bidt Bayerisches Forschungsinstitut für Digitale Transformation
EIN INSTITUT DER BAYERISCHEN AKADEMIE DER WISSENSCHAFTEN

IMPULSE

Lücken schließen:

Der verantwortungsbewusste Umgang mit IT-Sicherheitslücken

AutorInnen:
Oliver Vettermann
Manuela Wagner
Maximilian Leicht
Felix Freiling

Impressum

bidt Impulse Nr. 5

bidt – Bayerisches Forschungsinstitut
für Digitale Transformation
Gabelsbergerstraße 4
80333 München
www.bidt.digital

Koordination
Margret Hornsteiner, Nadine Hildebrandt
dialog@bidt.digital

Gestaltung
made in – Design und Strategieberatung
www.madein.io

Veröffentlichung
April 2023

ISSN: 2701-2395
DOI: 10.35067/b0bj-im05

Das Bayerische Forschungsinstitut für Digitale Transformation (bidt) trägt als Institut der Bayerischen Akademie der Wissenschaften dazu bei, die Entwicklungen und Herausforderungen der digitalen Transformation besser zu verstehen. Damit liefert es die Grundlagen, um die digitale Zukunft der Gesellschaft verantwortungsvoll und gemeinwohlorientiert zu gestalten.

Praktisch ausnutzbare Sicherheitslücken bedrohen die IT-Sicherheit privater wie staatlicher Infrastrukturen. Die Beseitigung der Lücken ist daher für alle Akteure wünschenswert. Dennoch fehlt oftmals ein auf Kooperation basierendes Schwachstellenmanagement. Zudem sind durch die Rechtsunsicherheiten für Forschende Abschreckungseffekte zu beobachten. Die Autorinnen und Autoren skizzieren in diesem „bidt Impuls“ den Status quo und zeigen Lösungsansätze auf, um die konfligierenden Interessens- und Rechtspositionen zu entwirren.

AutorInnen

Dr. Oliver Vettermann ist wissenschaftlicher Mitarbeiter am FIZ Karlsruhe – Leibniz-Institut für Informationsinfrastruktur.
E-Mail: oliver.vettermann@fiz-karlsruhe.de

Dr. Manuela Wagner ist wissenschaftliche Mitarbeiterin am Forschungszentrum für Informatik Karlsruhe.
E-Mail: manuela.wagner@fzi.de

Maximilian Leicht, LL.M. ist wissenschaftlicher Mitarbeiter an der Universität des Saarlandes.
E-Mail: maximilian.leicht@uni-saarland.de

Prof. Dr.-Ing. Felix Freiling ist Professor für Informatik an der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) und Mitglied im Direktorium des bidt.
E-Mail: felix.freiling@bidt.digital

Abstract

Praktisch ausnutzbare Sicherheitslücken bedrohen die IT-Sicherheit privater wie staatlicher Infrastrukturen. Die Beseitigung der Lücken ist daher für alle Akteure, wie Produktherstellerinnen und -hersteller, Betreiberinnen und Betreiber sowie Nutzerinnen und Nutzer, wünschenswert. Dennoch zeigten Konflikte zwischen Herstellerseite und unabhängigen, proaktiv tätigen Sicherheitsforschenden, dass ein auf Kooperation basierendes Schwachstellenmanagement oftmals fehlt. Obwohl sich Expertinnen und Experten überwiegend bezüglich der grundsätzlichen Notwendigkeit eines koordinierten Zusammenwirkens durch Coordinated-Vulnerability-Disclosure-Prozesse (CVD) einig sind, ist dieses aktuell weder rechtlich verpflichtend geregelt noch flächendeckend umgesetzt. Vielmehr sind durch die Rechtsunsicherheiten für Forschende Abschreckungseffekte zu beobachten.

Der „bidt Impuls“ skizziert diesen Status quo und zeigt Lösungsansätze auf, um die konfligierenden Interessens- und Rechtspositionen zu entwirren. Neben der Beseitigung einiger rechtlicher Hemmnisse durch die Gesetzgebung wird von den Autorinnen und Autoren die Einrichtung einer koordinierenden und im Konfliktfall schlichtenden Meldestelle zur Unterstützung von Disclosure-Prozessen empfohlen.

