digital | recht

Staat und digitale Gesellschaft

Manuela Wagner, Oliver Vettermann et al.

Verantwortungsbewusster Umgang mit IT-Sicherheitslücken

Problemlagen und Optimierungsoptionen
für ein effizientes Zusammenwirken zwischen
IT-Sicherheitsforschung und IT-Verantwortlichen

Band 4

Manuela Wagner,
Oliver Vettermann et al.

Verantwortungsbewusster Umgang mit IT-Sicherheitslücken

Problemlagen und Optimierungsoptionen für ein effizientes Zusammenwirken zwischen IT-Sicherheitsforschung und IT-Verantwortlichen

digital | recht
Staat und digitale Gesellschaft

Herausgegeben von
Prof. Dr. Matthias Bäcker, LL.M.
Prof. Dr. Roland Broemel
Prof. Dr. Thomas Burri, LL.M.
Prof. Dr. Albert Ingold
Prof. Dr. Antje von Ungern-Sternberg
Prof. Dr. Silja Vöneky

Trier, 2023
Band 4

Manuela Wagner ist wissenschaftliche Mitarbeitern am FZI Karlsruhe und befasst sich mit Datenschutz-, IT-Sicherheitsrecht sowie Rechtsfragen um Smart Mobility.

Oliver Vettermann ist wissenschaftlicher Mitarbeiter bei FIZ Karlsruhe im Bereich Datenschutz- und IT-Sicherheitsrecht mit grundrechtlichen Bezügen.
ORCID: https://orcid.org/0000-0001-7393-1103

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Angaben sind im Internet über http://dnb.d-nb.de abrufbar.

Dieses Buch steht gleichzeitig als elektronische Version über die Webseite der Schriftenreihe https://digitalrecht-oe.uni-trier.de zur Verfügung.

ISBN: 9783757528034
URN: urn:nbn:de:hbz:385-2023020707
DOI: https://doi.org/10.25353/ubtr-xxxx-8597-6cb4

Karlsruhe/Leipzig
Die Schriftenreihe wird gefördert von der Universität Trier und dem Institut für Recht und Digitalisierung Trier (IRDT).
Anschrift der Herausgeber: Universitätsring 15, 54296 Trier.

UNIVERSITÄT TRIER

IRDT Institut für Recht und Digitalisierung Trier

Vorwort

IT-Sicherheitslücken in Hard- und Software betreffen private, unternehmerische und auch staatliche Systeme. Sobald eine Ausnutzung der Lücken technisch möglich ist, stellen sie eine Bedrohung für die IT-Sicherheit aller Beteiligten dar. Konkret betroffen sind Bürger:innen und Unternehmen als Nutzende, 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.

Die politischen wie gesetzlichen Gegebenheiten der letzten Jahre weisen allerdings in eine andere Richtung. Gerade IT-Sicherheitsforschende, die sich der Beseitigung von IT-Sicherheitslücken widmen, leiden unter den juristischen Hemmnissen. Das inter- wie intradisziplinäre Kollektiv *sec4research* widmet sich daher seit 2020 dem Abbau der Hemmnisse durch verschiedene Herangehensweisen. Wegweisend sind dabei die Synergien, die sich durch IT-Sicherheitsforschende, Informatiker:innen und Jurist:innen mit wissenschaftlicher und/oder praktischer Expertise ergeben.

Das im Jahr 2021 veröffentlichte Whitepaper widmet sich der Darstellung der aktuellen Problemlage und der Implementierung der Coordinated Vulnerability Disclosure in die nationale IT-Sicherheitslandschaft. Das vorliegende Werk fungiert als Whitepaper 2023 und denkt den Ansatz von 2021 weiter in Form einer umfassenden defensiven Ausrichtung der IT-Sicherheitspolitik.

Auch dieses Werk wäre nicht ohne die zahlreiche Beteiligung von Kolleg:innen und Forscher:innen entstanden. Inhaltlich beteiligt sind bei diesem Papier: Steven Arzt, Dominik Brodowski, Roman Dickmann, Niklas Goerke, Sebastian Golla, Michael Kreutzer, Maximilian Leicht, Johannes Obermaier, Marc Schink, Linda Schreiber, Christoph Sorge, Oliver Vettermann und Manuela Wagner.

Inhaltsübersicht

Einleitung
Einführung und Gang der Untersuchung 1

Kapitel 1
Einblicke in die wissenschaftliche sowie politisch-gesellschaftliche Diskussion 5

Kapitel 2
Problemlagen und Lösungsansätze für einen verantwortungsbewussten Umgang mit Sicherheitslücken 29

Kapitel 3
Konzept einer Melde- und Koordinierungsstelle zur Unterstützung von Coordinated-Disclosure-Prozessen 63

Kapitel 4
Grenzen einer Meldestelle aus Praxissicht der Forschung 81

Zusammenfassung
Zusammenstellung der Ergebnisse 91

Inhaltsverzeichnis

Vorwort I
Inhaltsübersicht III
Inhaltsverzeichnis V
Abkürzungsverzeichnis IX

Einleitung
Motivation 1
Gang der Untersuchung 3

Kapitel 1
Einblicke in die wissenschaftliche sowie politisch- gesellschaftliche Diskussion 5
I. Zielsetzung der IT-Sicherheit 5
II. Empfehlungen zur Handhabung von Sicherheitslücken 9
1. Coordinated Disclosure und auftretende Probleme 9
a) Sicherheitslücken 10
b) Coordinated Disclosure 10
c) Praktische Probleme 11
d) Überblick über rechtliche Risiken einer Meldung 13
2. Empfehlungen an Produktverantwortliche und Minimalkonsens zum Umgang mit Sicherheitslücken 17
III. Hintergrund zu den Entdecker:innen von Schwachstellen 18
1. IT-Sicherheitsforschung im engeren Sinne 18
2. Ethisches Hacken 19
a) Definition der „Hacker:in“ 21
b) Ethische Grundsätze 23
3. IT-Sicherheitsanalysen im Rahmen der Aufgabenwahrnehmung des BSI 26

IV. Fazit 26

Kapitel 2
Problemlagen und Lösungsansätze für einen verantwortungsbewussten Umgang mit Sicherheitslücken 29
I. Schutzauftrag zur Gewährleistung von IT-Sicherheit im Spannungsverhältnis zur öffentlichen Sicherheit und privater Interessen 30
1. Rechtsprechung des Bundesverfassungsgerichts zum verantwortungsbewussten Umgang mit Sicherheitslücken durch staatliche Stellen 30
2. Grundrechtskonflikte bei der verantwortungsbewussten Offenlegung von Schwachstellen durch Sicherheitsforschende 33
a) Perspektive der Produkt-/Systemnutzenden 34
b) Perspektive der Produkt-/Systemverantwortlichen 35
c) Perspektive der Forschung 35
3. Zwischenfazit 36
II. Das Strafrecht als Hemmnis für proaktive, unabhängige Sicherheitsüberprüfungen 36
1. Aktueller Rechtsrahmen – Strafrechtliche Risiken und Abschreckungseffekte 37
2. Grundsätzliche Erwägungen zu Reformoptionen in Deutschland 40
a) Ergänzung der Tatbestände der §§ 202a ff., 303a f. StGB 41
b) Erweiterung der Sozialadäquanzklauseln als Tatbestandsausschluss für Sicherheitsforschung 41
c) Schaffung einer IT-sicherheitsspezifischen Ausnahmeregelung 44
d) Ausnahmen auf strafprozessualer Ebene 45
e) Diskussion zur konkreten Gestaltung eines Strafausschlusses 46
3. Zwischenfazit zum Strafrecht 47
III. Impulse für ein koordiniertes IT-Schwachstellenmanagement aus Compliance-Erwägungen 47
1. IT-Schwachstellenmanagement zur Umsetzung neuer Pflichten bei Consumer-Products 48
2. IT-Schwachstellenmanagement zur Reduktion von Haftungsrisiken im B2B-Bereich 52
3. IT-Schwachstellenmanagement als Konformitätserfordernis für das Anbringen des CE-Kennzeichens an Funkanlagen 54
a) Konkretisierung des Stands der Technik durch technische Standards 55
b) Haftungsrisiken als Motor für die Etablierung von Coordinated-Disclosure-Prozessen 57
4. IT-Schwachstellenmanagement als Bestandteil der DSGVO-Compliance 58
5. Impulse aus dem IT-Sicherheitsrecht 59

