GESELLSCHAFT
FÜR INFORMATIK

WHITEPAPER

REFORM DES COMPUTERSTRAFRECHTS

AUGUST 2026

WHITEPAPER

REFORM DES COMPUTERSTRAFRECHTS

AUGUST 2026

Impressum

Herausgeber:
Gesellschaft für Informatik e.V. (GI)
Weydingerstraße 14–1
10178 Berlin
Deutschland
Tel: +49 30 240 09-805
E-Mail: *berlin@gi.de*
Internet: *https://gi.de*

Autorinnen und Autoren:
Marieke Petersen, GI
Wiebke Dönnebrink, GI
Eva Mattes, GI
Nikolas Becker, GI
Helen Zotz, GI

In Zusammenarbeit mit
LOAD e.V. - Verein für liberale Netzpolitik
AG KRITIS
Prof. Dr. Daniel Loebenberger, Sprecher des Fachbereichs Sicherheit der GI
Maximilian Kroker, Junior-Fellow der GI
Dr. Aleksandra Sowa, Leitungskreis der Fachgruppe Privacy Enhancing Technologies (PET) der GI
Stand: August 2026

AG KRITIS
Arbeitsgruppe
Kritische Infrastrukturen

LOAD e.V.
Verein für liberale Netzpolitik

Inhaltsverzeichnis

1. Einleitung: Wer findet die Schwachstellen?

Es steht schlecht um die Cybersicherheitslage in Deutschland. Insbesondere Schwachstellen in IT-Systemen bieten große Angriffsmöglichkeiten für Kriminelle und staatliche Akteure, die sensible Informationen ausspähen wollen. Das BSI berichtet in seiner Lagebewertung für 2025, dass besonders Schwachstellenexploits und damit verbundene Datenleaks beliebte Methoden für Cyberkriminelle sind[1]. Durch den Einsatz von KI-Tools wird das Finden und Ausnutzen solcher Schwachstellen in Zukunft noch leichter werden[2].

2025 wurden weltweit fast 50.000 CVEs[3] gemeldet. Bereits im ersten Quartal 2026 stieg die Zahl gemeldeter Schwachstellen weltweit um 25 Prozent im Vergleich zum Vorjahr.[4] Auch der Schaden durch das Ausnutzen von Schwachstellen nimmt zu: In Deutschland erlitten Unternehmen nach eigenen Angaben einen Schaden in Höhe von knapp 300 Mrd. Euro aufgrund von IT-Systemausfällen, Ermittlungs- und Verfahrenskosten oder Produktionsausfällen.[5] Solche Cyberangriffe führen darüber hinaus zu Verunsicherung: Nicht immer ist klar, ob und wie viele Datensätze erbeutet wurden und wie schwerwiegend der tatsächliche Schaden ist.[6]

Während der Cyber Resilience Act Schwachstellenmeldungen durch Unternehmen verpflichtend vorsieht, verhindert die deutsche Gesetzgebung das verantwortungsvolle Melden von Schwachstellen durch Außenstehende (sogenanntes White Hat Hacking). Das Computerstrafrecht (§§ 202a-c StGB) kriminalisiert das (vorbereitete) Ausspähen und Abfangen von Daten, ungeachtet der Motivation der Findenden oder der Ursache des Findens von Schwachstellen. Seit seiner Einführung 2007 kritisiert die Gesellschaft für Informatik e.V. (GI) daher das geltende Computerstrafrecht und insbesondere die Kriminalisierung von Hacker*innentools (§ 202c StGB).[7]

Die schwarz-roten Koalitionsparteien haben sich Rechtssicherheit für Cybersicherheitsforschung als Ziel in den Koalitionsvertrag geschrieben. Wir befürworten dieses Vorhaben und wollen die Bundesregierung daher unterstützen, Rechtssicherheit für Cybersicherheitsforschung zu schaffen. Zu diesem Zweck haben wir eine Konsultation mit Teilnehmenden aus der Cybersicherheitsforschung, der Automobilindustrie und der digitalen Zivilgesellschaft durchgeführt. Unser Ziel war es, einen Lösungsweg zu finden, der Cybersicherheitsforschung ermöglicht und auf die Bedarfe aller Seiten (Meldende, betroffene Entwickler*innen, betroffene Nutzer*innen, staatliche Aufsicht) eingeht. Dafür fanden im Zeitraum Mai/Juni 2026 drei Workshops und mehrere Expert*innengespräche zu der Frage statt, wie ein verantwortungsbewusster Umgang mit Schwachstellen (Responsible Disclosure) aussehen kann und wie der rechtliche Rahmen hierfür aussehen muss.

Das folgende Whitepaper fasst die wesentlichen Erkenntnisse dieser Gespräche zusammen. Darüber hinaus gibt es einen Überblick über die unterschiedlichen Motivationen von Hacker*innen, die bei einer Änderung des Computerstrafrechts bedacht werden müssen.

---

1 BSI (2025)

2 s. beispielsweise der Angriff auf Hugging Face (Hugging Face (2026))

3 Common Vulnerabilities and Exposures, System zur vereinheitlichen Meldung von Schwachstellen. CVE (2026)

4 CVE (2026)

5 Wintergerst (2025)

6 NDR (2026)

7 Gesellschaft für Informatik (2007)

2. Problemstellung: Wer Lücken findet, muss sie behalten?

Die Gesetzeslage in Deutschland baut auf der Idee auf, dass die Suche nach und das Auffinden von Schwachstellen primär mit schädlichen Absichten erfolgen. Dabei ist die tatsächliche Lage deutlich diverser. Cybersicherheitsforschende und ehrenamtliche Hacker*innen suchen auf eigene Initiative hin Lücken, um sie betroffenen Unternehmen zu melden und sie so schließen zu lassen. Bug-Bounty-Programme motivieren Expert*innen, für einen monetären Gewinn Schwachstellen zu finden. Gesetze schreiben Unternehmen vor, beispielsweise mithilfe von Pen-Tests Produkte auf ihre Cybersicherheit zu testen.

SORGE VOR STRAFVERFOLGUNG VERHINDERT DIREKTE MELDUNGEN

Schwachstellenmeldungen von außerhalb werden von Unternehmen oder Herstellern oftmals mit Dank entgegengenommen. Trotzdem reichen die bekannten negativen Schlagzeilen der Fälle rund um das Unternehmen „Modern Solutions“ (s. Exkurs) und unklare Definitionen für Cybersicherheitsforschende aus, um von einer direkten Meldung abzusehen oder eine skurrile Selbstanzeige vorzunehmen[8]. Die fehlende Unterscheidung im Gesetz zwischen einer Schädigungsabsicht und dem gemeinwohlorientierten Finden und Melden zur Gefahrenminimierung ermöglicht es, Meldende trotz ihrer ehrlichen Intention anzuzeigen. Freiwillige haben Sorge vor Strafverfolgung und melden eher über Stellen wie das BSI oder den Chaos Computer Club e. V. (CCC). Das hat zur Folge, dass bei diesen Stellen übermäßige viele Meldungen auflaufen und gerade ehrenamtlich agierende Organisationen auf freiwillige Unterstützung angewiesen sind.

EXKURS: MODERN SOLUTIONS

Im Fall Modern Solutions wurde der IT-Experte Hendrik Heinle 2021 verurteilt, nachdem er eine gravierende Sicherheitslücke in der E-Commerce-Software des Unternehmens entdeckt und diese selbständig geprüft hatte, um Kundendaten zu schützen. Obwohl sein Handeln als „ethisches Hacking" motiviert war und der Hersteller gravierende Sicherheitsmängel hatte, werteten Staatsanwaltschaft und Gerichte den Zugriff auf passwortgeschützte Systeme als Straftat nach § 202c StGB. Das Bundesverfassungsgericht lehnte 2024 seine Verfassungsbeschwerde endgültig ab[9].

