Whitepaper zur Rechtslage der IT-Sicherheitsforschung

Reformbedarf aus Sicht der angewandten Sicherheitsforschung

Autor*innen: Silvia Balaban, Franziska Boehm, Dominik Brodowski, Roman Dickmann, Fabian Franzen, Niklas Goerke, Sebastian Golla, Stephan Koloßa, Michael Kreutzer, Jochen Krüger, Maximilian Leicht, Johannes Obermaier, Maria Pieper, Marc Schink, Linda Schreiber, Dieter Schuster, Christoph Sorge, Hoa Tran, Oliver Vettermann, Stephanie Vogelgesang, Daniel Vonderau, Manuela Wagner

Inhaltsverzeichnis

Executive Summary

Dieses Whitepaper beschreibt die Rechtslage der IT-Sicherheitsforschung im Hinblick auf relevante Strafnormen, den urheberrechtlichen Schutz von Computerprogrammen, das Datenschutzrecht, den Schutz von Geschäftsgeheimnissen sowie vertrags- und deliktsrechtliche Haftungsfragen. Es soll eine wissenschaftliche Grundlage für die Diskussion zum Umgang mit gefundenen Schwachstellen bzw. Sicherheitslücken bilden, denn:

Unabhängige IT-Sicherheitsforschung ist ein essenzieller Baustein für eine sichere Digitalisierung: Produkte der Informations- und Kommunikationstechnik sind trotz größtmöglicher Sorgfalt selten frei von Sicherheitslücken. Werden diese nicht oder erst nach Inverkehrbringen des Produkts entdeckt, können sie von Unbefugten ausgenutzt werden. Dadurch entstehen unmittelbar erhebliche Gefahren für die internationale Gemeinschaft, Staaten, die Gesellschaft und die Wirtschaft. Es wird daher immer wichtiger, Schwachstellen so früh wie möglich zu finden und zu beheben. Folglich besteht auch ein großes gesamtgesellschaftliches Interesse an einer starken IT-Sicherheitsforschung durch neutral agierende Stellen, die rechtzeitig Risiken aufzeigen, sowie auf ihre Minimierung bzw. Beseitigung hinwirken, bevor es zum Schaden kommt.

Die Gefahr, dass entdeckte Sicherheitslücken ausgenutzt werden können, wird durch den Coordinated Vulnerability Disclosure (CVD) Prozess minimiert. Hier werden gefundene Sicherheitslücken zunächst derjenigen Stelle gemeldet, die in der Lage ist, die Schwachstelle zu beheben (in der Regel Produkthersteller*innen). Nach einer angemessenen Frist, innerhalb der im Regelfall die Schwachstelle beseitigt worden ist bzw. eine andere Lösung bereitgestellt wurde, erfolgt eine Warnung gegenüber der Öffentlichkeit, damit gefährdete Personenkreise erforderliche Schutzmaßnahmen ergreifen können. Zum Teil fehlt allerdings noch das entsprechende Bewusstsein für die Notwendigkeit eines solchen Prozesses. Daher beschreibt dieses Whitepaper typische Probleme und unterbreitet Vorschläge zu deren Lösung.

Selbst bei einem verantwortungsbewussten Umgang mit Sicherheitslücken sind **IT-Sicherheitsforschende in Deutschland von Haftungs- und Strafbarkeitsrisiken bedroht.** Dies zeigt sich etwa im Urheberrecht: Für die Durchführung von IT-Sicherheitsuntersuchungen ist in vielen Fällen Reverse Engineering notwendig. Dabei wird systematisch die Funktions- und Konstruktionsweise eines unbekannten Systems oder Produkts ermittelt und insbesondere auf ungewollte Funktionen bzw. Fehler untersucht. Urheberrechtlich sind einige Formen des Reverse Engineerings ohne Zustimmung der Urheber*innen verboten. Da IT-Systeme i.d.R. aus verschiedenen Komponenten unterschiedlicher, weltweit tätiger Hersteller*innen zusammengesetzt sind, ist die Erlangung einer Einwilligung für alle diese Elemente praktisch kaum zu erreichen. Bestehende urheberrechtliche Erlaubnisnormen greifen für die Forschung regelmäßig zu kurz.

Die IT-Sicherheitsforschung muss sich zudem realistischer Angriffsszenarien und -methoden bedienen, um die Vorgehensweise von Angreifer*innen nachvollziehen zu können und aufbauend neue Sicherheitsmechanismen und Präventionswerkzeuge zu entwickeln bzw. bestehende zu analysieren. Forschende müssen sich also in Bezug auf produktiv eingesetzte Hard- und Software teils ähnlicher Methoden und technischer Vorgehensweisen bedienen wie Cyberkriminelle. Das aktuelle IT-Strafrecht differenziert jedoch nur unzureichend nach den verfolgten Absichten.

Kommt es im Rahmen der IT-Sicherheitsforschung zur Verarbeitung personenbezogener Daten, bedarf es einer Rechtsgrundlage: Hier ergibt sich ein Zielkonflikt zwischen den datenschutzrechtlichen Pflichten zur Datensicherheit sowie dem Urheber- und Strafrecht, welcher auch auf die Auslegung der Forschungsprivilegien im Datenschutzrecht ausstrahlt. Im Hinblick auf die Gewichtung der wissenschaftlichen Forschung gegenüber Datenschutzrechten lässt sich trotz punktueller Privilegierung der Forschung keine klare Linie des Gesetzgebers erkennen, sodass stets eine Einzelfallentscheidung erforderlich ist.

Wird von allen Beteiligten das Ziel verfolgt, die Schwachstelle im Sinne der Betreiber*innen und Nutzer*innen der vulnerablen Hard- bzw. Software zu beseitigen, wird damit das Risiko etwa von Produkthaftung auf Herstellerseite verringert. Allerdings verstärken manche - insbesondere dem anglo-amerikanischen Rechtsverkehr entnommene - als AGB ausgestalteten Nutzungs- bzw. Lizenzbestimmungen die Rechtsunsicherheit, wenn Reverse Engineering und/oder IT-Sicherheitstests pauschal verboten oder von prohibitiv wirkenden Anforderungen abhängig gemacht werden. Wenngleich viele solcher Klauseln in ihrer Wirksamkeit nach deutschem und europäischem Recht höchst fragwürdig sind: Forschende müssen befürchten, dass auf freiwillige Meldungen von Schwachstellen mit dem Vorwurf von Rechtsverletzungen samt Schadenersatz- und Unterlassungsansprüchen reagiert werden könnte.

Eine Änderung der Rechtslage erfolgte hingegen im Bereich des Schutzes von Geschäftsgeheimnissen, wo mittlerweile in Grenzen Reverse Engineering erlaubt ist. Die eng gefasste Erlaubnis betrifft allerdings nur bestimmte Konstellationen und steht im Widerspruch mit dem Urheberrecht.

Es verbleibt aber eine weitläufige Rechtsunsicherheit, die schon bei der Entscheidung für oder gegen einen Forschungsgegenstand ggf. abschreckende Wirkung hat. Da Hochschulen gesetzlich zu wissenschaftlicher Redlichkeit verpflichtet sind, dürfen sie keine Projekte betreiben, wenn diese gegen geltendes Recht verstoßen könnten.

Als Fazit zur Analyse der aktuellen Rechtslage in Deutschland kann festgehalten werden: der gesetzliche Rahmen sollte so angepasst bzw. angewandt werden, dass Forschende in Deutschland nicht aufgrund drohender rechtlicher Konsequenzen vom Untersuchen und Melden von IT-Sicherheitslücken abgeschreckt werden. So würden auf Basis der präsentierten Analyse bspw. mit der Schaffung von **Erlaubnisnormen für IT-Sicherheitsuntersuchungen im Urheber- und Strafrecht** rechtliche Hemmnisse abgebaut. Dies würde auch in das Vertrags- und Deliktsrecht ausstrahlen. Zusätzlich bedarf es der Implementierung einer Fehlerkultur und Kommunikation auf Augenhöhe, anstatt mit Rechtsverfolgung zu drohen, da die Empfänger*innen einer Meldung von Sicherheitslücken unentgeltlich eine wertvolle Leistung erhalten.

Die Geheimhaltung von Schwachstellen führt nicht zur Erhöhung der Sicherheit von Produkten und Systemen. Erfolgversprechend und auch wirtschaftlich nachhaltig ist nur das Beheben der Fehler sowie eine Veröffentlichung der Erkenntnisse der IT-Sicherheitsforschung. Dabei ist zu bevorzugen, den Produktverantwortlichen erst die Möglichkeit zur Fehlerbehebung zu geben und für einen angemessenen Zeitraum die Veröffentlichung der Forschungsergebnisse aufzuschieben. Die Erfahrung hat gezeigt, dass eine kooperative Zusammenarbeit zur Aufdeckung und Behebung zahlreicher Schwachstellen führt und damit einen wertvollen Beitrag zur nachhaltigen Verbesserung der Sicherheit von Informationssystemen leistet. Daher möchten die Autor*innen sowohl das Bewusstsein für die Bedeutung der Zusammenarbeit zwischen Hersteller*innen und der IT-Sicherheits-Community stärken, als auch auf rechtliche Hemmnisse hinweisen und für Verbesserungen etwa durch die Einrichtung einer zentralen Meldestelle eintreten.

1 Einleitung

Mit zunehmender Digitalisierung und Vernetzung wächst die Abhängigkeit unserer Gesellschaft von der Informations- und Kommunikationstechnik – in Bereichen wie bspw. kritischen Infrastrukturen sind wir auf deren korrekte Funktionsweise sogar zwingend zur Vermeidung von Personen-, Sach- und Vermögensschäden angewiesen. Die potenziellen Auswirkungen von Sicherheitsschwachstellen erscheinen damit immer durchgreifender und gravierender. Aufgrund der hohen Komplexität der Technik weisen selbst mit größtmöglicher Sorgfalt entwickelte Produkte oft IT-Sicherheitslücken auf.[1] In vielen Fällen werden diese erst längere Zeit nach Markteinführung entdeckt oder durch Updates nachträglich in Produkte eingetragen und können bis zu ihrer Schließung von (Klein-)Kriminellen, kriminellen Organisationen, böswilligen Konkurrenten (Industriespionage), Aktivist*innen oder bürgerrechtsfernen Regimen ausgenutzt werden.[2] Dadurch entstehen nicht nur Gefahren für die Bevölkerung wie Datenabfluss oder Identitätsdiebstahl. Auch für Unternehmen, die betroffene Produkte herstellen oder nutzen, drohen potenziell existenzgefährdende Risiken in Form von Reputationsschäden, Abfluss von Geschäftsgeheimnissen, staatlichen Sanktionen oder Schadensersatzforderungen. Entsprechend drohen auch Nachteile für die Gesellschaft als Ganzes. Es wird daher immer wichtiger, Schwachstellen zu finden und zu beheben, bevor sie von Kriminellen oder anderen Angreifer*innen ausgenutzt werden können.

> „the important role of third party security researchers in discovering vulnerabilities in existing products and services needs to be acknowledged and conditions to enable coordinated vulnerability disclosure should be created across Member States…"[3]

In der Fachliteratur sowie der Hochschullehre hat sich das Prinzip etabliert *„… wonach die IT-Sicherheit nicht von der Geheimhaltung von Entwurf und Implementierung abhängig sein darf*."[4] In Bezug auf Kryptographie ist dies nach dem Kerckhoffs'schen Prinzip bekannt.[5] Dahinter steht die Erkenntnis, dass sich Schwachstellen nicht auf Dauer geheim halten lassen. Parallel- und Wiederentdeckungen sind jederzeit möglich.[6] Dass eine Hackergruppe im Jahr 2017 in der Lage war, das Wissen um die Sicherheitslücke EternalBlue vom amerikanischen Geheimdienst NSA abzuschöpfen, zeigt dies exemplarisch. Nach dem Wissensabfluss erfolgte eine weltweite Verbreitung der Schadsoftware WannaCry, welche Schäden in Millionen- bis Milliardenhöhe in mindestens 150 Ländern verursachte.[7] Staatliche Akteure finden sich in einer Doppelrolle als Ausnutzende

[1] Zur Definition Definition von IT-Sicherheit und Lücken/Schwachstellen vgl. ENISA Definition of Cybersecurity – Gaps and overlaps in standardisation, Juli 2016 https://www.enisa.europa.eu/publications/definition-of-cybersecurity (zuletzt aufgerufen 23.09.2021).

[2] Der Motivkanon ist breit gefächert, Beispiel für die interessante Motivlage eines 16jährigen für dDoS-Attacken und Angriffe auf Server mittels Exploits: https://netzpolitik.org/2020/ddos-serie-angriff-aus-einsamkeit/ (zuletzt aufgerufen 21.08.21).

[3] EU-Kommission, Joint Communication "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU".

[4] Bishop, Computer security: Art and Science. Addison-Wesley Professional (2003).

[5] Ob dies in den Bereichen System- oder Softwaresicherheit ebenso strikt gilt, könnte noch diskutiert werden. Kerckhoffs, Auguste. La cryptographie militaire, ou, Des chiffres usités en temps de guerre: avec un nouveau procédé de déchiffrent applicable aux système à double clef.Libraieiw militire de L. Baudoin, 1883.

[6] Herr/Schneier/Morris, Taking Stock: Estimating Vulnerability Rediscovery, Paper, Cyber Security Project, Belfer Center, July 2017.

[7] Berr, "WannaCry" ransomware attack losses could reach $4 billion, in: CBS, Stand 16.05.2017 abrufbar unter: https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/ (zuletzt aufgerufen 11.10.2021).

und Opfer von Schwachstellen wieder und verletzten dabei ihre Schutzpflichten gegenüber Bürger*innen und Unternehmen.[8]

> „Disclosing vulnerabilities […] is crucial to protect our digital society. If we do not seriously address this issue in EU cybersecurity policies, we are acting as if only simply rearranging the deck chairs on the Titanic."[9]

Produktverantwortliche treffen regelmäßig haftungs- und datenschutzrechtliche Pflichten zur angemessenen Produktsicherheit. Daneben besteht ein großes gesamtgesellschaftliches Interesse an unabhängiger Sicherheitsforschung durch neutrale Stellen, damit diese rechtzeitig auf Risiken aufmerksam machen können, bevor es zu einem Schaden kommt. Die Wissenschaft leistet einen wertvollen Beitrag zur Analyse von Angriffs- und Verteidigungsmechanismen und der Weiterentwicklung von letzteren. Es ist in der Wissenschaft unstrittig, dass die dauerhafte Geheimhaltung von Schwachstellen nicht zur Erhöhung der Sicherheit führt, sondern nur das Beheben von und das Warnen vor Sicherheitslücken erfolgreich ist.

> „Um exzellente und letztlich verwertbare Ergebnisse produzieren zu können, muss sich die Cybersicherheitsforschung an möglichst realistischen Rahmenbedingungen orientieren."[10]

Der Wirtschafts- und Forschungsstandort Deutschland soll auch im Bereich IT-Sicherheit unter dem Label „*Made in Germany*" eine Vorreiterrolle einnehmen. Hierfür werden auf Bundes- und Landesebene Kompetenzzentren, Institute und Forschungseinrichtungen für IT-Sicherheit staatlich gefördert. Aufgabe dieser Zentren ist u.a. die Sensibilisierung der Bevölkerung und Industrie durch Aufdeckung und Warnung vor IT-Sicherheitsrisiken. Dies erfordert jedoch auch die proaktive Untersuchung von öffentlich verfügbaren Produkten und Systemen auf Sicherheitslücken zur Unterstützung der Hersteller*innen bei der Umsetzung eines angemessenen Sicherheitsniveaus. Daneben erfordert das Studium von Sicherheitsmechanismen in einigen Fällen auch Handlungen, mit denen Forschende selbst in den Fokus juristischer Auseinandersetzungen geraten könnten. Der staatliche Anspruch an die Umsetzung innovativer IT-Sicherheitsforschung kann somit aufgrund bestehender Rechtsunsicherheit nicht immer erfüllt werden. IT-Sicherheitsforschung muss dabei nicht institutionalisiert erfolgen, sondern kann auch durch privat Forschende wichtige neue Erkenntnisse hervorbringen. Diese Erkenntnisse dienen nicht nur innerstaatlichen, sondern auch supranationalen Interessen an der IT-Sicherheit, etwa dem Infrastrukturschutz, Wirtschaftsschutz, Zivilschutz oder der Friedenswahrung. Forschungseinrichtungen, aber auch Sicherheitsforschende persönlich, sind rechtlichen Risiken ausgesetzt, die zum Hemmnis für innovative IT-Sicherheitsforschung werden.

[8] Vgl. zu staatlichen Schutzpflichten: BVerfG, Beschluss vom 08.06.2021, Az. 1 BvR 2771/18.
[9] MEP Schaake (ALDE), Leiterin der Task Force on Software Vulnerabilities in Europe „EU needs solid vulnerability disclosure rules", 2018.
[10] Waidner/Backes/Müller-Quade, Positionspapier Cybersicherheit in Deutschland, 2017 (14, 19).

2 Was ist Sicherheitsforschung?

Im Rahmen dieses Whitepapers legen wir folgendes Verständnis zu Grunde: IT-Sicherheitsforschung hat zum Ziel, die IT-Sicherheit zu verbessern – hierzu zählen die Vermeidung und Beseitigung von Schwachstellen, die Abmilderung der Folgen bei deren Ausnutzung und die technische Verfolgung von An- und Eingriffen. Methoden und Mittel sind im sehr dynamischen Umfeld der IT im Fluss und folglich nicht abschließend aufzählbar. Eine Ausprägung ist die Suche nach Schwachstellen in Hard- und/oder Software und bei Entdeckung deren Dokumentation und Mithilfe zur Beseitigung, insbesondere durch Meldung an den oder die Verantwortlichen.

> „Wurde in der Vergangenheit eher defensiv-orientierte Cybersicherheitsforschung durchgeführt, so wird die Cybersicherheitsforschung zur Stärkung von Prävention, Detektion und Reaktion auch verstärkt offensiv ausgerichtet sein müssen.“[11]

Die IT-Sicherheitsforschung widmet sich u.a. der „Aufgabe, Unternehmen und deren Werte (Know-How, Kundendaten, Personaldaten) zu schützen und wirtschaftliche Schäden, die durch Vertraulichkeitsverletzungen, Manipulationen oder auch Störungen der Verfügbarkeit von Diensten des Unternehmens entstehen können, zu verhindern“.[12] Die Forschungsfreiheit umfasst sowohl Grundlagen- als auch die angewandte Forschung und hat grundsätzlich einen weiten Schutzbereich, der unabhängig von der Organisationsform ist.[13] Wissenschaftliche Tätigkeit erstreckt sich auf alles, was nach Inhalt und Form als ernsthafter planmäßiger Versuch zur Ermittlung der Wahrheit anzusehen ist.[14] IT-Sicherheitsforschung ist demnach die wissenschaftliche Untersuchung von Methoden, Grundsätzen und Mängeln der IT-Sicherheit – anwendungs- und technikbezogen – vor allem zum Schutz vor vertraulichkeits- und integritätsbeeinträchtigenden Angriffen. Eine typische Vorgehensweise dieses Forschungszweigs ist der IT-Sicherheitstest von Produkten.[15]

> Forschung ist der nach Inhalt und Form ernsthafte und planmäßige Versuch zur Ermittlung der Wahrheit, und zwar in einem methodisch geordneten Verfahren mit einem Kenntnisstand, der in der Regel auf einem wissenschaftlichen Studium beruht. (BVerfG 35, 79 (113); 47, 327 (367))

Im Bereich der IT-Sicherheit „stolpern“ Expert*innen oftmals in alltäglichen Konstellationen über Sicherheitslücken (Zufallsfunde).[16] Bereits dies kann zur Forschung gezählt werden, wenn sie diese methodisch-systematisch analysieren und neue Erkenntnisse mit der Intention zur Verbesserung der IT-Sicherheit erschließen. Sofern allerdings kein planmäßiges Vorgehen vorliegt, oder die Tätigkeit als bloße Anwendung bekannter Methoden zu werten wäre, würden diese Tätigkeiten aus dem Forschungsbegriff herausfallen. Im Rahmen dieses Dokuments sollen diese Tätigkeiten von Entdecker*innen und Melder*innen von Sicherheitslücken nichtsdestotrotz den Sicherheitsforschenden gleichgestellt werden, da deren Beitrag zur Schließung von Sicherheitsmängeln ein gleichrangiges Schutzbedürfnis zukommt.

[11] Waidner/Backes/Müller-Quade, Positionspapier Cybersicherheit in Deutschland, 2017 (14, 19).
[12] Eckert, IT-Sicherheit, 10. Aufl. 2018, S. 1.
[13] BT-Drs. V/4335, S. 4; BVerfGE 35, 79 (113) – Hochschul-Urteil.
[14] BVerfGE 35, 79 (113) – Hochschul-Urteil; BVerfGE 47, 327 (367) - Hessisches Universitätsgesetz.
[15] Vettermann/Wagner, InTeR 2020, 126 (127).
[16] Bspw. der Fund von Sicherheitslücken bei Corona-Teststationen durch das Team Zerforschung.

Beispiel: Die IT-Sicherheitsforscherin P untersucht einen zu Testzwecken von ihr erworbenen Saugroboter. Dieser ist per WLAN an einen Cloud-Service des Herstellers angebunden, was per App die Steuerung des Geräts durch den Nutzenden ermöglicht. Bei der Untersuchung der Schnittstelle zum Cloud-Service findet sie eine Sicherheitslücke, die eine Übernahme der Kontrolle fremder Geräte unter Eingabe einer für sie nicht transparenten Identifikationsnummer (ID) erlaubt. Für P ist damit im Vorhinein ohne Test einer zufälligen ID nicht zu ermitteln, ob und für welchen Saugroboter sie die Steuerrechte in welchem Umfang erlangen wird.

P versucht vergeblich, den Herstellern des Saugroboters zu kontaktieren, der seinen Sitz im Ausland hat und auf Mails nicht reagiert. Ein Patch wird nicht entwickelt und die Kunden werden nicht auf die Schwachstelle hingewiesen, welche u. a. den Zugriff auf das Kamerasystem des Roboters ermöglicht.

3 Überblick über die aktuelle Rechtslage in Deutschland

3.1 Strafrecht

Dominik Brodowski / Sebastian Golla

Um Sicherheitslücken aufzudecken, muss sich die IT-Sicherheitsforschung trotz völlig anderer Zielsetzung oftmals der gleichen Methoden und technischen Vorgehensweisen bedienen wie Cyberkriminelle.[17] Daraus resultieren Strafbarkeitsrisiken.

Beispiel: Ein*e Hersteller*in hinterlegt in einem Produkt ein Passwort, das explizit nicht zum Auslesen durch den Nutzer*in bestimmt ist, und beschränkt den Zugang durch eine besondere technische Sicherung. Eine Sicherheitsforscherin analysiert das Produkt auf Sicherheitslücken, findet das Passwort und überwindet damit die Sicherung. Dies berichtet sie in ihrer Forschungsgruppe und meldet es dem/ der Hersteller*in.

Wenn Forschende Penetrationstests (kurz: Pentests) durchführen, um Sicherheitslücken aufzuspüren, können sie sich nach § 202a Abs. 1 StGB (Ausspähen von Daten) strafbar machen. Der Tatbestand ist erfüllt, wenn der Handelnde unter Überwindung einer Zugangssicherung Zugang zu Daten, die nicht für sie bestimmt sind, erlangt. Das ist etwa in dem beschriebenen Beispiel der Fall.

---

§ 202a StGB – Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

Der Wortlaut der Vorschrift differenziert nicht zwischen kriminellen und anderen Zielrichtungen der Handlung. Unbeschadet früherer Erwägungen, „einfaches Hacking“ nicht unter Strafe zu stellen,[18] besteht inzwischen ein erhebliches Risiko, dass aus Sicht der Strafverfolgungsbehörden und Gerichte auch Forschende den Tatbestand erfüllen. Die Überwindung einer Zugangssicherung ist – vor allem in der weiten Interpretation, den dieses Tatbestandsmerkmal in der Rechtsprechung gefunden hat[19] – eine typische Handlungsweise bei IT-Sicherheitstests. IT-Sicherheitstests können dabei nicht immer in einer künstlichen Testumgebung durchgeführt werden, sondern müssen regelmäßig echte, am Markt angebotene Produkte und Systeme einbeziehen.

[17] Vgl. Gamero-Garrido/Savage/Levchenko/Snoeren, Quantifying the Pressure of Legal Risks on Third-party Vulnerability Research, CCS'17, Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security 2017, S. 1501; Vonderau/Wagner, DSRITB 2020, 525 (527); Böken, in: Kipker, Cybersecurity, Kap. 15 Rn. 64.

[18] Vgl. statt vieler, Kargl, in: NK-StGB, 5. Aufl. 2017, § 202a StGB Rn. 1 m.w.N.

[19] Etwa in BGH NStZ-RR 2020, 278; s. auch BGH NStZ 2018, 401, 403; BGH NStZ 2016, 339, 340; BGH NJW 2015, 3463, 3464 Rn. 8.

Um eine Strafbarkeit nach § 202a Abs. 1 StGB sicher auszuschließen, müssen Forschende das Einverständnis sämtlicher Berechtigter an den getesteten IT-Systemen erlangen.[20] Dies kann praktisch schwierig sein. Ansonsten lässt sich eine Strafbarkeit nach derzeitigem Stand in Rechtsprechung und Rechtswissenschaft nicht verlässlich ausschließen. So ist eine forschungsfreundliche Auslegung des Tatbestands zwar denkbar, dass ein Verhalten nicht „unbefugt" oder aber gerechtfertigt ist, wenn es (wie in dem genannten Beispiel) überwiegenden Forschungsinteressen dient. Doch noch ist nicht hinreichend geklärt, ob sich aus der Forschungsfreiheit der IT-Sicherheitsforschenden eine solche Rechtfertigung ihres Verhaltens ergibt. Daher begründet die Strafdrohung des § 202a Abs. 1 StGB eine erhebliche Rechtsunsicherheit für IT-Sicherheitsforschende.

Etwas geringer sind die Strafbarkeitsrisiken im Zusammenhang mit der Weitergabe von Informationen, die Forschende durch Pentests und andere Forschungsaktivitäten erlangt haben. Eine Strafbarkeit nach § 23 Abs. 1 Nr. 2 GeschGehG, § 202d Abs. 1 StGB und § 42 BDSG wird hier zwar im Ergebnis regelmäßig nicht in Betracht kommen, weil die Aktivitäten von Forschenden nicht die geforderten subjektiven Merkmale erfüllen. Es wird kein Handeln aus Eigennutz[21], in Schädigungs- oder Bereicherungsabsicht vorliegen – so etwa in dem oben beschriebenen Beispiel. Diese subjektive Tatseite lässt sich aber vor allem in frühen Stadien strafrechtlicher Ermittlungen oftmals nicht hinreichend klären. Daher verbleibt ein erhebliches Risiko von belastenden und in die Grundrechte der IT-Sicherheitsforschenden eingreifenden Ermittlungsmaßnahmen, wenn Ermittlungsbehörden nach dem äußeren Erscheinungsbild eines Falles trotzdem zunächst den Verdacht einer Schädigungsabsicht annehmen. Bei § 42 Abs. 2 BDSG besteht zusätzlich 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.[22]

---

§ 202d StGB – Datenhehlerei

(1) Wer Daten (§ 202a Absatz 2), die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. (…)

§ 23 GeschGehG –Verletzung von Geschäftsgeheimnissen

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen,

1. entgegen § 4 Absatz 1 Nummer 1 ein Geschäftsgeheimnis erlangt,

2. entgegen § 4 Absatz 2 Nummer 1 Buchstabe a ein Geschäftsgeheimnis nutzt oder offenlegt (…).

Für IT-Sicherheitsforschende ist es zudem unverzichtbar, sich über aktuelle Angriffsmethoden zu informieren, Schadsoftware zu analysieren und Evidenzen für die Ausnutzbarkeit von Sicherheitslücken (sogenannte

[20] Vgl. auch Erwägungsgrund 17 RL 2013/40/EU.
[21] Ein wissenschaftliches Interesse ist hiervon nicht erfasst.
[22] Vgl. BGHSt 58, 268 (Rn. 49 ff.) zum gleichlautenden Merkmal bei § 44 Abs. 1 BDSG a.F.