6. Zwischenfazit zu Impulsen der Compliance-Anforderungen für ein koordiniertes Schwachstellen-Management 61
IV. Fazit 61

Kapitel 3
Konzept einer Melde- und Koordinierungsstelle zur Unterstützung von Coordinated-Disclosure-Prozessen 63
I. Motivation einer Melde- und Koordinierungsstelle für Coordinated-Disclosure-Prozesse 63
II. Aktuelle Rechtslage zu möglichen Melde- und Koordinierungsstellen 63
1. Rechtliche Ausgestaltung des BSI 64
2. Kompetenzbeschreibung der Datenschutzaufsichtsbehörden 66
III. Ziel: Ausgleich kollidierender Interessen 68
1. Interessen der Finder:innen von Schwachstellen 68
2. Interessen der IT-Sicherheitsforscher:innen 69
3. Interessen der Wirtschaft 70
4. Interessen der Allgemeinheit 71
IV. Anforderungen an eine Melde- und Koordinierungsstelle 71
1. Funktionale Anforderungen 72
a) Option zur anonymen Meldung 72
b) (Mindest-)Umfang einer Meldung und Standardisierung 74
c) Meldung ohne Details 75
d) Prüfung der Meldung 75
e) Bereitstellen von sicheren Kommunikationskanälen 76
f) Vermittlung bei Streit 76
2. Nicht-funktionale Anforderungen 77
a) Zentrale oder dezentrale Struktur 77
b) Organisatorische Ansiedelung 78
c) Ausrichtung auf defensive Sicherheit 79
V. Fazit 80

Kapitel 4
Grenzen einer Meldestelle aus Praxissicht der Forschung 81
I. Zahnloser Tiger: Schwachstellenmeldungen nach End-of-life 81
II. Überlastung: Massenfindings und Mehrfachnennungen 83
1. Zur Funktionsweise automatisierter Testverfahren 84
2. Optionen zum Umgang mit Massenfindings 86

III. Ineffektive Maßnahmen: Risikoeinschätzung trotz lückenhafter Informationen 87
IV. Fazit 88

Zusammenfassung 91

Literaturverzeichnis 93

Abkürzungsverzeichnis

Abs.	*Absatz; Abschnitt*
AEUV	*Vertrag über die Arbeitsweise der Europäischen Union*
AöR	*Archiv des öffentlichen Rechts*
Art.	*Artikel*
Aufl.	*Auflage*
Bd.	*Band*
BeckOK	*Beck'scher Online Kommentar*
Beschl.	*Beschluss*
BGB	*Bürgerliches Gesetzbuch*
BGBl.	*Bundesgesetzblatt*
BGHZ	*Entscheidungen des Bundesgerichtshofes in Zivilsachen*
BK	*Bonner Kommentar*
BVerfG	*Bundesverfassungsgericht*
BVerfGE	*Entscheidungen des Bundesverfassungsgerichts*
BVerfGG	*Bundesverfassungsgerichtsgesetz*
CR	*Computer und Recht*
DAV	*Deutscher Anwaltverein*
ders.; dies.	*derselbe; dieselbe(n)*
DÖD	*Der Öffentliche Dienst*
DÖV	*Die Öffentliche Verwaltung*
DSGVO	*Datenschutzgrundverordnung*
DuD	*Datenschutz und Datensicherheit*
EDV	*Elekronische Datenverarbeitung*
EG	*Europäische Gemeinschaft*
EGMR	*Europäischer Gerichtshof für Menschenrechte*
EL	*Ergänzungslieferung*
et al.	*et alii (und andere)*
EU	*Europäische Union*
EuGH	*Europäischer Gerichtshof*
EUV	*Vertrag über die Europäische Union*
f.; ff.	*folgende; fortfolgende*
GDPR	*General Data Protection Regulation*
gem.	*gemäß*

GG	*Grundgesetz*
GmbH	*Gesellschaft mit beschränkter Haftung*
GRC	*Charta der Grundrechte der Europäischen Union*
GRUR	*Gewerblicher Rechtsschutz und Urheberrecht*
GRUR-Prax	*Gewerblicher Rechtsschutz und Urheberrecht, Praxis im Immaterialgüter und Wettbewerbsrecht*
GVG	*Gerichtsverfassungsgesetz*
Hdb.	*Handbuch*
Hrsg.	*Herausgeber; Herausgeberin*
HStR	*Handbuch des Staatsrechts der Bundesrepublik Deutschland*
HVerfR	*Handbuch des Verfassungsrechts der Bundesrepublik Deutschland*
i.E.	*Im Erscheinen*
IEEE	*Institute of Electrical and Electronics Engineers*
IFIP	*International Federation for Information Processing*
IGH	*Internationaler Gerichtshof*
IJCAI	*International Joint Conference on Artificial Intelligence*
InTer	*Zeitschrift zum Innovations- und Technikrecht*
IT	*Informationstechnologie*
JA	*Juristische Arbeitsblätter*
JI-RL	*Richtlinie Justiz/Inneres EU 2016/680*
JR	*Juristische Rundschau*
JURA	*Juristische Ausbildung*
JurPC	*Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*
JuS	*Juristische Schulung*
JZ	*Juristenzeitung*
lit.	*littera (= Buchstabe)*
LV	*Landesverfassung*
m. w. N.	*mit weiteren Nachweisen*
MDR	*Monatsschrift für Deutsches Recht*
ML	*Machine Learning*
MMR	*Multimedia und Recht*
n. F.	*neue Fassung*
NJOZ	*Neue Juristische Online-Zeitschrift*
NJW	*Neue Juristische Wochenschrift*
NJW-RR	*Neue Juristische Wochenschrift-Rechtsprechungsreport*
Nr.	*Nummer*
NStZ	*Neue Zeitschrift für Strafrecht*
NVwZ	*Neue Zeitschrift für Verwaltungsrecht*
NZFam	*Neue Zeitschrift Familienrecht*
NZS	*Neue Zeitschrift für Sozialrecht*
NZV	*Neue Zeitschrift für Verkehrsrecht*
o. ä.	*oder ähnliche(s)*
o. O.	*ohne (Verlags-)ort*

Rn.	*Randnummer(n)*
Rs.	*Rechtssache*
S.	*Seite(n); Satz/Sätze*
sog.	*sogenannt(e -es)*
StGB	*Strafgesetzbuch*
StPO	*Strafprozessordnung*
StVO	*Straßenverkehrsordnung*
u. a.	*und andere(s); unter anderem*
v.	*vom; von; van*
v. d.	*von der; van den*
VerfGH	*Verfassungsgerichtshof*
vgl.	*vergleiche*
VVDStRL	*Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer*
VwGO	*Verwaltungsgerichtsordnung*
VwVfG	*Verwaltungsverfahrensgesetz*
Web-Dok	*Web Dokument*
WRV	*Weimarer Reichsverfassung*
ZD	*Zeitschrift für Datenschutz*
ZeuP	*Zeitschrift für europäisches Privatrecht*
ZfP	*Zeitschrift für Politik*
ZG	*Zeitschrift für Gesetzgebung*
ZGS	*Zeitschrift für das gesamte Schuldrecht*
ZIS	*Zeitschrift für Internationale Strafrechtsdogmatik*
ZRP	*Zeitschrift für Rechtspolitik*
ZUM	*Zeitschrift für Urheber- und Medienrecht*
ZZP	*Zeitschrift für Zivilprozess*