ZUSTIMMUNG FÜR TESTS EINZUHOLEN IST, DE FACTO KAUM MÖGLICH

In Branchen wie der Automobilindustrie sind Pen-Tests bereits vorgeschrieben, auch KRITIS-Anwendungen müssen regelmäßig auf ihre Sicherheit kontrolliert werden. Produkte bestehen in der Regel jedoch aus mehreren Komponenten, die wiederum zum geistigen Eigentum des jeweiligen Herstellers zählen. Zwar kriminalisiert der § 202a ff. StGB lediglich den unbefugten Zugang zu Daten innerhalb eines Systems, wodurch ein Pen-Test mit der Zustimmung der Hersteller grundsätzlich möglich wäre. Jedoch muss hier von allen Beteiligten eine Zustimmung erfolgen. Aufgrund der Vielzahl an Komponenten ist es mit einem unverhältnismäßig großen Aufwand verbunden, von allen Seiten eine Zustimmung einzuholen[10]. Beispielsweise antworten Prozessverantwortliche nicht oder sehen keine Notwendigkeit für einen Test. In anderen Fällen können Schwachstellen sich außerhalb der ursprünglich betrachteten Systeme befinden, für das ein*e Cybersicherheitsforschende*r eine Testerlaubnis hatte.

8 Bachfeld (2008)

9 Stiftung Datenschutz (2025)

10 Matheus (2026)

Auch bei Angeboten, Produkte auf Schwachstellen zu testen, gibt es wenig Resonanz: Im Kontext einer Studie zu IT-Produkten antworteten über die Hälfte der kontaktierten Produktverantwortlichen nicht. Ein in der EU ansässiger unabhängiger Sicherheitsforscher erhielt bei einem ähnlichen Versuch eine Antwortquote von 15 Prozent, und nur ca. 13 Prozent der angefragten Produktverantwortlichen erlaubten Sicherheitsanalysen ohne einschränkende Bedingungen. Zudem dauerte die Antwort teils mehrere Monate[11].

Sofern keine Pflicht zum Testen besteht, bauen viele Hersteller auf dem Prinzip „Security by Obscurity“ auf. Das Konzept beruht auf der irreführenden Idee, dass ein System sicher ist, solange Schwachstellen geheim oder versteckt sind.

EIN VERBOT VON HACKER*INNENTOOLS BESCHRÄNKT DIE MÖGLICHKEITEN ZUM UMFASSENDEN TESTEN

Nicht nur das strafrechtliche Verbot der Herstellung und Verbreitung von Computerprogrammen, die zur Überwindung von Sicherungsvorkehrungen dienen, sondern auch das Verbot von Reverse Engineering oder Dekompilierern fremder Software behindert eine sichere IT-Landschaft in Deutschland. Einerseits können Sicherheitsforschende nicht den Umgang mit diesen Tools lernen, ohne in die Illegalität zu rutschen. Zum anderen beschränkt es die Arbeit, da ein wesentlicher methodischer Teil wegfällt.

Dabei übersieht der Gesetzgeber, dass solche Tools trotz Verbots existieren und auch verwendet werden, jedoch für kriminelle Absichten. Das Verbot der Entwicklung und Anwendung verhindert de facto vor allem, dass gutwillige Sicherheitsforschende diese verwenden können, um Schwachstellen zu finden und sie zu melden, bevor sie ausgenutzt werden können.

„SECURITY BY OBSCURITY“ IST KEIN SICHERHEITSKONZEPT

Das Bild des „Hackers“ ist in Deutschland historisch geprägt durch Vorfälle wie den KGB-Hack (1987)[12] oder BTX-Hack (1984).[13] In vielen Fällen besteht Sorge, dass Schwachstellen gefunden und zu eigenen Zwecken, beispielsweise der Suche nach Anerkennung, ausgenutzt würden: „Wenn die Grey Hat Hacker auf die Systeme zugreifen, besteht immer die Gefahr, dass die Daten verändert oder an die Öffentlichkeit herangetragen werden, wovon dann Reputationsschäden für die Unternehmen ausgehen", sagt Patrick Schönowski[14], Referent des Deutschen Mittelstandbunds (DMB). Er verweist dabei auf fehlende finanzielle Ressourcen, um eine Lücke zu schließen. Wer auf das Prinzip „Security by Obscurity“ aufbaut, übersieht jedoch, dass Lücken bereits an anderen Stellen beispielsweise Kriminellen oder staatlichen Akteuren bekannt sein und von diesen ausgenutzt werden könnten. Ein Verschleiern von Sicherheitslücken und eine Klage gegen die meldende Person löst dabei das Problem unsicherer IT nicht, sondern verschreckt ehrenamtliche Akteure mit guten Intentionen.

KÜNSTLICHE INTELLIGENZ ALS HOFFNUNG UND RISIKO

Neue KI-Werkzeuge wie Claude Mythos sind in der Lage, bisher unbekannte Schwachstellen zu finden. Durch ihren Einsatz ist es sowohl leichter geworden, Schwachstellen zu identifizieren und auszunutzen, als auch sie zu melden. Zeitgleich birgt sogenanntes Vibe Coding die Gefahr, selbst Schwachstellen in Code zu erzeugen. Mit der angestiegenen Verwendung von Vibe Coding und fehlendem Wissen über Software auf der anderen Seite steigt das Risiko, ungewollt eine Schwachstelle zu erzeugen. Aus diesen Gründen ist es notwendig, KI-

11 Gamero-Garrido, A., Savage, S., Levchenko, K., & Snoeren, A. C. (2017), S.1501-1507

12 Lossie (2010)

13 Borchers (2014)

14 Deutscher Mittelstandsbund (2025)

Programme zur agentischen Kontrolle von Software einzusetzen und darüber hinaus die Unterstützung anzunehmen, die die Zivilgesellschaft mit ethischen Hacker*innen bietet.

Die deutsche Rechtslage verhindert eine Umsetzung dessen, was für eine sichere IT-Landschaft in Deutschland dringend benötigt wird: Schutz für verantwortungsvolle Meldende, die unbürokratische Test-Durchführung für IT-Systeme aus mehreren Komponenten sowie die Möglichkeit, legal Cybersicherheitskompetenzen durch praktische Anwendungen zu erlangen. Damit einher geht auch die Wahrnehmung und der Umgang mit Sicherheitsforschenden und Meldenden: Solange diese als Bedrohung statt als wertvolle Bereicherung in der eigenen Cybersicherheit gesehen werden, geht wichtiges Potenzial verloren.

3. Begriffsdefinition: Nachts sind alle Hacker*innen grau.

Hacken beschreibt ursprünglich die Intention, die Grenzen des Machbaren zu erkunden[15]. Inzwischen ist „Hacken“ konnotiert als der Versuch, in Computer und IT-Systeme einzudringen und dabei etwa Sicherheitsbarrieren zu überwinden. Dieses Vorgehen findet bei Wettbewerben wie „Capture the Flag“-Turnieren statt, bei denen Teilnehmende praktische Erfahrungen durch die spielerische Anwendung von Angriffs- und auch Abwehrtechniken erlangen, und so ihre Kompetenzen im Bereich der Cybersicherheit erweitern können. Das Eindringen in Systeme dient hier dazu, die Cybersicherheit von künftig zu entwickelnden Systemen zu steigern.

Beim Hacken kommt es stark auf die Motivation der Hacker*innen an. Allgemein unterscheidet man zwischen White Hats, Black Hats und Grey Hats, angelehnt an alte Western-Filme: Die Guten tragen weiß, die Bösen schwarz[16].

EXKURS: HACKETHIK

Die Hackethik wurde ursprünglich 1984 von Steven Levy entwickelt und Ende 1980 als Folge des KGB-Hacks um zwei Punkte erweitert, die heute einen hohen Stellenwert besitzen:

- *Mülle nicht in den Daten anderer Leute*: Wer eine Schwachstelle findet, sollte diese nicht missbrauchen, um anderen zu schaden.
- *Öffentliche Daten nützen, private Daten schützen*: Der Zugriff auf private und personenbezogene Daten, ungeachtet des Zugriffs, sollte begrenzt sein und nicht für eigene Zwecke ausgenutzt werden.

Die Hackethik bildet die Grundsätze des CCC und lässt sich in Anforderungen übertragen, die an ein Responsible-Disclosure-Verfahren gestellt werden können: Das Dokumentieren und Melden von Schwachstellen an die Stellen, die sie beheben können, angemessene Reaktions- und Bearbeitungsfristen und ein strukturierter Disclosure-Prozess.

White-Hat-Hacker*innen werden auch als ethische Hacker*innen bezeichnet: Sie dringen in Computersysteme ein, um Schwachstellen zu finden, zu melden und/oder zu schließen. Ihre Motivation ist es, Systeme damit sicherer vor Angreifenden zu machen. White Hats agieren teilweise im Auftrag eines Unternehmens, beispielsweise als Pen-Tester*innen, oder untersuchen freiberuflich oder in ihrer Freizeit Code auf Schwachstellen. Für diese Art des Hackings werden auch Bug-Bounty-Programme ausgeschrieben, um eine extrinsische Motivation zum Melden zu bieten.