„Proof of Concept“) zu entwickeln. Derartige Verhaltensweisen fallen zumindest in den Dunstkreis des – auch im internationalen Vergleich – bedenklich weit formulierten § 202c Abs.1 Nr. 2 StGB, dem sogenannten „Hacker-Paragrafen“,[23] auch i.V.m. §§ 303a Abs. 3, 303b Abs. 5 StGB sowie § 263a Abs. 3 StGB. Zwar hat hierzu das Bundesverfassungsgericht die restriktive Auslegung des Tatbestands betont, was die Strafbarkeit von Forschenden weitgehend ausschließen dürfte,[24] weil der „Zweck“ eines „Proof of Concept“ eine wissenschaftliche Evidenz und nicht die Begehung von Straftaten ist. Wenn sich IT-Sicherheitsforschende über Angriffsmethoden informieren und sich fremde Schadsoftware zur Analyse verschaffen, fehlt es am erforderlichen Vorsatz der Vorbereitung einer anderen IT-Straftat. Es verbleiben dennoch erhebliche Risiken, dass Ermittlungsbehörden aufgrund des äußeren Erscheinungsbildes zunächst einen Anfangsverdacht bejahen und hierauf erhebliche Eingriffe in die Grundrechte der IT-Sicherheitsforschenden stützen.

§ 202c StGB – Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder

2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

Im Ergebnis gehen Strafbarkeitsrisiken für Forschende vor allem von § 202a Abs. 1 StGB aus, aber auch von weiteren Tatbeständen des IT- und Datenschutzstrafrechts; hinzu treten Strafbarkeitsrisiken bei der Veröffentlichung von Sicherheitslücken einschließlich eines Proof-of-Concept.[25] Wenngleich es praktisch unwahrscheinlich ist, dass in naher Zukunft IT-Sicherheitsforschende nach § 202a Abs. 1 oder § 202c StGB verurteilt werden,[26] sind die durch eine mögliche Strafbarkeit und Ermittlungsverfahren drohenden Abschreckungseffekte ernst zu nehmen. Staatsanwaltschaften und Polizeibehörden können gerade in Fällen, in denen das Vorgehen von Sicherheitsforschenden jenem von kriminellen Hacker*innen dem ersten Anschein nach ähnelt, Verfahren eröffnen, aus denen Grundrechtseingriffe durch Ermittlungsmaßnahmen folgen und die Forschung hemmen können. Dass dieses Risiko real ist, zeigte im Sommer 2021 der Fall von Lilith Wittmann. Nachdem die Forscherin eine Sicherheitslücke in der App CDU-Connect entdeckte und diese im Wege des Responsible Disclosure offenlegte, erstattete die CDU Anzeige gegen Wittmann und die Staatsanwaltschaft leitete ein Ermittlungsverfahren wegen des Verdachts des Ausspähens von Daten (§ 202a Abs. 1StGB) ein. Dieses wurde mittlerweile eingestellt.

Um diese Strafbarkeitsrisiken und vor allem die abschreckenden Straf*verfolgungs*risiken zu minimieren, sollten die Tatbestände des IT- und Datenschutzstrafrechts die Interessen der IT-Sicherheitsforschung ausdrücklich berücksichtigen. Dies wäre etwa durch die Einfügung eines Tatbestandsausschlusses für Handlungen im

[23] Vgl. statt vieler, Brodowski, in: Kipker, Cybersecurity, Kap. 13 Rn. 42, 48.
[24] BVerfGK 15, 491.
[25] Hierzu Brodowski, it – Information Technology 57 (2015) 357.
[26] Insgesamt wird die Vorschrift selten angewandt, im Jahr 2019 kam es etwa nur zu 27 Verurteilungen; Statistisches Bundesamt, Fachserie 10 Reihe 3, 2019, S. 162.

wissenschaftlichen Interesse in § 202a StGB, ähnlich zu § 86 Abs. 4 StGB, und durch eine restriktivere Formulierung des § 202c StGB – etwa ähnlich zu § 126c öStGB – möglich.

3.2 Urheberrecht

Manuela Wagner / Hoa Tran/ Fabian Franzen

Ein wesentlicher Baustein zur Erforschung von Sicherheitsschwachstellen besteht darin, ein Programm in Funktionen zu dekonstruieren.[27] In der IT-Sicherheitsforschung anzutreffende Formen des Reverse Engineering sind u. a. folgende Vorgehensweisen:

- *Dekompilieren*, Übersetzen von Maschinen- oder Objektcode in einen für Menschen lesbaren Quelltext in einer Hochsprache;
- *Disassemblieren*, Umwandlung des Maschinencodes in eine für Menschen (mit hohem Aufwand) lesbare Assemblersprache*;*
- *Binary Lifting*, Umwandlung des Maschinencodes in eine andere Repräsentation;
- *Code Emulation*, Übertragung des zu untersuchenden Codes in eine spezielle virtuelle Umgebung.[28]

Beispiel: Eine Sicherheitsforscherin kopiert die Software von einem IoT-Gerät in eine Testumgebung. Dort muss sie den Maschinencode zunächst in eine Anzeigeform transferieren, die sie gut lesen kann.

Um urheberrechtlich geschützte Computerprogramme (Software) zu untersuchen, kann es erforderlich werden – sofern kein Zugang zum Quellcode besteht – den Maschinencode zu vervielfältigen, zu übersetzen oder auf sonstige Weise zu bearbeiten. Diese Handlungen zählen zu den zustimmungsbedürftigen Handlungen (§ 69c UrhG) und erfordern folglich die Zustimmung des Urhebers bzw. Rechteinhabers oder eine gesetzliche Erlaubnis.

Des Weiteren wird die Umgehung technischer (Kopier-)Schutzmaßnahmen bei urheberrechtlichen Werken nach § 95a UrhG und bei Computerprogrammen indirekt über einen Vernichtungsanspruch bzgl. der Software zur Umgehung technischer Programmschutzmechanismen nach § 69f Abs. 2 UrhG sanktioniert.[29] Technische Programmschutzmechanismen umfassen alle Vorrichtungen, die Nutzungshandlungen von urheberrechtlich geschützten Computerprogrammen einschränken, um Urheberrechtsverletzungen zu verhindern.[30] Es besteht zwar kein direktes und umfassendes Umgehungsverbot, allerdings wird diskutiert, ob in der Umgehung eine nicht bestimmungsgemäße Nutzung vorliege, die zum Verstoß gegen § 69c UrhG führt.[31]

---

[27] Bao/Burket/Woo/Turner/Brumley, ByteWeight: Learning to Recognize Functions in Binary Code, Proceedings of the 23rd USENIX Security Symposium, 2014, S. 845; Brumley, Game Theory: Why System Security Is Like Poker, Not Chess, abrufbar unter https://thenewstack.io/game-theory-why-system-security-is-like-poker-not-chess/ (zuletzt abgerufen 11.05.2020).

[28] Franzen/Maier/Wagner, DuD 2020, 511 (513).

[29] Bei hybriden Werken wie Computerspielen, richtet sich der Schutz für audiovisuelle Elemente nach § 95a ff. UrhG, siehe hierzu: Wiebe, in: Spindler/Schuster, 4. Aufl. 2019, UrhG § 69f, Rn. 5 m.w.N.

[30] Für Beispiele siehe: Grützmacher in: Wandtke/Bullinger, 5. Aufl. 2019 Rn. 14, UrhG § 69f Rn. 14.

[31] Grützmacher, in: Wandtke/Bullinger, 5. Aufl. 2019, UrhG § 69f Rn. 13.[32] EuGH, Urteil vom 06.10.2021 – C-13/20 – Top System SA/Belgien.

3.2.1 Ausnahmen von den zustimmungspflichtigen Handlungen

Eine explizite Erlaubnis für IT-Sicherheitstest fehlt im Gesetz. Die Regelungen sind als Umsetzung der Richtlinie 2009/24/EG über den Rechtsschutz von Computerprogrammen richtlinienkonform auszulegen.

Mit der jüngsten Entscheidung des EuGHs für die Zulässigkeit des Dekompilierens zur Fehlerberichtigung und damit klaren Absage einer bisher vielfach präferierten engen Auslegung der Ausnahmen, welche in einem Quasi-Dekompilierverbot gemündet hätte, wurde nun auch für IT-Sicherheitstests die Tür einen Spalt breit geöffnet.[32] Allerdings betraf der Fall einen aufgetretenen Fehler, welcher das ordnungsgemäße Funktionieren der Anwendung beeinträchtigte. Damit bleibt die Frage weiterhin offen, ob das Dekompilieren auch zur Fehlersuche zulässig ist.

Die Nutzung urheberrechtlich geschützter Werke für Bildung und Forschung wurde mit dem Urheberrechts-Wissensgesellschafts-Gesetz reformiert. Zweck des Gesetzes war die Nutzbarmachung für wissenschaftliche Publizistik; es gibt keine Anhaltspunkte dafür, dass der Gesetzgeber die Sicherheitsforschung im Blick hatte. So gestattet bspw. § 60c UrhG für die nicht kommerzielle wissenschaftliche Forschung bis zu 15 % eines Werkes zu vervielfältigen. Zunächst stellt sich die Frage, ob die Regelung überhaupt auf Computerprogramme anwendbar ist.[33] Der Gesetzgeber hatte Druckwerke, Noten, Filme, Musik und Abbildungen im Sinn.[34] Ohnehin wird das für IT-Sicherheitsforschung relevante Reverse Engineering nicht erwähnt. Es fehlt somit eine Regelung im Hinblick auf den urheberrechtlichen Schutz von Computerprogrammen, die eindeutig und rechtssicher IT-Sicherheitsanalysen erlaubt.

	Produktbeobachtung § 69d Abs. 3 UrhG	Fehlerberichtigung § 69d Abs. 1 UrhG	Dekompilieren § 69e UrhG
Reichweite	Umfasst sind bspw. die Beobachtung des Programmablaufs, der Bildschirmausgabe, Einspielen von Testdaten, sog. Black-Box-Tests, aber keine Eingriffe in den Programmcode wie insbesondere im Wege des in § 69e UrhG geregelten Dekompilierens.[35] Ziel der Tests muss die Ermittlung der einem Programmelement zugrundeliegenden Ideen und Grundsätze sein.	Erlaubt ist als bestimmungsgemäße Benutzung eines Computerprogramms für den rechtmäßigen Erwerber die Behebung von Programmfehlern. Fehler ist jedes Element bzw. Nichtvorhandensein eines Elements, dass die bestimmungsgemäße Nutzung beeinträchtigt – unabhängig ob Teil des Programms (Bugs) oder später hinzutretend (z.B. Viren, Trojaner, etc.).[36]	Erlaubt ist Dekompilieren nur, sofern zur Herstellung der Interoperabilität mit einem eigenen Computerprogramm unerlässlich. Eine Definition des Begriffs fehlt. Umstritten ist, ob und wieweit Dekompilieren über die sehr enge gesetzliche Erlaubnis hinaus auch in anderen Fällen zulässig ist.[37] Ob Disassemblieren auch – und mit welchen Folgen – erfasst wird, bleibt unklar.

[32] EuGH, Urteil vom 06.10.2021 – C-13/20 – Top System SA/Belgien.
[33] Anton, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, UrhG § 60c Rn. 2.
[34] Bundestags-Drucksache 18/12329, S. 35.
[35] BGH, Urteil vom 06.10.2016 – I ZR 25/15 – World of Warcraft I, Rn. 57; Dreier in: Dreier/Schulze, UrhG § 69d Rn. 22; Grützmacher in: Wandtke/Bullinger, UrhG § 69d Rn. 75.
[36] Dreier in: Dreier/Schulze, UrhG § 69d Rn. 9 ff.; Grützmacher in: Wandtke/Bullinger, UrhG § 69d Rn. 21 ff.
[37] Zur Sperrwirkung ggü. anderen Urheberrechtsschranken als lex specialis: Dreier in: Dreier/Schulze, UrhG § 69e Rn. 12; Wiebe in Spindler/Schuster, Recht der elektronischen Medien, (3. Aufl. 2015), UrhG § 69e Rn. 2; zur Darlegungs- und Substantiierungslast siehe: OLG Düsseldorf, Urteil vom 16. 01. 2001 – 20 U 142/00.

Grenzen	Nicht erfasst ist die Nutzung audiovisueller Daten wie Grafiken, Musik, Filmsequenzen, Texte oder Modelle, die im Computerprogramm enthalten sind, noch existiert eine entsprechende Regelung, die eine Vervielfältigung der in einem Computerspiel enthaltenen Werke zur Programmbeobachtung erlaubt.[38] Sofern die Untersuchung eine Vervielfältigung erfordert, muss hierfür eine Berechtigung vorliegen.[39]	Umstritten war bisher,[40] ob auch Übersetzungen des Maschinencodes in eine menschlich verständliche Sprache (d.h. Disassemblieren/Dekompilieren) erlaubt wird.[41] Der EuGH hat dies mittlerweile bestätigt.[42] Die Entfernung von Programmschutzmechanismen ist nicht zur Fehlerbehebung erlaubt, es sei denn der Fehler beruht auf diesem Mechanismus oder der/die Hersteller*in verweigert die Fehlerbeseitigung.[43]	Aufgrund des eng gefassten Wortlauts gehen Teile des Schrifttums bisher davon aus, dass Dekompilieren in allen Fällen außerhalb des § 69e UrhG nicht erlaubt ist, selbst zur Behebung von Fehlern.[44] Diese enge Auslegung hat der EuGH abgelehnt: für die Fehlerberichtigung geht keine Sperrwirkung von § 69e UrhG aus.[45] Inwiefern die Argumentation des EuGHs auch auf die Programmbeobachtung übertragbar ist, bleibt offen.
Ergebnis	Legitimiert nach herrschender Auslegung nicht alle für IT-Sicherheitstests erforderlichen Handlungen.	Unklar ist, ob das Recht zur Fehlerberichtigung auch die Möglichkeit der *Fehleranalyse* einschließt – ohne, dass bereits ein Fehler bekannt ist.[46]	§ 69e UrhG stellt keine Ausnahme zur Softwarebearbeitung zum Zweck der Beseitigung von Sicherheitslücken bereit.[47]

Ob mitgliedstaatliche Ausnahmen mit der RL 2009/24/EG vereinbar wären, hängt vom Grad der Harmonisierung ab. Grundsätzlich enthält die Richtlinie keine expliziten Öffnungsklauseln, die abweichende mitgliedstaatliche Spielräume eröffnen würden.[48] Allerdings deuten die Erwägungsgründe 5 und 19 darauf hin, dass Mitgliedstaaten unterschiedliche Regelungen, die das Funktionieren des Binnenmarktes *nicht in erheblichem Maße beeinträchtigen*, weder beseitigen noch ihre Entstehung verhindern müssen. Die Richtlinie berührt demnach nicht die in den einzelstaatlichen Rechtsvorschriften in Übereinstimmung mit der Berner Übereinkunft vorgesehenen Ausnahmeregelungen für Punkte, die nicht von der Richtlinie erfasst werden. Die Sicherheitsforschung bzw. der Umgang mit Sicherheitsanalysen ist in der RL 2009/24/EG nicht bedacht worden.

[38] BGH, Urteil vom 06.10.2016 – I ZR 25/15 – World of Warcraft I, Rn. 65.
[39] Wurden Nutzungsrechte nur stillschweigend eingeräumt, wird angenommen, dass dies nur die für das Erreichen des Vertragszwecks unerlässlichen Nutzungsarten umfasst; vgl. BGH, Urteil vom 29.04.2010 - I ZR 68/08, GRUR 2010, 623 Rn. 20 - Restwertbörse I; BGH Urteil vom 24.09.2014 - I ZR 35/11, GRUR 2015, 264 Rn. 49 - Hi Hotel II.
[40] OLG Karlsruhe, Urt. v. 10.1.1996 – 6 U 40/95 –, Rn. 37; OLG Düsseldorf, Urt. v. 27.3.1997 – 20 U 51/96; a. A. König, NJW 1995, 3293, 3294; Kreutzer, CR 2006, 804, 806; ähnlich Meyer-Spasche/Störing/Schneider, CR 2013, 131, 135.
[41] Grützmacher in: Wandtke/Bullinger, UrhG § 69d Rn. 26; a.A. Wiebe, in: Spindler/Schuster Recht der elektronischen Medien, UrhG § 69d Rn. 18; Dreier, in: Dreier/Schulze, UrhG § 69d Rn. 10; Lehmann, NJW 1993, 1822 (1823).
[42] EuGH, Urteil vom 06.10.2021 – C-13/20 – Top System SA/Belgien.
[43] OLG Karlsruhe, Urteil vom 10.1.1996 – 6 U 40/95 –, Rn. 37; OLG Düsseldorf, Urteil vom 27.3.1997 – 20 U 51/96; a. A. König, NJW 1995, 3293, 3294; Kreutzer, CR 2006, 804, 806; ähnlich Meyer-Spasche/Störing/Schneider, CR 2013, 131, 135.
[44] Siehe Fn. 37.
[45] EuGH, Urteil vom 06.10.2021 – C-13/20 – Top System SA/Belgien.
[46] Spindler, JZ 2016, 805 (810); für eine weite Auslegung: König, NJW 1995, 3293 (3294).
[47] Von Maltzan/Moshashai, DSRITB 2018, 143 (155) konstatieren ein "(Quasi-)Verbot für Softwarenutzende, Softwarefehler selbst zu beheben.
[48] Anders ist dies bspw. im Rahmen der InfoSoc Richtlinie (Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft).

3.2.2 Einholung von Lizenzen

Bei Computerprogrammen, die auf verschiedenen Komponenten aufbauen, kann die Klärung der Rechtsinhaberschaft aufwändig ausfallen, sodass die Einholung von Lizenzen keine realistische Alternative darstellt.[49] In der Praxis fehlt oftmals das Bewusstsein für die Notwendigkeit regelmäßiger Tests; oder einfach eine Ansprechpartner*in für Anfragen, oder Anfragen werden aus anderen Gründen nicht beantwortet.

IT-Sicherheitsforschung beschränkt sich zudem nicht auf die Sicherheitsanalyse einzelner Produkte. Beim sog. „Scanning" arbeiten Forschende oft „rückwärts" ausgehend von Schwächen in der Standardisierung von Protokollen oder auch bloß vermuteten Implementierungslücken aufgrund allgemeiner Prinzipien, so dass erst die Sicherheitslücke identifiziert wird und dann Produkte gesucht werden, die verwundbar sind. Dazu testen sie in Stichproben oder führen breit angelegte Scans im Internet durch, bei denen sie möglichst non-invasiv flächendeckend nach den potenziell von Sicherheitslücken betroffenen Systemen suchen, um dann erst Produktverantwortliche oder betroffene Anwender*innen zu ermitteln und zu warnen. Folglich besteht keine Möglichkeit, vorab um eine Lizenz zu ersuchen.

In der Praxis hat sich gezeigt, dass nur wenige Forscher*innen von der Lizenzierung profitieren. Eine US-Studie an exemplarischen IT-Produkten zeigte, dass über die Hälfte der kontaktierten Produktverantwortlichen nicht antworteten. Ein in der EU ansässiger unabhängiger Sicherheitsforscher erhielt auf 20 Anfragen lediglich 3 Antworten.[50] Nur ca. 13% der angefragten Produktverantwortlichen erlaubten Sicherheitsanalysen ohne einschränkende Bedingungen.[51] Daneben variierte die Zeitspanne zwischen Anfrage und Rückmeldung von wenigen Stunden bis mehreren Monaten.[52] Für Forschungsprojekte stellt dies daher keine praktikable Lösung dar.

3.2.3 Fazit zum Urheberrecht

Der im Jahr 2018 veröffentlichte Bericht einer Task Force des Centre for European Policy Studies (CEPS) bietet die erste umfassende Darstellung der rechtlichen Herausforderungen in der EU zur Aufdeckung und Offenlegung von Sicherheitslücken.[53] In diesem Zusammenhang kommt die Task Force ebenfalls zum Ergebnis, dass der Schutz des Urheberrechts die Weitergabe von Informationen über Schwachstellen verhindern kann und damit Sicherheitsforschung sowie den Umgang mit Sicherheitslücken rechtlich herausfordernd gestaltet.[54]

---

[49] Eine "Lizenz zum Hacken" erhalten Forschende zwar ggf. auf Einladung zu Hackathons, über Bug-Bounty-Programme oder Meldeprozesse mit festgelegten „Spielregeln". Problematisch bleibt allerdings auch in diesen Konstellationen, wenn nach Regeln des Herstellers unklar bleibt was angegriffen werden darf (siehe bspw. http://www.digitalmunition.com/WhyIWalkedFrom3k.pdf) oder einseitig festgelegte Regeln prohibitiv wirkende Verhaltens- und Geheimhaltungsklauseln enthalten. Zudem sind solche Strukturen aktuell eher in IT-/Großunternehmen zu finden.

[50] Gamero-Garrido/Savage/Levchenko/Snoeren, Quantifying the Pressure of Legal Risks on Third-party Vulnerability Research, CCS'17, Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security 2017, S. 1501 (1502).

[51] Gamero-Garrido/Savage/Levchenko/Snoeren, CCS'17, S. 1501 (1507).

[52] Gamero-Garrido/Savage/Levchenko/Snoeren, CCS'17, S. 1501 (1506).

[53] Pupillo/Ferreira/Varisco, Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges, Report of a CEPS Task Force June 2018, abrufbar unter https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/ (zuletzt aufgerufen 19.09.2019).

[54] Pupillo/Ferreira/Varisco, Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges, Report of a CEPS Task Force June 2018, S. 47.

3.3 Datenschutzrecht

Oliver Vettermann / Daniel Vonderau / Maximilian Leicht / Jochen Krüger / Stephanie Vogelgesang / Christoph Sorge

Im Gegensatz zu anderen Teilgebieten enthält das Datenschutzrecht Normen, die sich ausdrücklich auf Aspekte der Forschung beziehen. Im Folgenden wird thematisiert, inwieweit diese Regelungen Erleichterungen für IT-Sicherheitsforschende bedeuten können und welche Rechtsunsicherheiten dennoch bestehen.

3.3.1 Reichweite von Art. 89 DSGVO

Zentraler Anlaufpunkt für die Datenverarbeitung im Forschungskontext ist Art. 89 DSGVO, der besondere Vorgaben für die wissenschaftliche Forschung enthält. Gemäß Erwägungsgrund 159 ist der dort angelegte Begriff der „wissenschaftlichen Forschungszwecke“ weit zu fassen und erstreckt sich auch auf „die Verarbeitung für beispielsweise die technologische Entwicklung und die Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung“. Zudem wird der Begriff im Lichte des Art. 179 Abs. 1 AEUV verstanden, wodurch der Forschungsbegriff eine ähnliche Färbung wie das (unions-)verfassungsrechtliche Verständnis der Art. 13 EU-GrC, Art. 10 EMRK sowie Art. 5 Abs. 3 S. 1 GG erhält: die Unterstützung von Universitäten und Forschungszentren zur Freiheit der Wissenschaft, der Verbreitung von Erkenntnissen und Entwicklungen, die Förderung von Zusammenarbeitsbestrebungen (auch über Grenzen hinweg), und die Unterstützung ihrer Wettbewerbsfähigkeit. Insofern ist Forschung als solche als „geistige Tätigkeit mit dem Ziele, in methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen“[55] zu definieren. National reflektiert § 27 BDSG die konkretisierte Forschungsfreiheit und greift das dargelegte Verständnis unverändert auf. In dieses weite Verständnis ist auch die Disziplin der IT-Sicherheitsforschung[56] zu integrieren.

3.3.2 Wechselspiel zwischen Art. 32 und 89 DSGVO

Darüber hinaus findet die IT-Sicherheitsforschung aber mittelbar Anklang in dem Wechselspiel zwischen Art. 32 und 89 DSGVO. Die Durchdringung der DSGVO mit Technikrelevanz und technikbezogenem Schutz manifestiert sich in den Anforderungen des Art. 32 DSGVO, technische und organisatorische Maßnahmen für ein angemessenes Sicherheitsniveau zu ergreifen. Die IT-Sicherheitsforschung ist mit dem Gedanken des Art. 89 sowie ErwGr 159 also insofern in Art. 32 DSGVO hineinzulesen, als dass die Ergebnisse der Forschenden für die Fortentwicklung des Stands der Technik notwendig sind. Nur auf diese Weise ist es möglich, den Status quo zu überprüfen und weiterzuentwickeln, um wiederum das übergeordnete Prinzip der Vertraulichkeit und Integrität gem. Art. 5 Abs. 1 lit. f DSGVO zu gewährleisten. Konkret enthält Art. 32 Abs. 1 lit. d DSGVO die Pflicht für den Verantwortlichen, ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu etablieren. Sofern also Nutzende von IT-Produkten dieser Verpflichtung nachkommen möchten, könnten sie bei der Verarbeitung von personenbezogenen Daten dazu verpflichtet sein, ihr zur

[55] BVerfGE 35, 79 – Hochschulurteil.
[56] Ausführlich zum Begriff siehe Ziff. 2 des Whitepapers.

Datenverarbeitung genutztes Produkt (technische Anlage oder Software) auf die o.g. Kriterien hin zu untersuchen. Derartige Überprüfungen – insbesondere hinsichtlich der Anforderungen nach Abs. 1 lit. b – werden in der Informatik etwa als Pentests[57] durchgeführt, bei denen gezielte Angriffe auf ein System simuliert werden, um u.a. die Empfindlichkeit des Systems zu überprüfen.[58] Dies kann jedoch zu einem Konflikt zwischen der datenschutzrechtlichen Anforderung einerseits sowie den o.g. Vorgaben aus dem Urheberrecht und Strafrecht andererseits führen, sofern diese Pentests die bereits oben angesprochene Dekompilierung urheberrechtlich geschützter Computerprogramme oder den Zugriff bzw. die Veränderung von Daten erfordern, über die der Systemnutzer keine Verfügungsberechtigung besitzt. Somit besteht eine Kollisionslage zwischen dem datenschutzrechtlichen Gebot und dem zivil- oder strafrechtlichem Verbot: Ob Art. 32 DSGVO als vorrangiges Recht die Berechtigung zum Datenumgang gewähren könnte, was über das Merkmal „unbefugt" eine Strafbarkeit ausschließen würde, ist nicht geklärt.[59] Dagegen sprechen die Unbestimmtheit des Art. 32 DSGVO sowie grundsätzliche Bedenken bezüglich der Anwendung der DSGVO als Unionsrecht im Kontext der Auslegung nationaler strafrechtlicher Normen. Sofern man jedoch von einer strafbarkeitsausschließenden Berechtigung zum Datenumgang zur Durchführung von Pentests ausgehen würde, wären davon nicht alle Konstellationen erfasst, in denen sich IT-Sicherheitsforscher*innen wiederfinden könnten. Dieser Umstand spricht für die Notwendigkeit der Forderung einer Kollisionsnorm, die diesen und weiteren Aspekten gebührend Rechnung trägt und der aufgezeigten Rechtsunsicherheit entgegenwirkt.

3.3.3 Rechtsgrundlagen der IT-Sicherheitsforschung

3.3.3.1 Art. 6 Abs. 1 S. 1 lit. a DSGVO (Forschung auf Datenbasis des Einwilligenden)

Zunächst ist als Rechtsgrundlage eine Einwilligung der Betroffenen nach Maßgabe der Art. 6 Abs. 1 S. 1 lit. a, Art. 7 DSGVO denkbar. Im Rahmen der praktischen Umsetzung bestehen jedoch insbesondere bezüglich der Kriterien der Freiwilligkeit, der Informiertheit, sowie der Zweckbestimmung Unsicherheiten. Die Einholung einer Einwilligung stellt im Forschungskontext zwar oft bereits auf Basis ethischer Überlegungen eine sinnvolle Vorgehensweise dar.[60] Selbst wenn jedoch die Kriterien der Informiertheit und Zweckbestimmung im Einzelfall rechtssicher erfüllt werden können, so können Betroffene die Einwilligung dennoch jederzeit widerrufen, vgl. Art. 7 Abs. 3 S. 1 DSGVO. Datenverarbeitungen auf dieser Rechtsgrundlage unterliegen – mit Blick in die Zukunft – daher immer einer gewissen Unsicherheit. Im Ergebnis ist die Einwilligung nach Art. 6 Abs. 1 S. 1 lit. a DSGVO daher oft nur mit Einschränkungen eine praktisch und/oder rechtssicher verwendbare Rechtsgrundlage.

3.3.3.2 Art. 6 Abs. 1 S. 1 lit. e DSGVO (Forschung auf Basis eines öffentlichen Interesses)

Außergewöhnlich bleibt wohl die universitäre bzw. institutionelle Forschung auf dem Gebiet der IT-Sicherheit: Wenngleich in dem Regelkonstrukt der DSGVO primär keine Unterscheidung mehr zwischen öffentlich-rechtlichen und privatrechtlichen juristischen Personen in der Rolle des Verarbeitenden gemacht wird (vgl. Art. 4 Abs. 1 Nr. 7), finden sich vereinzelt in der DSGVO spezifische Vorgaben für eine Verarbeitung. So greift

[57] Hladjk, in: Ehmann/Selmayr, DS-GVO Art. 32 Rn. 10; Jandt, in: Kühling/ Buchner, DS-GVO Art. 32, Rn. 29; Martini, in: Paal/Pauly, DS-GVO Art. 32 Rn. 44; Mantz, in: Sydow, DSGVO Art. 32, Rn. 20; Hansen, in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO Art. 32, Rn. 56.
[58] Hladjk, in: Ehmann/Selmayr, DS-GVO Art. 32 Rn. 10.
[59] Befürwortend: Wagner, PinG 2020, 66 (70).
[60] So auch Golla, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 1. Aufl. 2019, § 23 Rn. 21.