Einleitung

Motivation

Sicherheitslücken[1] in Hard- und Software betreffen private, unternehmerische und staatliche Infrastrukturen. Sind sie in der Praxis ausnutzbar, stellen sie eine Bedrohung der IT-Sicherheit dar.[2] Deshalb ist die Beseitigung von Sicherheitslücken sowohl aus Sicht der Produkthersteller:innen bzw. Produktverantwortlichen, die unter Zugriff auf den Quellcode Fehler beseitigen (lassen) können, wie auch Betreiber:innen und Nutzer:innen wünschenswert.[3] Es ist im gesamtgesellschaftlichen Interesse die Zahl der ausnutzbaren Sicherheitslücken in verwendeten Produkten und Systemen so gering wie möglich zu halten. Dies dient vor allem dem Daten-, Gesundheits-, Eigentums- und/oder Vermögensschutz des Einzelnen, der Unternehmen und des Staates, aber auch der Resilienz digitaler Infrastrukturen gegen (wirtschafts-)kriminelle Akte, Sabotage, Spionage oder im Falle internationaler Konflikte. Eine entsprechend defensive Ausrichtung[4] verlangt nach der Förderung der IT-Sicherheitsforschung, insbesondere um die von ihr entdeckten Sicherheitslücken melden und beseitigen zu können. Das Geheimhalten von Sicherheitslücken verschlechtert die IT-Sicherheitslage, weil eine parallele Entdeckung oder der Abfluss entsprechenden Wissens und damit unkontrollierbarer Missbrauch jederzeit möglich sind.[5] Bedroht sind alle, die das betroffene Produkt herstellen, ver-/betreiben, einsetzen oder mit ihm verbunden sind.[6] Dies beinhaltet

---

[1] Der Begriff soll hier weit verstanden werden und umfasst sicherheitsrelevante (ausnutzbare) Fehler in Soft- und Hardware aber auch ebensolche Konfigurationsfehler oder den Einsatz von mit Blick auf die IT-Sicherheit untauglichen Mitteln.

[2] Zur Definition vgl. *Eckert*, IT-Sicherheit, S. 7 ff.

[3] Ausführlich Whitepaper zur Rechtslage der IT-Sicherheitsforschung 2021 – abrufbar unter https://sec4research.de.

[4] Die schon deshalb angezeigt ist, weil eine technologische Abschottung oder Zwangsabschaltungen (sei es auf Ebene von Beschaffung/Einsatz von Hard- und Software, aber auch bzgl. der Vernetzung) nicht möglich und in einem demokratischen Rechtsstaat nicht legal auszugestalten sind.

[5] Bsp.: Abfließen von Exploit-Daten der NSA, was zur WannaCry-Ransomware-Welle 2017 führte, vgl. *Shane/Perlroth/Sanger*, The New York Times online vom 12.11.2017 – abrufbar unter https://www.nytimes.com; *Buchanan*, The Hacker and the State, S. 242 ff.; *Schmidt*, heise security vom 24.02.2021, abrufbar unter https://www.heise.de (letzter Abruf 10.12.2021).

[6] Vgl. *Abelson* et al., "Keys under doormats: mandating insecurity by requiring government access to all data and communications" Journal of Cybersecurity, 1(1), 2015, S. 69–79 – DOI: 10.1093/cybsec/tyv009.

auch staatliche IT-Infrastruktur. Daher liegt es im allgemeinen Interesse, keinen Markt für ausnutzbare Sicherheitslücken entstehen bzw. expandieren zu lassen.[7] Staatliche Anreize zur Meldung und Beseitigung von ausnutzbaren Sicherheitslücken helfen zudem, eine IT-Risiken reflektierende Fehlerkultur in Politik, Wirtschaft und Gesellschaft zu etablieren und die IT-Sicherheit digitaler Produkte – und damit deren Qualität – zu verbessern.

Nichtsdestotrotz zeigten jüngste Konflikte zwischen Hersteller:innen einerseits und unabhängig sowie proaktiv tätigen Sicherheitsforscher:innen bzw. ethischen Hacker:innen andererseits, dass noch ein weiter Weg zu einem auf Kooperation fußenden IT-Schwachstellenmanagement zurückgelegt werden muss.[8] Obwohl im Kreis der IT-Sicherheitsexpert:innen eine überwiegende Einigkeit über die grundsätzliche Notwendigkeit eines koordinierten Zusammenwirkens zwischen Sicherheitsforschung mit Produkt- bzw. Systemverantwortlichen im Wege eines sogenannten Coordinated -Disclosure-Prozesses besteht,[9] ist dieser weder im Rechtsrahmen verankert[10] noch in allen Branchen bereits umgesetzt.[11] Vielmehr entsteht aufgrund von rechtlichen Risiken für die proaktive Untersuchung fremder Produkte und Systeme die Besorgnis von ernst zu nehmenden Abschreckungseffekten. Dies könnte sich insgesamt negativ auf das IT-Sicherheitsniveau auswirken. Diese Untersuchung soll dazu beitragen, die Gemengelage der bei der Handhabung von Sicherheitslücken in Konflikt stehenden Interessens- und

---

[7] Solche Märkte bestehen bereits seit mehr als 20 Jahren – grundlegend *Camp/Wolfram*, Pricing Security, Proceedings of the CERT Information Survivability Workshop, S. 31.

[8] Siehe bspw. *Wolfnagel,* Danke für den Hinweis, Anzeige ist raus, in: Zeit Online vom 5. August 2021 – abrufbar unter https://www.zeit.de/digital/datenschutz/2021-08/cdu-connect-app-it-sicherheit-lilith-wittmann-forscherin-klage/komplettansicht; *Franzen/Maier/Wagner*, DuD 2020, 511 – DOI: 10.1007/s11623-020-1316-y.

[9] Vgl. die Handreichung des *BSI*, Handhabung von Schwachstellen, BSI-CS 019, Version 2.0 vom 11.07.2018 – https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_019.pdf?__blob=publicationFile&v=1; *ENISA - European Union Agency For Network And Information Security*, Good Practice Guide on Vulnerability Disclosure (2015), DOI 10.2824/610384; *National Cyber Security Centre*, Coordinated Vulnerability Disclosure: the Guideline, October 2018, abrufbar unter: https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline; CIO Platform Nederland/Rabobank, Coordinated Vulnerability Disclosure Manifesto, abrufbar unter: https://www.cio-platform.nl/en/publications.

[10] Siehe zu rechtlichen Risiken der Sicherheitsforschung: *Brodowski*, it – Information Technology (57) 2015, 357, DOI: 10.1515/itit-2015-0014; *Golla*, JZ 2021, 985; *Vettermann/Wagner*, InTeR 2020, 126; *Vonderau/Wagner*, DSRITB 2020, 525; *Wagner*, PinG 2020, 66; *Wagner*, DuD 2020, 111.

[11] Bspw. zeigt die Studie *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) die geringe Verbreitung von Responsible-Disclosure-Policies im IoT-Bereich.

Rechtspositionen zu entwirren und praxistaugliche Lösungen in rechtlicher und organisatorischer Hinsicht zu unterbreiten. Ein Schwerpunkt liegt dabei auf der Konzeption einer koordinierenden und im Konfliktfall schlichtenden Meldestelle zur Unterstützung von Disclosure-Prozessen.

Gang der Untersuchung

Zunächst gewährt die Arbeit Einblicke in die wissenschaftliche sowie politisch-gesellschaftliche Diskussion zum Umgang mit Sicherheitslücken. Hierfür erfolgt eine kurze Einführung in die Zielsetzung der IT-Sicherheit, die aktuellen Empfehlungen zur Handhabung von Sicherheitslücken über einen Coordinated-Disclosure-Prozess sowie die dabei auftretenden praktischen und rechtlichen Probleme. Als Startpunkt für weitere Diskussionen wird ein Minimalkonsens für proaktive Sicherheitsuntersuchungen von dritter Seite – z.B. IT-Sicherheitsforscher:innen – festgehalten. Zum besseren Verständnis solcher unabhängigen und proaktiven Untersuchung von Produkten und Systemen werden die Hintergründe der Entdecker:innen von Sicherheitslücken beleuchtet, welche entweder der Sicherheitsforschung im engeren Sinne oder dem ethischen Hacken zugeordnet werden können.