Inhalt

01 Einleitung 6

02 Problem: IT-Sicherheitslücken und Coordinated Disclosure in der IT-Sicherheitsforschung und darüber hinaus 10

2.1 IT-Sicherheitslücken als Risiko und Chance 12
2.2 Probleme der Coordinated Disclosure 13
2.3 Institutionelle Forschung, ethisches Hacken und Zufallsfunde 14

03 Lösungsansatz 1: Juristische Impulse für einen Rechtsrahmen 16

3.1 Verfassungsrechtlicher Schutzauftrag zur Gewährleistung der IT-Sicherheit 18
3.2 Strafrecht als Hemmnis für unabhängige Sicherheitsüberprüfungen 19
3.3 Aspekte aus IT-Sicherheits- und Datenschutzrecht 21

04 Lösungsansatz 2: Etablierung einer Melde- und Koordinierungsstelle 24

4.1 Ziel: Koordinierter Ausgleich von Interessen 25
4.2 Anforderungen an eine Melde- und Koordinierungsstelle 26

05 Fazit: Interdisziplinäre Übersetzungsarbeit aller Beteiligten 30

Literaturverzeichnis 34

01

Einleitung

IT-Sicherheitslücken in Hard- und Software betreffen private, unternehmerische und staatliche Systeme. Sobald eine Ausnutzung der Lücken technisch möglich ist, stellen sie eine Bedrohung für die IT-Sicherheit aller Beteiligten dar. Konkret betroffen sind Bürgerinnen, Bürger und Unternehmen als Nutzende, Herstellerinnen und Hersteller von Soft- und Hardware sowie staatliche (kritische) IT-Infrastruktur. Es ist daher im gesamtgesellschaftlichen Interesse, die Zahl der ausnutzbaren Sicherheitslücken so gering wie möglich zu halten.

Gelingen kann dies nur durch ein defensives staatliches Handeln, das zur Behebung von IT-Sicherheitslücken beiträgt. Erst eine solche Ausrichtung erkennt den förderlichen Aspekt der IT-Sicherheitsforschung, die durch das Melden von entdeckten Sicherheitslücken auch zu deren effektiver und schneller Beseitigung beiträgt. Nach der klar überwiegenden Auffassung der IT-Sicherheitsforschung verschlechtert das Geheimhalten von Sicherheitslücken dagegen die IT-Sicherheitslage, weil eine parallele Entdeckung oder der Abfluss entsprechenden Wissens und damit ein unkontrollierbarer Missbrauch jederzeit möglich erscheinen.

Ein Baustein in der defensiven Ausrichtung ist der Prozess der Coordinated Vulnerability Disclosure (CVD). Dieser wird jedoch in den betroffenen Branchen kaum praktiziert, mutmaßlich auch weil ein solcher Prozess im Rechtsrahmen nicht verankert ist. In der Folge entstehen immer wieder Konflikte zwischen Herstellern von Produkten, die IT-Sicherheitslücken aufweisen, und proaktiv tätigen Sicherheitsforschenden bzw. ethischen Hackerinnen oder Hackern. Dadurch wird die Beseitigung der Lücken merklich beeinträchtigt.

CVD

Coordinated Vulnerability Disclosure

Dieser „bidt Impuls“ zeigt mit dem Konstrukt der Melde- und Koordinierungsstelle für CVD-Prozesse eine Lösung auf, IT-Sicherheitsforschende und sonstige Finderinnen und Finder von IT-Sicherheitslücken zugunsten des Gemeinwohls in die Beseitigung von Sicherheitslücken einzubeziehen. Dazu wird zunächst auf die aktuell bestehenden gesetzlichen Hemmnisse eingegangen. Diese sind durch eine Anpassung des Rechtsrahmens zu beseitigen. Anschließend werden rechtliche und institutionelle Mittel zur Gestaltung einer IT-Sicherheitslandschaft aufgezeigt, welche national existierende Systeme bei allen Betroffenen langfristig resilienter macht und die nationale IT auf zukünftige Angriffe vorbereitet.

Hinweis Dieser „bidt Impuls“ stellt eine Kurzfassung des im Frühjahr 2023 erschienenen Whitepapers (Wagner et al. 2023) dar, das eine vertiefte interdisziplinäre Analyse der Thematik einschließlich Quellen enthält. Für nähere Begründungen wird daher auf die Langfassung verwiesen.

02

PROBLEM:

IT-Sicherheitslücken und Coordinated Disclosure in der IT-Sicherheitsforschung und darüber hinaus

IT-Sicherheit hat das Ziel, Informationen samt den sie speichernden und verarbeitenden Systemen zu schützen. Es gilt unberechtigte Zugriffe auf Daten zu verhindern, zugleich berechtigte Zugriffsmöglichkeiten sowie die Zuverlässigkeit und Vertraulichkeit der Systeme zu erhalten. Dabei sind Soft- und Hardware nicht entkoppelt zu betrachten. Vielmehr lassen jüngere Angriffsformen die Grenze zwischen hardware- und softwarespezifischen Angriffsvektoren verschwimmen. Eine Verringerung der breiten Angriffsoberfläche (Mitigation) durch Patches oder andere Maßnahmen muss dies berücksichtigen.