Art. 6 Abs. 1 lit. e, Abs. 3 DSGVO in Abgrenzung zur Interessenabwägung nach lit. f gerade die institutionelle, staatliche Gewaltenausübung auf und überlässt lit. f dem privaten Sektor.[61] Obschon auch Universitäten regelmäßig als Körperschaft/Anstalt öffentlichen Rechts organisiert sind[62] und damit staatlicher Natur, mangelt es ihnen angesichts ihrer Unabhängigkeit im Rahmen der Forschungstätigkeit (Hochschulfreiheit, Art. 5 Abs. 3 S. 1 i.V.m. Art. 19 Abs. 3 GG) an der Ausübung hoheitlicher Gewalt. Es liegt daher fern, entgegen der national wie unionsrechtlich (hier: Art. 13 S. 1 EU-GrC; Art. 9, 10 EMRK) anzunehmenden grundrechtstypischen Gefährdungslage einen Gewaltenträger i.S.d. DSGVO zu erkennen. Das öffentliche Interesse des Art. 6 Abs. 1 S. 1 lit. e DSGVO erhält die Unsicherheit institutioneller Forschung in dieser Disziplin aufrecht, indem es stets einer entsprechenden gesetzlichen Verweisung zur Begründung des öffentlichen Interesses bedarf, welches sich etwa mithilfe der Forschungsklauseln der Landesdatenschutzgesetze begründen lässt. Diese bereitet bei Drittmittelforschung und je nach Forschungsmaterie im Lichte der Hochschulgesetze allerdings erhebliche Schwierigkeiten für Forscher*innen, schon aufgrund ihrer Komplexität und mangels klarer Definition. In Zweifelsfällen wird daher, wie auch für nicht-institutionelle Forschung, auf Art. 6 Abs. 1 S. 1 lit. f DSGVO zurückgegriffen.

3.3.3.3 Art. 6 Abs. 1 S. 1 lit. f DSGVO (Forschung auf Basis der Interessenabwägung)

In dieser Hinsicht lassen sich jedoch weitere Rechtsunsicherheiten feststellen: Bei der detaillierteren Abwägung der wissenschaftlichen (IT-Sicherheits-)Forschung als berechtigtes Interesse gegen die Interessen der Betroffenen lassen sich Schwierigkeiten bei der genauen Gewichtung der wissenschaftlichen Forschung feststellen.[63] Im Falle der Verarbeitung von Daten gem. Art. 9 DSGVO gelten zudem erhöhte Anforderungen an das Überwiegen der Interessen der Forschung, (§ 27 Abs. 1 S. 1 BDSG, sowie entspr. landesrechtliche Normen).[64] Insgesamt ist die im Rahmen des Art. 6 Abs. 1 lit. f DSGVO bzw. der bundes- oder landesrechtlichen Regelungen vorzunehmende Interessenabwägung daher für Verantwortliche von Grund auf als risikobehaftet einzuordnen. Zwar können die Wertungen der DSGVO zu wissenschaftlicher Forschung von Verantwortlichen im Rahmen der Interessenabwägung berücksichtigt werden. Zahlreiche Regelungen weisen auf die Intention des Verordnungsgebers hin,[65] so etwa Art. 5 Abs. 1 lit. b, e, Art. 9 Abs. 2 lit. j, Art. 14 Abs. 5 lit. b oder auch ErwG 33 DSGVO.[66] Daneben enthalten auch Art. 3 Abs. 3 EUV sowie Art. 179 Abs. 1 AEUV Zielbestimmungen der EU hinsichtlich des wissenschaftlichen Fortschritts bzw. eines europäischen Raumes der Forschung.[67] Doch auch unter Beachtung dieser gesetzgeberischen Wertungen bedeutet eine Interessenabwägung für die Verantwortlichen einen nicht unerheblichen Aufwand im Hinblick auf die einzelnen Verarbeitungsvorgänge. Regelmäßig wird eine Beurteilung aus einer – nicht juristisch vorgeprägten – Laiensphäre sehr herausfordernd sein. Selbst wenn Verantwortliche jedoch ihren IT-Sicherheitsforscher*innen juristische Hilfestellungen bereitstellen, ist das Risiko einer fehlerhaft durchgeführten Abwägung regelmäßig nicht vollständig auszuschließen. Die dadurch entstehende Rechtsunsicherheit erscheint mit der heutigen Relevanz von IT-Sicherheitsforschung nicht zufriedenstellend vereinbar.

[61] Zur Differenzierung auch Golla/Hofmann/Bäcker, DuD 2018, 89 (93 f).
[62] Exemplarisch insoweit BVerfGE 35, 79 (118): Staatsanstalten; § 2 Abs. 1 SächsHSFG und § 8 Abs. 1 S. 1 LHG BW: Körperschaften; § 1 Abs. 1 S. 1 NHG: Stiftungen.
[63] Vgl. Golla, in: Specht/Mantz, § 23 Rn. 44, Rn. 30.
[64] Vgl. hierzu ausführlich: Golla, in: Specht/Mantz, § 23 Rn. 30ff., Rn. 44.
[65] Vgl. Böken, in: Kipker, Cybersecurity, S. 495, 499.
[66] Roßnagel, ZD 2019, 157 (159); Pauly, in: Paal/Pauly DSGVO, 3. Aufl. 2021, Rn. 3.
[67] Vgl. Böken, in: Kipker, Cybersecurity, S. 495.

3.4 Vertragliche und deliktische Haftung

Roman Dickmann

Bei der eigentlichen Forschungstätigkeit, der Vor- und Nachbereitung, der Entwicklung und Nutzung von Hard- und Software zu Forschungszwecken, der Entdeckung und Meldung von Schwachstellen sowie deren Veröffentlichung bestehen vertragliche und deliktische Haftungsrisiken für IT-Sicherheitsforscher*innen. Vornehmlich geht es um Unterlassungs- und Schadenersatzansprüche, wobei Sonderkonstellationen wie etwa patent- und dienstrechtliche Fragen sowie mögliche Überschneidungen mit dem Presse- und Außenwirtschaftsrecht nicht untersucht werden.

Haftung der Forschenden als Software-/Cloud-Nutzer wegen Vertragsverletzung? Vertraglich kann sich eine Haftung von IT-Sicherheitsforscher*innen als Nutzer*innen von fremder Software insbesondere bei der Suche, Entdeckung, Dokumentation und demonstrativen Ausnutzung von Schwachstellen ergeben. Verbots- und Sanktionsklauseln für typische Nutzungsszenarien finden sich insbesondere in den als AGB ausgestalteten Nutzungsbedingungen von Software und Web-/Cloud-Diensten. Es stellt sich eingangs die Frage von deren wirksamer Einbeziehung. In einigen Fällen wurde IT-Sicherheitsforscher*innen vorgeworfen, dass sie die Kenntnisse über die Schwachstelle nur AGB- oder lizenzwidrig erlangt haben können, was aber die Anspruchsteller*in beweisen muss. Eine bloße Behauptung reicht nicht, zumal keine Vermutung zu Lasten der Forscher*innen spricht.

Bezüglich des AGB-rechtlichen Prüfungsmaßstabs ist zu klären, ob es sich bei der Forscher*in um eine Privatperson oder ein Unternehmen handelt, wobei juristische Personen der zweiten Kategorie zuzurechnen sind. Die Verbotsklauseln sind häufig sehr umfassend und weitreichend. Eine Recherche auf den Webseiten großer Anbieter hat gezeigt, dass vor allem Sicherheitstests und Reverse Engineering sowie dazu nötige Maßnahmen untersagt werden. Die Klauseln erscheinen meist als direkte Übersetzungen US-amerikanischer Bedingungswerke ohne Anpassungen etwa an deutsche Besonderheiten. Es erscheint äußerst fraglich, ob diese Klauseln selbst zwischen Unternehmen der Wirksamkeitsprüfung nach deutschem Recht standhalten würden. Dies gilt insbesondere mit Blick auf die urheberrechtlichen Mindestnutzungsrechte nach §§ 69d f. UrhG. Rechtsprechung fehlt hierzu, jedoch scheint es den Verwendern trotz für Juristen äußerst zweifelhafter Wirksamkeit um die Abschreckungswirkung zu gehen. Folglich sind IT-Sicherheitsforscher*innen hier erheblicher Rechtsunsicherheit ausgesetzt, die allein den Verwendern nutzt. Forscher*innen droht eine (diesbezüglich jedenfalls ungerechtfertigte) Inanspruchnahme insbesondere auf Abgabe strafbewehrter Unterlassungserklärungen samt Anfall (nicht erstattungsfähiger) eigener Rechtsverteidigungskosten.

Haftungsrisiken bei der Meldung von Schwachstellen? Außerhalb vertraglicher Sonderbeziehungen besteht bei der Entdeckung einer Sicherheitslücke regelmäßig keine gesetzliche Pflicht zur Meldung an Verantwortliche. Vielmehr handelt es sich um eine freie Entscheidung zum Ob und Wie. Ein Angebot auf weitere Unterstützung nur bei Erfüllung bestimmter Bedingungen wie etwa der Übernahme tatsächlich anfallender Kosten kann der Verantwortliche annehmen oder auch nicht. Forderungen nach finanziellem Ausgleich von Aufwand und Kosten der Forscher*innen bestehen mangels Auftrags für die Vergangenheit nicht. Andererseits besteht aber auch kein Rechtsanspruch auf deren zukünftiges Engagement. Ein solches würde vielmehr eine geldwerte Leistung darstellen, denn das Wissen um Schwachstellen hat einen Marktwert. Eine Weigerung an der weiteren Mitwirkung zur Beseitigung der Sicherheitslücke teilzunehmen, ist folglich rechtlich unproblematisch zulässig. Das Setzen einer Frist durch Forschende gegenüber der Hersteller*in bis zur Veröffentlichung ist hinzunehmen. Die Zeit sollte für die Entwicklung und Bereitstellung eines Updates/Patches

oder einer anderen Lösung genutzt werden. Die Frist sollte für diese Arbeit mit Blick auf technische Komplexität und Kritikalität der Schwachstelle angemessen lang sein, worauf aber kein Anspruch besteht.

Raum für Haftung besteht auch nicht, wenn ein Geldbetrag oder ein Sachpreis für die Meldung von Schwachstellen ausgelobt wurde (Bug Bounty) und diesbezüglich Ansprüche angemeldet werden. Vielmehr hat der Auslobende eine ablehnende Entscheidung mitzuteilen und zu begründen.

Haftung bei Veröffentlichung von Schwachstellen? Die Publikation von Schwachstellen insbesondere mit technischen Details kann Verantwortlichen insbesondere aus Angst vor negativer Presseberichterstattung ein Dorn im Auge sein. Gegen (mögliche bzw. angekündigte) Veröffentlichungen wird oft schon außergerichtlich und im einstweiligen Rechtsschutz mit dem Vorwurf des Verstoßes gegen Verschwiegenheitspflichten argumentiert. Ohne vertragliche Sonderbeziehungen können IT-Sicherheitsforscher*innen nicht zur Abgabe entsprechender Verschwiegenheitserklärungen gezwungen werden. Bei in AGB-Klauseln integrierten Verschwiegenheitspflichten erscheinen diese meist als überraschend und unwirksam. Dies gilt ebenso für eine Pflicht zur Meldung allein an die AGB-Steller*in. Auch hier wird häufig mit dem Faktor Abschreckung gearbeitet.

Andererseits müssen sich Unternehmen, die etwa auf ihrer Webseite selbstbindende Prozessangaben für die Meldung von Schwachstellen an das eigene Haus (Disclosure Policy) veröffentlicht haben, an diese halten. Entsprechende Texte sind jedoch, was die Pflichten der Unternehmen angeht, bewusst vage gehalten. Trotz erheblicher Zweifel an der Wirksamkeit der Klauseln, führt die einseitige Festlegung von Pflichten der IT-Sicherheitsforscher*innen zu einem Bedrohungsszenario mit teils sehr hohen Schadenersatzforderungen für entgangenen Gewinn, fiktive Lizenzkosten und Rechtsanwaltsgebühren.

Dies setzt sich im Deliktsrecht fort. Als Schutzgesetze i.S.v. § 823 Abs. 2 BGB kommen etwa § 202a bis § 202c StGB sowie § 303a f. StGB in Betracht.[68] Die weitreichende Vorfeldkriminalisierung erhöht gerade für die Sicherheitsforscher*innen neben Risiken der Strafbarkeit bzw. von Ermittlungsverfahren[69] auch solche der nachfolgenden zivilrechtlichen Haftung. Letztere kann dabei mit dem entsprechenden Kostenrisiko ein hohes Abschreckungspotenzial entwickeln.

Zur Verfolgung (vermeintlicher) Rechte von Verantwortlichen gegen IT-Sicherheitsforscher*innen spielt der Unterlassungsanspruch nach §§ 1004, 823 BGB mit entsprechender materiell-rechtlicher Grundlage eine große Rolle.[70] Als Anspruchsgrund wird häufig ins Feld geführt, dass überhaupt keine (ausnutzbare) Schwachstelle vorliege, die entsprechende Tatsachenbehauptung also unwahr sei. Auch gegen Werturteile

---

[68] Zur niedrigen Strafbarkeitsschwelle insbesondere in technischer Hinsicht zuletzt BGH NStZ-RR 2020, 278 (280; selbst, wenn nur einige Mausklicks zur Überwindung des Passwortschutzes nötig sind, hindert dies die Strafbarkeit nicht), kritisch Gercke ZUM 2020, 948 (958). Vgl. für einen US-Fall zur (extensiven) Auslegung des Computer Fraud and Abuse Acts durch die Ermittlungsbehörden Van Buren v. United States, US Supreme Court Case 19-783/18-12024.

[69] Vgl. zu einem Praxisfall mit einer Strafanzeige samt Ermittlungsverfahren gegen die meldende IT-Sicherheitsforscherin: Wolfangel, „Danke für den Hinweis, Anzeige ist raus“ in: Zeit online vom 05.08.2021, abrufbar unter https://www.zeit.de; Hurtz, „CDU blamiert sich mit Anzeige gegen IT-Expertin“ in: Süddeutsche Zeitung online vom 05.08.2021, abrufbar unter https://www.sueddeutsche.de/politik/cdu-connect-anzeige-wittmann-1.5373488 und Ernst, „Lücken in der CDU-connect-App: Datenschutzbeauftragte leitet Prüfverfahren ein“ in: heise online vom 06.08.2021, abrufbar unter https://www.heise.de/news/Luecken-in-der-CDU-connect-App-Datenschutzbeauftragte-leitet-Pruefverfahren-ein-6157570.html (zuletzt abgerufen am 01.10.2021). Die IT-Sicherheitsforscherin bleibt mit den Folgen bis hin zu potenziellen Durchsuchungs-/Beschlagnahmemaßnahmen belastet. Zu einem solchen (technisch ähnlichen) Fall mit einer Durchsuchung Beuth/Gnirke, Spiegel netzwelt vom 01.07.2021, abrufbar unter https://spiegel.de/netzwelt; Steier, wortfilter.de vom 18.09.2021, abrufbar unter https://wortfilter.de.

[70] Vgl. Ermert, „Offenlegung von Softwarelücken: Rechtsstreit endet mit Vergleich“ in Heise online, 2018, abrufbar unter: https://www.heise.de/newsticker/meldung/Offenlegungvon-Softwareluecken-Rechtsstreit-endet-mit-Vergleich-4156393.html (zuletzt abgerufen am 02.08.2019).

wie das Attribut „unsicher“ wird sich verwahrt. Gerade in solchen Fällen sollte die Verantwortliche mit den Forschenden in einen Dialog treten, um etwaige Missverständnisse und Fehleinschätzungen einvernehmlich auszuräumen und nicht ohne vorausgehende Kommunikation auf Augenhöhe mit Rechtsmitteln vorgehen. Die Meinungs- und Forschungsfreiheit sowie wettbewerbsrechtliche Aspekte sind jedenfalls in die etwaig nötigen Abwägungen einzustellen. Dabei ist die Darlegungs- und Beweislast auf jeder Ebene zu beachten.

Meist zu weitgehend sind schließlich Forderungen an Forscher*innen, keine weiteren Untersuchungen bezüglich der konkreten Schwachstelle oder den Produkten des Anspruchsstellers (mehr) vorzunehmen. Eine solch invasive Beschränkung der Wissenschaftsfreiheit ist auch mit Blick auf das gesamtgesellschaftliche Interesse an der Prüfung und Stärkung der IT-Sicherheit nicht vertretbar.

Die Veröffentlichung einer Schwachstelle wird nur äußerst selten unverhältnismäßig sein.[71] Nutzer*innen von mit Schwachstellen behafteten Produkten können nicht durch Verschweigen und Verschleiern, sondern nur durch Beseitigung der Schwachstelle geschützt werden. Dies oder zumindest eine Warnung fordern etwa Pflichten aus Vertrag zur Nachbesserung/-erfüllung bzw. der Produkt-/Produzentenhaftung insbesondere zur Beobachtung und Warnung. Einzig über die Notwendigkeit der Publikation technischer Details kann gestritten werden, wenn diese Angreifer*innen einen Wissensvorsprung etwa zum Lokalisieren weiterer Offensivvektoren verschaffen, für die Beseitigung und Einschätzung der Schwachstelle oder Gegenmaßnahmen aber unerheblich sind. Ein Recht auf Zensur durch den Verantwortlichen für das vulnerable Produkt wie auch eine Vorab-Vorlage-Pflicht für das Publikationsmaterial bestehen aber nicht.

Ein weiteres Feld spezialgesetzlicher deliktischer Haftung ergibt sich aus §§ 6, 10 GeschGehG bei unbefugter Erlangung, Nutzung oder Offenlegung von Geschäftsgeheimnissen. Bezüglich der Anwendbarkeit dieses nach der Geheimnisschutz-Richtlinie europarechtlich geprägten Gesetzes stellt sich die Frage, ob eine Schwachstelle überhaupt ein Geschäftsgeheimnis sein kann und zu ihrer Geheimhaltung ein berechtigtes Interesse besteht. In einigen Fällen werden die Schwachstellen bereits allgemein bzw. ohne Weiteres zugänglich und deshalb das Tatbestandsmerkmal nicht erfüllt sein. Schließlich müsste die Schwachstelle Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber sein. Hierzu wird es schon an der nötigen Kontrolle über die Schwachstelle fehlen, da diese bei einem am Markt befindlichen Produkt per se nicht mehr kontrollierbar ist und ihre Ausnutzung nur dadurch verhindert werden kann, dass für ihre Beseitigung gesorgt wird. Dies wird jedoch teilweise anders gesehen, wenn technischer Aufwand etwa mittels Reverse Engineering zur Erlangung notwendig ist. Für das Horten von Schwachstellen in (eigenen) Produkte jedenfalls besteht kein schutzwürdiges Interesse. Es bleiben rechtsunsichere Lösungen über die Erlaubnis von Reverse Engineering nach § 3 Abs. 1 Nr. 2 GeschGehG oder die Ausnahmetatbestände nach § 5 GeschGehG insbesondere für Whistleblowing. Auch für das GeschGehG wäre eine Privilegierung von Forschung samt Enthaftung wünschenswert.

Haftung von Forschenden als Hersteller*in von Soft-/Hardware für ein Proof of Concept? Mangels Inverkehrbringens sind Forschende keine Hersteller*innen von als Hilfsmittel für die eigene Forschung fabrizierter sowie allein dort verwendeter Hard-/Software und haben nicht nach der Produkthaftung einzustehen. Anders gelagert ist die Konstellation, in der insbesondere Software zur demonstrativen Ausnutzung von Schwachstellen (Exploits) etwa im Rahmen von Veröffentlichungen zum Nachweis der technischen Machbarkeit (Proof of Concept) zur Verfügung gestellt wird. Geschieht dies unter Offenlegung des Quellcodes unter

[71] Vgl. Rechtsbank Arnhem, Urteil vom 18.07.2008, Az. 171900/KG ZA 08-415 (Schwachstelle in der Kryptographiefunktion des Mifare-Classic-RFID-Chips für z.B. Zugangsberechtigungssysteme); zum technischen Hintergrund https://www.ru.nl/dis/removed-during-reorganisation/research/rfid/ (zuletzt abgerufen am 07.06.2020) sowie auch die britische Entscheidung England and Wales High Court, Entscheidung vom 25.06.2013, NCN [2013] EWHC 1832 (Ch), VW vs. Garcia and others.

einer Open Source bzw. freien oder Public Domain Lizenz, greift für die Haftung regelmäßig Schenkungsrecht, sodass die Forschenden nur Vorsatz und grobe Fahrlässigkeit zu vertreten haben. Eine Verschärfung nach den Grundsätzen der (deliktischen) Produkthaftung kommt aber insbesondere in Betracht, wenn Forscher zu beruflichen und wirtschaftlichen Zwecken tätig sind. Die Anwendbarkeit des ProdHaftG ist mit Blick auf z.B. nicht auf einem Datenträger oder in Hardware verkörperter Software mit erheblicher Unsicherheit belegt. Für die Haftung müsste es allerdings zu einem Sach- bzw. Personenschaden kommen. Viele Konstellationen werden jedoch zu nicht ersatzfähigen reinen Vermögensverlusten führen. Weiterhin steht eine Haftung nach § 823 Abs. 2 BGB i.V.m. § 202c Abs. 1 Nr. 2 StGB im Raume. Mit Dokumentation und Hinweisen dazu, dass es sich um Testsoftware zum Ausnutzen von Schwachstellen handelt, mag die zivilrechtliche Haftung minimiert oder gar ausgeschlossen werden. Strafrechtlich jedoch belastet die Rechtsunsicherheit der Pönalisierungsreichweite des § 202c StGB die Forscher*innen insbesondere auch durch die zivilrechtliche Relevanz von Durchsuchungs-/Beschlagnahmemaßnahmen und resultierenden Ermittlungsergebnissen.

Fazit IT-Sicherheitsforschende sind vielfältigen zivilrechtlichen Haftungsrisiken bei der Ausübung ihrer Kerntätigkeiten ausgesetzt. Diese ergeben sich vor allem aus Rechtsunsicherheiten hinsichtlich der Reichweite von Bestimmungen des StGB, UrhG und GeschGehG sowie der Wirksamkeit von AGB-Klauseln in Nutzungsvereinbarungen und Lizenzen. Dies führt zu Abschreckungseffekten, denen es gesetzgeberisch entgegenzutreten gilt.

3.5 Schutz von Geschäftsgeheimnissen und Whistleblower-Schutz

Manuela Wagner, Oliver Vettermann

3.5.1 Erlaubnis des Reverse Engineering im Rahmen des Schutzes von Geschäftsgeheimnissen

Das Reverse Engineering war lange Zeit auch unter dem Gesichtspunkt des Schutzes von Geschäftsgeheimnissen problematisch. Das UWG war allerdings nur anwendbar, wenn zwischen den Parteien ein konkretes Wettbewerbsverhältnis besteht.[72] Darüber hinaus hat sich durch die Richtlinie 2016/943 und deren Umsetzung im Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) die Rechtslage zum Reverse Engineering maßgeblich geändert. Reverse Engineering soll nun als rechtmäßiges Mittel zum Erwerb von Know-How angesehen werden.[73]

> **§ 3 Abs. 1 Nr. 2 GeschGehG**
>
> Ein Geschäftsgeheimnis darf insbesondere erlangt werden durch
>
> Beobachten, Untersuchen, Rückbauen oder Testen eines Produkts oder Gegenstands, das oder der
>
> a) öffentlich verfügbar gemacht wurde oder
>
> b) sich im rechtmäßigen Besitz des Beobachtenden, Untersuchenden, Rückbauenden oder Testenden befindet und dieser keiner Pflicht zur Beschränkung der Erlangung des Geschäftsgeheimnisses unterliegt;

3.5.2 Schutz des Whistleblowers

Nach § 5 Nr. 2 GeschGehG dürfen Geschäftsgeheimnisse erlangt und offengelegt werden, wenn dies zur Aufdeckung einer rechtswidrigen Handlung oder eines beruflichen oder sonstigen Fehlverhaltens erforderlich und gleichzeitig geeignet ist, das öffentliche Interesse zu schützen. In diesem Zusammenhang muss die Motivation auf einen Missstand hinzuweisen das Handeln dominieren.[74] Der Begriff des beruflichen Fehlverhaltens umfasst auch Verstöße gegen berufsständische Normen sowie Aktivitäten, die unethisches Verhalten darstellen, aber nicht notwendigerweise gegen Rechtsvorschriften verstoßen.[75] Dabei kann auch die Offenlegung gegenüber dem Rechtsgutsträger dem öffentlichen Interesse dienen, wenn dieser so in die Lage versetzt wird, Rechtsverstöße oder sonstiges Fehlverhalten zu beenden.[76]

[72] Auch wenn ein Wettbewerbsverhältnis zwischen der Tätigkeit von Hochschulen und Forschungseinrichtungen gegenüber Produktherstellern eher fernliegend erscheint, ist dies nicht in allen Fällen komplett von der Hand zu weisen. Fraunhofer hat beispielsweise eine Industriequote von 30-40% je nach Institut. D.h. es wäre unter Umständen argumentierbar, dass es zu einer Konkurrenzsituation kommen könnte.
[73] Bundestags Drucksache 19/4724, S. 25.
[74] Bundestags-Drucksache 19/4724, S. 29.
[75] Bundestags-Drucksache 19/4724, S. 29.
[76] Bundestags-Drucksache 19/4724, S. 29.

Würde diese Norm keine Wirkung im Urheber- und Strafrecht entfalten, bestünde die Gefahr, dass Whistleblower je nach Art und Weise der Informationsgewinnung, trotz dieser Regelung dem Risiko zivil- oder strafrechtlichen Konsequenzen auszusetzen. Der Schutz des Whistleblowers wäre unvollständig.[77] Es verbliebe bei Chilling Effects durch die Angst vor Schadensersatzrisiken.

Zum 17.12.2021 ist zudem die Richtlinie 2019/1937/EU („Whistleblower-Richtlinie" – WBRL)[78] umzusetzen. Diese ist anwendbar auf den Schutz von Personen, die Verstöße gegen den Schutz der Privatsphäre und personenbezogener Daten sowie Sicherheit von Netz- und Informationssystemen offenlegen (Art. 2 Abs. 1 Buchst. a) Nr. x) WBRL.[79] Allerdings gilt die Richtlinie nur für Personen, die im beruflichen Kontext Informationen über Verstöße erlangt haben (Art. 4 Abs. 1 WBRL). Art. 21 Abs. 2 und Abs. 7 WBRL legen fest, dass Hinweisgeber nicht haftbar gemacht werden dürfen (auch bzgl. Urheberrechtsverstößen). Allerdings spezifiziert Absatz 3, dass eine Sanktionierung der Informationsbeschaffung weiterhin nach nationalem Recht möglich ist, wenn diese eine eigenständige Straftat darstellt. Nach Art. 20 Abs. 1 Buchst. c) WBRL soll Hinweisgebern Prozesskostenhilfe gewährt werden. Die Mitgliedstaaten dürfen bei der Umsetzung der Richtlinie ausdrücklich einen stärkeren Schutz von Hinweisgebern etablieren.[80] Die Übertragung ins deutsche Recht könnte folglich genutzt werden, um auch den Schutz der Personen, die Produkte und Systeme auf IT-Sicherheitslücken untersuchen und Schwachstellen offenlegen, zu regulieren.

3.5.3 Verhältnis zum Urheber- und Strafrecht

Ausweislich der Gesetzesbegründung des GeschGehG berührt die Erlaubnis des Reverse Engineerings den immaterialgüterrechtlichen Schutz nicht.[81] Im Bereich des Hardwaretesting wird der durch die Forschungsfreiheit nach Art. 5 Abs. 3 GG geschützte Freiraum durch § 11 Nr. 2 PatG und § 6 Abs. 2 Nr. 2 HalblSchG gewährleistet.[82] Das PatG erlaubt die Verwendung der patentierten Erfindung zu Versuchszwecken. Der BGH versteht den Begriff „Versuch" weit als „jedes (planmäßige) Vorgehen zur Gewinnung von Erkenntnissen, und zwar unabhängig davon, welchem Zweck die Erkenntnisse letztendlich zu dienen bestimmt sind".[83] Schaltelemente, die dem HalblSchG unterfallen, dürfen zwar grundsätzlich nicht nachgebildet werden. Dieser Schutz erstreckt sich aber nicht auf Handlungen zum Zweck der Analyse, Bewertung oder Ausbildung.[84] Insofern bestehen hier wichtige Rechtsgrundlagen, die auch für die IT-Sicherheitsforschung genutzt werden können. Anders sieht es im Bereich des Softwareschutzes aus.