Die im ersten Kapitel dargestellten Interessen werden zu Beginn des Kapitel 2 in grundrechtlich geschützte Rechtspositionen überführt. Daraus ergeben sich auch Konflikte im Hinblick auf den staatlichen Schutzauftrag zur Gewährleistung der IT-Sicherheit und die öffentliche Sicherheit, die näher diskutiert werden. Die Diskussion bildet die Grundlage für weitere rechtliche Problemlagen und Lösungsansätze für einen verantwortungsbewussten Umgang mit Sicherheitslücken. Entsprechend der Intention des Koalitionsvertrags, das Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren (z. B. in der IT-Sicherheitsforschung) legal zu ermöglichen, werden zunächst die aktuelle Rechtslage im Strafrecht fokussiert und grundsätzliche Reformoptionen in Deutschland diskutiert. Daneben wird der Frage nachgegangen, inwiefern insbesondere jüngste Novellen der verbraucherschützenden Normen sowie Regelungen zur Produktsicherheit bereits Impulse setzen, ein IT-Schwachstellenmanagement zu etablieren, welches einen Coordinated-Disclosure-Prozess implementiert.

Eine Option zur Optimierung der Meldeprozesse von Sicherheitslücken zwischen Sicherheitsforschenden und Produktverantwortlichen liegt in der Konzeption und Einrichtung einer (staatlichen) Melde- und Koordinierungsstelle für Coordinated-Disclosure-Prozesse. Ausgehend von der aktuellen Rechtslage wird aufgezeigt, welche zusätzlichen Aspekte zu bedenken sind, um die zentrale Zielsetzung des Ausgleichs kon-

fligierender Interessen zu gewährleisten. Dabei werden funktionale und nicht-funktionale Anforderungen an eine Melde- und Koordinierungsstelle herausgearbeitet. Berücksichtigt wird auch der jüngst veröffentlichte Entwurf zum Cyber Resilience Act.

Diesem theoretischen Fundament werden im letzten Kapitel ausgewählte Praxisprobleme aus dem Erfahrungswissen von Sicherheitsforschenden gegenübergestellt. An realen Beispielen wird untersucht, welche rechtlichen Ansätze die erfolgreiche Umsetzung von Meldeprozessen dabei unterstützen bzw. unterstützen könnten und welche praktischen Lösungsoptionen jeweils bestehen, um das von Sicherheitslücken ausgehende Risiko bestmöglich zu minimieren.

Kapitel 1

Einblicke in die wissenschaftliche sowie politisch-gesellschaftliche Diskussion

I. Zielsetzung der IT-Sicherheit

„If there's anything we've learned about IT security in recent years, it's that successful attacks are inevitable."[1]
— Bruce Schneier

IT-Sicherheit[2] hat den Schutz von Informationen samt den sie speichernden und verarbeitenden Systemen als Ziel.[3] Sicherheit bezeichnet einen **relativen Zustand**, der im (nicht erreichbaren) Idealfall gefahrenfrei bzw. (realistisch) frei von unvertretbaren Risiken ist. Hierbei handelt sich um eine Momentaufnahme. In der Praxis bedarf es kontinuierlicher dynamischer **Prozesse**, um sich dem gewählten, jedoch stetig zu hinterfragenden und ggf. anzupassenden Zielniveau an IT-Sicherheit anzunähern. Im Rahmen der IT-Sicherheit und ihrer Schutzziele geht es darum, unberechtigte Zugriffe auf Daten zu verhindern und berechtigte Zugriffsmöglichkeiten jeweils bei Datenauthentizität, Datenintegrität, Zuverlässigkeit, Verbindlichkeit und Vertraulichkeit zu erhalten, also für Verfügbarkeit zu sorgen.[4]

Verfügbarkeit besteht nicht, wenn berechtigte Zugriffsmöglichkeiten beeinträchtigt oder unterbunden werden, wobei etwa Kapazitätsengpässe, Priorisierung anderer Prozesse und Auszeiten für Wartung, also zeitlich wie technisch plan- und erwartbare Soll-Abweichungen, nicht hierunter fallen. Die **Authentizität** ist verletzt, wenn die Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit von Daten nicht (mehr) gegeben

---

[1] *Schneier*, Secrets & Lies, 15th Anniversary Edition, S. X.

[2] Häufig synonym verwendet: Computersicherheit (veraltet), Informationssicherheit oder Informations- und Telekommunikationssicherheit. Im angloamerikanischen Raum vor allem „Cyber Security". Zur uneinheitlichen Begriffsverwendung auch auf internationaler Ebene Schallbruch in *Hornung/Schallbruch*, IT-Sicherheitsrecht, S. 89.

[3] Vgl. *Eckert*, IT-Sicherheit, S. 3, 6.

[4] Vgl. *Eckert*, IT-Sicherheit, S. 7 ff.

sind.[5] Die **Integrität** ist nicht mehr gewährleistet, wenn Subjekte unautorisiert (und ggf. unbemerkt) Daten verändern können. **Unzuverlässig** ist der Zugriff auf Daten, wenn diese unzulässige (etwa nicht lesbare) Zustände annehmen und mit ihnen spezifizierte Funktionen nicht zuverlässig erbracht werden können. **Verbindlichkeit** fehlt, wenn der Zugriff auf Objekte[6] und/oder nachfolgende Aktionen nicht (eindeutig) einem Subjekt zugeordnet und damit abgestritten werden können. **Vertraulichkeit** besteht nicht, wenn über den Kreis der autorisierten Subjekte hinaus Zugriff erfolgen kann.[7]

Software[8] besteht aus ausführbarem Code, der Anweisungen des Verfassers zur Ausführung durch Hardware oder andere Software enthält. Vor allem bei der Programmierung können **Fehler (Bugs)**[9] eingetragen werden. Solche Fehler im Code können ein bloßes Ärgernis sein und etwa die Benutzbarkeit einschränken. Sie gefährden jedoch ggf. (auch) die Sicherheit der Software selbst bzw. anderer Software, Hardware oder Systeme. Zur Wahrung des gewünschten Sicherheitsniveaus[10] geht es darum, die zuvor genannten Schutzziele zu erreichen, wobei fehlerfreier Code meist eine Utopie bleibt.[11] Mit der Vernetzung sind für Webanwendungen, Apps sowie Client- und Server-Software besondere Ausprägungen von Fehlern entstanden.[12] Durch die zunehmende Wiederverwendung von Code, sei es durch Übernahme oder Einbindung von fremden Modulen, können Programmierfehler ganze Klassen von Software betreffen.[13]

Wird die Funktion von **Hardware** durch Software definiert, gelten für Fehler im Code von etwa Firmware oder in ROMs die vorgenannten Punkte.[14] Es gibt jedoch

---

[5] Vgl. *Müller/Noß/Mainka/Mladenov/Schwenk,* Processing Dangerous Paths – abrufbar unter https://pdf-insecurity.org/.

[6] Bspw. eine Datei, ein Verzeichnis oder eine Partition.

[7] Siehe *Eckert*, IT-Sicherheit, S. 7 ff. zu den Definitionen.

[8] Software soll im hiesigen Zusammenhang als ausführbarer Code verstanden werden; zu unterscheiden ist zwischen Quellcode und dem letztlich ausgeführten Maschinencode, der durch Übersetzung des Quellcodes entsteht. „Software" umfasst Programme wie auch Skripte, nicht aber Dateien, die dem bloßen Abspeichern von Daten dienen. Vgl. *Tukey*, The American Mathematical Monthly, Vol. 65, Nr. 1 (Jan. 1958), S. 1 (2).