2.1 IT-Sicherheitslücken als Risiko und Chance

Ein Fehler in Form einer Kompromittierung von Soft- oder Hardware ist dann eine Schwachstelle, wenn sich der Fehler potenziell zur Verletzung der Schutzziele der IT-Sicherheit eignet. Wandelt sich das Potenzial so, dass die Schwachstelle in der Praxis tatsächlich ausnutzbar ist, handelt es sich um eine Bedrohung. Je nach Wirkung und Folgen einer Ausnutzung wird durch Bedrohungsanalysen von fachlich kompetenten Personen der Schweregrad der Bedrohung ermittelt. Eine derartige Analyse kann sowohl intern durch IT-Sicherheitsbeauftragte wie extern durch Forschende und Hackerinnen und Hacker erfolgen. Letztere verfolgen regelmäßig das Ziel, (neue) Bedrohungen zu erkunden.

Die Bedrohung durch eine Schwachstelle in Soft- und/oder Hardware entwickelt sich so zur echten Chance: Durch einen koordinierten Prozess der Offenlegung der Schwachstelle kann eine Vermittlung zwischen allen Beteiligten erfolgreich sein. Als Grundlage dienen die Standards ISO/IEC 30111 und ISO/IEC 29147:2018 sowie die Vorgaben der ENISA (ENISA 2015). Nach dem Prinzip der Coordinated Disclosure (auch Responsible Disclosure) meldet die Finderin/der Finder die gefundene Schwachstelle vertraulich an die produktverantwortliche Stelle, die die Schwachstelle – voraussichtlich – beheben kann. Der kontaktierte Produktverantwortliche oder das herstellende Unternehmen kooperiert dann mit der Finderin/dem Finder zur Analyse und Behebung der Schwachstelle. Um die schnelle Behebung möglichst ohne unberechtigte Ausnutzung der Schwachstelle zu ermöglichen, werden die zugehörigen Informationen idealerweise erst nach der Behebung der Schwachstelle oder dem Bereitstellen einer passenden Mitigation öffentlich gemacht. Die Veröffentlichung dient zusätzlich als Warnung für Produktnutzende. Insgesamt werden Risiken für potenziell Betroffene signifikant minimiert.

2.2 Probleme der Coordinated Disclosure

Der Prozess ist allerdings einer Vielzahl von Problemen ausgesetzt.

1

Identifikation und Kommunikation der Produktverantwortlichen:

Die Identifikation der produktverantwortlichen Stelle bereitet besonders bei importierten Produkten, vielgliedrigen Lieferketten und nur in einzelnen Modulen existenten Sicherheitslücken Probleme. Ähnlich schwierig ist die Identifikation, wenn durch eine Softwarebibliothek gleichzeitig mehrere Herstellerinnen und Hersteller betroffen sind. Auch ist unklar, ob innerhalb von Unternehmen die öffentliche Kontaktstelle (z. B. Kontaktformular, Support-Hotline) die richtige Stelle ist. Oft sind Mitarbeitende mit Nähe zur betroffenen IT nicht auf diesem Weg erreichbar.

2

Abweichende Einschätzung:

Die Einschätzung der Kritikalität der gefundenen Sicherheitslücke kann aus Sicht des Produktverantwortlichen anders (z. B. höher) ausfallen als die der Finderin/des Finders. Dies geschieht häufig durch fehlende Kenntnis der Interna oder fehlendes Fachwissen und damit unabsichtlich.

Juristische Grauzone:

3 In Einzelfällen werden Finderinnen und Findern juristische Maßnahmen angedroht und tatsächlich eingeleitet, um sie von einer Veröffentlichung oder weiteren Analyse der IT-Sicherheitslücke abzubringen. Selbst wenn die Untersuchung beispielsweise im Rahmen eines Beschäftigungsverhältnisses an einer Forschungseinrichtung durchgeführt wurde, zeigen Fälle aus der Praxis, dass Personen auch privat von juristischen Konsequenzen betroffen sein können.

Legacy-Problematik:

4 Wird die Hard-/Software nicht mehr gepflegt (z. B. aufgrund Insolvenz oder neuerer Produktzyklen und daraus resultierender End-of-Life-Problematiken), kann die produktverantwortliche Stelle nicht mehr einwandfrei ermittelt werden. Auch eine Beseitigung der IT-Sicherheitslücke ist nicht mehr möglich.

2.3 Institutionelle Forschung, ethisches Hacken und Zufallsfunde

Entsprechend den Zielen der IT-Sicherheit widmen sich IT-Sicherheitsforschende der tiefgehenden Analyse von Soft- und Hardware im Sinne einer anwendungsorientierten Forschung. Dabei betrachtet die Forschungsdisziplin die Informationstechnologie ganzheitlich aus Sicht von Angreifenden und Verteidigenden. Mit dem Finden einer Lücke gehen also sowohl das

Abschätzen und Testen der Angreifbarkeit (Risikoeinschätzung) als auch die Suche nach dem Ursprung der Schwachstelle (Prävention) einher. Diese Form der IT-Sicherheitsforschung findet hauptsächlich an Universitäten und Hochschulen statt, ist also meist institutioneller Natur.