Black-Hat-Hacker*innen verkörpern den medial verbreiteten Stereotyp von Hacker*innen: Sie dringen in IT-Systeme ein, um Daten zu entwenden, zu löschen oder zu verändern, Systeme zu übernehmen, zu stören oder abzuschalten oder Daten und Schwachstellen an Dritte zu verkaufen. Sie agieren aus eigenem kriminellen oder finanziellen Interesse, setzen auf Ransomware-Angriffe oder Datendiebstahl oder werden von Dritten, beispielsweise feindlichen Staaten engagiert. Bekannte Beispiele sind Hackergruppen aus Russland wie Fancy oder Cozy Bear[17].

15 Vaden, Stallmann (2002)

16 Moore (o.J.)

17 SWR, Simplicissimus (2024)

Grey-Hat-Hacker*innen decken einen breiten Graubereich in der Mitte des Spektrums ab. Ihnen geht es weniger um das Härten von Systemen, sondern um das Testen der eigenen Fähigkeiten. Sie verstoßen gegen anerkannte Werte wie die der Hackethik und missbrauchen Schwachstellen, aber nicht zur finanziellen Bereicherung. Mitunter werden zu Grey-Hat-Hacker*innen auch jene gezählt, die aus eigener politischer Motivation agieren wie das Kollektiv Anonymous, oder die wie der Hacker Khalil Shreateh gegen anerkannte Meldeprozesse verstoßen[18].

Während Sicherheitsforschende und Hacker*innen systematisch testen und nach Lücken suchen, gibt es auch zufällige Funde ohne fundierte Kenntnisse. Entscheidend ist hier weniger die Intention der Suche, sondern der Umgang mit der Schwachstelle: Meldet die Person sie verantwortungsvoll an den Hersteller, fällt sie in die Kategorie White Hat Hacker*in.

18 Warren (2013)

4. Betroffene Rechtsgebiete: Same same, but different

Der Begriff des Computerstrafrechts bezieht sich originär auf §§ 202a-c StGB, das Ausspähen oder Abfangen von Daten beziehungsweise die Vorbereitung desselben inklusive des Besitzes oder der Herstellung von „Computerprogramme[n], deren Zweck die Begehung einer solchen Tat ist“. Cybersicherheitsforschende streifen durch ihr Vorgehen jedoch noch weitere Rechtsgebiete, die für einen sicheren Rechtsrahmen mit in den Blick genommen werden sollten. Durch das Dekompilieren, das Testen oder den Rückbau von Software können die Urheberrechte der Rechtsinhaber verletzt oder ein Geschäftsgeheimnis rechtswidrig erlangt werden. Bisherige Ausnahmen wie beispielsweise für Whistleblower schließen das Melden von Schwachstellen nicht ein.

4.1. STRAFRECHT

§§ 202a-c, 303a-b StGB

Der Kern des Computerstrafrechts bezieht sich auf das (vorbereitete) Ausspähen oder Abfangen von Daten sowie deren Veränderung und Sabotage.

§ 202a StGB kriminalisiert das Ausspähen von Daten durch die Überwindung einer Zugangssicherung und ohne Befugnis, dies zu tun. Dies umfasst einen erheblichen Aufwand bei Täter*innen sowie eine besondere Zugangssicherung, zu deren Überwindung „grundsätzlich ein zeitlicher und technischer Aufwand notwendig ist, der nicht nur unerheblich ist“[19]. Dabei kommt es jedoch nicht auf die objektive Schwierigkeit der Überwindung an, sondern darauf, dass eine Sicherung vorliegt[20].

Der Paragraph legt dabei fest, was einen rechtswidrigen Zugang zu Daten ausmacht, und wird damit zur Grundlage der weiteren Gesetzgebung im Computerstrafrecht. Die Intention des Täters findet dabei keine Beachtung, sodass sich Meldende von Schwachstellen selbst belasten müssen: Durch die Meldung geben sie gleichzeitig zu, unbefugt Zugang zu fremden Daten erlangt zu haben. Dabei ist bereits der Titel des § 202a StGB „Ausspähen von Daten“ irreführend. Ein tatsächliches Ausspähen von Daten ist nicht nötig, um den Tatbestand zu erfüllen. Bereits mit der Verschaffung der Zugangsmöglichkeit, auch wenn diese nicht genutzt wird, ist der Tatbestand erfüllt.[21]

§ 202b StGB ergänzt den § 202a StGB um das unbefugte Abfangen von Daten durch technische Mittel aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage (sog. Seitenkanalangriffe).

§ 202c StGB ist der am stärksten kritisierte Punkt im Computerstrafrecht. Er kriminalisiert das Vorbereiten eines Ausspähens oder Abfangens von Daten und umfasst auch die Herstellung und Verbreitung von „Computerprogramme[n], deren Zweck die Begehung einer solchen Tat [Ausspähen oder Abfangen von Daten] ist“.

Diese Definition von sogenannten Hacker*innentools wird von Jurist*innen mit Schwerpunkt Cyber und IT als zu weitgehend angesehen. Bereits bei der Einführung des § 202c kritisierte Prof. Dr. Alexander Roßnagel, damals Jurist an der Universität Kassel und jetzt hessischer Datenschutzbeauftragter, dass der Paragraph ein eigentlich wünschenswertes Verhalten, nämlich das Untersuchen der Sicherheit eines Systems, durch die Verwendung der dafür notwendigen Werkzeuge kriminalisiert: Das „digitale Dietrichset“ würde durch die Formulierung unter

19 Ohlig (2025), S. 65

20 BGH, 5 StR 614/19 Rn. 24

21 Beck in: Schuster, Grützmacher (2025)

Strafe gestellt.[22] Ähnlich sieht dies auch der Rechtsanwalt Carsten Hoenig, spezialisiert auf Cybercrime: Er kritisiert, dass die Absicht zur Verwendung im Gesetz nicht berücksichtigt wird[23].

Während §§ 202a-c StGB nur den unbefugten Zugriff auf fremde Daten regelt, umfasst der § 303a StGB die (versuchte) Datenveränderung, also das Löschen, Unterdrücken oder unbrauchbar machen. § 303b StGB umfasst die Störung der Datenverarbeitung durch deren Veränderung, die unbefugte Weitergabe fremder Daten oder die Zerstörung und Beschädigung von Hardware. Beide Fälle werden als Cybercrime anerkannt und liegen außerhalb des White-Hat-Hackings, da sie die Beschädigung oder Veränderung von Daten oder Datenträgern vorsehen.

§ 5 TDDDG

Das in § 5 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) festgehaltene Abhörverbot verbietet das Abhören von Nachrichten außerhalb des bestimmten Adressatenkreises. Ziel des Gesetzes ist der Schutz der Privatsphäre und von Daten in der Telekommunikation. Als Folge verhindert es jedoch auch, dass Sicherheitsforschende unverschlüsselte und damit unsichere Funkverbindungen im Sinne des Gemeinwohls rechtssicher melden können, da dies zu einer unmittelbaren Selbstbelastung führt. Die AG KRITIS, ein Zusammenschluss von Expert*innen zu IT-Sicherheit und Resilienz kritischer Infrastruktur, kritisiert regelmäßig, dass in sensiblen Feldern wie Energie- oder medizinischer Versorgung trotz der breiten Verfügbarkeit von Verschlüsselungstechnik nach wie vor oft offene Funkkommunikation stattfindet[24] [25]. Dies kann gerade im KRITIS-Bereich beispielsweise zu missbräuchlichem Auslösen von Sirenen führen.

§ 42 ABS. 2 BDSG

Das Bundesdatenschutzgesetz (BDSG) bestraft an dieser Stelle Akteure, die gewerbsmäßig „nicht allgemein zugängliche personenbezogene Daten“ ohne Berechtigung einer großen Zahl an Personen zugänglich machen. Dies kann auch der Fall sein, wenn Sicherheitsforschende im Auftrag agieren, dabei über eine unbekannte Stelle zufällig auf andere Daten stoßen und damit der unberechtigte Zugang zu gesicherten Daten (s. § 202a StGB) erfolgt. „Bei § 42 Abs. 2 BDSG besteht […] das Risiko, dass Ermittlungsbehörden und Gerichte ein Handeln „gegen Entgelt“ weit verstehen und die Gehaltszahlungen an IT-Sicherheitsforschende ausreichen lassen, um deren Strafbarkeit bei der Weitergabe nicht allgemein zugänglicher personenbezogener Daten zu postulieren“[26].