Im Hinblick auf das Verhältnis zum Strafrecht gilt zu berücksichtigen, dass § 3 GeschGehG auf Geschäftsgeheimnisse anwendbar ist, während sich das IT-Strafrecht auf Daten nach § 202a Abs. 2 StGB bezieht, also solche Daten, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden. Da ein Geschäftsgeheimnis per Definition angemessene Geheimhaltungsmaßnahmen

[77] Wagner, DuD 2020, 111 (118).
[78] Richtlinie 2019/1937/EU des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden.
[79] Die zugehörigen EU-Rechtsakte sind im Anhang I der Richtlinie aufgelistet. Nicht geregelt ist allerdings die Meldung von Verhaltensweisen, die zwar rechtmäßig, aber unethisch sind oder dem öffentlichen Interesse zuwiderlaufen. Für einen kohärenten Rechtsrahmen sollte die Umsetzung auch Verstöße gegen nationales Recht erfassen; siehe hierzu: Schmolke, NZG 2020, 5 (6, 10).
[80] Art. 25 Abs. 1, 2 Abs. 2 WBRL; zu den Spielräumen: Schmolke, NZG 2020, 5 (8 ff.).
[81] Bundestags-Drucksache 19/4724, S. 25.
[82] Mes, 4. Aufl. 2015, PatG § 11 Rn. 5.
[83] BGH, Urteil vom 11.07.1995 - X ZR 99/92 GRUR 1996, 109, 112 – Klinische Versuche I.
[84] Schmidl, IT-Recht von A-Z, Reverse Engineering, 2. Auflage 2014.

erfordert, kann davon ausgegangen werden, dass die Erlangung in der Regel die Überwindung dieser Maßnahmen erfordert. Somit wäre bei einer nach § 3 GeschGehG erlaubten Handlung stets der Tatbestand des § 202a StGB erfüllt. Eine solche Handlung könnte folglich nicht unbefugt bzw. rechtswidrig sein, da eine gesetzliche Erlaubnis vorliegt.[85] Man könnte anregen, im Wege des Erst-Recht-Schlusses diese Erlaubnis auf sonstige Daten, die keine Geschäftsgeheimnisse darstellen, zu erweitern. Um Rechtssicherheit herzustellen, ist eine Klarstellung notwendig, dass der Schutz sonstiger Daten über §§ 202a, 202b StGB nicht weiter gehen darf als der von Geschäftsgeheimnissen. Denn die hier vorgeschlagene Auslegung ist zwar denkbar, wird aber nicht zwingend diejenige der Rechtsprechung sein.

[85] Wagner, PinG 2020, 66 (72).

4 Vulnerability Disclosure

Niklas Goerke / Johannes Obermaier / Marc Schink / Dieter Schuster / Manuela Wagner

Solange es keine vollkommen sichere Software gibt, ist die bestmögliche Bereitstellung von Informationen über Schwachstellen ein wichtiger Faktor für die Stabilität der „Informationsgesellschaft“.[86] Die koordinierte und verantwortungsbewusste Aufdeckung und Offenlegung von IT-Sicherheitslücken stellt dabei kein unlösbares Problem dar. Ein Mechanismus der Interessen von Wissenschaft, Gesellschaft und Produktverantwortlichen in Einklang bringen soll, ist die *Coordinated Vulnerability Disclosure* bzw. auch *Responsible Disclosure* genannt. Die Grundprinzipien dieses Prozesses wurden auf internationaler Ebene bereits erarbeitet und erprobt.[87] Ziel dieses Prozesses ist sicherzustellen, dass Schäden für die Gesellschaft und Wirtschaft minimiert werden.

4.1 Coordinated Vulnerability Disclosure - Koordiniertes Zusammenwirken

Bei diesem iterativen Prozess werden gefundene Schwachstellen zunächst nur derjenigen Stelle gemeldet, die die Schwachstelle verifizieren und beheben kann. Hierbei handelt es sich in der Regel um das herstellende Unternehmen (dessen Identifikation bei Lieferketten, Vertriebseinheiten, Import, etc. bereits herausfordernd sein kann). Erst nachdem eine Lösung für die Schwachstelle bereitgestellt wurde, oder wenn nach Ablauf einer angemessenen Frist zu vermuten ist, dass keine Lösung erstellt wird, wird eine Warnung an Dritte oder die Öffentlichkeit weitergegeben. Dieser Schritt ist erforderlich, um Schaden von Produktnutzenden abzuwenden und ihnen zu ermöglichen, Schutzmaßnahmen zu ergreifen. Dieser Mechanismus ist in Deutschland jedoch noch nicht flächendeckend etabliert und im geltenden Rechtsrahmen nicht verankert.

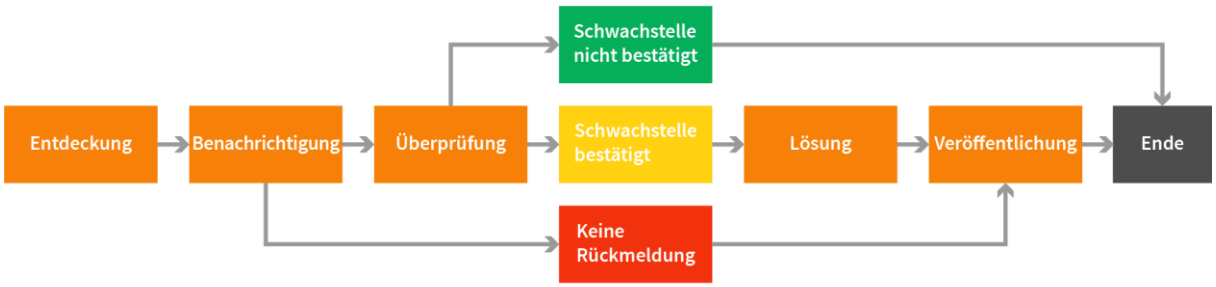

Abbildung 1 Ablauf eines Coordinated / Responsible Disclosure Prozesses[88]

[86] Böhme, A Comparison of Market Approaches to Software Vulnerability Disclosure, proceedings of ETRIC - International Conference on Emerging Trends in Information and Communication Security 2006, 298 (298) m.w.N.

[87] Householder et al., The CERT® Guide to Coordinated Vulnerability Disclosure, SPECIAL REPORT CMU/SEI-2017-SR-022, August 2017; National Cyber Security Centre, Ministry of Justice and Security, Netherlands, Coordinated Vulnerability Disclosure: the Guideline, October 2018; ENISA - European Union Agency For Network And Information Security, 2015. Good Practice Guide on Vulnerability Disclosure, From challenges to recommendations, DOI 10.2824/610384, abrufbar unter https://www.enisa.europa.eu/publications/vulnerability-disclosure (zuletzt abgerufen am 16.03.2020).

[88] Vgl. ENISA - European Union Agency For Network And Information Security, 2015. Good Practice Guide on Vulnerability Disclosure, From challenges to recommendations, DOI 10.2824/610384, S. 22.

Die Namensänderung von „*Responsible Disclosure*“ zu „*Coordinated Vulnerability Disclosure*“ beruht auf der Erwägung, dass sich gezeigt hat, dass dieser Begriff zu viel Betonung auf die Verantwortung der Melder*in legt, während nach dem Grundprinzip die Melder*in und die potenziell gefährdete Organisation gleichberechtigte Partner*innen im Dialog sein sollten.[89] Diese Nuancierung wird besser im neutralen und aktuell allgemein verwendeten Begriff *Coordinated Vulnerability Disclosure* transportiert.[90]

4.2 CVD in Normen und Standards

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das Fachgremium für die weltweite Normung und Standardisierung. Im Bereich des Schwachstellenmanagements sind die ISO/IEC 30111 *„Information technology — Security techniques — Vulnerability handling processes“* und ISO/IEC 29147 *„Information technology — Security techniques — Vulnerability disclosure“* relevant.

ISO/IEC 30111	Dieses Dokument beschreibt Prozesse für Anbieter*innen bzw. Hersteller*innen von IT-Produkten und Diensten zur Bearbeitung von Berichten über potenzielle Schwachstellen in ihren Produkten und Dienstleistungen. Die Zielgruppe für dieses Dokument umfasst Entwickler*innen, Anbieter*innen, Gutachter*innen und Benutzer*innen von Produkten und Dienstleistungen der Informationstechnologie. Es richtet sich nicht direkt an Wissenschaftler*innen. Es betrifft folglich eher die Compliance-Seite im Unternehmen.
ISO/IEC 29147:2018	Dieses Dokument enthält Empfehlungen für Anbieter*innen von IT-Produkten bzw. Diensten zur Offenlegung von Schwachstellen in Produkten und Dienstleistungen und damit den externen Prozess zwischen Melder*in und Meldeempfänger*in. Die Offenlegung von Schwachstellen ermöglicht es den Anwender*innen, ein technisches Schwachstellenmanagement durchzuführen, ihre Systeme und Daten zu schützen und Risiken besser einzuschätzen. Um bei dem Ziel der Offenlegung von Schwachstellen, welches darin liegt, das mit der Ausnutzung von Schwachstellen verbundene Risiko zu verringern, zu unterstützen, enthält die ISO/IEC 29147:2018 Orientierungshilfen für den Empfang von Berichten über potenzielle Schwachstellen; zur Offenlegung von Informationen über die Behebung von Schwachstellen; einen Überblick über die Konzepte, Techniken und Grundsatzüberlegungen zur Offenlegung von Schwachstellen sowie Beispiele für Techniken, Policies und Kommunikationshilfen. Als Hauptziele der Offenlegung von Schwachstellen werden hervorgehoben: – Risikominderung durch Behebung von Schwachstellen und Warnung der Benutzer*innen; – Minimierung der mit der Offenlegung verbundenen Schäden und Kosten; – Bereitstellung ausreichender Informationen für die Nutzenden, um das mit Schwachstellen verbundene Risiko zu bewerten; – Transparenz, um die kooperative Interaktion und Koordination zwischen den Beteiligten zu erleichtern.

[89] National Cyber Security Centre, Ministry of Justice and Security, Netherlands, Coordinated Vulnerability Disclosure: the Guideline, October 2018, S. 5.
[90] ENISA - European Union Agency for Network and Information Security, 2015. Good Practice Guide on Vulnerability Disclosure, From challenges to recommendations, DOI 10.2824/610384, S. 24.

Die CEPS Task Force zu Software Vulnerability Disclosure in Europe fordert die Europäische Kommission und die EU-Mitgliedsstaaten dazu auf, gemeinsam einen Rahmen auf europäischer Ebene zu entwerfen, der durch nationale Gesetzgebung in Übereinstimmung mit den in ISO/IEC 29147 und ISO/IEC 30111 definierten Empfehlungen ergänzt wird, um rechtliche Klarheit für die Entdeckung und Offenlegung von Softwareschwachstellen zu schaffen.[91]

4.3 Abwägungen beim Offenlegungsprozess und andere Arten der Offenlegung

Neben rechtlichen Verpflichtungen, wie bspw. gem. Art. 33, 34 DSGVO, bietet die Offenlegung (Disclosure) unabhängig von der gewählten Art die folgenden Vorteile:

- Systemadministratoren werden in die Lage versetzt, entsprechende Schutzmaßnahmen zu treffen[92]
- Technische Details können genutzt werden um Defensivmaßnahmen zu entwickeln
- Programmierer*innen können zukünftig vergleichbare Fehler vermeiden
- Hersteller*innen werden motiviert, Sicherheitslücken zeitnah zu beheben und insgesamt mehr in IT-Sicherheit zu investieren um negative Berichterstattung oder Haftungsrisiken zu vermeiden

Full Disclosure: Vor über 10 Jahren schrieb der bekannte Kryptograph Bruce Schneier, dass „die vollständige Offenlegung eine verdammt gute Idee ist".[93] Der Begriff „Full Disclosure" ist nicht klar definiert und darin liegt ein Großteil des Problems. Er kann damit umschrieben werden, „so viele Informationen über System-Schwachstellen und Angriffswerkzeuge wie möglich zu verbreiten, so dass potenzielle Opfer so gut informiert sind wie diejenigen, die sie angreifen".[94] Um anderen dabei zu helfen die Schwachstelle zu reproduzieren, wurden oft vollständige technische Details einschließlich eines Proof-of-Concept-Codes veröffentlicht, womit aber auch die Gefahr der Ausnutzung steigt, bevor ein Patch bereitsteht.[95] Zusätzlich zu den oben genannten, bietet Full Disclosure die folgenden Vorteile:

- Durch die sofortige und vollständige Information gibt es keine Personen mit Wissensvorsprung
- Senkung des Missbrauchspotentials bei bereits in Verwendung befindlichen bzw. von Dritten zuvor gefundenen Lücken

Auch wenn das Konzept die Benachrichtigung des Produktverantwortlichen nicht ausschließt, liegt der Hauptkritikpunkt in der geringen Zeitspanne, die eine umgehende Full Disclosure für die Problembehebung belässt.[96]

No Disclosure: Eine „Politik der Geheimhaltung" bedeutet, die Informationen über die Schwachstellen geheim zu halten, sodass weder die Öffentlichkeit, noch der/die Produktverantwortliche davon erfährt. Der

[91] Pupillo/Ferreira/Varisco, Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges, Report of a CEPS Task Force June 2018, S. v.
[92] Je nach Sicherheitslücke können auch ohne Verfügbarkeit eines Patches Sicherheitsmaßnahmen ergriffen werden, wie bspw. Konfigurationen zu ändern oder Dienste temporär einzuschränken oder abzuschalten.
[93] Schneier, Full Disclosure of Security Vulnerabilities a 'Damned Good Idea', 2007 abrufbar unter https://www.schneier.com/essays/archives/2007/01/schneier_full_disclo.html (zuletzt abgerufen am 13.05.2020).
[94] Zurückgehend auf Jay Heiser, zitiert in: Shepherd, How do we define Responsible Disclosure? SANS Institute Information Security Reading Room, 2003, S. 3
[95] Shepherd, How do we define Responsible Disclosure? SANS Institute Information Security Reading Room, 2003, S. 7.
[96] Shepherd, How do we define Responsible Disclosure? SANS Institute Information Security Reading Room, 2003, S. 8; Cavusoglu/Cavusoglu/Raghunathan, Emerging Issues in Responsible Vulnerability Disclosure, WEIS. 2005, S. 2.

Hauptfehler dieses Denkens ist der Glaube, dass die Informationen kontrolliert werden können.[97] Erfahrungsberichte weisen darauf hin, dass erst die Gepflogenheit Details zu den Schwachstellen zu veröffentlichen, Anreize für verantwortliche Unternehmen setzte, Sicherheitslücken zu beheben.[98] Es hat sich eine Art Konsens entwickelt, dass ein besserer Informationsaustausch gesellschaftlich vorteilhaft ist.[99] Neben der (oft falschen) Hoffnung, dass eine geheim gehaltene Sicherheitslücke nicht ausgenutzt werden wird, kann ein weiteres Argument für Non Disclosure der zu erwartende Aufwand für den/die Entdecker*in sein. Die Kommunikation mit der/dem produktverantwortlichen Hersteller*in erfordert einen Zeitaufwand, für den oft keine Gegenleistung erbracht wird. Außerdem können mögliche Non Disclosure Agreements oder potenzielle Interessenskonflikte für Non Disclosure sprechen. Ebenso kann die begründete Angst vor rechtlichen Konsequenzen dazu führen, dass sich der/die Entdecker*in für Non Disclosure und damit gegen die Meldung der Schwachstelle bei der Hersteller*in (oder einer anderen geeigneten Stelle) entscheidet. Die Forschung hat gezeigt, dass weder Full Disclosure noch Non Disclosure optimal ist.[100]

Andere Definitionen sehen das ausschließliche Informieren der Hersteller*innen auch als Non Disclsoure. Wir behandeln diesen Fall im Abschnitt Limited Disclosure.[101]

Limited Disclosure: Hier wird nur eine ausgewählte Gruppe über die Schwachstelle informiert, in der Regel der/die Hersteller*in, sonstige Produktverantwortliche*n und evtl. ein/eine Koordinator*in. Die Öffentlichkeit wird bloß über die Existenz einer Sicherheitslücke in einem Produkt bzw. System informiert, ohne dass technische Details preisgegeben werden.[102] Dieses Modell beinhaltet allerdings die Gefahr, dass Produktverantwortliche entscheiden, Lücken bspw. aus Kostengründen oder fehlendem wirtschaftlichen Interesse nicht, oder nur mit erheblichem zeitlichen Verzug zu schließen und damit sowohl die Gefahr für die Rechtsgüter der Produktnutzenden zu verlängern als auch die Forschungsarbeiten hinauszögern.[103] Die Zurückhaltung technischer Details kann verhindern, dass Betroffene effektive Schutzmaßnahmen umsetzen und Programmierer künftiger Produkte aus der Schwachstelle lernen können.[104] Im Einzelfall können allerdings Konstellationen auftreten wie leicht behebbare operative Schwachstellen (z.B. Fehlkonfigurationen von Routern, Schwachstellen von Websites etc.), die keine öffentliche Bekanntgabe erfordern.[105]

4.4 Aspekte in Coordinated Vulnerability Disclosure (CVD)

Sind mit dem/der Finder*in der Sicherheitslücke und dem Produktverantwortlichen nur zwei Parteien am Prozess beteiligt, lässt sich der Kommunikationsprozess theoretisch leicht organisieren (Siehe 4.1). In der Praxis stellen sich dagegen oftmals wesentliche Herausforderungen und Abwägungen, die getroffen werden müssen:

---

[97] Shepherd, How do we define Responsible Disclosure? SANS Institute Information Security Reading Room, 2003, S. 6. Vgl. Hierzu auch die Gefahren der Parallelentdeckungen in Abschnitt 6.2.1.

[98] Bruce Schneier, Full Disclosure of Security Vulnerabilities a 'Damned Good Idea', 2007 abrufbar unter https://www.schneier.com/essays/archives/2007/01/schneier_full_disclo.html (zuletzt abgerufen am 13.05.2020); Böhme, A Comparison of Market Approaches to Software Vulnerability Disclosure, proceedings of ETRIC - International Conference on Emerging Trends in Information and Communication Security 2006, 298 (299 f.).

[99] Böhme, A Comparison of Market Approaches to Software Vulnerability Disclosure, proceedings of ETRIC 2006, 298 (298).

[100] Pupillo/Ferreira/Varisco, Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges, Report of a CEPS Task Force June 2018, S. 5.

[101] Shepherd, How do we define Responsible Disclosure? SANS Institute Information Security Reading Room, 2003, S. 6.

[102] Shepherd, How do we define Responsible Disclosure? SANS Institute Information Security Reading Room, 2003, S. 8.

[103] Cavusoglu/Cavusoglu/Raghunathan, Emerging Issues in Responsible Vulnerability Disclosure, WEIS. 2005, S. 2.

[104] Shepherd, How do we define Responsible Disclosure? SANS Institute Information Security Reading Room, 2003, S. 8 f.

[105] Pupillo/Ferreira/Varisco, Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges, Report of a CEPS Task Force June 2018, S. 5.

4.4.1 Identifikation der Ansprechpartner

Beim Limited Disclosure, Coordinated Disclosure (und je nach Ausgestaltung, auch bei anderen Arten) ist es erforderlich, diejenige Stelle über die betreffende Sicherheitslücke zu informieren, die in der Position ist, diese zu behandeln und zu beheben. Die Identifikation der jeweiligen Ansprechpartner*innen ist ein zweistufiger Prozess.

Zunächst müssen die jeweiligen Hersteller*innen oder Betreiber*innen des Produkts identifiziert werden. Insbesondere im Rahmen von Lieferketten, unterschiedlichen Hersteller*innen von Komponenten, Anbieter*innen und Systembetreiber*innen kann es mitunter Schwierigkeiten bereiten, die richtige Organisation zu identifizieren. Bei komplexeren Produkten kann eine Sicherheitslücke in einer Komponente nicht nur für das untersuchte Produkt, sondern für eine Vielzahl von anderen Produkten relevant sein, daher ist es wichtig, den/die Hersteller*in der Komponente zu identifizieren, damit das Sicherheitsproblem möglichst an der Wurzel gelöst wird. Sind mehrere Stellen von einer Sicherheitslücke betroffen, kann es erforderlich werden einen „Multiparty CVD“ durchzuführen. Das Forum of Incident Response and Security Teams (FIRST) hat Leitlinien für die Koordination und Offenlegung von Sicherheitslücken, die mehrere Parteien betreffen, veröffentlicht.[106]

Ist oder sind die betroffenen Organisationen identifiziert, so müssen diese jeweils kontaktiert werden. Oft handelt es sich bei Sicherheitslücken um technisch komplexe Zusammenhänge, die nur von Fachleuten korrekt eingeschätzt werden können. Je nach Schwere der Lücke muss (in den meisten Disclosure Verfahren) außerdem sichergestellt werden, dass diese nicht Unbefugten bekannt wird. Aus diesen Gründen ist es meist nicht sinnvoll, die Sicherheitslücke an eine beliebige Kontaktadresse der Organisation zu melden. Insbesondere Support Hotlines sind nicht geeignet, da die Mitarbeiter oft die Relevanz des Anliegens nicht einschätzen können und den Fall nicht an die zuständige Fachabteilung weiterleiten. In vielen Fällen sind die für IT-Sicherheitsanliegen zuständigen Ansprechpersonen nicht öffentlich bekannt. Vorgeschlagene Best-Practices[107] für das Hinterlegen von dedizierten Sicherheitskontakten werden zwar von einigen großen US-Tech Konzernen umgesetzt, haben sich aber noch nicht flächendeckend durchgesetzt. Beispiele von bekannten Sicherheitsforschern zeigen, dass auch diese oft Schwierigkeiten haben, die richtige Kontaktperson zu identifizieren.[108]

4.4.2 Mitwirkung der Produktverantwortlichen

Das bestmögliche Ergebnis erzielt der CVD, wenn Produktverantwortliche an der Behebung der Schwachstelle mitwirken. Pflichten für Unternehmen ergeben sich derzeit eher mittelbar, bspw. über die Produktbeobachtungspflichten im Rahmen der Produzentenhaftung nach § 823 Abs. 1 BGB oder vertragliche Mängelgewährleistungsrechte. Kommt es durch einen Produktfehler zu einem Datenverlust, Personen- oder Sachschaden, können Geschädigte Schadensersatzansprüche geltend machen, wenn der/die Produkthersteller*in auf

[106] FIRST - Forum of Incident Response and Security Teams, Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure, Version 1.1, 2020, abrufbar unter: https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.1 (zuletzt abgerufen am 13.05.2020).

[107] https://securitytxt.org/ (zuletzt abgerufen am 11.10.2021).

[108] Siehe bspw: https://twitter.com/taviso/status/676568269680074753; https://twitter.com/troyhunt/status/1313638775755481088 (zuletzt abgerufen am 11.10.2021).

Warnungen und Hinweise zum Fehler nicht in angemessener Weise reagiert hat.[109] Im Rahmen des Vertragsrechts wurden die Rechte der Verbraucher*innen durch eine Anpassung des Sachmangelbegriffs sowie expliziter Updatepflichten gestärkt, welche Auswirkungen darauf haben, ob das Produkt als nicht vertragsmäßig reklamiert werden kann.[110] Vielfach kommt es aber dazu, dass die Hersteller*innen oder anderweitig Verantwortliche kein Interesse am Beheben der Sicherheitslücke haben und nicht am Prozess mitwirken (siehe dazu auch Abschnitt 7.3).

4.4.3 Fristsetzung

Produktverantwortliche sollten vor Veröffentlichung der Sicherheitslücke eine angemessene Zeitspanne zur Behebung der Lücke erhalten. Als sinnvolle Zeitspannen werden bspw. zwischen 30,[111] 45[112] 90[113] oder 120 Tagen[114] vorgeschlagen. Je nach Art der Sicherheitslücke, Risiko für die Allgemeinheit sowie Mitwirkung der verantwortlichen Stelle, sollte diese Frist erweitert oder verkürzt werden (Eine Diskussion zur technischen Behebung von Sicherheitslücken findet sich auch in 7.2.2). Sind Tatsachen bekannt, dass die Lücke bereits ausgenutzt wird, müssen die Informationen umgehend bereitgestellt werden. Eine Deadline sollte nicht auf unbestimmte Zeit verlängert werden können.[115] (Siehe dazu auch Abschnitt 7.3.1)

4.4.4 Informationsbereitstellung

Auch die Presse kann eine essenzielle Rolle bei der Verbreitung der Informationen bezüglich aufgedeckter Schwachstellen einnehmen.[116] Vertreter*innen entsprechender Fachmedien verfügen oftmals über ein hohes Maß an Wissen und Fachkenntnissen und sind dadurch gut in der Lage, über ein Thema präzise zu berichten. Kritisiert wird hingegen, wenn die Medienberichterstattung einen Hype um eine Schwachstelle erzeugt, der die Information zu technischen Merkmalen der Schwachstelle überschatten und als solche die Öffentlichkeit und andere Interessengruppen unnötig beunruhigen kann.[117] Der positive Einfluss der Medien besteht darin, die Aufmerksamkeit auf die Informationssicherheit im Allgemeinen und zu lenken. Dabei kann diese Art der Berichterstattung Druck auf die Verantwortlichen ausüben, die Behebung von Sicherheitslücken ernst zu

[109] Zu den Produktbeobachtungspflichten: Rockstroh/Kunkel, MMR 2017, 77 (80); Spindler, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären Studie im Auftrag des BSI 2007, Rn. 128; Sprau, in: Palandt, BGB § 823 Rn. 175; BGH, Urteil vom 17. 03. 1981 – VI ZR 286/78 –, BGHZ 80, 199–205; BGH, Urteil vom 17. 10. 1989 – VI ZR 258/88, Rn. 27.

[110] Die Reform greift ab dem 01.01.2022, siehe: Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, vom 25. Juni 2021, Bgbl. 2021 Teil I Nr. 37, 2123 ff.; Gesetz zur Regelung des Verkaufs von Sachen mit digitalen Elementen und anderer Aspekte des Kaufvertrags, Bgbl. 2021 Teil I Nr. 37, 2133 ff.

[111] Shepherd, How do we define Responsible Disclosure? SANS Institute Information Security Reading Room, 2003, S. 9.

[112] CERT, Vulnerability Disclosure Policy, FAQ, abrufbar unter: https://vuls.cert.org/confluence/display/Wiki/Vulnerability+Disclosure+Policy (zuletzt abgerufen am 13.05.2020).

[113] Project Zero, abrufbar unter: https://googleprojectzero.blogspot.com/2015/02/feedback-and-data-driven-updates-to.html (zuletzt abgerufen am 13.05.2020).

[114] Zero Day Initiative (ZDI), Disclosure Policy, abrufbar unter: https://www.zerodayinitiative.com/advisories/disclosure_policy/ (zuletzt abgerufen am 13.05.2020).

[115] IETF – Internet Engineering Task Force, Draft Responsible Vulnerability Disclosure Process draft-christey-wysopal-vuln-disclosure-00.txt, abrufbar unter: https://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00 (zuletzt abgerufen am 13.05.2020); Shepherd, How do we define Responsible Disclosure? SANS Institute Information Security Reading Room, 2003, S. 9.

[116] ENISA - European Union Agency For Network And Information Security, 2015. Good Practice Guide on Vulnerability Disclosure, From challenges to recommendations, DOI 10.2824/610384, S. 22.

[117] ENISA - European Union Agency For Network And Information Security, 2015. Good Practice Guide on Vulnerability Disclosure, From challenges to recommendations, DOI 10.2824/610384, S. 23.

nehmen. Der zweite Aspekt ist die Fähigkeit der Medien, die Öffentlichkeit zu informieren, wenn eine Schwachstelle Maßnahmen seitens der Endbenutzenden erfordert, wie z.B. die Installation eines Patches.[118]

Zusätzlich zur Presse kann es sinnvoll sein, weitere Dritte im Rahmen der Veröffentlichung einzubeziehen. Hierfür kommen beispielsweise die Datenschutzaufsichtsbehörden, fachspezifische Behörden (z.B. Bundesinstitut für Arzneimittel und Medizinprodukte) oder Interessensverbände von Nutzern in Frage.

[118] ENISA - European Union Agency For Network And Information Security, 2015. Good Practice Guide on Vulnerability Disclosure, From challenges to recommendations, DOI 10.2824/610384, S. 23.