Der CVD-Prozess ist hierbei ein entscheidendes Mittel, um diese ganzheitliche Betrachtung den Betroffenen effektiv zu vermitteln. Auf diese Weise könnten Fehler behoben und langfristig Soft- und Hardware mit weniger Schwachstellen entwickelt werden. Die Forschung hat damit unmittelbar gesellschaftlichen Nutzen. Das Analysieren und Testen wird regelmäßig als „ethisches Hacken" verstanden, da Hacken auch als kreativer Ansatz der Problemlösung (z. B. der Überwindung von IT-Sicherheitsmechanismen) definiert ist. Das Agieren zum Wohle der Allgemeinheit stellt den Kern des Ethikkodex dar. Die Motive sowie der Hintergrund ethischer Hackerinnen und Hacker sind divers, oftmals handelt es sich um Expertinnen und Experten, die ihr Fachwissen zur Verbesserung der IT-Sicherheit einsetzen. Wiederholt wird als Ansporn Neugier sowie Forscherdrang genannt (siehe Wagner et al. 2023, S. 51 f.; Freiling 2009). Diese Form des Hackings ist nicht zu verwechseln mit jenen Angriffen auf IT-Infrastrukturen und Systeme von Nutzerinnen und Nutzern, welche mit einer schädigenden oder bereichernden Absicht einhergehen.

Funde ereignen sich allerdings nicht nur in der IT-Sicherheitsforschung oder bei ethischem Hacking, sondern auch rein zufällig. Schon ein aufmerksames Beobachten während der Nutzung oder ein Abweichen von Abläufen im Handbuch können Hinweise auf Fehler liefern oder ein Verhalten auslösen, das über die vorgesehenen Grenzen von Hard- und Software hinausführt. Finderinnen und Finder einer Schwachstelle können damit nicht nur Menschen mit Fachexpertise oder Interesse für Informationstechnologien sein, sondern auch Personen mit fehlender Sachkenntnis. Es braucht daher ein breites Begriffsverständnis der Finderin und des Finders im CVD-Prozess. Dies ist bei den folgenden Lösungsansätzen stets zu berücksichtigen.

03

LÖSUNGSANSATZ 1:

Juristische Impulse für einen Rechtsrahmen

Um die IT-Sicherheitslandschaft resilienter und defensiver zu gestalten, bedarf es zweier parallel anzustrebender Lösungsansätze: eine Anpassung des Rechtsrahmens sowie die Installation einer neutralen Melde- und Koordinierungsstelle zwischen den betroffenen Beteiligten.

Die Anpassung des Rechtsrahmens ist umfangreich und sollte mit dem Fokus auf forschendes, die Soft- und Hardware nicht gemeinschädigend ausnutzendes Handeln in den folgenden Rechtsgebieten ausgerichtet werden.

3.1 Verfassungsrechtlicher Schutzauftrag zur Gewährleistung der IT-Sicherheit

Grundlage für die vorgeschlagenen Anpassungen ist der Beschluss des Bundesverfassungsgerichts vom 8. Juni 2021 (Az. 1 BvR 2771/18): Mit der behördlichen Kenntnis von IT-Sicherheitslücken ergibt sich ein Zielkonflikt zwischen der Meldung an die Herstellerin/den Hersteller und dem behördlichen Interesse der Nutzung der Sicherheitslücke zu Ermittlungszwecken (z. B. Quellen-Telekommunikationsüberwachung). Aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme folgt eine grundrechtliche Schutzpflicht, die zur Abwägung beider Interessen zwingt: Nur wenn der Nutzen aus der Geheimhaltung der IT-Sicherheitslücke die Risiken für die Allgemeinheit und für die Herstellerin/den Hersteller wesentlich überwiegt, sei ein Geheimhalten zulässig. Andernfalls sei eine Meldung an die Herstellerin/den Hersteller abzugeben.

In diesem Urteil wird der staatliche Schutzauftrag herausgebildet, der sich aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ergibt. Es bedarf gesetzgeberischer Klärung, wie mit eigenen behördlichen oder gemeldeten Funden zu verfahren ist und welche Faktoren zur Ermittlung von Nutzen und Risiken herangezogen werden (z. B. der Begriff der Kritikalität). Ebenso müssen die Leitplanken für die Abwägung im Rahmen einer Verhältnismäßigkeitsprüfung gesetzlich verankert werden. Dabei ist nicht nur ein Zusammenspiel von Bundes- und Landesgesetzgebung herausfordernd, sondern auch die Überschneidung von IT-Sicherheitsrecht, Polizei- und Ordnungs- bzw. Sicherheitsrecht sowie Datenschutzrecht. Gerade die multipolare Grundrechtslage zwischen Forschenden, Produktnutzenden und Herstellerinnen und Herstellern bzw. Unternehmen fordert und erfordert das ausgleichende Handeln der Gesetzgebung.