[9] Zur Begrifflichkeit im historischen Kontext *Kidwell,* IEEE Annals of the History of Computing, Vol. 20, Nr. 4, 1998, 5.

[10] Der von Programmierer:innen intendierte Grad an Absicherung gegen Bedrohungen erfolgt i.d.R. nach einem individuell erstellten Risikomodell. Vgl. *Eckert*, IT-Sicherheit, S. 239 ff. konkreter für den Software-Bereich Shostack, Threat Modelling, S. 3 ff.

[11] *Myers/Sandler/Badgett*, The Art of Software Testing, S. 8.

[12] Vgl. *Gebeshuber/Teiniker/Zugaj*, Exploit!, S. 51 ff.

[13] Vgl. *Schneier*, Click here to kill everybody, S. 31 f.

[14] Anschaulich zeigen dies FPGAs (Field Programmable Gate Arrays), also integrierte Schaltkreise, die mittels Software mit (unterschiedlichen und ggf. wechselnden) logischen Schaltungen belegt werden können. Ohne Kenntnis des Programmiercodes kann nicht etwa durch Bauteilidentifikation auf die konkret

auch hardware-spezifische Fehlerquellen wie z.B. Mängel im Design, von Gehäusen, der Bauteilsicherheit, der fehlenden Absicherung der Signalverarbeitung und -speicherung an Leiterbahnen und elektronischen Bauteilen oder durch das (ungewollte) Einbringen von Komponenten.[15] Aufgezählt sind nicht abschließend Faktoren, für deren Ausnutzung zur Kompromittierung es eines physischen Zugriffs auf die Hardware bedarf.[16] Dieser verlangt nicht unbedingt nach Messungen und Manipulationen direkt an Leiterbahnen und elektronischen Bauteilen. Manchmal genügt auch das Detektieren, Aufzeichnen und Analysieren von Emissionen der Hardware wie Schall, Wärme, Licht sowie Veränderungen von Magnetfeldern aus einiger Entfernung oder das vergleichende Messen von Stromverbrauch und Rechenzeit. Dann spricht man – insbesondere aus kryptoanalytischer Sicht zum Bruch von Verschlüsselungsimplementierungen – von **Seitenkanal-Attacken**. Die **Grenzen zwischen hardware- und softwarespezifischen Vektoren verschwimmen immer mehr**, wobei mit Netzwerkfähigkeiten von Geräten sich der Fokus zunehmend auf die Software-Komponenten richtet. Im Feld des Internets der Dinge (IoT) sind dies meist die Firmware und die Schnittstellen zu Bedien-Software und vor allem zu Cloud-Diensten.

Ist ein Fehler zur Kompromittierung in einer der vorgenannten Kategorien potenziell ausnutzbar, um ein Schutzziel zu verletzen, liegt eine **Schwachstelle** vor. Ist diese in der Praxis tatsächlich ausnutzbar, wird daraus eine **Bedrohung**.[17] Die Möglichkeit dazu kann mittels Machbarkeitsstudien, dezidierter Hard- bzw. Software oder Anleitungen zum An- oder Eingriff demonstriert werden **(Exploits)**. Von der Wirkung und den Folgen bei Realisierung wird der **Schweregrad der Bedrohung** ermittelt.[18] Dabei sind auch Wechselwirkungen mit anderer Hard- und Software bzw. deren Schwachstellen samt Auswirkungen von und auf diese zu beachten.[19] Auf die Detektion einer Schwachstelle kann etwa damit reagiert werden, dass der fehlerhafte Code berichtigt,

---

in der Hardware umgesetzten Funktionen geschlossen werden. Der Code ist das prägende Element. Dies gilt es im Folgenden zu berücksichtigen, wenn zwar gleichrangig Hardware genannt wird, im Kern jedoch ein Fehler in Software wie Firmware liegt.

[15] Zu letzterem *Speith/Becker/Ender/Puschner/Paar,* DuD 2020, 446.

[16] Vgl. *Mangel/Bicchi*, Praktische Einführung in Hardware Hacking, S. 83 ff. Die Manipulation von Firmware bedarf ggf. keines physikalischen Zugriffs und kann über den Online-Pfad erfolgen. Vgl. für die Angreifbarkeit von (Multifunktions-)Druckern über das Netzwerk *Ries*, heise security vom 12.08.2019, abrufbar unter https://www.heise.de.

[17] Insbesondere von verwendeten Drittanbieterkomponenten wird oftmals nur ein Bruchteil der gesamten Funktionalität eingesetzt. Dennoch kann die gesamte Komponente eingebunden sein, wodurch auch Schwachstellen in nicht verwendeten Teilen relevant sein können.

[18] Etwa mittels der Metrik des Common Vulnerability Scoring Systems (CVSS), abrufbar unter https://www.first.org.

[19] So können Schwachstellen auf einander aufbauend in einer bestimmten Reihenfolge ausgenutzt werden, um das endgültige Ziel, die Übernahme der Kontrolle mit allen Rechten über ein System, zu erreichen.

eine neue Version bzw. ein Patch erstellt und installiert wird oder anderweitige Maßnahmen zum Schutz, wenigstens aber zur Verringerung der Angriffsoberfläche (**Mitigation**) getroffen werden.[20] Das Ergebnis ist nicht zwangsläufig statisch, da neue Ansätze für die Ausnutzung oder die technische Weiterentwicklung eine Neubewertung der Bedrohung jederzeit erforderlich machen können. Einen speziellen Fall bilden Sicherheitslücken in Bibliotheken oder Komponenten, die in verschiedener Software als Bausteine eingesetzt werden. Die präzise Risikobewertung ist hierbei abhängig vom jeweiligen Einsatzumfeld, auch wenn es sich um dieselbe unveränderte Komponente handelt (z.B. log4j-Schwachstelle).

Schwachstellen können jeder Person etwa beim Besuch einer Website, der Nutzung von Webdiensten oder dem Ausführen von Apps auffallen.[21] Es bedarf also nicht zwingend einer gezielten Suche. Manchmal reicht schon aufmerksames Beobachten oder Benutzen. Abweichungen von nach Handbüchern oder Anleitungen vorgesehenen Abläufen stellen ebenso Indizien dar. Insbesondere wenn sich in der Folge reproduzierbar etwa Zugriffsmöglichkeiten auf eigentlich als unzugänglich vorgesehene Funktionen oder Daten ergeben, deutet alles auf einen sicherheitsrelevanten Fehler hin.[22] Dessen Schwere ist eine Frage des Einzelfalls und meist nur vom nötigen Aufwand zur Ausnutzung und deren erwartbaren Folgen aus einschätzbar. Spätestens hier spielen beruflich in der IT tätige oder aus privatem Interesse mit Fachkenntnissen ausgestattete Entdecker:innen, besonders aber IT-Sicherheitsforscher:innen ihre größere Expertise gegenüber interessierten Laien aus. Diese kommt auch zum Tragen, wenn für Recherche, Entdeckung und Dokumentation von Schwachstellen bzw. die Entwicklung von Exploits Spezialwissen oder besondere Ausrüstung notwendig sind.[23]

---

[20] Vgl. *Magnusson*, Practical Vulnerability Management, S. 31 ff.

[21] Einfach aufzuspürende Schwachstellen werden häufig als „low hanging fruits" („tief hängende Früchte") bezeichnet.

[22] Bsp.: Zugriffsmöglichkeiten auf die Daten eines anderen Benutzers oder Konfigurationsmöglichkeiten, die eigentlich nur dem Administrator zustehen sollten.

[23] Individuell oder über ein Kollektiv (Forschergruppe, Netzwerk, Community) zugänglich. Vgl. für Ausrüstungsbeispiele *Mangel/Bicchi*, Praktische Einführung in Hardware Hacking, S. 24 ff.; *Kofler* et al., Hacking & Security, S. 295 ff.; *Amberg/Schmid*, Hacking, S. 811 ff.

