiert. Trotzdem ist aus kriminologischer Sicht durchaus zweifelhaft, ob man mit dem Bandenbegriff (alle) erhöht strafwürdigen Erscheinungsformen unter Hackern erfassen kann. Denn eine Bande liegt nur vor, wenn sich mindestens drei Personen zu einer fortgesetzten Begehung von im Einzelnen noch ungewissen Taten zusammenschließen. Bei Hackern kommt es aber häufig vor, dass sich mehrere Personen nur für einzelne „Projekte“ zusammenschließen (vgl. Brodowski/Freiling, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, S. 64 m. w. N. Ausführlich, auch zur OK-Kriminalität Bundeskriminalamt, Täter im Bereich Cybercrime, S. 44 ff.). Dann würde es an einer Bande fehlen, weil sich diese Personen nicht zur Begehung von mehreren und auch noch ungewissen Taten zusammenschließen. Taten eines derartigen Zusammenschlusses mögen typisiert auch weniger strafwürdig sein als solche einer klassischen „Bande“. Im Einzelfall besteht aber auch hier ein erhöhtes Strafbedürfnis, insbesondere wenn durch den Zusammenschluss eine besonders große Organisationsgefahr geschaffen wird. Hier wird man ggf. einen unbenannten schweren Fall annehmen können.

Das weitere Regelbeispiel in **Nummer 2**, das „Handeln aus Gewinnsucht“, wird auch an anderen Stellen im StGB verwendet (§ 236 Absatz 4 Nummer 1 (dort als Verbrechensqualifikation), §§ 283a Nummer 1, 283d Absatz 3 Nummer 1, 330 Absatz 1 Nummer 4 StGB). Gewinnsucht ist ein Gewinnstreben um jeden Preis (BGH, NJW 1952, 983, NStZ-RR 2017, 282; Petermann/Hoffmann, Münchener Kommentar zum StGB, 4. Auflage 2021, § 283a, Rn. 5 f.). Es geht über eine allgemeine Bereicherungsabsicht hinaus, was bei § 202a StGB sinnvoll erscheint, um ein besonders schweres Unrecht zu kennzeichnen, weil dieser Tatbestand typischerweise mit „einfacher“ Bereicherungsabsicht begangen wird, diese allein aber nicht zum besonders schweren Fall führen soll (Vgl. die Überlegungen zu § 283a StGB, Petermann/Hoffmann a. a. O., Rn. 5.) In der Literatur wird dieses Regelbeispiel vorgeschlagen, wenn der Täter plant, sich einen großen Vermögensvorteil zu verschaffen (Petermann/Hoffmann a. a. O., Rn. 6; Kindhäuser/Bülte, in: Nomos Kommentar zum StGB, 6. Auflage 2023, § 283a, Rn. 4.) Daran wird kritisiert, dass die Formulierung unangemessen moralisierend wirken kann (Hoyer, in: Systematischer Kommentar zum StGB, 9. Auflage 2019, § 283a, Rn. 4). Solange die Rechtsprechung in der konkreten Auslegung aber nicht auf moralisierende Aspekte abstellt, sondern nur gefordert wird, dass zu einer Bereicherungsabsicht zusätzliche Umstände vorliegen, welche die Strafwürdigkeit erhöhen, erscheint dies unbedenklich.

Das Regelbeispiel in **Nummer 3** der Beeinträchtigung der „Verfügbarkeit, Funktionsfähigkeit, Integrität, Authentizität oder Vertraulichkeit einer kritischen Infrastruktur oder die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder“ wurde aufgenommen, um den Schutz kritischer Infrastrukturen und des Staates selbst zu gewährleisten. Der Begriff der kritischen Infrastrukturen[5)] ist in Anlehnung an die Legaldefinition in § 2 Absatz 10 BSI-Gesetz zu verstehen. Kritische Infrastrukturen sind danach Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefahren für die öffentliche Sicherheit eintreten würden. Zu den kritischen Infrastrukturen im Sinne des hier vorgeschlagenen Regelbeispiels zählen also etwa Krankenhäuser, Kernkraftwerke, Flughäfen oder Banken. Die Aufnahme dieser kritischen Infrastrukturen in den Katalog der Regelbeispiele trägt dem Umstand Rechnung, dass diese Infrastrukturen besonders schutzwürdig sind, da sie aufgrund der fortschreitenden Digitalisierung in hohem Maße auf informationstechnische Systeme angewiesen sind und unberechtigte Zugriffe auf diese Systeme schwerwiegende Folgen auch für die Allgemeinheit haben können. Der Schutzbereich der kritischen Infrastrukturen umfasst in Anlehnung an § 8a Absatz 1 Satz 1 BSI-Gesetz deren Verfügbarkeit, Funktionsfähigkeit, Integrität, Authentizität und Vertraulichkeit. Die Voraussetzungen sind in einer für künftige Entwicklungen offenen und zugleich einer rechtssicheren Anwendung zugänglichen Weise gefasst worden. Die Sicherheit der Bundesrepublik Deutschland umfasst die innere und äußere Sicherheit. Die Begriffsbestimmung kann sich – wie bei § 303b Absatz 4 Satz 2 Nummer 3 StGB – an § 92 Absatz 3 Nummer 2 StGB orientieren. Gemeint ist also die Fähigkeit der Bundesrepublik, sich nach außen und innen gegen Störungen zur Wehr zu setzen. Entsprechendes gilt für die Sicherheit eines der Länder der Bundesrepublik Deutschland.