22 Gesellschaft für Informatik (2007)

23 Hoenig (2026)

24 Rundfeldt (2024)

25 Der Spiegel (2026)

26 Balaban et al. (2024), S.10

4.2. ÖFFENTLICHES RECHT

DSGVO

ART. 32 DSGVO

Das Eindringen in IT-Systeme ist oftmals mit dem (ungewollten) Zugriff auf personenbezogene Daten verbunden. Datenverarbeitende Organisationen sind verpflichtet, „geeignete technische und organisatorische Maßnahmen [umzusetzen], um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“ (Art. 32 Abs. 1 DSGVO). Dies schließt die „regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit [...] zur Gewährleistung der Sicherheit der Verarbeitung“ (Art. 32 Abs. 1 lit. d DSGVO) mit ein. Daraus schließt sich eine Notwendigkeit für Hersteller, ihre Systeme auch durch Sicherheitsforschende erproben zu lassen[27]. Unklar ist jedoch, wie dabei eine unbefugte Offenlegung oder ein unbefugter Zugang zu personenbezogenen Daten (Art. 32 Abs. 2 DSGVO) zu verstehen ist. Hier bedarf es Rechtssicherheit für die DSGVO-Verantwortlichen oder Auftragsverarbeitenden.

ART. 89 DSGVO

Art. 89 DSGVO i.V.m. Erwägungsgrund 159 ermöglicht die Verarbeitung personenbezogener Daten zu unter anderem wissenschaftlichen Forschungszwecken. Das systematische Vorgehen von Sicherheitsforschenden ist nach dem Verständnis von Forschung als „geistige Tätigkeit mit dem Ziele, in methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen“[28], davon erfasst.

4.3. BÜRGERLICHES RECHT

§ 5 Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)

Das Erlangen eines Geschäftsgeheimnisses durch „Rückbauen oder Testen“ (§ 3 Abs. 1 Nr. 2 GeschGehG) ist durch eine Änderung des Gesetzes gegen den unlauteren Wettbewerb (UWG) auf Grundlage der Richtlinie 2016/943 ermöglicht worden und schließt damit auch das sogenannte Reverse Engineering ein[29], sofern keine Pflicht zur Beschränkung der Erlangung des Geschäftsgeheimnisses besteht.

§ 5 GeschGehG beschreibt mögliche Ausnahmen für solche Beschränkungen und Handlungsverbote. § 5 Nr. 2 GeschGehG greift dabei die „Aufdeckung einer rechtswidrigen Handlung oder eines beruflichen oder sonstigen Fehlverhaltens auf, wenn die Erlangung, Nutzung oder Offenlegung geeignet ist, das allgemeine öffentliche Interesse zu schützen“.

Fraglich ist jedoch, ob die Voraussetzung des allgemeinen öffentlichen Interesses in jedem Fall gegeben wäre, wenn Sicherheitsforschende eine Schwachstelle aufdecken. Damit besteht auch im Rahmen des GeschGehG Rechtsunsicherheit für Sicherheitsforschende.

§ 69d und e Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz)

Das Urheberrechtsgesetz regelt die Nutzungsbedingungen und umfasst damit auch den Schutz von Computerprogrammen. Dies umfasst auch das Dekompilieren oder Deassemblieren[30] von Software. Diese „Übersetzung“ kann notwendig sein, wenn kein Zugang zum Quellcode besteht. Zum Schutz dieses geistigen

---

27 Balaban et al. (2024)

28 BVerfGE 35, 79 – Hochschulurteil

29 Bundestagsdrucksache 19/4724, S. 25

30 Disassembling ist vom UrhG nicht namentlich erfasst.

Eigentums nennt das UrhG Fälle, die die Zustimmung der Eigentümer*in erfordern, wie etwa die Vervielfältigung oder Veränderung des Programms und hält einen Vernichtungsanspruch für Verstöße fest.

Rechtmäßige Erwerber eines Computerprogramms dürfen dieses bestimmungsgemäß verwenden und auch untersuchen, um Fehlerkorrekturen vornehmen zu können (§ 69d UrhG). Unklar ist bisher aber, ob dies auch Deassassemblieren oder Dekompilieren beinhaltet. Dekompilieren ist nach § 69e UrhG nur erlaubt, wenn es für die Interoperabilität notwendig ist. Die Formulierung schließt damit die Möglichkeit einer Fehleranalyse durch das Dekompilieren eines Codes aus. Um mögliche Schwachstellen zu finden, müssen Cybersicherheitsforschende diese Methoden jedoch straffrei nutzen können.

EXKURS: WHITE-HAT-HACKING IN EUROPA

In Europa ist ethisches Hacking in sieben Staaten explizit erlaubt, in zwei weiteren entfällt die Strafverfolgung, wenn bestimmte Umstände vorliegen[31] [32]. Wir stellen hier drei Länder vor, die nach Ansicht der Gesellschaft für Informatik als Best-Practice-Beispiele gesehen werden können:

In Polen[33] sind Personen, die ausschließlich zum Zweck der Sicherung von Systemen handeln, explizit von der Strafbarkeit ausgenommen. Der polnische Ansatz ist im Vergleich am liberalsten.

Ethisches Hacking ist in Portugal[34] unter kumulativen Voraussetzungen erlaubt: Die Handlung muss in guter Absicht und ohne finanzielle Motivation erfolgen, darf keine Schäden verursachen und gefundene Schwachstellen sollen zeitnah gemeldet werden.

In Belgien[35] ist ethisches Hacking unter bestimmten kumulativen Bedingungen gestattet. Dazu zählen eine zeitnahe Meldung an das belgische Cybersicherheitszentrum, das Fehlen einer Schadensabsicht sowie die Einhaltung der Prinzipien von Notwendigkeit und Verhältnismäßigkeit. Zusätzlich unterhält Belgien eine „Hall of Fame", um IT-Sicherheitsforschende für ihren Beitrag zur nationalen Cybersicherheit zu würdigen.

31 Piltz Legal, (o.J.), teilweise veraltet

32 Wissenschaftlicher Dienst des Bundestags (2024)

33 Art. 269b §1a, Kodeks karny (Strafgesetzbuch) (Stand: 21.01.2026)

34 Art. 8.º-A, Atos não puníveis por interesse público de cibersegurança (Straffreie Handlungen wegen öffentlichen Interesses an Cybersicherheit), Decreto-Lei n.º 125/2025 (04.12.2025)

35 Art. 23, Wet tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (Gesetz zur Schaffung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit); Somers und Vranckaert (2025)

5. Ergebnisse des Konsultationsprozesses: Don‘t shoot the messenger

Eine Gesetzesänderung und damit Entkriminalisierung des gemeinwohlorientierten Aufdeckens von Schwachstellen ist dringend notwendig, um das Cybersicherheitsniveau in Deutschland zu erhöhen. Eine Gesetzesänderung stellt dabei einen wesentlichen Teil der Lösung dar. Daneben braucht es einen ganzheitlichen Ansatz, der neben Anpassungen von Gesetzgebung auch ein wirkungsvolles Meldeverfahren und eine aktive Meldekultur erfordert. Zudem ist eine stärkere gesellschaftliche Anerkennung ethischen Hackens ein wichtiger Beitrag.

5.1. GESETZESÄNDERUNGEN

Im Rahmen einer gesetzlichen Anpassung muss die Intention der meldenden Person zentrales Kriterium sein. Die gemeinwohlorientierte Meldung einer entdeckten Sicherheitslücke an den Hersteller oder die betroffene Organisation, statt deren missbräuchliche Nutzung zum eigenen Vorteil, stellt einen wesentlichen Unterschied zu böswilligem Hacking dar. Entsprechend ist die Absicht eines*r Hackers*in auch in Gesetzestexten anderer Nationen ein entscheidendes Kriterium.

EIN SUBJEKTIVER TATBESTAND KANN MELDENDE ENTLASTEN.