5 Risikobewertung von Schwachstellen

Michael Kreutzer / Linda Schreiber

5.1 Schaden am Gemeinwohl durch das Horten von Schwachstellen

Die Sicherheit von IT-Systemen ist von entscheidender Bedeutung. Ausfälle von IKT im Bereich der kritischen Infrastrukturen können eine unmittelbare Bedrohung für die Umwelt und sogar Menschenleben darstellen[119], Cyber-Angriffe verursachen erhebliche wirtschaftliche Schäden und ermöglichen den Diebstahl von geistigem Eigentum sowie Spionage und Erpressung von staatlichen Institutionen, Unternehmen[120], Privatpersonen[121] und nichtstaatlichen Organisationen. Umgekehrt werden sichere, vertrauenswürdige und zuverlässige IT-Systeme als Voraussetzung für eine gemeinwohlorientierte Digitalisierung und als Grundlage für die Förderung von Grundfreiheiten und demokratischen Werten im Cyberraum gesehen.[122]

Betrachtet man nicht nur die Bedeutung von IT-Sicherheit im Allgemeinen, sondern insbesondere den Umgang mit Schwachstellen, so sind Erkenntnisse über Schwachstellenmärkte zu berücksichtigen. Märkte für nicht behobene, Zero-Day-Schwachstellen und Malware sind in den letzten Jahren erheblich gereift. Auf diesen schwarzen und grauen Märkten werden Schwachstellen unter der Annahme gehandelt, dass das Wissen über die Schwachstelle exklusiv ist und nicht an den/die Hersteller*in bzw. Produktanbieter*in weitergegeben wird - oft zu böswilligen Zwecken wie Cyberangriffen.[123]

Im Vergleich dazu argumentieren politische und staatliche Akteur*innen, dass das Horten von Schwachstellen notwendig sei, beispielsweise zur Strafverfolgung und Terrorismusbekämpfung. Dies führt jedoch zu einer Marktwirtschaft des Kaufs und Verkaufs von Informationen über Schwachstellen zwischen kriminellen Gruppen, Unternehmen und Regierungen. Allerdings kann kein/e Akteur*in sicher sein, dass er alleinig von der Existenz einer Schwachstelle weiß. Die Wahrscheinlichkeit von unabhängigen Parallelentdeckungen durch andere kann nie ausgeschlossen werden und steigt mit der Zeit.[124]

Diese Situation ist vergleichbar zur Tragik der Allmende, bei der die Sicherheit des Cyberraums, ggf. im jeweils nationalen Interesse, auf Kosten des Gemeinwohls gemindert wird.[125]

---

[119] Robles/Perlroth, Dangerous Stuff: Hackers Tried to Poison Water Supply of Florida Town, New York Times, 08. Februar 2021, https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html (zuletzt abgerufen am 03.04.2021).

[120] Bitkom, Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie, Studienbericht 2018, https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf (zuletzt abgerufen am 09.08.2021).

[121] Zu den Risiken für Privatpersonen bei Verletzungen der Schutzziele von Vertraulichkeit und Integrität informationstechnischer Systeme siehe auch BVerfG, Urteil vom 27. 2. 2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 (824).

[122] Europäische Kommission, Neue Cybersicherheitsstrategie der EU und neue Vorschriften zur Erhöhung der Widerstandsfähigkeit kritischer physischer und digitaler Einrichtungen, 16. Dezember 2020, https://ec.europa.eu/commission/presscorner/detail/de/IP_20_2391 (zuletzt abgerufen am 09.08.2021).

[123] Schneier, The Vulnerabilities Market and the Future of Security, Forbes, 31. Mai 2012 https://www.forbes.com/sites/bruceschneier/2012/05/30/the-vulnerabilities-market-and-the-future-of-security/?sh=50aa5c5e7536 (zuletzt abgerufen am 23.04.2021).

[124] Herr/Schneier/Morris, Taking Stock: Estimating vulnerability rediscovery, Belfer Cyber Security Project White Paper Series 2017.

[125] Schulze/Reinhold, Wannacry about the tragedy of the commons? Game-theory and the Failure of global vulnerability disclosure. European Conference on Information Warfare and Security, ECCWS. 2018.

Jede nicht geschlossene Schwachstelle ist ein Risiko. Jede gehortete und verborgene Schwachstelle stellt darüber hinaus ein potenziell unwägbares Risiko dar. Aus diesen Gründen sind alle Schwachstellen vorbehaltlos und ausnahmslos zu schließen sowie zu veröffentlichen, und zwar zum Zeitpunkt minimierten Risikos nach einer Risikoabwägung durch die Publikation.

5.2 Risikobewertung auf Basis anerkannter Metriken und Umgebungsparameter

Die koordinierte Offenlegung von Schwachstellen umfasst den gesamten Prozess von der Entdeckung einer Schwachstelle bis hin zum Einsatz von Abhilfemaßnahmen. Durch das Vorgehen entsprechend dem Coordinated Vulnerability Disclosure (CVD) soll grundsätzlich das Risiko, das von der Möglichkeit der Ausnutzung einer Schwachstelle ausgeht, minimiert werden.

Als Schwachstelle kann grundsätzlich ein Funktionsverhalten eines Produktes oder einer Dienstleistung verstanden werden, dass eine explizite oder implizite Sicherheitsrichtlinie verletzt.[126] Im Angreifermodell ist eine Schwachstelle eine unerwünschte, unbeabsichtigte und ausnutzbare Eigenschaft von Soft- oder Hardware, die es Angreifern ermöglicht, Aktionen auszuführen, die ihnen ansonsten nicht zur Verfügung stehen würden.[127]

Soft- und Hardwaretests sowie Scans können eine große Anzahl an Schwachstellen (weaknesses) aufzeigen. Dabei stellt nicht jede Schwachstelle eine ausnutzbare Verwundbarkeit (vulnerability) dar, von der direkte Sicherheitsrisiken ausgehen. Die Bewertung der Schwachstelle und eben jener Risiken spielt beim Umgang mit Schwachstellen, etwa der Priorisierung von Aktivitäten auf Herstellerseite, der Form und dem Zeitpunkt der Veröffentlichung von Informationen zur Schwachstelle sowie der Art der Abhilfemaßnahmen, eine entscheidende Rolle. Abhilfemaßnahmen reichen von der Minderung der Wahrscheinlichkeit oder Auswirkungen von Angriffen bzw. Ausnutzen der Schwachstelle (eventuell mit vermindertem Nutzen/Effizienz/Effektivität des Produktes oder Dienstes) bis hin zum vollständigen Beseitigen durch Patches/Updates. Auf Nutzerseite hilft die Risikobewertung wiederum bessere Entscheidungen hinsichtlich des Schutzes der Systeme und Daten, der Maßnahmen zur Behebung und möglicherweise Ausgaben für IT-Sicherheitsmaßnahmen zu treffen.[128]

Wenn Sicherheitsforschende eine erste Risikobewertung - auf Basis allgemein anerkannter Metriken und Umgebungsparameter - zusammen mit der Schwachstellenmeldung an Hersteller*innen übermitteln, dann kann die CVD in der Regel effektiver und effizienter durchgeführt werden als ohne.

Die ISO/IEC 29147:2018 empfiehlt die Nutzung des Common Vulnerability Scoring System (CVSS).[129] Dieses System liegt auch bei der Vergabe von CVE-Einträgen zu Grunde. Der CVSS Score geht von 0 bis 10 und unterteilt sich in die *severity ratings low*, *medium*, *high* und *critical*.

Der CVSS Sore setzt sich aus drei Metrik-Gruppen zusammen: der *Base metric group*, *Temporal metric group* und *Environmental metric group*. In der Regel wird nur der Wert der *Base metric group* veröffentlicht, da dieser sich im Laufe der Zeit nicht ändert. Dieser kann sowohl vom Herstellenden des Produkts, das die Verwundbarkeit enthält, ermittelt werden, wie auch von einer externen Partei. Nutzer des verwundbaren Produkts können den *Base Score* durch die anderen Metriken ergänzen, um eine spezifische zeitliche und umgebungsbezogene Bewertung entsprechend für das jeweilige organisatorische Umfeld durchzuführen.

[126] ISO/IEC 29147:2018.
[127] Householder/Wassermann/Manion/King, The CERT Guide to Coordinated Vulnerability Disclosure. Carnegie Mellon University, August 2017, S. 2.
[128] ISO/IEC 29147:2018, Introduction/ Kap. 1.
[129] ISO/IEC 29147:2018, Kap. 7.4.11.

Die Metriken aus der *Base metric group* umfassen intrinsische Merkmale der Schwachstelle, die unabhängig von äußeren Einflussfaktoren sind. Dazu gehören *Exploitability metrics*, die sich darauf beziehen, wie leicht und mit welchen technischen Mitteln sich eine Schwachstelle ausnutzen lässt; *Impact metrics* spiegeln die direkten Auswirkungen und Konsequenzen eines *exploits* wider und *scope metric* messen die Auswirkungen auf andere Komponenten/Systeme als der anfälligen Komponente.

Die *Temporal metric group* umfasst Charakteristiken, die sich über die Zeit ändern können, wie beispielsweise die Verfügbarkeit von Patches oder Exploit-Kits. Die *Environmental metric group* bezieht sich auf die spezifische Umgebung des jeweiligen Nutzers, wie beispielsweise das Vorhandensein von Sicherheitsmechanismen oder die Bedeutung des verwundbaren Systems in der Gesamtinfrastruktur der jeweiligen Organisation.[130]

Der CVSS Wert sollte allerdings nicht als alleiniger Indikator zur Risikobewertung herangezogen werden. Um eine umfassende Risikobewertung vorzunehmen, müssen insbesondere auch kontextbezogene Attribute hinzugezogen werden. Diese werden zwar zum Teil durch die CVSS-Temporal und –Environment Metriken erfasst und können bei Veränderungen erneut ermittelt werden, allerdings muss immer auch die spezifische Bedrohungs- und Gefährdungslage betrachtet werden, die außerhalb des Anwendungsbereichs von CVSS liegt.[131]

Ein weiteres System, welches bei der Bewertung von Schwachstellen hilft, ist das *Common Weakness Enumeration* System. Dabei handelt es sich um eine *community*-erarbeitete Liste von Schwachstellentypen in Hard- und Software, die zur besseren Kommunikation, als Maßstab für Sicherheitstools, Grundlage für die Identifizierung von Schwachstellen sowie für Maßnahmen zur Abschwächung und Prävention dient.[132] Die Schwachstellen werden in Baumstruktur auf verschiedenen Abstraktionslevel dargestellt. Die Darstellung umfasst neben einer ausführlichen Beschreibung des Schwachstellentyps die Beziehung zu anderen Schwachstellentypen, typische Auswirkungen und Beispiele, zum Teil mit Verlinkung auf entsprechende CVE Einträge[133]. Auf Basis der Anzahl und des Schweregrads von zugeordneten CVE Einträgen wird eine „CWE Top 25 Most Dangerous Software Weaknesses“-Liste erstellt, die Entwicklern, Testern, Anwendern sowie Sicherheitsforschenden einen Einblick in die schwerwiegendsten und aktuellen Sicherheitsschwachstellen geben soll.[134] CWE verfügt ebenfalls über ein Scoring System (Common Weakness Scoring System, CWSS), welches in Ergänzung zum CVSS genutzt werden kann. CWSS soll im Unterschied zu CVSS nicht erst auf bereits verifizierte Schwachstellen Anwendung finden, sondern schon zu einem früheren Zeitpunkt, beispielsweise bei automatisierten Code-Scans zur Priorisierung von Funden beitragen.[135]

Ein anderer Indikator für die Bewertung des Schweregrads einer Schwachstelle ist deren Wert auf schwarzen oder grauen Märkten. Plattformen, wie Zerodium (zerodium.com) zahlen hohe Beträge an Personen, die der Plattform (zero-day) Schwachstellen und Exploits übermitteln. Die öffentliche Übersicht zu möglichen Rewards für eingereichte Schwachstellen auf der Seite zeigt, dass insbesondere Schwachstellen, die bei mobilen Betriebssystemen einen *full chain* Exploit ohne Nutzerinteraktion erlauben bzw. bei Desktop und Server

[130] Common Vulnerability Scoring System v3.1: Specification Document, https://www.first.org/cvss/v3.1/specification-document (zuletzt abgerufen am 25.09.2021).
[131] Common Vulnerability Scoring System v3.1 User Guide, 2.1. https://www.first.org/cvss/v3.1/user-guide (zuletzt abgerufen am 21.09.2021).
[132] Mitre Common Weakness Enumeration, https://cwe.mitre.org/about/index.htm (zuletzt abgerufen am 15.08.2021).
[133] Common Vulnerabilities and Exposures im Rahmen der National Vulnerability Database (NVD) https://nvd.nist.gov/vuln/full-listing (zuletzt abgerufen am 15.08.2021).
[134] 2020 CWE Top 25 Most Dangerous Software Weaknesses https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html (zuletzt abgerufen am 15.08.2021).
[135] Common Weakness Scoring System, https://cwe.mitre.org/cwss/cwss_v1.0.1.html (zuletzt abgerufen am 11.10.2021).

Betriebssystemen eine *remote code execution* oder Privilegien-Eskalation in Windows oder Linux Umgebungen erlauben, von hohem Wert sind.[136]

5.3 Empfehlungen für die Meldung von Schwachstellen an Hersteller*innen

Der Wert und die Vorteile, den die Meldung von Schwachstellen in IT-Produkten durch externe Sicherheitsforschende den Hersteller*innen dieser Produkte bieten ist vielen, hauptsächlich größeren, Unternehmen bewusst. Dementsprechend haben viele Unternehmen sichere Meldewege, Prozesse oder gar Reward Programme[137] definiert, die die Meldung und den Umgang mit Schwachstellen von externen Entdecker*innen regeln.[138] Manche Unternehmen arbeiten mit Plattformen wie HackerOne zusammen, die bei der Koordinierung von Schwachstellenmeldungen bzw. der Kommunikation zwischen Sicherheitsforschenden und Unternehmen sowie der Durchführung von Bug Bounty Programmen unterstützen.[139]

Grundsätzlich helfen veröffentlichte Policies und Prozesse sowohl auf Seite der Hersteller*innen als auch auf Seite der Entdeckenden, um ein berechenbares Vorgehen zu demonstrieren und damit einen möglichst reibungslosen Meldeprozess zu vollziehen. Diese veröffentlichten Dokumente können unterschiedlich ausgestaltet sein, beispielsweise auch als grundsätzlicher Code of Ethics.[140]

Ein anderes Beispiel ist die Initiative security.txt. Dabei handelt es sich um einen Vorschlag für einen Internetstandard, der es Meldenden erleichtern soll, Schwachstellen von Webdiensten an Einrichtungen zu kommunizieren. Dieser Standard schreibt eine Textdatei namens „security.txt“ vor, die sich an einem festen Ort einer Webseite befindet und deren Syntax formal definiert ist (analog robots.txt) und zugleich von Menschen gelesen werden kann. Die Datei „security.txt“ gibt an, wer wegen Sicherheitsproblemen kontaktiert werden kann und wie der Meldeweg aussieht.[141]

In der Praxis bestehen verschiedene Aspekte und Dynamiken, die erfolgreiche CVD Prozesse erschweren oder verhindern. Sicherheitsforschende werden in vielen Fällen, in denen sie an Unternehmen mit einer gefundenen Sicherheitslücke herantreten, von diesen nicht ernst genommen oder ihnen wird sogar drohend oder feindselig begegnet. Häufig ist die Kommunikation mit Unternehmen auch mangelhaft und stockend. Hierfür lassen sich in der Praxis verschiedene Gründe identifizieren:

- Es fehlt an Ansätzen, mit denen Entscheidungstragende die spezifischen Schäden, Auswirkungen und Risiken von Schwachstellen induzierten Sicherheitsvorfällen oder der spezifische Nutzen von CVD für das jeweilige Unternehmen bewusst gemacht werden.
- Kleine und mittlere Unternehmen (KMU) scheinen eine Umsetzungslücke bei organisatorischen IT-Sicherheitsmaßnahmen zu haben, die auf eine fehlende Verknüpfung mit der C-Ebene zurückgeführt wird.[142]

---

[136] Zerodium Exploit Acquisition Program http://zerodium.com/program.html (zuletzt abgerufen am 11.10.2021).
[137] Bspw. das Google Vulnerability Reward Program https://www.google.com/about/appsecurity/reward-program/index.html (zuletzt abgerufen am 23.07.2021).
[138] Bspw. SAP, Disclosure Guidelines for SAP Security Advisories https://wiki.scn.sap.com/wiki/display/PSR/Disclosure+Guidelines+for+SAP+Security+Advisories (zuletzt abgerufen am 26.08.2021).
[139] Hackerone https://www.hackerone.com/ (zuletzt abgerufen am 09.08.2021).
[140] Vgl. usd AG, Code of Ethics https://herolab.usd.de/code-of-ethics/
[141] Foudil/Shafranovich, A file Format to Aid in Security Vulnerability Disclosure (11.03.2021) https://datatracker.ietf.org/doc/html/draft-foudil-securitytxt-11 (zuletzt abgerufen am 15.06.2021).
[142] Hillebrand et al. Aktuelle Lage der IT-Sicherheit in KMU. Kurzfassung der Ergebnisse der Repräsentativbefragung, Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste, 2017, S. 55

- Es gibt Bedenken hinsichtlich hoher Kosten für die Bearbeitung von Schwachstellenmeldungen.[143]
- Die Tatsache, dass jede Hard- und Software Schwachstellen enthält, wird nicht in jedem Unternehmen erkannt und ist nicht Teil einer gelebten „Fehlerkultur".

Folgende fünf Regeln sollten als Minimalkonsens für Entdeckende und Herstellende gelten:

(1) Schwachstellen müssen unter allen Umständen an die Stellen gemeldet werden, die sie beheben oder die Behebung erzwingen können - in der Regel sind dies die Hersteller*innen oder das Unternehmen, das die Schwachstelle oder die Fehlkonfiguration hat oder verursacht hat.
(2) Die Meldung muss so schnell wie möglich erfolgen und insbesondere dürfen keine Interessen Dritter die Ursache für eine Verzögerung der Meldung durch die Entdeckende sein.
(3) Die Stelle, an die die Schwachstellen gemeldet wurden, muss die Abhilfemaßnahme so schnell wie möglich entsprechend dem Risiko bereitstellen. Insbesondere dürfen keine Interessen Dritter der Grund für eine Verzögerung bei der Suche nach der Behebung oder Entschärfung sein.
(4) Die Abhilfemaßnahmen müssen so einfach wie möglich anzuwenden und leicht zugänglich sein.
(5) Die Entdeckenden dürfen die Schwachstelle nach einer plausiblen Zeitspanne nach der Behebung der Schwachstelle veröffentlichen und können so zumindest eine gewisse Anerkennung erhalten. Bug Bounties dürfen verwendet werden, solange sie den vorherigen Aussagen nicht widersprechen.

[143] Al-Banna/Bentallah/Schlagwein/Barukh/Bertino, Friendly Hackers to the Rescue: How Organizations Perceive Crowdsourced Vulnerability Discovery. PACIS 2018

6 Die Sicherheitsforschung: Fundamente, Bedeutung und Rolle im internationalen Vergleich

6.1 Eine sehr kurze Geschichte der Sicherheitsforschung

Roman Dickmann

> „If there's anything we've learned about IT security in recent years, it's that successful attacks are inevitable."
>
> Bruce Schneier[144]

Die junge Querschnittsdisziplin der IT-Sicherheitsforschung befasst sich vor allem mit dem Schutz vor An- und Eingriffen auf IT-Systeme in der modernen vernetzten Welt. In den Anfängen der 1960er Jahre ging es eher um die Betriebs- und Funktionssicherheit, also den Schutz der Sachsubstanz und vor Personenschäden. Mit der zunehmenden Dominanz von Software etwa zur Definition und Steuerung von Hardware-Funktionalitäten ist deren Absicherung über den Quellcode, also solchem mit möglichst wenigen ausnutzbaren Schwachstellen, in den Mittelpunkt getreten.

Erst in den 1970er Jahren entwickelte sich Software von einer weitgehend quelloffenen Zugabe zur Hardware bzw. selbst programmierten Arbeitsmittel zu einem eigenständigen Wirtschaftsgut. Der im folgenden Jahrzehnt statuierte Urheberrechtsschutz führte außerhalb von Open Source und freier Software zu mehr proprietärem Code. Das Thema IT-Sicherheit ist bislang keine Kategorie des Urheberrechts. Die Nutzer*innen von proprietärer Software können regelmäßig nicht den Quellcode einsehen und folglich nicht oder nur sehr eingeschränkt Fehler suchen und berichtigen. IT-Sicherheit wurde zunehmend zu einer Sache blinden Vertrauens. Die Qualität von Code hatte und hat mit Blick auf die produzierte Menge bis heute keine hohe Priorität. Vielmehr ging und geht es gerade bei größeren und zeitkritischen Projekten darum, überhaupt einen lauf- und einsatzfähigen Zustand zu erreichen. Sicherheitsanforderungen blieben daher lange rudimentär. Vielfach wurden und werden sie erst spät in der Projekthistorie gestellt und implementiert. Bis in die 1980er Jahre beschränkten sich Sicherheitsmaßnahmen z.B. auf Passwortschutz und (nachträgliche) Kontrolle des Verhaltens potenzieller Innentäter. Erste akademische Auseinandersetzungen wiesen häufig einen hohen Abstraktionsgrad zu Themen wie Sicherheitskonzepten für (fiktive) Betriebssysteme auf. Die Autor*innen kamen meist aus dem universitären und militärischen Bereich oder Branchen wie dem Finanz- oder sich entwickelnden Computersektor.

Die 1980er Jahre brachten eine Phase, in der sich Schadsoftware über Datenträger verbreitete, was erste Anti-Virus-Lösungen und kontinuierliche Untersuchungen dazu hervorbrachte. In den Blick des deutschen Gesetzgebers gerieten aber erste netzwerkbasierende Hacking-Vorfälle, die zur Einführung des bis heute geltenden materiellen Computerstrafrechts 1986 führten. Dieses stammt also aus der pre-Web-Zeit mit lokal installierten Einzelplatzrechnern und sehr beschränkter Vernetzung von System zu System über das analoge Telefonnetz.

[144] Schneier, Secret & Lies, 15th Anniversary Edition, S. X.

Das auf offenen Protokollen basierende Internet hatte als Nukleus der globalen Vernetzung in seiner Urform nur wenige Sicherheitsmerkmale implementiert. Die meisten wie etwa die Verschlüsselung von Verbindungen wurden nachträglich hinzugefügt. Die resultierenden Probleme sind tiefgreifend und anhaltend. Sie führten zu einem systemischen Vorteil der Angreifer gegenüber den Verteidigern, da erstere nur das schwächste Glied im System oder Netzwerk finden müssen. Die Angreiferperspektive stellte lange Zeit einen blinden Fleck dar. Unter anderem dies, wie auch die Kommerzialisierung online, führte ab Mitte der 1990er Jahre zu einer rasanten Entwicklung internetbasierender krimineller Geschäftsmodelle. Diese reichten vom Betrug bei Zahlungs- und Banktransaktionen über das Unterschieben von Dialern zur Entgeltgenerierung oder unerwünschter Werbung (Spam) bis zum Angebot von Digitalgütern unter Urheberrechtsverstößen.

Um die kriminellen Ziele zu erreichen, wurden und werden häufig Schwachstellen in Betriebssystemen und Anwendungsprogrammen wie Browsern oder Textverarbeitungsprogrammen ausgenutzt. Als Achillesferse erwies sich die fehlende Pflege von Software, die insbesondere in Webanwendungen immer mehr Interaktion und Datenaustausch zuließ. Sicherheitsrelevante Fehler wurden von gutwilligen Entdecker*innen an die Entwickler*innen und Hersteller*innen gemeldet. Der Adressatenkreis zeigte sich jedoch häufig wenig interessiert und ignorierte die Meldungen einfach, denn Sicherheit wurde oft als bloßer Kostenfaktor ohne Verkaufspotenzial angesehen. In der Konsequenz wurden viele Schwachstellen im Internet etwa in Foren oder über Mailinglisten veröffentlicht. Dies erhöhte ab Mitte der 1990er Jahre den Druck gerade auf die immer marktmächtiger werdenden großen Software-Hersteller*innen, die Schwachstellen zu beseitigen. Unter anderem deshalb, aber auch wegen Infektionswellen mit Malware und der Ausbreitung von Bot-Netzen, wurde die IT-Landschaft sensibler für das Thema Sicherheit. Neben Software-Lösungen, wie etwa Firewalls, setzten sich Zyklen für Updates und Patches durch. Die einsetzende technische Monokultur erleichterte aber den Angreifern die Zielauswahl, denn weitverbreitete Software birgt eine höhere Zahl potenzieller Opfer.

In den 2000er Jahren begannen sich langsam Strukturen zur IT-Sicherheitsforschung im universitären Bereich, aber auch der Privatwirtschaft zu etablieren. Dies ging mit der Schaffung von Angeboten für Dienstleistungen zur Beratung, Prüfung aber auch zum Outsourcing von sicherheitsrelevanten Funktionen einher. Auf gesetzgeberischer Ebene führte die Einführung des § 202c StGB zu Verunsicherung und Abschreckung unter IT-Sicherheits-Forschenden und Dienstleistern.

Insbesondere die großen Software-Hersteller*innen erkannten den Wert der für sie kostenlosen Meldungen von Schwachstellen. Diesen Status wollte man sich erhalten und verstand unter verantwortlichem Umgang mit Schwachstellen, die Pflicht der Entdeckenden diese allein dem Verantwortlichen (meist also dem/der Hersteller*in von Software) zu melden, um ihm dann alles Weitere zu überlassen. Dies führte häufig zu ausbleibender Kommunikation mit Meldern oder unverhältnismäßig langen Reaktionszeiträumen. Die Melder*innen verliehen ihrem Ansinnen zur zeitnahen Verbesserung der IT-Sicherheit durch das Setzen von Fristen zur Bereitstellung von Patches/Updates Nachdruck und verlangten nach einem Prozess auf Augenhöhe (Coordinated Disclosure). Für letzteren wurde zur Abbildung im Unternehmen gar ein ISO/IEC-Standard entwickelt. In der Folge begannen Unternehmen Prämien (Bug Bounty) für die Meldung von Schwachstellen auszuloben. Dies war eine (nicht unumstrittene) Reaktion auf stetig steigende Preise insbesondere für langlebige oder besonders verbreitete Systeme betreffende Schwachstellen auf dem Grau- und Schwarzmarkt der IT-Unsicherheit. Als Käufer entsprechender Informationen treten vor allem staatliche Akteure und private Dienstleister, aber auch das Organisierte Verbrechen auf. Vertiefte Erkenntnisse zu diesem Markt gibt es bislang nur wenige.[145]

[145] Vgl. Perlroth, This is how they tell me the world ends (2021).

Nach Aufdeckung der zunehmenden anlasslosen Massenüberwachung des internationalen Datenverkehrs nach dem 11. September 2001 durch Edward Snowden in 2013, rückte staatliches Handeln etwa in Form von Hacking und dem Einsatz von Cyberwaffen auch durch Staaten wie Russland und China wieder stärker in den Fokus. Verschlüsselung erwies sich als taugliches Gegenmittel zum Schutz von (personenbezogenen) Daten vor dem Ausspähen. IT-Sicherheitsforschung ist ein wichtiger Kontrollfaktor insbesondere für die fehlerhafte Programmierung oder Implementierung von Chiffriermechanismen geworden.

Mit zunehmender Geschwindigkeit und der Konvergenz der kabelgebundenen sowie -losen Netze wurden (mobile) Echtzeitanwendungen, Soziale Netzwerke und Instant-Messaging möglich. Mit dem steigenden Synchronisationsbedarf besonders von Mobilgeräten wurden Cloud-Lösungen immer wichtiger. Der Speicherort von Daten wurde damit immer weniger greifbar. Dies und die Cloud als lohnenswertes Angriffsziel bzw. Einfallstor stellte die IT-Sicherheitsforschung vor neue Herausforderungen. Die Aufklärung im Internet sowie die Sammlung und das Teilen von Analysedaten wurde wichtiger. Cloud-Infrastruktur ist jedoch häufig für die Forscher*innen eine Black Box.

Die 2010er Jahre brachten Wellen neuer Malware insbesondere in Form von Erpressungstrojanern (Ransomware). Erste Versionen waren vor allem darauf ausgelegt, Daten zu Erpressungszwecken zu verschlüsseln. Die Herausgabe eines Dechiffriercodes wird davon abhängig gemacht, dass die Zahlung eines Betrags in Digitalwährung erfolgt ist. Mittlerweile werden auch Daten zur weiteren kriminellen Verwertung ausgeleitet. Dazu hat sich im Organisierten Verbrechen eine Arbeitsteilung von der Entwicklung von Ransomware, Bereitstellung von IT-Infrastruktur wie Kontrollservern über Aufklärung und Angriff bis zur Erpressung und Zahlungsabwicklung gebildet. Teilweise agieren die Täter*innen gar in Affiliate-Modellen. Diese zu beobachten und zu analysieren ist ein weiteres Feld der IT-Sicherheitsforschung geworden.