II. Empfehlungen zur Handhabung von Sicherheitslücken

„Bei Cybersicherheit gibt es keinen
Königsweg – und es gibt keine absolute Sicherheit."[24]
— Lepassaar

Behörden und Institutionen wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder die Agentur der Europäischen Union für Cybersicherheit (ENISA) empfehlen, dass nach dem Prinzip des „Coordinated Disclosure" (auch „Responsible Disclosure") verfahren wird.[25] „Koordiniert" bedeutet, dass eine Sicherheitslücke nach Auffinden durch Dritte (z.B. Sicherheitsforschende) zunächst vertraulich an die Stelle gemeldet wird, die sie beheben kann (i.d.R. das herstellende Unternehmen bzw. den Produktverantwortlichen) und beide Parteien bei der Analyse und Behebung der Sicherheitslücke kooperieren.[26] Im Idealfall werden Informationen zur Sicherheitslücke erst nach Behebung der Schwachstelle, oder dem Bereitstellen einer passenden Mitigation (z.B. Softwareupdate) offengelegt, sodass Risiken für potenziell Betroffene hinreichend minimiert werden können. Allerdings stellen sich in der Praxis oftmals erhebliche Probleme. So gaben 58% der Befragten einer aktuellen Umfrage zu ethischem Hacken an, dass sie Schwachstellen nicht melden konnten, wenn das Unternehmen keinen eindeutigen Kommunikationsprozess hat.[27]

1. Coordinated Disclosure und auftretende Probleme

Wird eine Sicherheitslücke durch Dritte (z.B. im Rahmen der IT-Sicherheitsforschung, durch sog. ethische Hacker:innen oder durch Zufall) entdeckt, liegt es an der Finder:in diese ggf. über Vermittler:innen zu melden. Wenn der Fund nicht innerhalb einer beauftragten Untersuchung mit vertraglichen Meldepflichten allein an die Vertragspartnerin auftritt, erfolgt die Meldung freiwillig. Sie kann nach dem Coordinated-Disclosure-Verfahren erfolgen.

---

[24] Interview im Tagesspiegel, vom 18.11.2021 https://background.tagesspiegel.de/cybersecurity/bei-cybersicherheit-gibt-es-keinen-koenigsweg (zuletzt abgerufen am 18.11.2021).

[25] *BSI*, Handhabung von Schwachstellen, BSI-CS 019 | Version 2.0 vom 11.07.2018 https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_019.pdf?__blob=publicationFile&v=1 (zuletzt abgerufen am 21.012.2021); *ENISA*, Good Practice Guide on Vulnerability Disclosure.

[26] Whitepaper Rechtslage der IT-Sicherheitsforschung 2021, S. 27 ff.

[27] *Bugcrowd*, Inside the Mind of a Hacker 2021, S. 4. Ähnlich die Ergebnisse einer Umfrage der National Telecommunications and Information Administration (NTIA) von 2016: Vulnerability disclosure attitudes and actions: A research report, https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf.

a) Sicherheitslücken

Sicherheitslücken sind Schwachstellen oder Fehler in Design, Implementierung oder Konfiguration, die zu unerwarteten und unerwünschten Ereignissen führen können und dabei die Sicherheit eines Computersystems, Netzwerks, Programms, einer Hardwarekomponente oder eines Protokolls beeinträchtigen.[28] Sicherheitslücken können in allen IT-Produkten sowohl im Konzept wie auch in Software oder Hardware auftreten. In den letzten Jahren wurden allein über das CVE-System[29] mehr als 10.000 Sicherheitslücken pro Jahr in verschiedensten Produkten registriert.[30] Sicherheitslücken können einzelne Instanzen, z.B. einzeln entwickelte Webseiten, oder ganze Produktklassen, wie z.B. Standardsoftware die vielfach installiert ist, betreffen.

b) Coordinated Disclosure

Der Coordinated-Disclosure-Prozess[31], früher auch Responsible Disclosure[32] genannt, soll die Interessen der Beteiligten in Ausgleich bringen und auf ein möglichst schnelles Schließen der Sicherheitslücken hinwirken.

Im Idealfall läuft der Prozess dabei wie folgt ab: Nach dem Finden einer Sicherheitslücke identifiziert die Melder:in diejenige Stelle, im Folgenden Produktverantwortliche genannt, die vermeintlich als Sachnächste die Sicherheitslücke verifizieren und beheben kann. Auf deren Homepage findet sie die Kontaktdaten der benannten Ansprechpartner:in und meldet dieser über einen geschützten Kanal die Details der Sicherheitslücke und skizziert den weiteren Verlauf des Prozesses. Nach einer Bestätigung des Eingangs der Meldung erstellt und testet die Produktverantwortliche eine technische Lösung zur Beseitigung der Sicherheitslücke; gegebenenfalls beantwortet die Melder:in technische Rückfragen. Nachdem die technische Lösung – zumeist ein Softwareupdate – veröf-

[28] *ENISA*, Glossary – https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary#G52.

[29] Common Vulnerabilities and Exposures ist ein Referenziersystem für Sicherheitslücken, siehe https://www.cve.org/.

[30] Seit 2017 jährlich über 10.000 im CVE System, siehe https://www.cvedetails.com/browse-by-date.php

[31] Siehe zum Vergleich zur Non-Disclosure, Limited Disclosure oder Full-Disclosure: *Shepherd*, How do we define Responsible Disclosure? SANS Institute Information Security Reading Room, 2003.

[32] Ursprünglich hatte sich der Begriff „Responsible Disclosure" etabliert, wurde aber zugunsten des stärker die Kooperation unterstreichenden Begriffs der Coordinated Vulnerability Disclosure abgelöst, um auch die Notwendigkeit eines Prozesses "auf Augenhöhe" zwischen zwei gleichberechtigten Partnern aufzuzeigen: *National Cyber Security Centre*, Coordinated Vulnerability Disclosure: the Guideline (2018), S. 5; vgl. auch Whitepaper zur Rechtslage der IT-Sicherheitsforschung 2021, S 39 ff.; *Weulen/Kranenbarg/Holt/van der Ham*, Crime Science (2018) 7:16 – https://doi.org/10.1186/s40163-018-0090-8.

fentlicht wurde, publizieren die Melderin:in und die Produktverantwortliche abgestimmte Informationen für die Öffentlichkeit. Die Melder:in kann zusätzlich weitere Details zur Sicherheitslücke veröffentlichen, z.B. im Rahmen einer wissenschaftlichen Publikation. Ebenso kann eine öffentlich einsehbare CVE-Nummer beantragt werden, um die Information über die Lücke in einem standardisierten Format für Anwender:innen bereitzustellen.

In der Praxis zeigen sich immer wieder Probleme, sodass vom oben dargestellten Muster-Ablauf abgewichen werden muss. Der Coordinated-Disclosure-Prozess sieht dafür vor, dass die Melder:in bei der Meldung einen Zeitraum festlegt, innerhalb dessen die Produktverantwortliche eine Lösung für das Problem entwickeln kann. Die Länge dieses Zeitraums hängt von der Art und den Umständen der betroffenen Sicherheitslücke ab, in vielen Fällen werden z.B. 90 Tage angesetzt. Wenn zu erwarten ist, dass die Produktverantwortliche keine technische Lösung für die Sicherheitslücke bereitstellen wird, z.B. weil keinerlei Reaktion erfolgt, oder die Frist abgelaufen ist, müssen die Interessen der Gesellschaft und der Produktverantwortlichen neu abgewogen werden. Dabei ergibt sich regelmäßig, dass die Interessen der potenziell betroffenen Personenkreise an der Veröffentlichung von Informationen zur Sicherheitslücke überwiegen, damit Produktnutzer:innen und Dritte angemessene Schutzmaßnahmen (Mitigation) ergreifen und damit potenziellen Schaden abwenden können.[33] Auf Basis dieser Informationen kann ggf. auch öffentlicher Druck auf die Produktverantwortliche aufgebaut werden, eine technische Lösung zu erstellen.