Eine Reform des Computerstrafrechts sollte das ethische Melden von Schwachstellen erleichtern, indem sie ethischen Hacker*innen besseren Schutz bietet. Die Sorge vor einem solchen Verfahren, verbunden mit den anfallenden Prozess- und Anwaltskosten und Berichten über die Beschlagnahmung von Arbeitsmitteln und Hausdurchsuchungen, schreckt jedoch mögliche Melder*innen ab. Eine Gesetzesänderung sollte daher diesen „Chilling Effect“ bedenken.

Eine sinnvolle Lösung wäre es, eine Schädigungsabsicht als Vorsatz und damit als weiteres Tatbestandsmerkmal zur Fassung der § 202a-b StGB zuzufügen. Damit wäre die Intention der Handelnden schon bereits damit erkennbar, dass sie eine Schwachstelle dem betroffenen Hersteller gegenüber melden, anstatt sie auszunutzen. Bei einer Reform darf das Ziel nicht aus dem Blick geraten: der Schutz von ethischen Hacker*innen.

Ebenso müssen andere Gesetze angepasst werden, die eine Selbstbelastung der Meldenden beinhalten, wie bspw. § 5 TDDDG. Dieser kriminalisiert in seiner aktuellen Form das Melden einer Schwachstelle, auch wenn diese auf eine schlechte oder fehlende Sicherung auf Herstellerseite zurückzuführen ist. Hier muss eine gesetzliche Lösung es Meldenden ermöglichen, über eine Schwachstelle zu informieren.

SCHLECHTE SICHERUNGEN DÜRFEN NICHT ALS „BESONDERE SICHERUNG“ ANERKANNT WERDEN

Ein wichtiger Kritikpunkt ist das oberflächliche Verständnis von „besonderer Sicherung“, die in § 202a StGB als Tatbestandsmerkmal festgehalten ist. Relevant ist hier insbesondere der Fall „Modern Solutions“ (s. Exkurs Modern Solutions, S. 5), bei dem die entdeckten Passwörter unverschlüsselt zu finden waren. Das Landgericht Aachen sah dies trotzdem als eine besondere Sicherung an[36].

Zukünftig ist es unerlässlich, dass auf Seiten der Gerichte und Staatsanwaltschaften ausreichend Wissen über Sicherungsmaßnahmen vorhanden ist. Eine unzureichende oder fehlende Sicherung erfüllt das Merkmal der besonderen Sicherung nicht und entkräftet damit auch eine Strafanzeige. Hierfür sollten Expert*innen mit Gutachten unterstützen, um einen „State of the Art“ darzulegen und so eine sachgerechte Bewertung zu ermöglichen.

---

36 LG Aachen, Urt. v. 27.07.2023 - Az.: 60 Qs 16/23.

EINSATZ VON DEKOMPILIEREN UND WEITEREN WERKZEUGEN LEGALISIEREN

Während manche Schwachstellen durch Zufall gefunden werden, tauchen andere beim Dekompilieren, beim Testen oder dem Rückbau von Software auf. Hier tritt ein wesentlicher Diskussionspunkt zu Tage: der Schutz von geistigem Eigentum und die Notwendigkeit, Schwachstellen in Software zu melden, um sie zu schließen. § 69e UrhG und § 5 GeschGehG nennen zum jetzigen Zeitpunkt eine Anzahl an Fällen, zu deren Zweck das Dekompilieren oder das Offenlegen eines Geschäftsgeheimnisses erlaubt ist, wie beispielsweise das Aufdecken eines Fehlverhaltens mit allgemeinem öffentlichen Interesse (§ 5 Nr. 2 GeschGehG) oder zur Herstellung der Interoperabilität (§ 69e Abs. 1 UrhG). Hier schlagen wir vor, das Melden von Schwachstellen an Hersteller und/oder staatliche Stellen zu ergänzen, aufbauend auf einem reformierten § 202a StGB.

Damit einhergehend müsste auch der § 202c StGB angepasst oder sogar abgeschafft werden: Nicht die Herstellung oder das Zugänglichmachen von „Hacker*innentools“ sollte kriminalisiert werden, da diese zur Aufdeckung solcher Schwachstellen verwendet werden, sondern die Verwendung für eine verbotene Handlung.

REPUTATIONS- UND MITTELBARE SCHÄDEN AUSKLAMMERN

Hersteller und Betreiber befürchten oft einen Reputationsverlust, der bei der Meldung einer Schwachstelle entstehen könnte: Kund*innen könnten das Vertrauen in das Produkt verlieren oder die Verwendung könnte sinken, weil Aufträge ausfallen. Im Falle eines Cybercrimes mit einem ähnlichen Effekt lassen sich diese indirekten Kosten selten beziffern: Kosten treten oft erst versetzt auf[37]. Da diese Schäden nicht unmittelbar attribuierbar sind, sollten sie auch ethischen Hacker*innen nicht angelastet werden. Unternehmen, die einen CVD[38]-Prozess umsetzen und so mit den Meldenden zusammenarbeiten, können somit auch eine öffentliche Meldung zu dem Zeitpunkt vermeiden, an dem die gefundene Schwachstelle noch nicht behoben ist.

FREIWILLIGE MELDUNGEN ALS ERGÄNZUNG DES CYBER RESILIENCE ACTS EINBRINGEN

Ab September 2026 gelten für Softwarehersteller Meldepflichten über Schwachstellen gegenüber dem BSI und ENISA sowie gegenüber Nutzer*innen bezüglich Schwachstellen und verfügbaren Patches.

Für die Workshopteilnehmenden schien es sinnvoll, mit der Meldepflicht für Hersteller auch eine Meldemöglichkeit für externe und/oder ehrenamtlich agierende Sicherheitsforschende einzuführen. Damit würde der Charakter des Cyber Resilience Acts gestärkt und die Cybersicherheit im Land gefördert werden.

5.2. MELDEVERFAHREN

Die aktuelle Gesetzeslage fördert einen Umgang mit Meldungen, der auf „Security by Obscurity“ statt Transparenz basiert. Die Forderung nach Transparenz mag widersinnig klingen: Warum sollte gefördert werden, dass Dritte Schwachstellen finden und vielleicht auf kritische Informationen stoßen? Dies ist jedoch kurzfristig gedacht: Eine einmal identifizierte Schwachstelle kann auch ein zweites und drittes Mal durch andere ausfindig gemacht werden. Im Idealfall wird die Schwachstelle bereits beim ersten Fund gemeldet und durch das betroffene Unternehmen geschlossen, um künftig den Zugriff durch weitere Akteure mit potenziell schlechten Absichten zu verhindern. Die Meldung ist demnach eine Hilfestellung für das Unternehmen und sollte als solche behandelt werden.

---

37 Weber (2024), S. 5

38 Coordinated Vulnerability Disclosure, das strukturierte Melden, Bearbeiten und Schließen von Sicherheitslücken in Kooperation zwischen Meldenden, Betroffenen und gegebenenfalls relevanten Behörden.

Wie oben ausführlich dargelegt, stellt die derzeitige Strafbarkeit von Meldungen ein Hindernis dar. Trotz guter Intentionen angeklagt zu werden[39], hat nachhaltig abschreckende Wirkungen auf Sicherheitsforschende, sodass bei weiteren gefundenen Schwachstellen im Zweifel gar nicht mehr Bescheid gegeben wird[40]. Viele White-Hat-Hacker*innen treffen daher umfangreiche Vorsichtsmaßnahmen beim Melden, darunter die anonyme Meldung über historisch gewachsene Strukturen wie die des CCC. Diese „Chilling Effects" führen zu negativen Auswirkungen auf die gesamtgesellschaftliche Cybersicherheit.

5.3. MELDEKULTUR

Eine Rückbesinnung auf eine positive Fehler- und Feedbackkultur, die viele Unternehmen intern bereits praktizieren, ist hier hilfreich. Eine Meldung ist letztlich weder Anzeige noch Erpressung, sondern der Hinweis auf einen unentdeckten Fehler. Während ansonsten auch das Motto „Don't shoot the messenger" gilt, erstreckt sich dieses derzeit noch nicht auf den Umgang mit externen Meldungen von Schwachstellen. Hier gilt weiterhin: Wer eine Schwachstelle findet und diese meldet, um den Sicherheitsstandard effektiv zu erhöhen, kann für unternehmensinterne Versäumnisse abgestraft werden.