Für Ransomware-Kampagnen werden gerne Netzwerkgeräte des Internets der Dinge (IoT) als Bots eingesetzt. Dabei wird der häufig desolate Sicherheitszustand solcher Geräte, die oft mit Firmware voll bekannter Schwachstellen belastet sind, ausgenutzt. IoT-Geräte, die sich mittlerweile in Privathaushalten wie in der Industrie oder kritischen Infrastrukturen zur Steuerung von Maschinen und Anlagen finden, sind ein zentraler Untersuchungsgegenstand der IT-Sicherheitsforschung geworden. Dadurch sind auch hardware-nahe Sicherheitsmechanismen wieder stärker ins Blickfeld gerückt. Die bislang fehlende IT-Sicherheits- und Fehlerkultur führt hier zu besonders hohen Risiken, wenn ganze Klassen von Geräten mit Schwachstellen behaftet sind.

Mit der Datenschutz-Grundverordnung setzte ab 2018 eine stärkere Verzahnung von IT-Sicherheit und Datenschutz ein. Beide Bereiche sind nur noch schwer voneinander zu trennen. Dies zeigt sich auch im noch sehr jungen Bereich der Sicherheitsfragen rund um selbstlernende Systeme (Machine Learning) und „Künstliche Intelligenz“ (KI). Die Covid19-Pandemie führte die Relevanz der Verletzlichkeit privater Netzwerke (von Mitarbeiter*innen) auch für die Sicherheit der Unternehmen vor Augen. IT-Sicherheitsforschung, die hier Schwachstellen aufdeckt und an der Beseitigung beteiligt ist, wird zu einer aktiven Komponente des technischen Staats-, Wirtschafts- und Verbraucherschutzes.

6.2 Notwendigkeit einer gesetzlichen Klarstellung

Silvia Balaban / Daniel Vonderau / Maria Pieper / Manuela Wagner

Zwar ist nachvollziehbar, dass der Gesetzgeber mit möglichst weit gefassten Deliktstatbeständen Strafbarkeitslücken vermeiden wollte. Jedoch darf dies nicht dazu führen, dass Forschende durch diese Ungewissheit potenzielle Strafbarkeits- und Haftungsrisiken auf sich nehmen müssen, wenn solche Normen erst in gerichtlichen Verfahren durch richterliche Entscheidungen die notwendigen Konturen gewinnen. Dies sollte weder Ziel noch Folge des Computerstrafrechts sein, da die Aufdeckung der Sicherheitslücken ja gerade im Interesse der Allgemeinheit erfolgt.

Ebenso ist das Anliegen eines umfassenden Urheberrechtsschutzes von Computerprogrammen begrüßenswert. Während jedoch die Ziele des Urheberrechtsschutzes durch die Sicherheitsforschung kaum beeinträchtigt werden, hindern fehlende Lizenzen und Erlaubnistatbestände berechtigte Nutzer*innen an der praktischen Durchführung von IT-Sicherheitstests. Erst diese würden ihnen aber eine Einschätzung dahingehend erlauben, ob die Leistung (für die sie i.d.R. bezahlen) sicher und damit vertragsgemäß ist. IT-Sicherheitsforschung kann hier zu mehr Transparenz beitragen. Viele Forschende könnten wegen der schwer kalkulierbaren Haftungsrisiken aber von der Aufdeckung oder Warnung vor bereits gefundenen Sicherheitslücken zurückschrecken.

Durch gesetzliche Grauzonen wird nicht nur die Konkurrenzfähigkeit der deutschen Sicherheitsforschung im internationalen Vergleich beeinträchtigt. Es leidet sowohl ein wirksamer Verbraucherschutz als auch der Schutz der Wirtschaft vor Cyberspionage oder staatlicher Akteure vor Hackerangriffen,[146] wenn sich Forschende (je nach Interpretation der Rechtslage) zivil- und strafrechtlichen Gerichtsverfahren ausgesetzt sehen. Dass diese Risiken nicht nur theoretischer Natur sind, zeigte ein Fall von Sicherheitsforschern aus Berlin, Erlangen-Nürnberg und München, die sich vor Gericht wegen mutmaßlichem Reverse Engineering verteidigen mussten.[147] Zudem sind Zivilverfahren gegen Wissenschaftler*innen aus anderen Ländern bekannt.[148] Eine Strafanzeige wurde im Sommer 2021 gegen eine unabhängige Sicherheitsforscherin gestellt, die Sicherheitslücken dem Produktverantwortlichen gemeldet hatte.[149] Das Ermittlungsverfahren wurde eingestellt, da eine Zugangssicherung fehlte (vgl. die Voraussetzungen des § 202a StGB in Abschnitt 3.1).[150] In einem weite-

[146] Siehe bspw. zur Zunahme von Hackerangriffen im Zuge der Bundestagswahl 2021: Der Tagesspiegel, Angriffswellen russischer Hacker auf Abgeordnete, Stand: 24.07.2021, abrufbar unter: https://www.tagesspiegel.de/politik/gefahr-fuer-die-bundestagswahl-angriffswellen-russischer-hacker-auf-abgeordnete/27418978.html (zuletzt abgerufen am 01.10.2021).

[147] Ermert, „Offenlegung von Softwarelücken: Rechtsstreit endet mit Vergleich“ in Heise online, 2018, abrufbar unter: https://www.heise.de/newsticker/meldung/Offenlegungvon-Softwareluecken-Rechtsstreit-endet-mit-Vergleich-4156393.html (zuletzt abgerufen am 02.08.2019).

[148] Volkswagen AG vs. Garcia Case [2013] EWHC 1832 (Ch), 25.06.2013; Rechtbank Arnhem, Urteil im vorläufigen Rechtsschutz vom 18.07.2008, AZ 171900 / KG ZA 08-415.

[149] Wolfangel, „Danke für den Hinweis, Anzeige ist raus“ in: Zeit online vom 05.08.2021, abrufbar unter https://www.zeit.de; Hurtz, „CDU blamiert sich mit Anzeige gegen IT-Expertin“ in: Süddeutsche Zeitung online vom 05.08.2021, abrufbar unter https://www.sueddeutsche.de/politik/cdu-connect-anzeige-wittmann-1.5373488 und Ernst, „Lücken in der CDU-connect-App: Datenschutzbeauftragte leitet Prüfverfahren ein“ in: heise online vom 06.08.2021, abrufbar unter https://www.heise.de/news/Luecken-in-der-CDU-connect-App-Datenschutzbeauftragte-leitet-Pruefverfahren-ein-6157570.html (zuletzt abgerufen am 01.10.2021).

[150] Reuter, „Ermittlungsverfahren gegen Sicherheitsforscherin Lilith Wittmann eingestellt“, in: netzpolitik.org vom 16.09.2021, abrufbar unter: https://netzpolitik.org/2021/cdu-connect-ermittlungsverfahren-gegen-sicherheitsforscherin-lilith-wittmann-eingestellt/ (zuletzt abgerufen am 01.10.2021).

ren Fall mündete die Entdeckung und Meldung eines umfangreichen Datenlecks bei einem Dienstleistungsunternehmen für Online-Händler*innen in einer Hausdurchsuchung und Beschlagnahme der Arbeitscomputer des Meldenden.[151] Dieser war laut Zeitungsbericht auf das Datenleck im Rahmen einer beauftragten Beseitigung eines Softwareproblems durch einen der Online-Händler gestoßen und war nachdem die Meldung beim Produktverantwortlichen keine Abhilfe schaffte an die Öffentlichkeit getreten. Durch die Beschlagnahme der Arbeitsgeräte sieht sich der Sicherheitsexperte in seiner beruflichen Existenz gefährdet.[152] Auf einer GitHub-Seite wurde eine fortlaufende, weltweite Sammlung realer Fälle solcher und vergleichbarer rechtlicher Bedrohungen für Sicherheitsforscher*innen angelegt, wie Forderungen von Unterlassungserklärungen sowie Drohungen mit Klagen und Strafanzeigen.[153]

6.2.1 Gefahren vernachlässigter IT-Sicherheit

Deutsche Unternehmen schätzen das Risiko von Cybervorfällen wie IT-Ausfälle, Spionage und Datenmissbrauch als eine der größten Gefahren für ihr Geschäft ein.[154] Selbst Unternehmen, die große finanzielle Ressourcen für die Sicherheitsanalyse ihrer Produkte zur Verfügung haben, finden in der Regel nicht alle Schwachstellen. Einige Unternehmen haben darüber hinaus Schwierigkeiten bei der Schwachstellenerkennung, wofür oftmals zwei Ursachen bestehen: (a) der Anbieter ist vergleichsweise klein oder neu und muss noch eine Reaktionsfähigkeit auf Sicherheitsvorfälle für das Produkt aufbauen, oder (b) der Anbieter verfügt zwar über umfassende technische Erfahrung in seinem traditionellen Produktbereich, hat aber die Risiken der Netzwerkfähigkeit seiner Produkte noch nicht vollständig in seine technische Qualitätssicherungspraxis integriert.[155] Aktuell wird geschätzt, dass durchschnittliche Programme mindestens 14 verschiedene Punkte der Verwundbarkeit aufweisen.[156] Selbst in Fällen, in denen die Entwickler*innen über das erforderliche Sicherheitsbewusstsein verfügen, erschaffen sie oft Systeme aus bereits bestehenden Komponenten oder Bibliotheken, die möglicherweise nicht mit dem gleichen Grad an Sicherheitserwägungen entwickelt wurden.[157] Folglich können insbesondere staatlich geförderte Forschungseinrichtungen einen wertvollen Beitrag leisten bei der Optimierung des Sicherheitsniveaus zu unterstützen, indem sie Sicherheitslücken suchen, finden, melden und vor deren Schadenspotential warnen.

Die Verbesserung der IT-Sicherheit hat weitreichende Implikationen für:

- **Verringerung der Cyberkriminalität:** Ein höheres allgemeines IT-Sicherheitsniveau erschwert etwa die Reichweite und Durchschlagskraft von Ransomware-Kampagnen.
- **Verbraucherschutz:** Gerade im Bereich der Verbraucherprodukte nimmt der Grad der Digitalisierung und damit die Möglichkeit von Schäden durch IT-Sicherheitsschwachstellen zu.

---

[151] Tremmel, „Hausdurchsuchung statt Dankeschön“ in: golem.de, Stand 14.10.2021, abrufbar unter: https://www.golem.de/news/nach-datenleck-hausdurchsuchung-statt-dankeschoen-2110-160269.html (zuletzt abgerufen am: 22.10.2021).

[152] Tremmel, Fn. 151.

[153] Research Threats: Legal Threats Against Security Researchers, https://github.com/disclose/research-threats (zuletzt abgerufen am: 22.10.2021).

[154] Allianz Risk Barometer 2019, abrufbar unter https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf (zuletzt abgerufen am 02.08.2019).

[155] Householder et al., The CERT® Guide to Coordinated Vulnerability Disclosure, SPECIAL REPORT CMU/SEI-2017-SR-022, August 2017, S. VIII.

[156] Pupillo/Ferreira/Varisco, Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges, Report of a CEPS Task Force June 2018, S. 1.

[157] Householder et al., The CERT® Guide to Coordinated Vulnerability Disclosure, SPECIAL REPORT CMU/SEI-2017-SR-022, August 2017, S. VIII.

- **Stärkung bzw. Schwächung digitaler staatlicher und gesellschaftlicher Souveränität:** Auch staatliche Stellen sind Konsumenten von IT-Produkten und somit gefährdet durch Sicherheitslücken. Schutz der digitalen Infrastruktur als ziviler Bevölkerungsschutz.
- **Datenschutz:** Sicherheitslücken werden oftmals genutzt um personenbezogene Daten zu erlangen. Negative Folgen hat dies nicht nur für die betroffenen Personen. Unternehmen in der Rolle des Verantwortlichen können dann Sanktionen wie auch ein Imageverlust treffen.
- **Wirtschaftsschutz:** Know-How-Schutz sowie der Schutz vor Wirtschaftsspionage erfordert ein hohes Sicherheitsniveau genutzter IT-Produkte und Systeme.
- **Kompetenz:** IT-Sicherheitsforschung als Motor für Bildung und Innovation.
- **Vertrauen**: Langfristige Resilienz gegenüber technischer Innovation und digitalem Wandel, sodass die Akzeptanz und Nutzung dieser Produkte stark gehemmt wird oder verzögert erfolgt; die Folge sind eine gesellschaftliche Spaltung und ein Rückgang des Innovationspotentials in Deutschland.

In den USA werden eine erhebliche Anzahl kritischer Sicherheitslücken durch unabhängige Stellen wie Sicherheitsforscher*innen aufgedeckt, die die Software aus eigenem Antrieb und aus verschiedenen Gründen (wie bspw. Forschungsinteressen, Eigennutzung, Altruismus, Reputationssteigerung, etc.) prüfen. Dies ist in der Tat nicht überraschend, da es weit mehr solcher unabhängigen Sicherheitsforscher*innen gibt, als ein einzelner Software-Hersteller beschäftigen kann.158 In diesem Sinne kam ein vom Joint Research Centre (JRC) der EU-Kommission 2017 organisierter Workshop zum Ergebnis, dass die Forschung der Hauptantrieb für die Aufdeckung von Sicherheitslücken sein sollte.159 Folglich erkannte auch die EU-Kommission den wesentlichen Beitrag unabhängiger Sicherheitsforschung an:

> „Außerdem muss die wichtige Rolle gewürdigt werden, die dritten Sicherheitsexperten bei der Aufdeckung von Schwachstellen in bestehenden Produkten und Diensten zukommt; daher sollten die Voraussetzungen für eine mitgliedstaatsübergreifende, koordinierte Offenlegung von Sicherheitslücken auf der Grundlage bewährter Verfahren und der einschlägigen Standards geschaffen werden.“[160]

Zu bedenken gilt auch, dass Erkenntnisse der IT-Sicherheitsforschung als Input für die Entwicklung sicherer Produkte einfließen und eine aktive Sicherheitsforschung somit einen Standortvorteil begründen kann. Ebenso relevant wird die Tätigkeit für die Aufklärung und Ausbildung der Bevölkerung in Sicherheitsfragen.

Der Stellenwert einer unabhängigen Sicherheitsforschung ist in der Literatur ausführlich diskutiert worden. Ebenso wird intensiv diskutiert, ob Regierungen sog. „Zero Day“-Schwachstellen für die Erfüllung staatlicher Aufgaben zurückbehalten oder offenlegen sollten, damit sie gepatcht werden können. Eine Studie über Zero-Day-Schwachstellen zeigte, dass eine hohe durchschnittliche Lebenserwartung der Exploits und deren zugrundeliegenden Sicherheitslücken von ca. 6,9 Jahren darauf hindeuten, dass die meisten Zero-Day-Schwachstellen älter sind, als oft erwartet.[161] Der Begriff „Zero-Day“ ist eine etwas irreführende Bezeichnung.

[158] Gamero-Garrido/Savage/Levchenko/Snoeren, CCS’17, Fn. 50, S. 1501.
[159] Pupillo/Ferreira/Varisco, Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges, Report of a CEPS Task Force June 2018, S. 3.
[160] Europäische Kommission, Gemeinsame Mitteilung an das Europäische Parlament und den Rat, Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen, Brüssel, den 13.9.2017 JOIN(2017) 450 final, S. 7.
[161] Ablon/Bogart. Zero Days, Thousands of Nights. RAND Corporation, 2017, S. 52.

Wenn eine bisher nicht gemeldete Schwachstelle gefunden wird, bedeutet das nicht, dass niemand sonst davon weiß. Was es bedeutet ist, dass kein anderer sie bisher öffentlich bekannt gemacht hat.[162] Wissenschaftler*innen berichten zudem, dass etwa 40% der untersuchten Schwachstellen innerhalb von 14 Jahren mindestens zweimal unabhängig voneinander entdeckt wurden.[163] Folglich kann nicht sicher davon ausgegangen werden, dass noch nicht bekannt gewordene oder bewusst geheim gehaltene „Zero-Day" Sicherheitslücken nicht bereits in schädigender Absicht ausgenutzt werden.

> „Wir leben in einer Zeit, in der Verwundbarkeiten durch Kriminelle mit potenziell geopolitischen Motiven durchsickern und in der bestimmte Regierungen Verwundbarkeiten horten, um offensive Cyber-Waffen zu entwickeln. Dies kann nicht in einem Verantwortungsvakuum geschehen. Es bedarf jetzt transparenter Entscheidungsprozesse, um die Rechtsstaatlichkeit im Internet zu wahren und die Regierungsstellen zur Rechenschaft zu ziehen. […]."[164]

Die Auswahl der Forschungsthemen kann zumeist kaum auf Faktoren wie bspw. Teilnahme an Bug-Bounty-Programmen gekoppelt werden. Bei diesen wird von Aktivist*innen zudem bemängelt, dass diese oftmals keinen offenen Umgang mit Erkenntnissen zur Sicherheitslücken fördern, sondern Verschwiegenheit verbindlich einfordern.[165]

6.2.2 Selbstkontrolle und Redlichkeit der Forschung

Das Potential der IT-Sicherheitsforschung in Deutschland kann nicht ausgeschöpft werden, wenn die Unsicherheit rechtlicher Grauzonen vor der Durchführung von Forschungsaktivitäten abschreckt. Abschreckungswirkung entfalten die Kostenbelastung durch Rechtsstreitigkeiten, die Sorge des Reputationsverlusts beim Vorwurf vermeintlicher Rechtsverletzungen bis hin zu Sorge vor Schadensersatzforderungen oder gar Angst vor einer drohenden Strafbarkeit. Zu nennen ist aber auch das Legalitätsprinzip der Öffentlichen Hand, d.h. die Selbstbindung der Verwaltung oder der Verstoß gegen interne Compliance-Vorschriften oder Ethik-Codes. Auch die Nachwuchsförderung kann beeinträchtigt sein, wenn mit Unsicherheiten behaftete Tätigkeiten Bewerber*innen abschrecken.

Insofern reicht der Befund der Rechtswidrigkeit eines Forschungsvorhabens aus, dass sich die Forschungseinrichtung gegen die Durchführung entscheiden muss. Hochschulen sind i.d.R. über die Hochschulgesetze bei ihrer wissenschaftlichen Tätigkeit zu wissenschaftlicher Redlichkeit verpflichtet.[166] Dazu zählt bspw. auch, das geistige Eigentum anderer nicht zu verletzten.[167] Im Rahmen der Selbstkontrolle sind Hochschulen dazu aufgerufen, Regeln zur Einhaltung der allgemein anerkannten Grundsätze guter wissenschaftlicher Praxis und zum Umgang mit wissenschaftlichem Fehlverhalten aufzustellen.

---

[162] Brumley, Game Theory: Why System Security Is Like Poker, Not Chess, abrufbar unter https://thenewstack.io/game-theory-why-system-security-is-like-poker-not-chess/ (zuletzt abgerufen am 11.05.2020).
[163] Ablon/Bogart. Zero Days, Thousands of Nights. RAND Corporation, 2017, S. 43.
[164] Vorwort Marietje Schaake in: Pupillo/Ferreira/Varisco, Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges, Report of a CEPS Task Force June 2018 [Zitat übersetzt aus dem Englischen].
[165] Schneier, Bug Bounty Programs Are Being Used to Buy Silence, abrufbar unter: https://www.schneier.com/blog/archives/2020/04/bug_bounty_prog.html (zuletzt abgerufen am 01.10.2021).
[166] § 3 Abs. 5 LHG BW; § 6 Abs. 1 S. 3 BayHschG; § 4 Abs. 3 S. 1 und 4 S. 1 und 2 HG NRW; § 79 SächsHSFG; § 3 Abs. 1 HmbHG; § 5 Abs. 5 SHSG; § 5 Abs. 3 BerlHG; § 1 Abs. 2 S. 2 HHG.
[167] § 3 Abs. 5 S. 3 LHG BW.

Nun stellt sich die Frage: Was bedeutet Redlichkeit der Forschung? Gemeinhin wird hierunter wissenschaftliches Fehlverhalten in Form eines Plagiats, der verfälschenden Manipulation von Daten und Ergebnissen oder Behinderung der Forschungstätigkeit anderer verstanden.[168] Die wissenschaftliche Redlichkeit geht über die Einhaltung von Gesetzen hinaus und umfasst die Beachtung der Regeln der Wissenschaftlichkeit und Abmachungen der Wissenschaftswelt.[169] Forscher*innen, die wegen wissenschaftlichen Fehlverhaltens strafrechtlich oder disziplinarrechtlich rechtskräftig verurteilt wurden, haben essentiell gegen die ethischen Prinzipien der Wissenschaft verstoßen.[170] Die DFG unterstreicht in ihren Leitlinien, dass sich die Verantwortung von Wissenschaftler*innen nicht *nur* auf die Einhaltung rechtlicher Vorgaben beschränkt, sondern darüber hinaus die Verpflichtung umfasst, bei ihrer Tätigkeit auftretende Risiken zu erkennen und zu bewerten.[171] Dabei sollen sie insbesondere die mit sicherheitsrelevanter Forschung verbundenen Aspekte berücksichtigen. „Hochschulen und außerhochschulische Forschungseinrichtungen tragen Verantwortung für die Regelkonformität des Handelns ihrer Mitglieder*innen und ihrer Angehörigen und befördern diese durch geeignete Organisationsstrukturen.“[172]

6.2.3 Offenlegung im Rahmen der Forschung

Zu einer nachhaltigen IT-Sicherheitsforschung gehört, wie in allen anderen Forschungsbereichen, auch die Veröffentlichung von reproduzierbaren Forschungsergebnissen. Die offene und öffentliche Diskussion über aktuelle Erkenntnisse der Wissenschaft ist fester Bestand jeglicher Forschung und von der Forschungsfreiheit umfasst.[173] Forschung und Lehre sind auf Publizität und Veröffentlichung der Forschungsergebnisse hin angelegt.[174] Hochschulen sind nicht nur berechtigt, sondern teilweise sogar verpflichtet ihre Forschungserkenntnisse zu veröffentlichen.[175]

> Die EU hat sich gemäß Art. 179 AEUV das Ziel gesetzt „ihre wissenschaftlichen und technologischen Grundlagen dadurch zu stärken, dass ein europäischer Raum der Forschung geschaffen wird, in dem Freizügigkeit für Forscher herrscht und wissenschaftliche Erkenntnisse und Technologien frei ausgetauscht werden, die Entwicklung ihrer Wettbewerbsfähigkeit einschließlich der ihrer Industrie zu fördern sowie alle Forschungsmaßnahmen zu unterstützen, die aufgrund anderer Kapitel der Verträge für erforderlich gehalten werden.“

In diesem Sinne unterstützt die EU akademische wie auch private Forschungsvorhaben u.a. durch Festlegung gemeinsamer Normen und Beseitigung einer grenzüberschreitenden Zusammenarbeit entgegenstehenden rechtlichen und steuerlichen Hindernisse.

[168] Selbstkontrolle der Wissenschaft und wissenschaftliches Fehlverhalten, Resolution des 50. Hochschulverbandstages 2000; von Bargen, JZ 2013, 714 (716).
[169] PH Zürich, Wissenschaftliche Redlichkeit. Policy Paper. Version vom 16. Januar 2014.
[170] Selbstkontrolle der Wissenschaft und wissenschaftliches Fehlverhalten, Resolution des 50. Hochschulverbandstages 2000.
[171] DFG, Leitlinien zur Sicherung guter wissenschaftlicher Praxis, September 2019, S. 16.
[172] DFG, Leitlinien zur Sicherung guter wissenschaftlicher Praxis, September 2019, S. 16.
[173] Weichert, ZD 2020, 18 (19); BVerfGE 35, 79, 112.
[174] BVerfGE 47, 327, 367 ff; 35, 79, 112.
[175] Vgl. bspw. § 3 Abs. 2 S. 1 LHG BW; § 5 Abs. 2 S. 1 sowie § 73 Abs. 2 SHSG; § 3 Abs. 2 S. 1 BayHschG; § 41 Abs. 2 S. 1 BerlHG; § 4 Abs. 1 S. 2, 70 Abs. 3 HG NRW; §§ 75, 76 HmbHG; §§ 5 Abs. 2 Nr. 9, 47 SächsHSFG.

Wenn die Forschungsergebnisse ein auf dem Markt verfügbares, d.h. in Verkehr gebrachtes, Produkt betreffen, müssen dabei selbstverständlich die Interessen der jeweiligen Hersteller*innen, Verkäufer*innen, Betreiber*innen und Nutzer*innen berücksichtigt werden. Dies kann im Einzelfall dazu führen, dass die Veröffentlichung von Forschungsergebnissen zurückgestellt werden muss, bis Risiken für die Rechte und Freiheiten der von Sicherheitslücken potenziell betroffenen Personenkreise abgemildert bzw. ausgeschlossen werden können.[176] Diese Erwägungen sollten allerdings nicht zur Verhinderung der Forschung, sondern auf der Ebene des verantwortungsvollen Umgangs mit Forschungserkenntnissen berücksichtigt werden, sodass diese nicht missbräuchlich zum Schaden Einzelner oder der Allgemeinheit verwendet werden können. Zur Frage dieses verantwortungsvollen Umgangs mit Forschungsergebnissen kann auf die Rechtsprechung des Bundesverfassungsgerichts im Hinblick auf die Einführung einer Rechtspflicht zum Mitbedenken gesellschaftlicher Folgen wissenschaftlicher Erkenntnis im Hochschulrecht (vgl. § 1 Abs. 3 HHG) zurückgegriffen werden.[177] Demnach wäre es mit dem verfassungsrechtlich geschützten Freiraum der Forschungsfreiheit unvereinbar, wenn Forschende dazu gezwungen wären, *alle* gesellschaftlichen und gesellschaftspolitischen Auswirkungen jeglicher Größenordnung zu bedenken. Zulässig ist hingegen eine Pflicht zur „*Berücksichtigung schwerwiegender Folgen für verfassungsrechtlich geschützte Gemeinschaftsgüter, deren Beeinträchtigung bei der im Einzelfall gebotenen Abwägung nach der Wertordnung des Grundgesetzes schwerer wiegt als die dem Wissenschaftler auferlegte Verpflichtung*“.[178] Wissenschaftler*innen können durchaus auch gesetzlich dazu angehalten werden, eine Verantwortung gegenüber der Allgemeinheit wahrzunehmen und die Allgemeinheit vor gefährlichen Auswirkungen der Wissenschaft zu schützen.

Die Wahrnehmung dieser Verantwortung ist bei der Offenlegung von Sicherheitsschwachstellen ambivalent: Erfolgt eine wissenschaftliche Veröffentlichung bevor die Sicherheitslücke geschlossen wurde, könnten Dritte die wissenschaftlichen Ergebnisse zu kriminellen Zwecken missbrauchen. Erfolgt die Offenlegung hingegen ausschließlich gegenüber der für die Sicherheitslücke verantwortlichen Stelle (i.d.R. Hersteller*in) ohne Veröffentlichung gegenüber der Allgemeinheit, besteht aus Erfahrung auch die Gefahr, dass die Sicherheitslücke nicht geschlossen wird und somit Risiken für die Allgemeinheit verbleiben. Ohne Warnung der Nutzerkreise oder der Öffentlichkeit, können diese nicht auf Schutzmaßnahmen oder die Wichtigkeit zügiger Updates hingewiesen werden.