Der Coordinated-Disclosure-Prozess wird in den Standards ISO/IEC 30111 und ISO/IEC 29147:2018 sowie von der ENISA[34] beschrieben. Er ist in Deutschland derzeit nicht im geltenden Rechtsrahmen verankert.

c) Praktische Probleme

In der Praxis zeigen sich mehrere Probleme bei der Umsetzung des Coordinated-Disclosure-Verfahrens. Die erfolgreiche Behebung der Sicherheitslücke gelingt meist nur bei Kooperation aller Beteiligten, nicht aber, wenn die Mitwirkung durch die Produktverantwortlichen verweigert wird.[35] Häufige Probleme sind:

- **Identifikation der Produktverantwortlichen:** In einigen Fällen bereitet die Identifikation der produktverantwortlichen Stellen Schwierigkeiten z.B. bei importierten Produkten, vielgliedrige Lieferketten und wenn die Sicherheitslücke

[33] *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.

[34] *ENISA*, Good Practice Guide on Vulnerability Disclosure (2015), S. 24 – DOI: 10.2824/610384.

[35] Hierzu der Vortrag von *Obermaier/Schink*, Tales from Hardware Security Research: From Research over Vulnerability Discovery to Public Disclosure, abrufbar unter: https://media.ccc.de/v/Camp2019-10292-tales_from_hardware_security_research.

in einem zugelieferten Modul (z.B. Softwarebibliothek) liegt. Ähnlich schwierig gestaltet es sich, eine große Zahl von Produktverantwortlichen zu identifizieren und so z.B. konkurrierenden Unternehmen dieselbe Sicherheitslücke zu melden, etwa wenn ganze Klassen der IT betroffen sind.[36]

- **Identifikation der Ansprechpartner:in bei der Produktverantwortlichen:** Nicht bei allen Produktverantwortlichen sind explizit Kontakte für die Meldung von Sicherheitslücken benannt. Öffentlich kommunizierte Kontaktstellen, z.B. der Kundenservice, können Sicherheitslücken insbesondere bezüglich ihrer Kritikalität oft nicht korrekt einschätzen und leiten diese daher häufig nicht weiter.
- **Unzureichende Kommunikation:** Selbst wenn Produktverantwortliche und die zuständige Ansprechpartner:in bekannt sind, reagieren diese teils nicht auf Anfragen oder brechen die Kommunikation plötzlich ab.[37] Zudem kann es zu unterschiedlichen Erwartungen an die Frequenz und Umfang der Kommunikation kommen.
- **Abweichende Einschätzung:** Nach Bereitstellung der Informationen zur Sicherheitslücke bewerten die Produktverantwortlichen in manchen Fällen die Lücke mit einer geringeren Kritikalität als die Melder:in.[38] Dies geschieht entweder unabsichtlich aufgrund von fehlendem Know-How oder technischen Missverständnissen. Auch geschäftstaktische Gründe sind denkbar, wenn Sicherheitslücken ad hoc nicht oder nur mit großem (Kosten-)Aufwand behoben werden könnten und die Produktverantwortliche daher die Lücke nicht oder erst später etwa im Rahmen anderweitiger Updates oder neuer Versionen beseitigen will. Die technische Argumentation zur Schwere der Lücke führt häufig zu deutlichem Mehraufwand auf Seite der Melder:in, den aber keinerlei Aufwandsentschädigung ausgleicht.
- **Juristische Grauzone:** In Einzelfällen haben Produktverantwortliche juristische Maßnahmen angedroht und tatsächlich eingeleitet, um die Finder:innen von Sicherheitslücken von einer Veröffentlichung bzw. weiteren Untersuchungen an den eigenen Produkten abzubringen.[39] Selbst unberechtigte juristische

[36] Empfehlungen bietet das *Forum of Incident Response and Security Teams (FIRST)*, Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure, Version 1.1 (Spring 2020).

[37] *Stock* et al., „Hey, You Have a Problem: On the Feasibility of Large-Scale Web Vulnerability Notification", USENIX 2016, S. 1015-1032.

[38] Bspw. zur Schwere der Lücke, ob es sich überhaupt um eine Sicherheitslücke handelt und ob diese ausnutzbar ist.

[39] Vgl. *Franzen/Maier/Wagner*, DuD 2020, 511; Volkswagen AG vs. Garcia and others, High Court of Justice [2013] EWHC 1832 (Ch); LJN: BD7578, Voorzieningenrechter Rechtbank Arnhem, 171900 /

Drohungen bedeuten meist enormen Aufwand und können zu persönlich stark belastenden Situationen führen.[40] Juristische Konsequenzen betreffen hierbei aufgrund der Rechtslage z.T. auch Privatpersonen, selbst wenn die Forschung im Rahmen eines Beschäftigungsverhältnisses durchgeführt wurde.[41]

- **Legacy-Problematik:** Bei Hard-/Software, die nicht mehr gepflegt wird, etwa weil Quellcode wegen Insolvenz oder fehlender Dokumentation unzugänglich ist, die aber immer noch verwendet werden, stellen sich Fragen zur Verantwortlichkeit und dem Weg zu technischen Lösungen. Zudem ist meist (ggf. nicht mehr vorhandenes) Spezialwissen zur technischen Einschätzung erforderlich. Letztlich kann sich hier nur an die Betreiber:innen/Nutzer:innen gewendet werden. Dies ist schon organisatorisch von Melder:innen nicht zu leisten, insbesondere wenn dies kritische Infrastrukturen betrifft.
- **„Too big to fix" sowie unklare Verantwortung und fehlende Möglichkeiten:** Es existieren Schwachstellen, die so viele (Mit-)Verantwortliche oder Produkte betreffen, dass die Melder:in das Ausmaß nicht überblicken kann (z.B. die log4j / log4shell Lücke, die Ende 2021 entdeckt wurde). Unter Umständen sind Meldungsempfänger:innen technisch und/oder rechtlich nicht in der Lage, die Schwachstelle zu evaluieren und zu beseitigen. Dies kann sich etwa aus fehlendem Know-How, fehlenden Kapazitäten, fehlender/unklarer Dokumentation oder einer restriktiven (vertraglichen) Rechtslage ergeben. Besonders in vielgliedrigen Lieferketten über Landesgrenzen hinweg ist dies in der globalisierten Wirtschaft ein größer werdendes Problem.

d) Überblick über rechtliche Risiken einer Meldung

Neben den genannten praktischen Hürden ergeben sich rechtliche Risiken für Personen, die eine Meldung bei einer Institution oder der produktverantwortlichen Stelle selbst beabsichtigen, nachdem sie zufällig oder proaktiv – jedenfalls aber ohne explizite Beauftragung - Sicherheitslücken gefunden haben.[42] Diese resultieren vor allem aus dem

KG ZA 08-415 vom 18 Juli 2008; zu rechtlichen Drohungen siehe auch: *Gamero-Garrido/Savage/Levchenko/Snoeren*, „Quantifying the Pressure of Legal Risks on Third-party Vulnerability Research", in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017, S. 1501 (1502) sowie Listen zu rechtlichen Drohungen gegenüber Sicherheitsforschenden unter: https://attrition.org/errata/legal_threats/ und https://github.com/disclose/research-threats (zuletzt abgerufen am 10.08.2022).

[40] Vgl. *Ermert*, in: heise vom 06.09.2018 https://www.heise.de/newsticker/meldung/Offenlegung-von-Softwareluecken-Rechtsstreit-endet-mit-Vergleich-4156393.html.

[41] Siehe hierzu *Franzen/Maier*, „Mehr schlecht als Recht: Grauzone Sicherheitsforschung", abrufbar unter https://media.ccc.de/v/35c3-9898-mehr_schlecht_als_recht_grauzone_sicherheitsforschung.