Gleiches gilt für die Entwicklung von Werkzeugen, die ethisches Hacken erleichtern. Gefundene Schwachstellen zu melden, ist primär eine – zudem häufig kostenlose – Dienstleistung für das entwickelnde Unternehmen, die im Rahmen von Pen-Testing sonst hätte bezahlt werden müssen. Dies kann Unternehmen nicht von der Pflicht entbinden, selbst Pen-Testing durchzuführen, aber unterstreicht die erbrachte Leistung durch meldende Cybersicherheitsforschende.

Bug-Bounty-Programme sind ein Positivbeispiel für ein CVD-Verfahren: Sie verdeutlichen von Unternehmensseite, dass Meldungen nicht nur explizit erwünscht sind, sondern die oftmals ehrenamtliche Arbeit der Sicherheitsforschenden auch entlohnungswürdig ist. Gleiches gilt für die Würdigung dieses Engagements für die kollektive Sicherheit durch eine Hall of Fame[41], wie sie das BSI bereits betreibt. Meldungen von Schwachstellen sollten als ehrenamtliche Arbeit stärker gewürdigt werden: Neben Capture-the-Flag-Wettbewerben und Hackathons, die unter anderem auch Nachwuchsfachkräfte einbinden, wäre auch die Berücksichtigung besonders aktiver ethischer Hacker*innen (s. Hall of Fame) beim Ehrenamtstag möglich. Gleichzeitig würde diese Praxis das verbreitete negative Bild von Hacker*innen im schwarzen Hoodie aufbrechen. Eine Normalisierung des Dienstes von White-Hat-Hacking für die Öffentlichkeit ist für den angesprochenen Kulturwandel zentral.

39 Hoenig (2026)

40 Neumann (2021)

41 BSI (o.J.-a)

5.4. MELDEPROZESSE

GEGENSEITIGES VERTRAUEN ALS VORAUSSETZUNG

Meldeprozesse sollten für alle Seiten möglichst effizient gestaltet sein und einen professionellen Umgang zwischen Meldenden und Herstellern ermöglichen. Sicherheitsforschende müssen sich darauf verlassen können, dass ihre Meldung ernst genommen wird. Unternehmen wiederum müssen darauf vertrauen können, dass die meldende Person die gefundene Schwachstelle inklusive möglicher Daten vertraulich behandelt.

FUNKTIONIERENDE KONTAKTSTELLE UND INTERNES MELDESYSTEM

Um Meldeprozesse für beide Seiten einfach zu gestalten, bietet sich der direkte Kontakt an. Hier ist beispielsweise eine security.txt hilfreich, die nicht nur eine unkomplizierte Kontaktstelle für Meldungen bietet, sondern auch homogen klare Kriterien für den Prozess vorgibt. Meldende sollten hierbei wie bisher auch die Möglichkeit zur anonymen Meldung haben. Unternehmen sollten zudem ein Information Security Management System (ISMS) bzw. ein Cybersecurity Management System (CSMS) etablieren, welches die adäquate Weiterleitung solcher Informationen an die relevanten internen und externen Stellen sichert. Dies erleichtert die Compliance, erhöht auf Seite der Meldenden und Nutzenden das Vertrauen und schützt das Firmenimage[42].

Grundsätzlich gilt: Sobald eine Schwachstelle gefunden wurde, sollte sie so schnell wie möglich an das Unternehmen gemeldet werden. Unternehmen sind in diesem Zuge verpflichtet, die jeweils relevanten Umsetzungsfristen aus dem Cybersecurity Act, DORA, NIS2 und weiteren Regulierungen für die Meldung an die verantwortlichen staatlichen Stellen (meist das BSI sowie ENISA) einzuhalten. Sofern Meldende den Unternehmen eine Frist für erste Schritte setzen, sollten diese die gesetzlichen Vorgaben berücksichtigen.

ÖFFENTLICHE MELDUNG ALS ULTIMA RATIO BEI FEHLENDER REAKTION

Viele Unternehmen fürchten den Gang an die Öffentlichkeit. Dieser sollte jedoch als Ultima Ratio fungieren oder verwendet werden, um nach dem Schließen einer Sicherheitslücke Außenstehende zu informieren. Ein verantwortungsvoller Meldeprozess umfasst zunächst die Ansprache des betroffenen Unternehmens. Erst wenn dieses untätig bleibt, sieht auch das vom BSI vorgeschlagene CVD-Verfahren vor, dass eine Meldung an die Öffentlichkeit möglich ist. Auch hier gilt: Eine warnende Meldung sollte nur so viel Informationen beinhalten, damit Aufmerksamkeit und Druck erreicht wird. Sie sollte jedoch, so lange die Schwachstelle nicht behoben ist, keine tiefergehenden Informationen über diese beinhalten, um sie nicht zu exponieren. Gleichzeitig sollte es Forschenden erlaubt sein, über das Finden einer Schwachstelle zu publizieren. Das BSI rät in seiner CVD-Leitlinie, diese Frist zwischen Herstellern und Sicherheitsforschenden zu besprechen. Hier haben sich international 45 bis 90 Tage als übliche Frist etabliert, innerhalb derer die Unternehmen eine Schwachstelle im Softwarebereich korrigiert haben sollten. Bei Schwachstellen in der Hardware kann der Zeitraum zur Behebung länger ausfallen[43]. Die Veröffentlichung dient primär dazu, Wissen über die Entdeckung und Ursachen von Schwachstellen zu verbreiten, und weniger der Bloßstellung eines Unternehmens.

INSTITUTIONALISIERUNG VON ÖFFENTLICHEN MELDESTELLEN

Mit der Umsetzung des CRA kommt dem BSI eine weitere Aufgabe als Meldestelle für Unternehmen zu. Dies darf nicht dazu führen, dass das BSI seine Rolle als Anlaufpunkt für Schwachstellenmeldungen von Externen vernachlässigen muss. Stattdessen muss das BSI fristgerecht auf die Meldungen reagieren und als Ansprechpartner für Unternehmen und Sicherheitsforschende fungieren können. Dafür müssen ausreichend Ressourcen und Stellen verfügbar sein, auch um andere indirekte Meldestellen wie den CCC zu entlasten.

---

42 Fraunhofer SIT (o.J.)

43 BSI (2022), S. 10

6. Empfehlungen: Protect the messenger, fix the (f)law

6.1. GESETZESÄNDERUNGEN

SCHÄDIGUNGSABSICHT ALS TATBESTAND EINFÜHREN

Eine Gesetzesänderung muss so gestaltet sein, dass ethisches Hacken legalisiert wird und Meldende nicht durch umfassende Ermittlungsverfahren abgeschreckt werden. Deshalb muss die Beweislast durch den Nachweis einer Schädigungsabsicht auf die Herstellerseite verlagert werden. Das bietet eine entscheidende Entlastung für Hacker*innen, wenn sie eine ordentliche Meldung vornehmen.

ÜBER DEN (NATIONALEN) TELLERRAND SCHAUEN

Zweck der angestrebten Reform ist der bessere Schutz von ethischen Hacker*innen vor ungerechtfertigter Strafverfolgung, auch als Mittel der Abschreckung. Aus diesem Grund dürfen erfüllte objektive Tatbestandsmerkmale nicht dazu führen, dass ein Vorsatz angenommen werden kann. Vielmehr braucht es einen angepassten objektiven Tatbestand, der einen effektiven Schutz ermöglicht. Andere europäische Staaten wie Belgien oder Portugal haben bereits Lösungen gefunden, an denen sich eine deutsche Lösung orientieren kann.

NICHT BEI § 202A STGB AUFHÖREN

Das Suchen, Finden und Melden von Schwachstellen in Software, Hardware und im Funk wird durch mehrere Gesetze blockiert. Allein eine Reform des Ausspähens von Daten (§ 202a StGB) zugunsten ethischer Hacker*innen oder beim Melden von unsicherem Funkverkehr genügt daher nicht, um ausreichend Rechtssicherheit zu schaffen. Auch müssen ethischen Hacker*innen die gleichen Werkzeuge wie böswilligen Hacker*innen zur Verfügung stehen, um realistische Bedrohungsszenarien untersuchen zu können. Entsprechend muss hierfür die Entwicklung, Verwendung und Verbreitung solcher Programme legalisiert werden. Dies umfasst auch die Entwicklung und Verwendung von dafür notwendigen Computerprogrammen wie Dekompilierern für solche Zwecke.