3.2 Strafrecht als Hemmnis für unabhängige Sicherheitsüberprüfungen

Um IT-Sicherheitsforschenden ein unbesorgtes Forschen und Analysieren von Schwachstellen zu ermöglichen, bedarf es einer Entlastung von (potenziellen) strafrechtlichen Sanktionen. Führen Forschende Penetrationstests an Soft- und/oder Hardware durch, besteht die Sorge, sich insbesondere nach § 202a Abs. 1 StGB (Ausspähen von Daten) strafbar machen zu können. Um eine Strafbarkeit sicher ausschließen zu können, müssten Forschende das Einverständnis sämtlicher Beteiligter an den getesteten IT-Systemen einholen. Dies ist aufgrund des Aufwands, gegebenenfalls entgegenstehender unternehmerischer Interessen oder gar Desinteresse der Herstellerin/des Herstellers nahezu unmöglich. Ob ein forschungsfreundliches Verständnis des Straftatbestands möglich erscheint, ist rechtswissenschaftlich umstritten (differenzierend Wagner et al. 2023, S. 56 ff.). Hinzu treten Tatbestände aus dem IT-Sicherheits- und Datenschutzrecht sowie Hürden im Urheberrecht (Wagner 2020, S. 111 f.). Das Recht wirkt insofern als starkes Hemmnis für unabhängige Analysen von IT-Anwendungen und -Systemen.

Der Koalitionsvertrag 2021–2025, Zeilen 445–446, benennt ausdrücklich: „Das Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren, z. B. in der IT-Sicherheitsforschung, soll legal durchführbar sein." In Anlehnung an diese Formulierung wäre denkbar, ähnlich wie das niederländische Modell, eine IT-sicherheitsspezifische Ausnahmeregelung zu schaffen. Die Tat des Forschenden ist danach nicht strafbar, wenn sie bzw. er:

1. in **Erfüllung eines öffentlichen Interesses** durch verantwortungsbewusste Offenlegung einer Sicherheitslücke handelt (Absicht der Durchführung eines CVD-Prozesses),

2. den **Grundsatz der Verhältnismäßigkeit** beachtet, also sich auf zur Zielerreichung erforderliche Handlungen beschränkt

sowie

3. den **Grundsatz der Subsidiarität** beachtet, d. h., es bestand kein anderer, weniger invasiver Weg zur Aufdeckung der IT-Sicherheitslücke.

Die Ausnahmeregelung sollte sowohl die institutionalisierte IT-Sicherheitsforschung als auch ethisches Hacken umfassen. Zugleich baut sie auf Kriterien eines etablierten CVD-Prozesses auf. Strafrechtlich wäre eine derartige Klausel sowohl als Tatbestandsausschluss als auch als Rechtfertigungsgrund denkbar.

3.3 Aspekte aus IT-Sicherheits- und Datenschutzrecht

Das IT-Sicherheitsrecht unterliegt aktuell europäischen Novellierungsvorhaben. Einerseits wurde kürzlich die NIS2-Richtlinie (Zweite Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Europäischen Union) verabschiedet. Andererseits wurde der Entwurf des Cyber Resilience Act zur Regelung horizontaler (unionsrechtlicher) Anforderungen für Produkte mit digitalen Elementen veröffentlicht. Beide geben Anlass, die IT-Sicherheitsforschung in einer defensiv ausgerichteten IT-Sicherheitslandschaft zu verankern.

Ziel der NIS2-Richtlinie ist nicht nur die Überarbeitung der vorangegangenen NIS-Richtlinie. Durch die erkennbare Auflösung der auch im nationalen IT-Sicherheitsrecht verankerten Kernbegriffe „Kritische Infrastruktur“ und „Digitale Dienste“ geht das IT-Sicherheitsrecht dazu über, das Merkmal der Kritikalität einer Infrastruktur bzw. einer Institution hervorzuheben. Zugleich soll der CVD-Prozess in Cybersicherheitsstrategien implementiert und durch die nationalen Cyber Security Incident Response Teams (CSIRT) umgesetzt werden. Die gefundene Schwachstelle soll aber nicht nur national – gegebenenfalls anonym – gemeldet, sondern auch in einem Schwachstellenregister der ENISA hinterlegt werden. Die NIS2-Richtlinie zielt damit erkennbar auf die Stärkung der Vertraulichkeit in IT-Infrastrukturen und -Systemen. „Das als Koordinator benannte CSIRT stellt sicher, dass in Bezug auf die gemeldete Schwachstelle sorgfältige Folgemaßnahmen durchgeführt werden, und sorgt für die Anonymität der die Schwachstelle meldenden natürlichen oder juristischen Person“, so Art. 12 Abs. 1 S. 5 der Richtlinie.