6.2.4 Abschreckungseffekte durch rechtliche Grauzonen bei der Aufdeckung und Meldung von Sicherheitslücken

Aufgrund der unklaren Rechtslage besteht die Gefahr, dass Finder*innen von Sicherheitslücken davor zurückschrecken diese an die verantwortlichen Unternehmen oder Intermediäre (bspw. CERT, Journalisten, Meldeportale, etc.) zu melden. Im Rahmen einer Studie einer Arbeitsgruppe der Nationalen Telekommunika-

[176] Vgl. Volkswagen AG vs. Garcia Case [2013] EWHC 1832 (Ch), 25.06.2013.
[177] BVerfGE 47, 327.
[178] BVerfGE 47, 327, Rn. 217. Daneben darf die im hessischen Hochschulgesetz zusätzlich normierte Informationspflicht (bei Bekanntwerden von Forschungsergebnissen, die eine erhebliche Gefahr für die Gesundheit, das Leben oder das friedliche Zusammenleben der Menschen herbeiführen können) nicht so verstanden werden, Forschungsergebnisse stets auf ihre Gefährlichkeit im Falle verantwortungsloser Verwendung zu überprüfen. Es müsste nur dann über Missbrauchsgefahren berichtet werden, wenn diese auch ein Fachmann nicht ohne weiteres erkennen kann und die nur Wissenschaftler*innen aufgrund ihrer Spezialkenntnisse erkennen.

tions- und Informationsverwaltung der USA (NTIA) aus dem Jahr 2015 gaben 60% der befragten Wissenschaftler*innen an, Angst vor rechtlichen Sanktionen zu haben, wenn sie ihre Arbeit offenlegen.[179] Dabei beteiligt sich die große Mehrheit der Forschenden (92%) in einer Form der CVD. Zumeist führten frustrierte Erwartungen, insbesondere in Bezug auf den Kommunikationsprozess, zu anderen Offenlegungsstrategien. Eine weitere Studie in den USA kam zum Ergebnis, dass rechtliche Bedenken ein wichtiges Anliegen sind und von 110 befragten Sicherheitsforscher*innen fast ein Viertel berichtete, dass sie rechtlichen Drohungen oder Maßnahmen im Rahmen ihrer Forschung ausgesetzt waren.[180] Im Rahmen dieser Befragung gaben ca. die Hälfte der Befragten an, Angst vor rechtlichen Konsequenzen zu haben. Dies führte wiederum bei etwa der Hälfte der Fälle zu einer Anpassung des Forschungsvorhabens.[181] Tatsächlich vor Gericht landeten aus dieser Gruppe nur zwei Fälle.[182] Exemplarisch zeigt diese Untersuchung, dass die Problematik sich nicht in zahlreichen Gerichtsprozessen manifestiert, und trotzdem erheblichen Einfluss auf die Forschung ausübt. Laut einer weiteren Umfrage verzichtet jeder vierte „Hacker" auf eine Meldung auch deshalb, weil Unternehmen oftmals keinen Prozess und keinen geeigneten Kommunikationskanal dafür implementiert haben.[183]

Zu bedenken ist ferner auch, dass Forschende die Ausnutzbarkeit von Sicherheitslücken dokumentieren und *proof-of-concepts* bereitstellen müssten, damit Hersteller*innen diese anerkennen und schneller schließen. Sofern die hierfür durchgeführten Tests – je nach Auslegung – rechtswidrig sein sollten, würden Forschende mit der Information der Hersteller*in selbst belastende Beweise gegen sich erzeugen. Die Rechtslage sollte nicht davor abschrecken Sicherheitslücken zu melden und dabei auch aufzuzeigen, wie konkret diese aufgedeckt wurden. Für die Unternehmen ist es oftmals entscheidend, nachvollziehen zu können, wie potenzielle Angreifer sich Zugang verschaffen können. Mit der freiwilligen Meldung von Schwachstellen erhalten sie einen geldwerten Vorteil und können eigene Haftungsrisiken minimieren. Daher gilt es durch eine ausgewogene Regulierung eine Fehlerkultur im Sinne der Implementierung von wirksamen Prozessen zur Entgegennahme von Meldungen und zur Beseitigung von Schwachstellen sowie einer Kommunikation auf Augenhöhe mit der Melder*in anzuregen. Der Grundsatz „don't shoot the messenger" sollte nicht durch zivil- und strafrechtliche Abschreckungsmaßnahmen schon im Vorfeld torpediert werden.

[179] NTIA Awareness and Adoption Group, Vulnerability Disclosure Attitudes and Actions, 2015, S. 6.
[180] Gamero-Garrido/Savage/Levchenko/Snoeren, CCS'17, Fn. 50, S. 1501 (1511).
[181] Gamero-Garrido/Savage/Levchenko/Snoeren, CCS'17, Fn. 50, S. 1501 (1511).
[182] Gamero-Garrido/Savage/Levchenko/Snoeren, CCS'17, Fn. 50, S. 1501 (1512).
[183] Koch/Schmitz in Security Insider, Vorteile einer Vulnerability Disclosure Policy - Vulnerability Disclosure Policy oder Bug Bounty, vom 26.09.2019, abrufbar unter https://www.security-insider.de/vulnerability-disclosure-policy-oder-bug-bounty-a-856672/ (zuletzt abgerufen am 12.03.2020).

6.3 Rechtsvergleich

Manuela Wagner

Um Lösungen für die aufgezeigten Problemlagen zu finden, bietet sich ein kurzer Blick über die Grenze an, wie bspw. die Niederlande, Frankreich, UK und die USA gerade mit Straf- und Urheberrechtsfragen umgehen.

6.3.1 Aktivitäten in den Niederlanden

Leitfäden und Kooperationen:

- Das *Nationaal Cyber Security Centrum (NCSC)* hat einen allgemeinen Leitfaden für CVD veröffentlicht, der als Modell für andere EU-Mitgliedstaaten herangezogen werden kann, und gleichzeitig Sicherheitsforschenden eine Anleitung gibt, wie sie bei der Suche nach und zur Meldung von Schwachstellen vorgehen sollen.[184]
- Am *Coordinated Vulnerability Disclosure Manifesto* von 2016 haben sich ca. 30 Organisationen beteiligt.[185] Die Unterzeichner verpflichten sich, Mechanismen zur öffentlichen Berichterstattung über Schwachstellen in ihren IKT-Systemen zu implementieren und fordern andere Organisationen auf, dies ebenfalls zu tun. Das Manifest zielt darauf ab, allen Parteien die Bedeutung der Zusammenarbeit zur Verbesserung der Cybersicherheit für alle bewusster zu machen.

Sicherheitsforschung vor Gericht: 2008 versuchte der/ die Hersteller*in von RFID-Karten u.a. für Zugangsausweise Forschenden die Veröffentlichung ihrer Erkenntnisse zu Sicherheitsschwächen dieser Karten sowie des Ansatzes „Security by Obscurity“ zu untersagen.[186] Der/die Hersteller*in berief sich auf geschütztes Know-How, urheberrechtlichen Schutz und Beihilfe gegenüber der Ausnutzung der Sicherheitslücke durch Dritte, welche das Gericht allesamt verneinte. Im Rahmen der Abwägung der im Konflikt stehenden Interessen betonte das Gericht die Bedeutung der wissenschaftlichen Forschung:

> Die wirtschaftliche und soziale Entwicklung der demokratischen Gesellschaft wird in hohem Maße von der wissenschaftlichen Forschung, von den daraus abgeleiteten Erkenntnissen und von deren praktischer Anwendung bestimmt. All dies steht und fällt mit der Möglichkeit der Veröffentlichung.[187]

Sicherheitsrisiken, die von einer frühzeitigen Offenlegung ausgehen könnten, wurden vor Gericht erörtert, mit dem Ergebnis, dass die Verantwortung für Schadensrisiken den Herstellenden zugewiesen werden, da Schadensmöglichkeit zu einem großen Teil auf die Herstellung und das Inverkehrbringen eines Chips mit intrinsischen Fehlern zurückzuführen ist, und nicht auf die Forschung, die diese Fehler nur aufgedeckt hat.

[184] National Cyber Security Centre, Ministry of Justice and Security, Netherlands, Coordinated Vulnerability Disclosure: the Guideline, October 2018.
[185] CIO Platform Nederland/Rabobank, Coordinated Vulnerability Disclosure Manifesto abrufbar unter: https://www.cio-platform.nl/en/publications; siehe auch: https://www.enisa.europa.eu/news/member-states/from-the-netherlands-presidency-of-the-eu-council-coordinated-vulnerability-disclosure-manifesto-signed (zuletzt abgerufen am 13.05.2020).
[186] Rechtbank Arnhem, Urteil im vorläufigen Rechtsschutz vom 18.07.2008, AZ 171900 / KG ZA 08-415.
[187] Rechtbank Arnhem, Urteil im vorläufigen Rechtsschutz vom 18.07.2008, AZ 171900 / KG ZA 08-415, Rn. 4.15.

Risiken erleichterter Angriffe des Chips mit Hilfe der Informationen der Forschenden müssten bis zu einem gewissen Grad in einer offenen demokratischen Gesellschaft akzeptiert werden.

Rechtslage im Strafrecht: Die niederländische Staatsanwaltschaft beachtet im Umgang mit sog. „ethischen Hacker*innen“, ob die Sicherheitslücken verantwortungsbewusst offenlegt wurden, die Aufdeckung der Sicherheitsschwachstelle einem öffentlichen Interesse diente, die Person unverhältnismäßig vorging und ob mildere Mittel möglich gewesen wären.[188] Auch das niederländische Strafrecht differenziert nicht explizit nach ethischen Motiven. Hacker machen sich weiterhin wegen „Computervredebreuk“ (Ausspähen von Daten) strafbar, auch wenn sie keine böswillige Absicht haben und ein Fehlverhalten – nämlich ein Sicherheitsleck – aufdecken wollen, sofern sie nicht die folgenden Anforderungen erfüllen: [189]

(1) Handeln im Rahmen eines **wesentlichen sozialen Interesses**, sowie Beachtung der Grundsätze

(2) der **Verhältnismäßigkeit** (nur zur Zielerreichung erforderliche Handlungen) und

(3) der **Subsidiarität** (kein anderer, weniger weitreichender Weg)

Im konkreten Fall hatte der Täter*innen mehrmals auf das System zugegriffen und mehr Informationen gesammelt, als notwendig gewesen wäre.[190] Dagegen gehen die Gerichte davon aus, dass der Nachweis von Mängeln bei der Sicherheit vertraulicher, medizinischer und persönlicher Daten einem erheblichen gesellschaftlichen Interesse dienen kann.[191] Auch das Aufspielen von Malware auf fremden Servern und der Zugriff ohne Erlaubnis auf hochsensible Daten können notwendige Handlungen darstellen, um Mängel der IT-Sicherheit aufzudecken. Diese Urteile zeigen somit einen Rahmen auf, an dem sich Sicherheitsforscher*innen orientieren können.

6.3.2 Ausnahmeregelung in Frankreich

Nach Art. 47 des Rechts für eine digitale Republik[192] ist die in Artikel 40 der Strafprozessordnung vorgesehene Pflicht zum Tätigwerden der Staatsanwaltschaft und sonstigen Behörden nicht anwendbar, wenn eine gutgläubig handelnde Person Informationen über das Bestehen einer Schwachstelle an das ANSSI (Agence nationale de la sécurité des systèmes d'information) übermittelt. ANSSI soll die Identität der übermittelnden Person vertraulich behandeln. Somit scheint zumindest der Weg über offizielle Stellen rechtlich abgesichert.

6.3.3 Fallbeispiel UK

Nachdem Forschende mittels Reverse Engineering eine Schwachstelle in einem Sicherheits-Mikrochip u.a. für die Schließsysteme von Kraftfahrzeugen fanden, den Mikrochiphersteller informierten und anschließend

[188] National Cyber Security Centre, Ministry of Justice and Security, Netherlands, Coordinated Vulnerability Disclosure: the Guideline, October 2018, S. 9.
[189] Rechtbank Den Haag, Urteil vom 17.12.2014, Nr. 09/748019-12.
[190] Zu den Prinzipien siehe auch: Rechtbank Oost-Brabant, Urteil vom 19.02.2013, Nr. 01/820892-12.
[191] Rechtbank Den Haag, Urteil vom 17.12.2014, Nr. 09/748019-12; Rechtbank Oost-Brabant, Urteil vom 19.02.2013, Nr. 01/820892-12.
[192] LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique.

ihre Erkenntnisse veröffentlichen wollten, wurden sie erfolgreich von dem/r Kfz-Hersteller*in auf Unterlassung verklagt.[193] Kernfragen des Rechtsstreits bestanden darin, ob bzw. wann die Forschenden in welcher Detailtiefe publizieren durften. Insbesondere aufgrund der Tatsache, dass (a) das Sicherheitsproblem nur durch kompletten Austausch der Komponente behebbar war, (b) kein Nachweis vorlag, dass die Sicherheitslücke bereits genutzt wurde, und (c) das zum Reverse Engineering genutzte Programm aus einer illegalen Quelle stammte, wurde entschieden, dass die Forschenden nach der Kontaktaufnahme durch VW die Publikation für eine angemessene Zeitspanne hätten aufschieben müssen, um dem Unternehmen Abhilfemaßnahmen zu ermöglichen. Das Gericht erkannte den hohen Wert der akademischen Redefreiheit an, aber gewährte die einstweilige Verfügung gegen die Forscher auch mit der Begründung: „es gibt noch einen weiteren hohen Wert, nämlich die Sicherheit von Millionen von Volkswagen-Autos“. Die Publikation durfte schlussendlich zwei Jahre später veröffentlicht werden.[194]

6.3.4 Rechtslage in den USA

Auch in den USA sehen sich IT-Sicherheitsforscher*innen einigen rechtlichen Herausforderungen gegenüber. Diese resultieren zum einen aus den urheberrechtlichen Vorgaben des Digital Millennium Copyright Acts (DMCA) sowie individuellen Vertragsbedingungen, welche Reverse Engineering ausdrücklich verbieten. Zum anderen müssen Forschende die Regelungen des Computer Fraud and Abuse Acts (CFAA), welcher unbefugten Zugang zu Computersystemen sanktioniert, sowie die Datenschutzvorgaben beachten. Daneben fürchten Wissenschaftler*innen auch vor einem gerichtlichen Vorgehen wegen Verleumdung oder Offenlegung von Geschäftsgeheimnissen.[195]

Reverse Engineering und Urheberrecht: Das US-amerikanische Recht enthält keine explizite Regelung zum Dekompilieren wie im EU-Recht. Die Zulässigkeit des Reverse Engineerings mittels Dekompilierens oder Disassemblierens sowie der Code-Emulation zur Ermittlung der Funktionsweise eines Programms ohne Zustimmung der Rechteinhaber bestimmt sich nach der Fair Use Doktrin (17 U.S.C. § 107).[196] Grundsätzlich wird es als zulässiges Mittel angesehen, wenn es die einzige Möglichkeit des Zugangs zu nicht geschützten Ideen und Funktionen darstellt und der Täter ein legitimes Ziel verfolgt.[197] Im Präzedenzfall *Sega Enterprises Ltd. vs Accolade, Inc*. führte das Gericht aus, dass, wenn es einen guten Grund gibt, die ungeschützten Aspekte eines urheberrechtlich geschützten Computerprogramms zu studieren oder zu prüfen, die Disassemblierung für die Zwecke eines solchen Studiums oder einer solchen Prüfung einen Fall des Fair Use darstellt.[198] Da die Fair-Use-Regel explizit auch Forschung nennt und einen 4-Faktor-Test vorsieht, wobei u.a. der Nutzungszweck sowie der nicht-kommerzielle Charakter eine Rolle spielen, könnte durchaus davon ausgegangen werden, dass Sicherheitsanalysen ebenfalls unter Fair-Use fallen. Höchstgerichtlich geklärt ist dies aber nicht.

---

[193] Volkswagen AG gegen Garcia and others, High Court of Justice, Urteil vom 25.06.2013 ([2013] EWHC 1832 (Ch).
[194] McKinney, Emma. VW loses legal battle over key security hack. BusinessLive (11.10.2015). https://www.business-live.co.uk/economic-development/vw-loses-legal-battle-over-10229596 (zuletzt abgerufen am 25.09.2021).
[195] Gamero-Garrido/Savage/Levchenko/Snoeren, CCS'17, Fn. 50, S. 1501.
[196] United States Court of Appeals, Ninth Circuit, Sega Enterprises Ltd. vs Accolade, Inc. Decided Oct. 20, 1992, No. 92-15655; United States Court of Appeals, Ninth Circuit, Sony Computer Entertainment Inc. vs Connectix Corp. Decided Feb. 10, 2000, No. 99-15852.
[197] United States Court of Appeals, Ninth Circuit, Sega Enterprises Ltd. vs Accolade, Inc. Decided Oct. 20, 1992, No. 92-15655; United States Court of Appeals, Ninth Circuit, Sony Computer Entertainment Inc. vs Connectix Corp. Decided Feb. 10, 2000, No. 99-15852.
[198] United States Court of Appeals, Ninth Circuit, Sega Enterprises Ltd. vs Accolade, Inc. Decided Oct. 20, 1992, No. 92-15655.

Umgehung technischer Schutzmaßnahmen: 17 U.S.C. § 1201 verbietet die Umgehung technischer Schutzmaßnahmen. Diese Regelung wurde so ausgelegt, dass sie grundsätzlich eine Reihe von Softwareschutzmechanismen abdeckt, die typischerweise bei der Durchführung von Sicherheitsaudits umgangen werden.[199] Ausnahmen bestehen bereits in 17 U.S.C. § 1201 (f), (g), (i) und (j) für Reverse Engineering, Security Testing, Encryption Research und den Schutz personenbezogener Daten. Trotzdem sind diese Ausnahmen noch zu eng gefasst, sodass Forschende eine generelle Ausnahme für Sicherheitsforschung forderten. Basierend auf der Möglichkeit temporäre Ausnahmen zu erlassen, folgte die Library of Congress diesen Forderungen, sodass „good faith security research" nun unter weniger restriktiven Bedingungen möglich ist.[200] Folglich sind Sicherheitsanalysen zu Forschungszwecken auch nach US-Recht nicht völlig frei von Regeln. Diese adressieren aber bereits anders als die auf EU-Recht basierenden Normen des UrhG die Bedürfnisse eines gewissen Freiraums für Forschung im Bereich IT-Sicherheit.

US-Strafnormen: Bezüglich des *Computer Fraud an Abuse Acts* kam der Supreme Court nach Differenzen zur Auslegung mehrerer US-Gerichte zum Ergebnis, dass dieser nicht eingreift für Personen, die grundsätzlich auf ein System oder dessen Daten zugreifen dürfen und können, dies aber im konkreten Zusammenhang unberechtigt tun (bspw. Verletzung von Nutzungsbedingungen oder Dienstbefehlen).[201] Diese Personen verstoßen nicht gegen den CFAA. Erforderlich sei vielmehr die Überwindung einer technischen Barriere. Für Aufsehen gesorgt hatte der Fall des Internetfreiheitsaktivisten Aaron Swartz, der für das Herunterladen von Artikeln aus einer Datenbank, zu der er legal Zugang besaß, strafrechtlich verfolgt wurde.[202] Eine derart weite Auslegung würde eine atemberaubende Menge an alltäglichen Computeraktivitäten mit strafrechtlichen Sanktionen belegen und bezüglich vertraglicher Nutzungsrestriktionen ein nicht hinnehmbares Maß an Willkür in die Beurteilung der strafrechtlichen Verantwortlichkeit hineintragen.[203]

Strafbar machte sich hingegen bspw. ein Täter, der sich über das Passwort-Reset mit Hilfe öffentlich zugänglicher Daten Zugang zum privaten E-Mail-Account einer Politikerin verschaffte. Er wurde wegen Verstoß gegen 18 U.S. Code § 2701 sowie 18 U.S. Code § 1030(1)(2) angeklagt.[204] Ob nach deutschen Recht die Überwindung einer (wirksamen) Zugangssicherung anzunehmen wäre, kann durchaus bezweifelt werden.[205] Allerdings läge im genannten Fall eine Verletzung von Persönlichkeitsrechten vor, da der Täter die privaten Daten öffentlich machte. Insofern fiel dieser Fall nicht in den Bereich des „ethischen Hackens".

[199] Gamero-Garrido/Savage/Levchenko/Snoeren, CCS'17, Fn. 50, S. 1501.
[200] Library of Congress, U.S. Copyright Office, 37 CFR Part 201 [Docket No. 2017–10] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Federal Register/ Vol. 83, No. 208 / Friday, October 26, 2018, S. 54025.
[201] Supreme Court, Urteil vom 03.06.2021- Van Buren v. United States, Az. 19-783.
[202] Sokolov, in: heise „USA: Hacking-Strafrecht eingeschränkt, Millionen User geschützt", 04.06.2021, abrufbar unter: https://www.heise.de/news/USA-Hacking-Strafrecht-eingeschraenkt-Millionen-User-gerettet-6061973.html (zuletzt abgerufen am 11.06.2021).
[203] Supreme Court, Urteil vom 03.06.2021- Van Buren v. United States, Az. 19-783.
[204] Vgl. die Anklageschrift: United States of Amerika vs. David C. Kernell, District Court Eastern District of Tennessee at Knoxville, 2008, Oct 7 - No. 3:08-CR-142.
[205] Nach § 202a StGB ist auf die allgemeine Sicherung der Daten gegenüber dem Zugriff Unbefugter abzustellen, ob die Überwindung typischerweise einen nicht unerheblichen Aufwand erfordert, sodass Fälle, in denen die Durchbrechung des Schutzes für jedermann ohne weiteres möglich ist, den Tatbestand nicht erfüllen: BGH, Beschl. v. 13.5.2020 – 5 StR 614/19.

Empfehlungen und Hilfestellungen

- Die Safety Working Group der NTIA (National Telecommunications and Information Administration) veröffentlichte 2016 das *„Early Stage" Coordinated Vulnerability Disclosure Template*.[206] Das Template bietet für die Zusammenarbeit zwischen Technologieanbietern und Sicherheitsforschenden Prinzipien und Verfahrensvorschläge, die unter Mitwirkung von Vertreter*innen der Industrie, des Staates sowie der Sicherheits-Community erarbeitet wurden
- Das US-Justizministerium (Cybersecurity Unit, Sektion für Computerkriminalität und geistiges Eigentum der Strafabteilung) publizierte im Juli 2017 die erste Version eines Rahmenwerks für ein Programm zur Offenlegung von Schwachstellen bei Online-Systemen.[207]

Die CEPS Task Force zu Software Vulnerability Disclosure in Europe empfiehlt dies als ein mögliches Modell für das EU-Recht zu nutzen. In Anerkennung der Tatsache, dass verschiedene Organisationen unterschiedliche Ziele und Prioritäten für ihre Programme zur Offenlegung von Schwachstellen haben können, schreibt der US-Rahmen weder die Form noch die Ziele für die Offenlegung von Schwachstellen vor. Stattdessen wird ein Prozess für die Gestaltung eines Programms zur Offenlegung von Schwachstellen skizziert, der das autorisierte Verhalten bei der Offenlegung und Aufdeckung von Schwachstellen klar beschreibt, und damit die Wahrscheinlichkeit erheblich verringert, dass solche beschriebenen Aktivitäten zu einer zivil- oder strafrechtlichen Verfolgung führen.[208]

[206] Abrufbar unter https://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf (zuletzt abgerufen am 13.05.2020).
[207] Cybersecurity Unit, A Framework for a Vulnerability Disclosure Program for Online Systems, 2017, abrufbar unter https://www.justice.gov/criminal-ccips/page/file/983996/download (zuletzt abgerufen am 13.05.2020).
[208] Pupillo/Ferreira/Varisco, Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges, Report of a CEPS Task Force June 2018, S. vi.

7 Herausforderungen und Lösungswege bei der praktischen Umsetzung der Vulnerability Disclosure in Deutschland

Niklas Goerke / Johannes Obermaier / Marc Schink / Dieter Schuster

7.1 Vulnerability Disclosure Policies

Um das Schadenspotential von Sicherheitslücken zu minimieren, sollten diese schnellstmöglich behoben werden, wofür die Produkthersteller*innen i.d.R. Patches erstellen oder Nutzende auffordern Schutzmaßnahmen zu treffen. Die Information der Hersteller*in und Nutzenden über gefundene Sicherheitslücken ist erforderlich, um diesen Prozess anzustoßen. Andererseits muss Hersteller*innen ausreichend Zeit eingeräumt werden, um einen Patch zu erstellen, zu testen und den jeweiligen Kund*innen zur Verfügung zu stellen – eine zu frühe Veröffentlichung einer Sicherheitslücke kann ebenfalls zu einer Gefährdung der Nutzenden führen. Dieser Interessenkonflikt wird derzeit durch *Responsible bzw. Vulnerability Disclosure Policies* adressiert, die einen Meldeprozess beschreiben. Der europäische Standard ETSI EN 303 645 V2.1.1 (2020-06) Cyber Security for Consumer Internet of Things: Baseline Requirements enthält in Provision 5.2-1 die Anforderung, dass Hersteller*innen eine Vulnerability Disclosure Policy öffentlich zugänglich zu machen. Diese Policy soll folgende Informationen umfassen:

- Kontaktinformationen für die Meldung von Schwachstellen und
- Informationen über den Zeitplan für
  - Erste Empfangsbestätigung und
  - Statusupdates bis zur Lösung der gemeldeten Schwachstelle.

Provision 5.2-2 fordert eine rechtzeitige /zeitgerechte Reaktion in a „timely manner“, hier werden 90 Tage als üblicher Zeitraum für den gesamten Prozess bis zur Schwachstellenbehebung einschließlich der Benachrichtigung betroffener Kreise bei Software genannt (siehe auch Abschnitt 4.4.3).

Dabei kann im Hinblick auf öffentliche Warnungen berücksichtigt werden, ob Hersteller*innen bemüht sind das Problem zu lösen, ob für die Nutzenden Möglichkeiten bestehen, zusätzliche Maßnahmen zum Selbstschutz zu treffen, oder ob durch die Veröffentlichung eine erhöhte akute Gefährdung der Nutzenden zu befürchten ist, weil etwa die veröffentlichten Informationen die Ausnutzung erleichtern.

Mit der Zunahme von IoT-Produkten wird befürchtet, dass bisher auf Hardware spezialisierte Hersteller*innen sich erstmals mit den Mechanismen der Disclosure von IT-Sicherheitslücken befassen müssen und nicht nur Kontroversen neu entfachen, sondern auch nicht auf die Entgegennahme und Handhabe von Meldungen zu IT-Sicherheitslücken vorbereitet sind.[209] So kam eine Studie im Jahr 2018 zum Ergebnis, dass in dem für Verbraucherschutz relevanten Bereich der IoT-Verbraucherprodukte lediglich 9,7 % der Unternehmen über eine Vulnerability Disclosure Policy verfügen.[210] Eine weitere Studie aus den USA offenbarte, dass zwar einige Produkthersteller*innen die Rolle der IT-Sicherheitsforschung durch Dritte anerkannt haben und explizite

[209] Householder et al., The CERT® Guide to Coordinated Vulnerability Disclosure, SPECIAL REPORT CMU/SEI-2017-SR-022, August 2017, S. VII. So wurde u.a. berichtet, dass einige Unternehmen nach Meldung von Sicherheitslücken zunächst die fünf Phasen des Sterbens nach Kübler-Ross durchlaufen: Leugnen, Zorn, Verhandeln, Depression und schlussendlich Annahme, siehe: Householder et al., S. VIII.

[210] IoT Security Foundation, Understanding the Contemporary Use of Vulnerability Disclosure in Consumer Internet of Things Product Companies, S. 6, abrufbar unter https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/Vulnerability-Disclosure-Design-v4.pdf (zuletzt abgerufen am 16.03.2020).

oder implizite Einwilligungen zur Durchführung solcher Arbeiten geben (entweder uneingeschränkt oder mit zeitlich begrenzter koordinierter Offenlegungspolitik), allerdings die meisten nur ungern auf den Rechtsweg verzichten und entweder nicht bereit sind, sich auf Fragen der Genehmigung einzulassen oder erhebliche Einschränkungen dafür auferlegen. Darüber hinaus fanden die Forscher*innen der University of California einen bedeutenden Unterschied in der Reaktion gegenüber akademischen Forscher*innen im Gegensatz zu unabhängigen Sicherheitsexpert*innen.[211] Ersteren wurde dabei signifikant häufiger gestattet, Produkte zu untersuchen als unabhängigen Expert*innen, welche häufig gar keine Antwort erhielten.

Da der aktuelle rechtliche Rahmen weder IT-Sicherheitsanalysen durch Forschende oder andere unabhängige, neutrale Stellen klar erlaubt, noch die Mechanismen der Coordinated Vulnerability Disclosure verankert hat, ist eine Policy des zur Einwilligung berechtigten Produktverantwortlichen derzeit ein wesentlicher Baustein, um proaktive Sicherheitsanalysen rechtssicher zu ermöglichen.

Einen Überblick über die Aktivitäten der EU-Mitgliedstaaten zur Erreichung einer national koordinierten Politik zur Coordinated Vulnerability Disclosure bietet der Bericht der CEPS Task Force aus dem Jahr 2018.[212] Eine herausragende Rolle nehmen hierbei die Niederlande und Frankreich ein, deren Regulierung auch den Schutz der unabhängigen Sicherheitsforscher zumindest partiell adressiert. In anderen Staaten beschränken sich die Aktivitäten auf die Einrichtung öffentlicher Stellen sowie Definition der Befugnisse, wie dem BSI und CERT-Bund in Deutschland.

Zusätzlich zu Disclosure Policies von Hersteller*innen haben auch Forschergruppen und andere Stellen Disclosure Policies implementiert, die einen klaren Ablauf und Regeln definieren, nach denen sie gefundene Sicherheitslücken an die jeweils verantwortlichen Stellen melden und veröffentlichen.[213] Dabei kann es zu Konflikten kommen, z.B. wenn eine Forschungsgruppe mit einer eigenen Disclosure Policy eine Sicherheitslücke einem/r Hersteller*in melden möchte, der eine konfligierende Policy entgegen hält.