Der Schutz von geistigem Eigentum oder von Geschäftsgeheimnissen muss gewährleistet werden können, ohne zum Verhinderungsgrund zu werden, eine Schwachstelle in einem Produkt zu beheben.

WINDSCHATTEN DES CRA NUTZEN

Der Cyber Resilience Act sieht Meldepflichten für Hersteller und Betreiber bei Schwachstellen vor und legt insgesamt ein höheres Maß an Cybersicherheit und damit mehr Anforderungen an den Umgang mit Schwachstellen an. Eine Legalisierung von ethischem Hacking wäre ein konsequenter Schritt, die Cybersicherheitslandschaft in Deutschland besser zu gestalten und das Potenzial zu nutzen, das Expert*innen aus der Sicherheitsforschung, Hobbytüftler*innen und gewissenhafte Nerds mitbringen.

6.2. UMGANG MIT HACKER*INNEN

STANDARDISIERTEN MELDEPROZESS IMPLEMENTIEREN

Um Schwachstellen schnell und effizient weiterzugeben und zu beheben, sollte die Arbeit für Meldende so einfach wie möglich gemacht werden. Hierfür braucht es einen standardisierten Meldeprozess. Um indirekte Meldeketten zu vermeiden, bietet sich eine Meldung der ehrlichen Finder*innen an die Hersteller selbst an. Dies wird beispielsweise mit einer security.txt begünstigt. Unternehmen sind infolge des CRA dazu verpflichtet, innerhalb der gesetzlichen Fristen eine identifizierte Schwachstelle an BSI und ENISA zu melden. Die Veröffentlichung der gefundenen Schwachstelle kann nach Ablauf einer angemessenen Frist beispielsweise bei öffentlichem Interesse oder im Rahmen einer wissenschaftlichen Arbeit folgen.

ETHISCHES HACKEN ALS EHRENAMT FÖRDERN

Das Suchen, Finden und Melden von Schwachstellen in der Freizeit sollte wie andere Gemeinschaftsdienste auch als Ehrenamt anerkannt werden. Dies ist einmal über die bereits bestehende Hall of Fame des BSI möglich. Weitere Anerkennung könnte durch die Einladung von ethischen Hacker*innen zum Ehrenamtstag oder die finanzielle Anerkennung durch ein öffentliches Bug-Bounty-Programm ausgedrückt werden. Auch Events wie Hackathons drücken Wertschätzung für die Community aus.

KULTURWANDEL: ETHISCHES HACKEN ALS ZUSÄTZLICHE SCHUTZMAßNAHME VERSTEHEN

Das gesellschaftliche Bild von Hacker*innen ist oft negativ besetzt. Die Änderung der Gesetzeslage kann die Wahrnehmung fördern, dass ethisches Hacking einen Beitrag zu besserem Cyberschutz leistet und die Sicherheitslage verbessert. Grundlegend ist allerdings ein Umdenken bzgl. Geheimhaltung als vermeintliche Sicherheitsmaßnahme im Cyberraum nötig. Die zunehmende Relevanz von „Security by Design“ geht in die richtige Richtung, kann jedoch noch stärker mit Transparenzgeboten verknüpft werden.

DEFINITION EINES „BESONDERS GESICHERTEN ZUGANGS“

Während die DSGVO die Vorgabe besitzt, dass die Sicherheit der Datenverarbeitung Faktoren wie den Stand der Technik oder Risiken und deren Eintrittswahrscheinlichkeiten berücksichtigen muss (Art. 32 Abs. 1 DSGVO), finden sich in § 202a StGB keine Anforderungen für einen besonders gesicherten Zugang. Damit ist der Rechtsprechung ein weiter Interpretationsspielraum gesetzt. Hier müssen Anforderungen anhand realistischer Kriterien geschaffen werden, die eine Bewertung ermöglichen.

6.3. DAVON RATEN WIR AB

HACKER*INNEN-REGISTER FÜR MELDENDE VERZÖGERT ZEITKRITISCHE MELDUNGEN

Viele Hacker*innen suchen in ihrer Freizeit nach Lücken und melden diese aus altruistischen Gründen. Dies sollte gefördert werden, statt durch zusätzliche bürokratische Anforderungen abzuschrecken. Darüber hinaus sollten Schwachstellen schnell gemeldet werden, um geschlossen werden zu können. Sicherheitslücken werden mitunter durch Zufall gefunden.[44] Eine Registrierungspflicht verhindert in diesem Kontext ein schnelles Melden, da Meldende gezwungen würden, erst auf ihre Registrierung zu warten[45]. Darüber hinaus besteht das Risiko, dass Black Hats sich hier registrieren könnten, um sich zu legitimieren und das Vertrauen von Entwickler*innen zu erschleichen.

DE-ANONYMISIERUNG VON MELDENDEN BIRGT EIN REPRESSIONSRISIKO

Aktuell können ethische Hacker*innen Meldestellen wie das BSI, den CCC oder andere Meldestellen nutzen, wenn sie sich dem Risiko eines Verfahrens nicht aussetzen möchten. Dies kann auch anonym geschehen, um Meldende zu schützen. Auch nach einer Legalisierung sollten anonyme Meldungen weiter möglich sein, da auch über Zivilklagen Repressionen befürchtet werden und abschrecken können.

ÜBERBORDENDE REPORTING-ANFORDERUNGEN SIND EINE SCHWACHSTELLE FÜR MELDENDE

Meldestellen sind darauf angewiesen, ausreichend Informationen und Details über eine Schwachstelle zu erfahren, um sie nachvollziehen zu können. Das BSI verweist hierfür auf ein Proof of Concept (s. exemplarisch die Schwachstellenmeldung des BSI[46]) und eine CVSS[47]-Bewertung. Werden diese Anforderungen von Herstellerseite zu detailliert und fordernd, laufen Meldende Gefahr, trotz gewissenhafter Angaben Fehler zu machen. Dies ist für beide Seiten ein Problem, da Hersteller mit unklaren Angaben zurechtkommen müssen und Meldende ungewollt falsche Angaben machen.

---

44 s. bspw. den Fall der Hotelkette Numa: kantorkel (2025)

45 Sowa (2026)

46 https://portal.bsi.bund.de/

47 Common Vulnerability Scoring System, System zur Bewertung von Schwachstellen in IT-Systemen

7. Quellenverzeichnis

Atos não puníveis por interesse público de cibersegurança, Gesetz Nr. 125/2025 (2025). https://diariodarepublica.pt/dr/detalhe/decreto-lei/125-2025-962603401

Bachfeld, D. (19. Dezember 2008). „Hacker-Paragraf“: iX-Chefredakteur zeigt sich selbst an. heise.de. https://www.heise.de/news/Hacker-Paragraf-iX-Chefredakteur-zeigt-sich-selbst-an-191403.html

Balaban, S., Boehm, F., Brodowski, D., Dickmann, R., Franzen, F., & Goerke, N. (2021). Whitepaper zur Rechtslage der IT-Sicherheitsforschung. sec4research. https://sec4research.de/assets/Whitepaper.pdf

BGH 5 StR 614/19 (BGH, 13. Mai 2020). https://www.hrr-strafrecht.de/5/19/5-614-19.php

Borchers, D. (18. November 2014). 30 Jahre Btx-Hack: Grau ist alle Vergangenheit. https://www.heise.de/news/30-Jahre-Btx-Hack-Grau-ist-alle-Vergangenheit-2459564.html

BSI. (o. J.-a). Danksagung—Hall of Fame. CVD-Richtlinie des BSI. Abgerufen 7. Juni 2026, von https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/IT-Schwachstellen/Hall_of_Fame/Hall_of_Fame_node.html

BSI. (o. J.-b). FAQ für Sicherheitsforschende. CVD-Richtlinie des BSI. Abgerufen 7. Juli 2026, von https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/IT-Schwachstellen/FAQ_Sicherheitsforschende/FAQ_Sicherheitsforschende_node.html

BSI. (2022). Leitlinie des BSI zum Coordinated Vulnerability Disclosure (CVD)-Prozess. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CVD/CVD-Leitlinie.pdf?__blob=publicationFile&v=4

BSI. (2025). Die Lage der IT-Sicherheit in Deutschland 2025. Die Lage der IT-Sicherheit in Deutschland 2025. https://medien.bsi.bund.de/lagebericht/de/zusammenfassung-und-bewertung/