---

5) Der Begriff der „kritischen Infrastrukturen“ in § 2 Abs. 10 BSI-Gesetz wird im NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz durch den Begriff der „kritischen Anlagen“ in § 2 Nummer 22 BSI-Gesetz-E ersetzt! Es muss im Laufe des Gesetzgebungsverfahrens geprüft werden, ob hier am Begriff der „kritischen Infrastrukturen“ festgehalten werden kann und sollte.

Zu Nummer 2

Zu Buchstabe a

Es handelt sich um eine redaktionelle Folge der Einfügung eines neuen Absatzes.

Zu Buchstabe b

Es gelten die Ausführungen zu Nummer 1 entsprechend.

Zu Nummer 3

Es gelten die Ausführungen zu Nummer 1 entsprechend.

§ 303a StGB spricht anders als die §§ 202a und 202b StGB nicht davon, dass die Tat „unbefugt“, sondern davon, dass sie „rechtswidrig“ sein muss. Wie dieses Merkmal bei § 303a StGB zu verstehen ist, ist umstritten. Eine beachtliche Mindermeinung (u. a. Hecker, in: Schönke/Schröder, StGB, 30. Auflage 2019, § 303a, Rn.10; Fischer, StGB, 71. Auflage 2024, § 303a, Rn. 10; Kargl, in: Nomos Kommentar zum StGB, 6. Auflage 2023, § 303a, Rn. 16) nimmt ein allgemeines Verbrechensmerkmal an. Die wohl überwiegende Meinung (Lackner/Kühl/Heger, StGB, 30. Auflage 2023, § 303a, Rn. 4; Weidemann, in: Beck’scher Online-Kommentar zum StGB, 62. Edition, § 303a Rn. 20; Wieck/Noock, in: Münchener Kommentar zum StGB, 4. Auflage 2022, § 303a, Rn. 17; Altenhain, in: Matt/Renzikowski, StGB, 2. Auflage 2020, § 303a, Rn. 12) und der Gesetzgeber (Bundestagsdrucksache 10/5058 S. 34) gehen aber auch hier von einem tatbestandseinschränkenden Merkmal aus.

§ 202a Absatz 3 StGB-E gilt daher mit der Maßgabe entsprechend, dass das Verhalten hier nicht rechtswidrig ist. Straflosigkeit ist auch im Fall der Datenveränderung angemessen, da es für die IT-Sicherheitsforschung im Rahmen ihrer Tätigkeiten kaum möglich ist, nicht auch den Tatbestand des § 303a StGB zu verwirklichen.

Für den Straftatbestand des § 303b StGB (Computersabotage) soll hingegen kein Tatbestandsausschluss vorgesehen werden, denn wenn bei der IT-Sicherheitsforschung eine derartig schwerwiegende Störung verursacht und zumindest billigend in Kauf genommen wird, scheint es angemessen, an der Strafbarkeit festzuhalten. Um dieses Ergebnis zu erreichen, muss das Merkmal der Erforderlichkeit in § 202a Absatz 3 StGB herangezogen werden. Denn nach § 303b Absatz 1 Nummer 1 StGB macht sich strafbar, wer eine Datenverarbeitung von wesentlicher Bedeutung dadurch erheblich stört, dass er, wie sich aus dem Verweis auf eine Tat nach § 303a Absatz 1 StGB ergibt, Daten löscht, unterdrückt, unbrauchbar macht oder verändert. Da die Tat rechtswidrig sein muss, ist die durch den Gesetzentwurf vorgesehene neue Vorschrift des § 303a Absatz 4 StGB-E zu beachten, der auf § 202a Absatz 3 StGB verweist.

Computersabotage wäre also zukünftig nicht mehr strafbar, wenn sie durch eine Datenveränderung (§ 303a Absatz 1 StGB) begangen würde, die ihrerseits unter entsprechender Anwendung von § 202a Absatz 3 StGB-E nicht „unbefugt“ erfolgte. Dieses unerwünschte Ergebnis kann dadurch vermieden werden, dass bei der Prüfung der Erforderlichkeit der Handlung berücksichtigt wird, dass in diesen Fällen die Datenveränderung nach § 303a Absatz 1 StGB vorgenommen wurde, um für eine Datensabotage nach § 303b Absatz 1 Nummer 1 StGB verwendet zu werden. Eine Datensabotage kann aber niemals erforderlich sein.

Unabhängig davon kommt eine Strafbarkeit nach § 303b Absatz 1 Nummer 3 StGB in Betracht, wenn im Rahmen der Erforschung von Sicherheitslücken Datenverarbeitungsanlagen oder Datenträger verändert werden.

Zu Artikel 2 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten des Gesetzes. Nach Ziffer I. 4 des Arbeitsprogramms Bessere Rechtsetzung 2018 sollen Regelungsvorhaben der Bundesregierung ein Inkrafttreten möglichst zum 1. Tag eines Quartals vorsehen. Einer Übergangsfrist bedarf es nicht.