7.2 Einbezug von Hardware-Schwachstellen

Schwachstellen in der Sicherheit eines Produkts können ihren Ursprung sowohl in der Software, wie auch in der Hardware haben. Während der in Leitfäden und Standards beschriebene CVD Prozess vergleichsweise klar auf Softwareschwachstellen anzuwenden ist, erscheint die Anwendung auf Schwachstellen in der Hardware auf den ersten Blick als nicht trivial oder sogar unpassend. Eine solche Unterscheidung ist in der Praxis nicht zielführend wie im Folgenden ausgeführt wird. Es muss darauf hingewirkt werden, dass rechtliche Grundlagen zu Disclosure jegliche Schwachstellen umfassen und hierbei Hardware gleichbehandelt wird.

[211] Gamero-Garrido/Savage/Levchenko/Snoeren, CCS'17, Fn. 50, S. 1501 (1502).
[212] Pupillo/Ferreira/Varisco, Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges, Report of a CEPS Task Force June 2018, S. 13 ff.
[213] https://www.zerodayinitiative.com/advisories/disclosure_policy/ (zuletzt abgerufen am 22.12.2020); https://googleprojectzero.blogspot.com/2015/02/feedback-and-data-driven-updates-to.html (zuletzt abgerufen am 22.12.2020); https://vuls.cert.org/confluence/display/Wiki/Vulnerability+Disclosure+Policy (zuletzt abgerufen am 22.12.2020)

7.2.1 Darstellung in Leitfäden und Standards

Die Meldung und Veröffentlichung von Hardwareschwachstellen tauchen, je nach Dokument, nur sehr untergeordnet und knapp auf. Beispielsweise nimmt der CVD Praxisleitfaden der ENISA[214] an mehr als 60 Stellen explizit Bezug zur Software, nennt den Begriff Hardware aber nur an drei Stellen. Am Anfang des Dokuments wird dargestellt, dass Schwachstellen die Sicherheit von Software als auch Hardwaresystemen kompromittieren können. In den weiteren Ausführungen wird der Hardwareaspekt allerdings vollständig ausgespart bis er, kurz vor Ende des Fließtexts erneut kurz angerissen wird.

Der Standard ISO/IEC 29147:2018 nimmt die Erläuterungen ebenfalls anhand von Softwareschwachstellen vor, verwischt allerdings die Abgrenzung von Hardware- zu Softwarekomponenten bewusst dahingehend, dass diese effektiv gleichgesetzt werden.[215] Bezogen auf die Erläuterungen bezüglich CVD im Dokument sei der Unterschied nur selten relevant. Zur Begründung wird angegeben, dass Schwachstellen in Hardwarekomponenten in den meisten Fällen von Soft- und Firmware herrührten, welche die Funktionalitäten definieren. Reine Hardwareschwachstellen seien rar.

Diese Ausführungen weisen explizit darauf hin, dass die CVD Regeln aus dem Softwarebereich auch für den Hardwarebereich grundsätzlich geeignet sind. Im Gegensatz hierzu lassen sich zahlreiche Einwände finden, die, allerdings nur auf den ersten Blick, eine Gleichsetzung zwischen Hard- und Softwareschwachstellen als unzulässig abtun.

7.2.2 Technische Aspekte

Eines der Hauptargumente ist die angebliche Unbehebbarkeit von Hardwareschwachstellen. Während bei Software das Einspielen eines Patches ausreiche, um eine Lücke zu beheben, sei dies bei Hardware nicht möglich. Dieses Argument greift allerdings zu kurz, da dieses Problem in vielen Fällen insbesondere Software betrifft:

Insolvenz/Liquidierung oder Weigerung des Herstellers: Existiert der/die Hersteller*in eines Geräts nicht mehr, oder nicht mehr in der ursprünglichen Form, vor allem nach Insolvenz oder Liquidation aber auch nach Verschmelzung oder Aufteilung des Unternehmens oder verweigert er sich aus wirtschaftlichen Gründen einer Fehlerbehebung, so ist auch ein offizielles Softwareupdate praktisch ausgeschlossen. Dies ist ein übliches Problem beispielsweise bei Betriebssystemen von Mobiltelefonen, welche bereits wenige Jahre nach Markteintritt oftmals keine Sicherheitsupdates mehr erhalten, bzw. diese nicht mehr über die Update Kanäle an die älteren Endgeräte ausgespielt werden.

Keine Update-Unterstützung: Nicht jedes Softwareprodukt weist die Möglichkeit eines nachträglichen Softwareupdates auf. Die Implementierung einer solchen Funktion ist für den/die Hersteller*in mit Mehraufwand verbunden und mag daher in der Produktentwicklung unwirtschaftlich erscheinen.

Unveränderbare Speicher: Falls Software in einem „ROM“ (nur-lesbarer Speicher) abgelegt ist, so kann diese nicht verändert und dadurch auch nicht aktualisiert werden. Dies ist beispielsweise beim sogenannten „Boot-ROM“ in Mobiltelefonen häufig der Fall,[216] was diese Geräte im Fall von entdeckten Sicherheitslücken dauerhaft unsicher macht.

---

[214] Vgl. ENISA - European Union Agency For Network And Information Security, 2015. Good Practice Guide on Vulnerability Disclosure, From challenges to recommendations, DOI 10.2824/610384.

[215] Vgl. ISO/IEC 29147:2018 - Information technology — Security techniques — Vulnerability disclosure, 2018, Kapitel 5.4.2

[216] heise.de, Checkra1n: Erster öffentlicher Jailbreak für iOS 13, abrufbar unter https://www.heise.de/mac-and-i/meldung/Checkra1n-Erster-oeffentlicher-Jailbreak-fuer-iOS-13-4583844.html (zuletzt abgerufen am 23.11.2020)

Diese Punkte verdeutlichen, dass Software von sehr ähnlich gelagerter Problematik wie Hardware betroffen ist. Paradoxerweise existieren aber auch Hardwareschwachstellen, welche dennoch per Software zu Teilen behebbar sind. Als Beispiel seien die Prozessor-Schwachstellen „Spectre“ [217] und „Meltdown“ [218] genannt, welche mehrere Generationen an Desktop- und Serversystemen betrifft. Mit Hilfe einer Aktualisierung der internen Ablaufsteuerung des Prozessors („Microcode Update“) konnten diese Schwachstellen in bestehenden Systemen mitigiert werden.[219] Somit verschwimmt die Grenze zwischen Hard- und Softwareschwachstellen derart, dass eine Argumentation anhand dieser Metrik nicht zielführend erscheint. Über die (Nicht-)Behebbarkeit beider Kategorien von Sicherheitslücken kann keine allgemeine Aussage getroffen werden.

7.2.3 Finanzielle Aspekte

Es lässt sich bezüglich der vermeintlichen zwei Klassen an Schwachstellen feststellen, dass Hardwarelücken oftmals als Sinnbild von „nicht behebbaren“ und teuren Schwachstellen gesehen werden, Softwareschwachstellen allerdings als nahezu trivial per „Update“ zu beseitigen.

Eine Softwareaktualisierung ist oftmals die wirtschaftlichste Option für eine/n Hersteller*in; Kosten dürfen aber nicht als Totschlagargument gegen Alternativen sprechen. Im Fall von unbehebbaren Schwachstellen besteht beispielsweise immer die Möglichkeit eines Rückrufs der entsprechenden Komponenten – egal ob Soft- oder Hardware. Die damit verbundenen Aufwände stellen ein zu berücksichtigendes Risiko in jeder Produktentwicklung dar. So musste beispielsweise Fiat in Folge von Schwachstellen in der Software im Jahr 2015 mehr als 1,4 Millionen Fahrzeuge zurückrufen.[220]

Eine Bewertung nach den Auswirkungen bzw. dem Aufwand zur Fehlerbehebung unterläuft außerdem die Zielsetzung von CVD (vgl. Kapitel 4.1). Sofern problematische Sicherheitslücken von einer Veröffentlichung ausgeschlossen werden, führt dies zu einem blinden Fleck in der IT-Sicherheit. Der Fehler existiert weiterhin und die Kunden sind nicht vor Angriffen geschützt (vgl. Kapitel 4.3 Abs. Non Disclosure). Ein solcher Fall trat 2013 auf, als eine Publikation über eine Schwachstelle in Millionen Fahrzeugschlüsseln vorerst gerichtlich verhindert[221] und erst mit zwei Jahren Verzögerung veröffentlicht werden konnte.[222] Kritiker sehen die Ursache des harten Vorgehens darin, dass die Lücke einen Austausch der Komponenten erfordert hätte, die Software nicht aktualisierbar sei, und dies immense Aufwände bedeutet hätte.[223]

---

[217] Vgl. Kocher et al., Spectre Attacks: Exploiting Speculative Execution, IEEE S&P 2019 (siehe auch https://meltdownattack.com/ (zuletzt abgerufen am 16.07.2021)

[218] Vgl. Lipp et al., Meltdown: Reading Kernel Memory from User Space, USENIX 2018 (siehe auch https://meltdownattack.com/ (zuletzt abgerufen am 16.07.2021)

[219] heise.de, Windows/Meltdown: Patch für 32 Bit, AMD-Problem behoben, abrufbar unter: https://www.heise.de/security/meldung/Windows-Meltdown-Patch-fuer-32-Bit-AMD-Problem-behoben-3946613.html (zuletzt abgerufen am : 16.07.2021]

[220] Heise.de, Nach Fernsteuerungs-Hack ruft Fiat Chrysler 1,4 Millionen Autos zurück, abrufbar unter https://www.heise.de/newsticker/meldung/Nach-Fernsteuerungs-Hack-ruft-Fiat-Chrysler-1-4-Millionen-Autos-zurueck-2762914.html (zuletzt abgerufen am 23.11.2020).

[221] Volkswagen AG vs. Garcia Case [2013] EWHC 1832 (Ch), 25.06.2013.

[222] Verdult/Garcia/Ege, Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer, USENIX 2013.

[223] Volkswagen-Hack nach langer Sperrverfügung veröffentlicht https://www.golem.de/news/autoschluessel-volkswagen-hack-nach-langer-sperrverfuegung-veroeffentlicht-1508-115731.html (zuletzt abgerufen am 11.10.2021).

7.2.4 Nutzen für Allgemeinheit in den Vordergrund stellen

Das Ziehen einer Grenze zwischen Hard- und Softwareschwachstellen, insbesondere mit a priori Berücksichtigung der Aufwände zu deren Behebung, ist in der Praxis somit nicht sinnvoll möglich. Erst recht kann diese Aufgabe zur Unterscheidung einem Meldenden nicht auferlegt werden.

Insbesondere bei sehr schwierigen und nicht behebbaren Lücken ist es wichtig, die Allgemeinheit über diese Problematik zu informieren. Nur eine offene Diskussion ermöglicht es Betroffenen, entsprechend ihrer Sicherheitsanforderungen zu reagieren und eigenständig Maßnahmen zu ergreifen. Eine Unterscheidung nach dem Ursprung der Schwachstelle ist für den/ die Endanwender*in in der Regel unerheblich. Die rechtliche Absicherung von IT-Sicherheitsforschung muss Soft- wie Hardwareaspekte identisch behandeln, um dieses Ziel erreichen zu können.

7.3 CVD in der Praxis

Eine erfolgreiche Durchführung des CVD Prozesses in der Praxis ist von der Mitwirkung sowohl des Meldenden als auch des betroffenen Unternehmens abhängig. In Hinblick auf Abbildung 1 (siehe Abschnitt 4.1) muss festgehalten werden, dass diese lediglich den theoretischen Ablauf eines optimalen Disclosure Prozesses darstellt, welcher in der Praxis abweichen kann. Inwiefern das Zusammenwirken von Meldenden und betroffenen Unternehmen auch in der Realität funktioniert, lässt sich im Allgemeinen schlecht erkennen, da Veröffentlichungen selten auch den vorangegangenen Prozess publik machen. Anders ist dies bei Google Project Zero, welches sämtliche gefundenen Sicherheitslücken samt der dazugehörigen Meldeprozesse (nach Ablauf der Frist) öffentlich dokumentiert.[224] Google selbst nutzt diese Daten auch, um ihren Prozess zu evaluieren. So kann man sehen, dass zum Stand April 2020 bei 95.9% der gemeldeten Schwachstellen von Project Zero, vor der allgemeinen Veröffentlichung, eine Behebung des Fehlers verfügbar war.[225] Diese Erfolgsquote könnte dem Ruf bzw. der Bekanntheit des Unternehmens geschuldet sein, so dass dessen Meldungen von Anfang an ernst genommen und mit entsprechender Priorität bearbeitet werden.

7.3.1 Fristen im Disclosure Prozess

Doch auch bei einem großen und bekannten Unternehmen als Melder*in gibt es Fälle, bei denen vor Ablauf der Frist keine Lösung verfügbar war. Dies liegt zum einen an der gesetzten Frist selbst, welche von den Betroffenen in einigen Fällen als nicht ausreichend angesehen wird. Hier äußerte sich zum Beispiel Microsoft öffentlich,[226] nachdem von Google eine Veröffentlichung einer Schwachstelle vor einem ausgerollten Patch erfolgte. Microsoft vertrat die Position, dass es keine feste Frist geben sollte, während in Koordination mit dem Melder an der Fehlerbehebung gearbeitet wird.

In einem Fall mit Logitech zeigte sich jedoch eine solche Frist als hilfreich.[227] Erst nach Ablauf der Frist und der damit einhergehenden Veröffentlichung erfolgte in diesem Fall innerhalb weniger Tage eine Behebung des Fehlers auf Seite des Herstellers. Dem veröffentlichten Verlauf lässt sich entnehmen, dass die Fehlerbehebung auf der Seite des Herstellers erst mit der Veröffentlichung der Lücke priorisiert wurde.

---

[224] https://bugs.chromium.org/p/project-zero/issues/list (zuletzt abgerufen am 11.10.2021).
[225] https://googleprojectzero.blogspot.com/p/vulnerability-disclosure-faq.html (zuletzt abgerufen am 11.10.2021).
[226] https://msrc-blog.microsoft.com/2015/01/11/a-call-for-better-coordinated-vulnerability-disclosure/ (zuletzt abgerufen am 11.10.2021).
[227] https://bugs.chromium.org/p/project-zero/issues/detail?id=1663 (zuletzt abgerufen am 11.10.2021).

Generell ist eine derartige Frist ein Richtwert und es wird mit damit unterschiedlich umgegangen (vgl. Kapitel 4.4.3).

So kann der Zeitraum beispielsweise verlängert werden, wenn die Behebung der Schwachstelle oder die Bereitstellung von Gegenmaßnahmen aus nachvollziehbaren Gründen, wie zuerst nicht zu erkennender Komplexität und nicht etwa wegen fehlenden Engagements des Herstellers, mehr Zeit in Anspruch nimmt, als anfangs angenommen. Auch eine drastische Verkürzung auf wenige Tage kommt in der Praxis vor. Das Team von Google Projekt Zero hat Informationen über eine Schwachstelle im Betriebssystem iOS von Apple bereits nach 7 Tagen veröffentlicht. Der Grund dafür waren Hinweise auf Angriffe mit Hilfe der entdeckten Schwachstelle.[228] Mit der zeitnahen Veröffentlichung sollte verhindert werden, dass betroffene Personen, beispielsweise Journalist*innen, zu lange einem Risiko durch die Schwachstelle ausgesetzt sind. Trotz der kurzen Zeit war Apple in der Lage die Schwachstelle zu beheben und Patches bereitzustellen. In jedem Fall sind betroffene Personen durch die frühzeitige Veröffentlichung in der Lage ihren Umgang mit den betroffenen Produkten zu ändern oder dessen Verwendung gar vollständig einzustellen. Bislang fehlt es noch an übertragbaren Erkenntnissen und Forschung dazu, für welche Kategorien von Schwachstellen welche Fristen üblicherweise angemessen sind. Die konkrete Festlegung bleibt daher eine Frage des Einzelfalls.

7.3.2 Bewertung der Schwachstelle und Inhaltliche Darstellung

Nicht nur der Zeitpunkt einer Veröffentlichung kann zum Streitpunkt zwischen Sicherheitsforschenden und Unternehmen werden. Die Bewertung einer Schwachstelle birgt weiteres Konfliktpotential. So bewerten Hersteller*innen oftmals die Kritikalität einer Schwachstelle aus verschiedensten Gründen (vgl. „Limited Disclosure“ in 4.3) eher als gering oder erkennen diese gar nicht an.[229] Die Verwendung des Common Vulnerability Scoring System (CVSS) zur Bewertung der Schwere kann in einigen Fällen Abhilfe schaffen. In diesem System wird die Schwere einer Schwachstelle Anhand eines standardisierten Fragenkatalogs bewertet (vgl. 5.2).

Art und Umfang einer Veröffentlichung sind oft weitere Streitpunkte. So werden von Hersteller*innen in einigen Fällen Änderungswünsche oder gar das Entfernen von kompletten Abschnitten aus Publikation gefordert. Dadurch soll eine Darstellung insbesondere von technischen Details verhindert werden, beispielsweise um die Nachvollziehbarkeit und damit die Auswirkung einer Schwachstelle abzuschwächen.[230] Zusätzlich geht es oft auch um Fragen der Aufdeckung und Zuschreibung von Nachlässigkeiten im Entwicklungsprozess. Verantwortliche befürchten hierzu Reputationsschäden und Haftung. Eine andere Art den Veröffentlichungsprozess zu beeinflussen ist die Forderung nach Geheimhaltungsverträgen, sogenannten Non-Disclosure Agreements (NDAs), bevor mit Sicherheitsforscher*innen inhaltlich kommuniziert wird.[231] Dadurch wollen Hersteller*innen den Informationsfluss über die Schwachstelle kontrollieren. Da in einigen Fällen keine ausführliche oder gar keine Beschreibung zu Schwachstellen durch die Hersteller*innen veröffentlicht wird, sind betroffene Kund*innen allerdings auf eine unabhängige Publikation der Sicherheitsforscher angewiesen.[232]

---

[228] A very deep dive into iOS Exploit chains found in the wild https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html (zuletzt abgerufen am 11.10.2021).

[229] Obermaier/Schink, Tales from Hardware Security Research: From Research over Vulnerability Discovery to Public Disclosure, 2019, abrufbar unter https://media.ccc.de/v/Camp2019-10292-tales_from_hardware_security_research (zuletzt abgerufen am 11.10.2021).

[230] Obermaier/Schink, Fn. 229.

[231] Obermaier/Schink, Fn. 229.

[232] Obermaier/Schink, Fn. 229.

7.3.3 Unterstützung durch Melde- und Koordinierungsstellen

In den im vorherigen Absatz genannten Fällen, bei einer kompletten Verweigerung einer Kontaktaufnahme oder verschleppenden oder verschleiernden Behandlung durch den/die Hersteller*in[233] oder wenn ein Dissens bezüglich Ob, Art oder Umfang einer Veröffentlichung besteht, der sich nicht auflösen lässt, kann eine neutrale Stelle einbezogen werden. Im Falle international tätiger Hersteller*innen verfügen unabhängige Koordinierungsstellen über entsprechende Kontakte zu Einrichtungen in anderen Ländern und informieren diese bei Bedarf. Ein Nachteil im CVD Prozess besteht allerdings darin, dass sich die Abstimmung in der Praxis als komplexer erweist, da nun drei Parteien eingebunden sind. Da es im Verlauf naturgemäß auch zu bilateralen Abstimmungen kommt, kann es dementsprechend aufwändiger sein, sicherzustellen, dass alle Parteien jederzeit auf dem identischen Informationsstand sind. Die Unterstützung einer Koordinierungsstelle kann allerdings entscheidend sein für den positiven Ausgang eines CVD Prozesses.

7.3.4 Asymmetrische Rechtssituation zwischen Meldendem und Betroffenen Unternehmen

Die Erfahrungen mit CVD erstrecken sich somit über ein breites Spektrum von positiv bis negativ. Während beispielsweise Googles Project Zero in mehr als 95% erfolgreich für eine Lösung des Problems sorgen konnte, beklagen andere Forschergruppen ausbleibende Antworten und mangelnden Willen zur Kooperation. Hierbei liegt der Schluss nahe, dass Ansehen und die Größe des meldenden Unternehmens, bzw. der Forscher*in einen Einfluss auf die Chance haben, CVD erfolgreich durchzuführen. Dies schränkt somit große Teile der Forschungsgemeinschaft ein, welche weitgehend unabhängig und eigenständig Schwachstellen zu melden versuchen.

Dies geht einher mit einem weiteren Problem, welches aus der rechtlichen Unsicherheit hervorgeht und diese langfristig sogar weiter verstärken könnte. Wie im vorhergehenden Kapitel beschrieben, können große Unternehmen wie Google, relativ frei Schwachstellen anhand selbst gesetzter Regeln publizieren und dabei beispielsweise sogar erfolgreich gegen Microsoft Stellung beziehen. Diese Möglichkeiten stehen aber nur sehr wenigen Forschenden und Forschungsabteilungen offen, welche das rechtliche und finanzielle Risiko eines möglichen Rechtsstreits tragen können und wollen. Dies kann langfristig dazu führen, dass CVD Gefahr läuft, durch finanziell gutgestellte Unternehmen entsprechend ihrer eigenen Interessen definiert zu werden. Dies führte bereits 2001 zu Diskussionen,[234] als Microsoft Regeln für „Responsible Disclosure“ aufzustellen versuchte,[235] welche die Veröffentlichung von Informationen über Schwachstellen einschränken würden. Die Akzeptanz von freieren Publikationsmöglichkeiten ist zwar inhaltlich begrüßenswert, darf aber nicht darüber hinwegtäuschen, dass dennoch ein Privatunternehmen und nicht die Legislative hierbei federführend war.

Ein weiterer Aspekt ist das Risiko der Forschenden und Forschungsinstitutionen ohne große zeitliche, rechtliche und finanzielle Kapazitäten beim Melden von Schwachstellen. Sobald ein*e Forscher*in eine Sicherheitslücke entdeckt hat und diese verantwortungsvoll entsprechend CVD dem/der Hersteller*in mitteilen will, muss die eigene Identität praktisch offengelegt werden. Im Hinblick auf eine zielführende Kommunikation ist es notwendig, Telefonnummer, E-Mailadressen, und Namen der Ansprechpartner auszutauschen. Diese Schritte sind nicht sinnvoll anonym durchführbar, da spätestens bei der wissenschaftlichen Publikation die Autoren sowie die Institution preisgegeben werden. Auf Seiten der Forscher*innen stellt dies ein signifikantes Risiko dar, wobei die betroffenen Unternehmen selbst praktisch keinerlei Verpflichtungen haben. Hierbei

[233] Obermaier/Schink, Fn. 229.
[234] http://www.attrition.org/security/rant/z/ms-disclose.html (zuletzt abgerufen am 11.10.2021).
[235] https://www.theregister.com/2001/11/09/ms_throttles_research_to_conceal/ (zuletzt abgerufen am 11.10.2021).

wird den Forschenden ein moralisches Dilemma auferlegt, wie sie die Mitteilung der Schwachstelle durchführen (vgl. Kapitel 4.3): Beim Full Disclosure setzt die sofortige Veröffentlichung der Schwachstelle die unvorbereitete Allgemeinheit und den/die Hersteller*in einem großen Sicherheitsrisiko aus, wobei die Meldenden dies in der Regel risikoarm, da anonym, durchführen können. Bei CVD hingegen liegt das primäre Risiko auf Seiten der Meldenden, da diese auf das Wohlwollen des betroffenen Unternehmens angewiesen sind. Dies drängt Forschende unmittelbar in Handlungsweisen wie Full-Disclosure (vgl. Kapitel 4.3), die aber nicht im Interesse der Allgemeinheit und betroffenen Unternehmen sein können. Dass die Angst vor rechtlichen Maßnahmen eine angebrachte Befürchtung ist, zeigen einige Fälle eindrucksvoll (vgl. Kapitel 7.2.3).[236]

Eine anhaltende rechtliche Unsicherheit in der praktischen Durchführung von CVD führt zu einem Abschreckungseffekt, der die Gemeinschaft der Forschenden betrifft. In erster Linie wird, wie auch in Kapitel 6.2.4 beschrieben, eine Einschränkung und Änderung von Forschungsvorhaben durch die Forschenden selbst berichtet. Darüber hinaus sind den Autor*innen Fälle bekannt, in denen auch Institute und Lehrstühle entsprechende Risiken scheuen und Beschränkungen bezüglich Forschungsthemen setzen. Die Risiken treffen aber auch private Sicherheitsforscher, welche, oftmals zufällig, auf Schwachstellen stoßen. Da diese Personen über keine übergeordnete und ggf. schützende Institution verfügen, sind sie insbesondere von der rechtlichen Unsicherheit betroffen.

[236] Maier/Franzen/Wagner, DuD 2020, 511.

8 Glossar

Bug Bounty	Auslobung von Sach- oder Geldpreisen für Entdecker*innen von Sicherheitslücken durch Unternehmen, staatlichen Stellen oder sonstigen Produktverantwortlichen
Hersteller*in	hier i.d.R. Bezeichnung für die für ein Produkt verantwortende Stelle
Melde- und Koordinierungsstelle	Neutrale Stelle, welche im Rahmen eines Coordinated-Disclosure-Prozesses unterstützt
Produkt	IT-Produkte im Sinne dieses Whitepapers sind Software, Hardware sowie alle einzelnen oder miteinander verbundenen Komponenten, die Informationen informationstechnisch verarbeiten (vgl. § 2 Abs. 9a BSIG)
Produktverantwortliche*r	Stelle, die ein Produkt verantwortet (i.d.R. herstellendes Unternehmen)
Schwachstelle	hier synonym verwendet für Sicherheitslücke
Sicherheitsforscher*in	Personen, die die Sicherheit von Produkten und Systemen sowie Sicherheitslücken erforschen, sowie Personen, die Sicherheitslücken durch methodisches Vorgehen entdecken und melden
Sicherheitslücke	Definiert in § 2 Abs. 6 BSIG als Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können, hier synonym verwendet für Schwachstelle / Sicherheitsmangel
System	informationsverarbeitende Systeme, Komponenten und Prozesse

Abkürzungen

AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AGB	Allgemeine Geschäftsbedingungen
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)
CVD	Coordinated Vulnerability Disclosure
DSGVO	Datenschutz-Grundverordnung
EMRK	Europäische Menschenrechtskonvention
ErwGr	Erwägungsgrund

EU-GrC	EU-Grundrechtecharta
GeschGehG	Gesetz zum Schutz von Geschäftsgeheimnissen
GG	Grundgesetz
HalblSchG	Halbleiterschutzgesetz
IKT	Informations- und Kommunikationstechnologie
PatG	Patentgesetz
StGB	Strafgesetzbuch
UK	United Kingdom
UrhG	Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz)
WBRL	„Whistleblower-Richtlinie“ – (EU) 2019/1937

9 Autor*innen

Dr. Manuela Wagner, Niklas Goerke, Daniel Vonderau, Hoa Tran, Maria Pieper, Silvia Balaban

FZI Forschungszentrum Informatik, Karlsruhe

Dr. Johannes Obermaier, Dieter Schuster, Marc Schink

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC), München

Dr. Michael Kreutzer, Linda Schreiber LL.M. (Darmstadt), LL.M. (Edinburgh)

Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE, Darmstadt

Jun.-Prof. Dr. Dominik Brodowski LL.M. (UPenn)

Juniorprofessur für Strafrecht und Strafprozessrecht, Universität des Saarlandes

Jun.-Prof. Dr. Sebastian Golla

Juniorprofessur für Kriminologie, Strafrecht und Sicherheitsforschung im Digitalen Zeitalter an der Ruhr-Universität Bochum

Prof. Dr. Franziska Boehm, Oliver Vettermann (geb. Bizuga)

FIZ Karlsruhe - Leibniz-Institut für Informationsinfrastruktur, Karlsruher Institut für Technologie (KIT)
Zentrum für Angewandte Rechtswissenschaft (ZAR)

Prof. Dr. Christoph Sorge, Dr. Jochen Krüger, Maximilian Leicht LL.M. (UdS)

Lehrstuhl für Rechtsinformatik, Universität des Saarlandes

Dr. Stephanie Vogelgesang LL.M. (UdS)

Saarbrücker Zentrum für Recht und Digitalisierung (ZRD-Saar)

Roman Dickmann LL.M. (Univ. Münster)

Fachanwalt für Versicherungsrecht

Stephan Koloßa

Mitglied der Forschungsgruppe „SecHuman“ der Ruhr-Universität Bochum (bis Ende 2020)

Fabian Franzen

Technische Universität München

Weitere Informationen unter: www.sec4research.de