CVE. (18. Mai 2026). Metrics—Published CVE Records. https://www.cve.org/About/Metrics

Deutscher Mittelstandsbund. (02. Mai 2025). ARD-Tagesthemen: Angst vor Strafverfolgung unter Hackern. https://www.mittelstandsbund.de/kompetenzbereiche/finanzen/beitrag/ard-tagesthemen-angst-vor-strafverfolgung-unter-hackern

Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, 19/4724, Bundestag (2018). https://dserver.bundestag.de/btd/19/047/1904724.pdf

Fraunhofer SIT. (o. J.). Schwachstellenmanagement durch CVD. Abgerufen 6. Juli 2026, von https://www.sit.fraunhofer.de/de/cvd/

Gamero-Garrido, A., Savage, S., Levchenko, K., & Snoeren, A. C. (2017). Quantifying the Pressure of Legal Risks on Third-party Vulnerability Research. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 1501–1513. https://doi.org/10.1145/3133956.3134047

Gesellschaft für Informatik. (03. Juli 2007). Entwurfsfassung des § 202c StGB droht Informatiker/innen zu kriminialisieren. https://gi.de/meldung/entwurfsfassung-des-202c-stgb-droht-informatiker-innen-zu-kriminialisieren

Hoenig, C. R. (18. Mai 2026). Shooting the Messenger. https://www.hoenig.de/2026/shooting-the-messenger/

Hugging Face (16. Juli 2026). Security incident disclosure — July 2026. https://huggingface.co/blog/security-incident-july-2026

kantorkel. (11. Juni 2025). Ausgecheckt: Hotelkette Numa veröffentlicht Ausweisdaten. https://www.ccc.de/de/updates/2025/ausgecheckt-hotelkette-numa-veroffentlicht-ausweisdaten

Kodeks karny, Gesetz Nr. 2025.0.383.

Lossie, H. (21. Mai 2010). Die Hacker aus Hannover. Süddeutsche Zeitung. https://www.sueddeutsche.de/wirtschaft/23-juni-1987-die-hacker-aus-hannover-1.834013

Matheus, K. (07. Juni 2026). »White Hat Hacking« – Legalisiert es! Jetzt! elektronik.net. https://www.elektroniknet.de/automotive/wirtschaft/white-hat-hacking-legalisiert-es-jetzt.43b8698a-b788-49c3-b614-1ce736c170ec.html

Modern Solutions, 60 Qs 16/23 (LG Aachen, 27. Juli 2023). https://nrwe.justiz.nrw.de/lgs/aachen/lg_aachen/j2023/60_Qs_16_23_Urteil_20230727.html

Moore, M. (o. J.). Black, Gray and White-Hat Hackers: What's the Difference? University of San Siego Online. Abgerufen 8. Juni 2026, von https://onlinedegrees.sandiego.edu/black-vs-gray-vs-white-hat-hackers/

NDR. (15. Mai 2026). Hackerangriff: Daten von Zehntausenden Versicherten betroffen? NDR. https://www.ndr.de/nachrichten/niedersachsen/hackerangriff-daten-von-zehntausenden-versicherten-betroffen,hackerangriff-132.html

Neumann, L. (04. August 2021). CCC meldet keine Sicherheitslücken mehr an CDU. https://www.ccc.de/de/updates/2021/ccc-meldet-keine-sicherheitslucken-mehr-an-cdu

Ohlig, M. S. L. (2025). Erlaubtes Gray-Hat-Hacking und neue Strafrahmen im Computerstrafrecht? Kriminalpolitische Zeitschrift, (2), 63–81.

Rundfeldt, J. (16. Dezember 2024). Stellungnahme „Hackerparagraph" für Verbändeanhörung im Justizministerium. https://ag.kritis.info/2024/12/16/stellungnahme-hackerparagraph-fuer-verbaendeanhoerung-im-justizministerium/

Schuster, F., Grützmacher, M., Antoine, L., Beck, S., Bergt, M., Cording, S., & Diedrich, K. (2026). IT-Recht Kommentar: EU-Recht, nationales Recht, besondere Vertragsbedingungen (2., neu bearbeitete und erweiterte Auflage). Otto Schmidt.

Der Spiegel. (08.Januar 2026). »Sicherheitspolitisches Armutszeugnis« – Funk von kritischer Infrastruktur teils unverschlüsselt. (08. Januar 2026). https://www.spiegel.de/politik/deutschland/kritische-infrastruktur-abhoergefahr-bei-funkverbindungen-in-deutschland-a-0afbfcc7-df55-4225-8877-fe124814204b

Somers, C., & Vranckaert, K. (29. April 2025). Ethical hacking under the Belgian NIS2-law: Still a safe haven? KU Leuven, CiTiP. https://www.law.kuleuven.be/citip/blog/ethical-hacking-under-the-belgian-nis2-law-still-a-safe-haven/

Sowa, A. (04. Juni 2026). Mensch, Maschine – und das deutsche Computerstrafrecht. Tagesspiegel Background. https://background.tagesspiegel.de/it-und-cybersicherheit/briefing/mensch-maschine-und-das-deutsche-computerstrafrecht

Stiftung Datenschutz. (02. Oktober 2025). Bundesverfassungsgericht lehnt Beschwerde gegen Modern Solution ab – Ethical Hacking bleibt riskant. Stiftung Datenschutz. https://stiftungdatenschutz.org/veroeffentlichungen/datenschutz-im-fokus/datenschutz-im-fokus-detailansicht/ethical-hacking-bleibt-riskant-636

Piltz Legal. (2025). Strafbarkeit von White-Hat-Hacking in Europa. https://www.piltz.legal/news-blog/strafbarkeit-von-white-hat-hacking-in-europa

SWR & Simplicissimus. (26. Februar 2024). Putins Bären – Die gefährlichsten Hacker der Welt [Dokumentation]. https://www.ardmediathek.de/video/putins-baeren/putins-baeren-die-gefaehrlichsten-hacker-der-welt/swr/Y3JpZDovL3N3ci5kZS9hZXgvbzIwMDQ0NjI

T-Sicherheitslücken (Zero-Day), 1 BvR 2771/18 (BVerfG, 08. Juni 2021).

Vaden, T., & Stallmann, R. (2002). The Hacker Community and Ethics. GNU Operating System. www.gnu.org/philosophy/rms-hack.html

Warren, T. (18. August 2013). https://www.theverge.com/2013/8/18/4633046/facebook-security-bug-let-anyone-post-on-walls. The Verge. https://www.theverge.com/2013/8/18/4633046/facebook-security-bug-let-anyone-post-on-walls

Weber, C. (2024). Kosten und Schäden durch Cyber-Kriminalität in Deutschland. (Nr. 1/2024; KKF-Aktuell, S. 1–46). Bundeskriminalamt. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2024KKAktuell_Kosten_Schaeden_Cyberkriminalitaet.pdf?__blob=publicationFile&v=4,

Wet tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, 2024202344 Wet NIS2. Abgerufen 29. April 2026, von https://www.stradalex.com/nl/sl_src_publ_leg_be_moniteur/toc/leg_be_moniteur_nl_17052024_1/doc/bs2024202344

Wintergerst, R. (2025). Wirtschaftsschutz 2025 (S. 1–21). bitkom. https://www.bitkom.org/sites/main/files/2025-09/bitkom-pressekonferenz-wirtschaftsschutz-cybercrime.pdf

Wissenschaftlicher Dienst. (2024). Die Strafbarkeit des „Hackings“ – Rechtslage im internationalen (WD 7-3000-104/23; S. 1–37). Deutscher Bundestag. https://www.bundestag.de/resource/blob/1005444/ed435cb1a5311bb688385a81f295c8a3/WD-7-104-23-pdf.pdf

GESELLSCHAFT FÜR
INFORMATIK E. V.
(GI)

Geschäftsstelle Bonn
Wissenschaftszentrum
Ahrstr. 45
53175 Bonn
Tel.: +49 228 302-145
Fax: +49 228 302-167
E-Mail: bonn@gi.de

Geschäftsstelle Berlin
Weydinger Straße 14-16
10178 Berlin
Tel.: +49 30 240 09-805
E-Mail: berlin@gi.de

gs@gi.de
www.gi.de

/informatik@mas.to
/company/gesellschaft-fuer-informatik
/informatik.bsky.social