Der Cyber Resilience Act beschäftigt sich dagegen nur mit Produkten mit digitalen Elementen. Dies betrifft jede Hard- und Software sowie Remoteanwendungen einschließlich dazugehöriger technischer Komponenten. Dieser Entwurf enthält aber nur eine oberflächliche Implementierung des CVD-Prozesses: Annex I Abschnitt 2 des Entwurfs gibt lediglich eine Coordinated Disclosure Policy vor. Ein Meldeprozess wird hier nur zwischen Herstellerin/Hersteller und ENISA errichtet; Meldungen durch Finderinnen/Finder (z. B. IT-Sicherheitsforschende) sind nicht benannt. Das Verhältnis zwischen der breiter formulierten NIS2-Richtlinie und dem enger formulierten und wirkenden Cyber Resilience Act ist bislang unklar. Hingegen klar ist, dass die Vertraulichkeit und Robustheit bzw. Resilienz der IT-Sicherheit nicht durch proaktive Ermittlungsbefugnisse gelingt, sondern durch den defensiv ausgerichteten, zwischen verschiedenen Stellen vermittelnden Prozess der Coordinated Disclosure.

Auch das Datenschutzrecht weist in diese Richtung: Die IT-Sicherheit in Form von Systemsicherheit sowie Datensicherheit sind zentraler Bestandteil des Datenschutzes. Hierauf weist nicht nur der Grundsatz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DSGVO) hin, sondern auch die Grundnorm zur Sicherheit der Verarbeitung durch Anwendung technischer und organisatorischer Maßnahmen (Art. 32 DSGVO). Um aus organisatorischer Perspektive eine DSGVO-Compliance sicherzustellen, bedarf es in der Regel der Einführung eines Datenschutzmanagementsystems (DSMS). In diesem ist auch zu hinterlegen, wie mit Informationen über (potenzielle) Schwachstellen zu verfahren ist. Hierfür eignet sich auch der dargestellte CVD-Prozess. Nach Art. 32 DSGVO sind Herstellerinnen und Hersteller von Soft- und Hardware allerdings nur dazu verpflichtet, sofern sie im Geltungs-

bereich der DSGVO agieren – also selbst als Verantwortliche oder Auftragsverarbeitende personenbezogene Daten verarbeiten. Das Datenschutzrecht enthält in Form der DSGVO somit den Impuls, den Meldeprozess zum Schutz betroffener Personen zu berücksichtigen. Da dies jedoch stark von der Rolle der Herstellerin/des Herstellers in Bezug auf die einzelne Datenverarbeitung abhängt, ist dieser Impuls im Zusammenspiel mit den übrigen Reformansätzen zu berücksichtigen.

04

LÖSUNGSANSATZ 2:

Etablierung einer Melde- und Koordinierungsstelle

Korrespondierend mit der Überarbeitung des Rechtsrahmens ist es nötig, eine koordinierende Meldestelle in die gesetzlich implementieren Prozesse einzubinden. Dieser Abschnitt definiert daher Grund, Anforderungen und Grenzen der Melde- und Koordinierungsstelle (MKS).

4.1 Ziel: Koordinierter Ausgleich von Interessen

Finderinnen und Finder von IT-Sicherheitslücken verfolgen ein redliches, gesamtgesellschaftlich förderungswürdiges Ziel, wenn sie die Beseitigung der Sicherheitslücken vor allem zur Erhöhung der eigenen und/oder fremden IT-Sicherheit erreichen wollen. Die Arbeit dieser Personen bedarf daher entsprechender Anerkennung und sollte nicht als sozialschädlich oder gar kriminell charakterisiert werden. Ebenso soll vermieden werden, dass Sicherheitslücken in die Arsenale etwa von Geheimdiensten, Sicherheitsbehörden oder Kriminellen zur Entwicklung von Angriffsmethoden eingehen.

Ziel

Ziel der Melde- und Koordinierungsstelle ist also, eine Vertrauensbasis zu schaffen und damit einen einvernehmlichen Prozess auf Augenhöhe zu gestalten. Sie nimmt damit eine vermittelnde Position zwischen allen Beteiligten ein. In dieser Funktion kann sie dazu beitragen, Hürden durch Unerfahrenheit, unterschiedliche (technische) Kenntnisse oder verschiedene Fach-/Muttersprachen der Beteiligten zu überwinden.

4.2 Anforderungen an eine Melde- und Koordinierungsstelle

Um diesen Interessenausgleich angemessen vornehmen zu können, bestehen funktionale wie nicht funktionale Anforderungen an die Melde- und Koordinierungsstelle. Grundlage dafür ist folgender Prozessablauf im Falle einer Meldung:

1. Entgegennahme der Meldung von der Melderin/dem Melder
2. Prüfung der Meldung auf Plausibilität
3. ggf. Klärung von Unklarheiten der Meldung
4. Identifikation der Produktverantwortlichen und der dazugehörigen Ansprechpartnerinnen und -partner
5. Übermitteln der Informationen zur Sicherheitslücke an Produktverantwortliche
6. ggf. Herstellung eines sicheren Kommunikationskanals zwischen Melderin/Melder und Produktverantwortlichem
7. Nach Fristablauf: Veröffentlichung der Informationen zur Sicherheitslücke (ggf. in Absprache mit der Melderin/dem Melder)
8. ggf. Löschkonzept bezüglich der Details zur IT-Sicherheitslücke und rechtlich geschützter Daten

Funktionale Anforderungen

Meldende sollten entscheiden können, ob die Meldung anonym oder unter Angabe des Klarnamens samt Kontaktdaten erfolgen soll. Alternativ könnte ein Pseudonym hinterlegt werden, mit dem sich die Melderin/der Melder nachträglich authentisieren und das Einreichen beweisen kann.

Die Kommunikation zwischen Meldendem und Meldestelle kann in drei verschiedenen Formen erfolgen:

- Mit Klarnamen und bidirektional: Die Melderin/der Melder kann sich gegenüber der MKS als Meldender der Sicherheitslücke authentisieren und (weitere) Informationen mitteilen; die MKS kann den Meldenden kontaktieren und antworten.

- Anonym und bidirektional: Die Melderin/der Melder kann sich gegenüber MKS authentisieren und (weitere) Informationen mitteilen; die MKS kann Rückfragen und Informationen für Meldende verschlüsselt hinterlegen, aber nicht aktiv kontaktieren.

- Anonym und einmalig: Die Melderin/der Melder kontaktiert MKS anonym und hinterlegt nur Informationen zur Sicherheitslücke; die MKS kann Meldende nicht kontaktieren oder antworten.

Technisch ist der Kommunikationskanal bei der anonymen Meldung so zu gestalten, dass Meldende durch technische Maßnahmen vor einer Deanonymisierung geschützt sind. Hier empfiehlt sich z. B. die Einbindung des TOR-Netzwerks. Im Übrigen sollte der Kommunikationskanal Ende-zu-Ende gesichert sein.

Für den Umfang der Meldung bedarf es einer Standardisierung einer einheitlichen Taxonomie, damit Meldende einheitlich die Herstellerin/den Hersteller, Produkt und Version an die MKS melden können. Einzelfallbezogene Webformulare oder eine öffentliche Anwendungsschnittstelle könnten sich als ungeeignet erweisen (Wagner et al. 2023, S. 90 f.). Eine Integration von Schwachstellendatenbanken wie CVE ist zur Berücksichtigung internationaler Standards anzuraten. Es ist jedoch nicht zu erwarten, dass die Meldung alle nötigen technischen Details enthält – sie werden im vermittelten Prozess zwischen der Herstellerin/dem Hersteller und der Melderin/dem Melder kooperativ zusammengetragen, wenn möglich.

Um ein etwaiges Ungleichgewicht der Positionen zu vermeiden, kann die MKS als vermittelnde Instanz auf expliziten Wunsch der Melderin/des Melders oder der produktverantwortlichen Stelle hinzugezogen werden und Lösungen vorschlagen. Im Übrigen bleibt die Kommunikation vertraulich und bilateral. Eine Fristsetzungskompetenz der MKS sollte nicht vorgesehen werden.

Zur Anregung der Meldung von IT-Sicherheitslücken erscheint es sinnvoll, Forschenden bzw. Meldenden eine immaterielle Kompensation anzubieten. Dies könnte beispielsweise durch Namensnennung bei der Danksagung durch Produktverantwortliche oder eine Bestenliste (Hall of Fame) bei der Meldestelle gelingen.

Für den Fall einer juristischen Auseinandersetzung soll das Verhalten von Meldendem und produktverantwortlicher Stelle belastbar dokumentiert werden. Beispielsweise kann über eine Quittung, kryptografische Hashverfahren und eine digitale Signatur der MKS eine sichere Enklave kon-

struiert werden. Im Einzelfall könnte die MKS als neutrale Zeugin auftreten und Angaben zum Ablauf des Verfahrens machen, um zur gerichtlichen Klärung in der Sache beizutragen.

Nicht funktionale Anforderungen

Für die Konstruktion der Stelle sind zwei Wege möglich: Es könnte eine einzelne, zentrale Anlaufstelle geschaffen werden – was mit einer zentralen Schwachstellensammlung die Gefahr des Single Point of Failure birgt. Andererseits könnten mehrere (Landes-)Stellen geschaffen werden – wodurch sich eine nicht standardisierte Bearbeitung und Begleitung der Meldeprozesse ergeben könnte. Das Für und Wider beider Entwürfe ist durch die Gesetzgebung abzuwägen.

Organisatorisch sollte in jedem Fall die Unabhängigkeit der Meldestelle nach dem Vorbild der Datenschutzaufsichtsbehörden (siehe Art. 52 DSGVO) gesetzlich verankert werden. Die MKS sollte daher institutionell eigenständig und weisungsfrei mit eigenen Befugnissen ausgestattet sein. Eine Verortung bei bestehenden Behörden empfiehlt sich nicht, da eine gebündelte Aufgabenvielfalt die Erfüllung der funktionalen Anforderungen beeinträchtigen könnte. Eine organisatorische Ansiedlung beim Bundesamt für Sicherheit in der Informationstechnik ist nur möglich, sofern die Unabhängigkeit des gesamten Verwaltungskörpers gesetzlich verankert würde. In der aktuellen Form eignet sich die Behörde aufgrund ihrer Nähe zum Bundesministerium des Innern und zu sicherheitspolitischen Bestrebungen nicht (Wagner et al. 2023, S. 94 f.).

05

FAZIT:

Interdisziplinäre Übersetzungsarbeit aller Beteiligten

Das eingangs aufgezeigte Problem der brüchigen IT-Sicherheitslage durch zahlreiche IT-Sicherheitslücken in Soft- und Hardware kann nur durch eine defensive und forschungsfreundliche Ausrichtung der IT-Sicherheitslandschaft und -politik gelöst werden. Grundvoraussetzung dafür ist eine offene Haltung aller Beteiligten – also IT-Sicherheitsforschende als Meldende, Herstellerinnen/Hersteller und sonstige produktverantwortliche Stellen sowie staatliche Akteure. Zwischen allen muss eine prozessorientierte, aber doch transparente Kommunikation erfolgen, um die IT-Sicherheit aller Geräte und Anwendungen resilienter zu machen. Nur so können IT-Sicherheitslücken effektiv und nachhaltig geschlossen werden.

Die erläuterte Umgestaltung des gesetzlichen Rahmens (Lösungsansatz 1) schafft die Grundlage dafür. Durch die Berücksichtigung der wegweisenden verfassungsgerichtlichen Rechtsprechung in Strafrecht, Datenschutz- und IT-Sicherheitsrecht werden IT-Sicherheitsforschende merklich entlastet. Zugleich wird das Melden von IT-Sicherheitslücken als Mittel zur Stärkung der IT-Sicherheit erklärt und nicht mehr ausschließlich als (befürchteter) erster Schritt zur Ausnutzung der Sicherheitslücken. Auch zukünftig sollte in weiteren, jüngeren Rechtsgebieten – beispielsweise dem in Entstehung befindlichen europäischen Datenrecht – darauf geachtet werden, diesen Wert beizubehalten oder gar zu stärken.

Die vorgeschlagene Melde- und Koordinierungsstelle (Lösungsansatz 2) dient dabei als Vehikel, die Entwicklung dieses Wertes in der gesellschaftlichen Ordnung voranzutreiben. Sichere und vertrauliche Kommunikationswege im Meldeprozess zwischen IT-Sicherheitsforschenden und Herstellerinnen/Herstellern bzw. produktverantwortlichen Stellen bauen Hemmungen ab. Die Begleitung und Standardisierung des CVD-Prozesses schafft Klarheit und Vertrauen zwischen den Beteiligten, aber auch für die Allgemeinheit. Daneben steigert die Unabhängigkeit der Stelle selbst das Vertrauen gegenüber dem Staat als schützendes Organ, den Produktverantwortlichen, aber vor allem in das eigene System.

Literaturverzeichnis

Die Bundesregierung (2021). Koalitionsvertrag 2021 – 2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), BÜNDNIS 90/DIE GRÜNEN und den Freien Demokraten (FDP). Mehr Fortschritt wagen, Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit.
↗ https://www.bundesregierung.de/breg-de/service/gesetzesvorhaben/koalitionsvertrag-2021-1990800
[15.02.2023].

ENISA –European Union Agency For Network And Information Security (2015). Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations.
↗ https://www.enisa.europa.eu/publications/vulnerability-disclosure
[15.02.2023].

Freiling, F.C. (2009). Ein Blick auf IT-Sicherheit aus Angreiferperspektive. In: Datenschutz und Datensicherheit – DuD 33, 214–217.
DOI: ↗ https://doi.org/10.1007/s11623-009-0053-z.

Wagner, M. (2020). IT-Sicherheitsforschung in rechtlicher Grauzone. In: Datenschutz und Datensicherheit – DuD 44, 111–120.
DOI: ↗ https://doi.org/10.1007/s11623-020-1233-0.

Wagner, M. et al. (2023). Verantwortungsbewusster Umgang mit IT-Sicherheitslücken – Problemlagen und Optimierungsoptionen für ein effizientes Zusammenwirken zwischen IT-Sicherheitsforschung und IT-Verantwortlichen, Schriftenreihe digital | recht, Band 4, Trier 2023 (Whitepaper).
DOI: ↗ https://doi.org/10.25353/ubtr-xxxx-8597-6cb4.

Für ausführliche Quellen verweisen die Autorinnen und Autoren auf das Whitepaper von Wagner et al. (2023).

bidt

bidt – Bayerisches Forschungsinstitut
für Digitale Transformation
Gabelsbergerstraße 4
80333 München
↗ www.bidt.digital