[42] Whitepaper Rechtslage der IT-Sicherheitsforschung 2021, S. 9 ff.

Straf- und Urheberrecht.[43] So bestraft § 202a StGB die Überwindung einer Zugangssicherung, um sich unbefugten Zugang zu Daten zu verschaffen, die nicht für die Täter:in bestimmt sind.[44] Nach der Motivation der Handlung wird nicht differenziert, die kriminelle Energie manifestiere sich aus Sicht des Gesetzgebers bereits in der Überwindung der Sicherung.[45] Dabei wurde nicht bedacht, dass solche Handlungen, wie auch die dabei genutzten „Hacker"-Werkzeuge, typischerweise auch in der IT-Sicherheitsforschung anzutreffen sind.[46] Zwar können Forschende versuchen, Testumgebungen zu nutzen, in denen sich die Zugangsverschaffung auf ihre „eigenen" Daten bezieht[47] Insbesondere Tests von Cloud- und Web-Anwendungen können allerdings oftmals nur direkt am Online-System durchgeführt werden, da weder die Anwendung für Forscher:innen verfügbar noch deren Konfiguration ausreichend bekannt ist. Häufige Funde betreffen daher regelmäßig reale Szenarien mit Daten Dritter.[48]

[43] *Golla*, JZ 2021, 985; *Brodowski,* ZIS 2019, 49*; Wagner,* DuD 2020, 111; *Vonderau/Wagner,* DSRITB 2020, 525.

[44] Siehe hierzu ausführlich Kapitel 2.

[45] BT-Drs. 16/3656, S. 10. Handelt es sich hingegen um einen Kopierschutz, sind urheberrechtliche Implikationen denkbar.

[46] Vgl. zur Abgrenzung von „Dual Use Tools" und Hackertools im Rahmen des sog. „Hackerparagraphen" § 202c StGB: BVerfG, Nichtannahmebeschluss vom 18. 05. 2009 – 2 BvR 2233/07, Rn. 69 ff.

[47] Die Strafbarkeit hängt davon ab, ob die handelnde Person über die sog. „Datenverfügungsberechtigung" verfügt, welche demjenigen zugewiesen wird, der die Daten erstmals gespeichert hat (sog. „Skripturakt"), vgl. *Welp,* IuR 1988, 443.

[48] Sind diese personenbezogen, muss zusätzlich das Datenschutzrecht bedacht werden.

	Relevante Handlungen bei IT-Sicherheitsanalysen	Strafbarkeitsrisiken
§ 202a	Die Überwindung einer Zugangssicherung zu Testzwecken ist eine typische Handlungsweise bei IT-Sicherheitstests.	Nach der Überwindung kann Zugang zu „fremden" Daten, die nicht für den Nutzenden bestimmt sind, bestehen.[49]
§ 202b	Bei Sicherheitstests kommen auch elektronische Messgeräte (z.B. Oszilloskopen) zum Einsatz, um die elektromagnetische Abstrahlung zu analysieren[50]	Trotz der Analyse eigener Geräte kann diese Daten tangieren, die nicht für den Nutzenden bestimmt sind.
§ 202c	Auffinden eines Passworts, Herstellung sog. „Exploit Code", um eine Sicherheitslücke auszunutzen, Nutzung von Sicherheitsanalysewerkzeugen	Dual-Use-Tools für Sicherheitstests sind zwar nicht erfasst, sofern diese Tests nicht unter §§ 202a, 202b, 303a StGB fallen;[51] zu den diesbezüglichen Risiken siehe dort.
§ 303a	Senden von Daten an ein fremdes System, um einen Kommunikationskanal zu eröffnen, welcher in dieser Form nicht vorgesehen war	Das Hinzufügen von Daten könnte bei Funktionsbeeinträchtigung der (Bestands-)Daten bspw. in Form der Öffnung eines Kommunikationskanals als Datenveränderung gewertet werden.[52]
§ 303b	Honeypot-Systeme können die Analyse des Aufbaus von Botnetzen und anschließender DDoS-Attacken (Distributed-Denial-of-Service Attack) ermöglichen[53]	Soweit der Honeypot durch den Angreifer und Botnetzbetreiber zur Computersabotage verwendet wird, könnte das Bereitstellen des Honeypots als Beihilfe gewertet werden.

Tabelle 1: Typische Forschungshandlungen und ihre Strafbarkeitsrisiken

[49] Auf eine tatsächliche Kenntnisnahme kommt es nicht an: BT-Drs. 16/3656, S. 9 f.

[50] Bspw. *Eisenbarth/Kasper/Paar,* DuD 2008, 507.

[51] BVerfG, Nichtannahmebeschluss vom 18. 05. 2009 – 2 BvR 2233/07 – Hacker-Tool, Rn. 59 ff.; zur Restunsicherheit: *Schuster*, DuD 2009, 742 (746).

[52] BGH, Beschluss vom 27. Juli 2017 – 1 StR 412/16 –, Rn. 34 m. Anm. *Brodowski*, StV 2019, 385.

[53] *Vogelgesang/Möllers/Potel,* MMR 2017, 291.

Je nach Vorgehensweise könnten weitere Straftatbestände erfüllt sein, wie bspw. die Fälschung beweiserheblicher Daten (§ 269 StGB) oder Urkundenunterdrückung (§ 274 StGB).[54] Ob im ersteren Fall eine Täuschung im Rechtsverkehr und im zweiten Fall eine Nachteilszufügungsabsicht im Raum stehen, erscheint allerdings für die meisten Fälle der Sicherheitsforschung eher fraglich.

Daneben betrifft die IT-Sicherheitsforschung häufig die Analyse von Computerprogrammen, die urheberrechtlichen Schutz genießen.[55] Methoden des Reverse Engineerings werden bspw. über die Regelung zum Dekompilieren in § 69e UrhG sehr engen Schranken unterworfen. Diese kommen praktisch einem Verbot für die Forschung gleich.[56] Zwar erlaubt § 3 Abs. 1 Nr. 2 GeschGehG das Reverse Engineering, aber nur im Hinblick auf die Erlangung von Geschäftsgeheimnissen. Ob dies auch Auswirkungen auf das Urheberrecht hat, bleibt unklar.[57] Zudem lassen sich nicht alle Informationen als Geschäftsgeheimnisse i.S.d. § 2 GeschGehG einstufen: Umstritten ist dies bspw. gerade bei Informationen über rechtswidriges Verhalten.[58] Andere Autoren sehen hingegen auch Informationen zu Sicherheitslücken grundsätzlich umfasst.[59] Ob Hersteller Reverse Engineering vertraglich untersagen können, ist ebenfalls noch nicht abschließend geklärt.[60] Sofern AGB bspw. Sicherheitstests, Prüfungen auf Sicherheitslücken, Reverse Engineering, Dekompilieren oder Disassemblieren verbieten, müssen diese zwar nur beachtet werden, wenn sie in den Nutzungs- bzw. Lizenzvertrag wirksam einbezogen sind (insbes. Hinweis vor Vertragsschluss, keine überraschenden Klauseln, vgl. §§ 305, 305a BGB) und keine unangemessene Benachteiligung nach § 307 BGB darstellen. Umfassende Verbote des Dekompilierens oder der Programmbeobachtung sind dabei nach § 69 Abs. 2 UrhG unwirksam, finden sich nichtsdestotrotz in einigen Nutzungsbestimmungen.[61] Selbst bei Quellcode von Behördensoftware wurde die Einsichtnahme bspw. über Informationsfreiheitsgesetze bisher verneint, da es sich nicht um amtliche Informationen handele.[62] Zudem wird explizit auf notwendige unverhältnismäßige Aufwände zur Trennung von sicherheitssensiblen und nicht-sicherheitssensiblen Teile des Quellcodes verwiesen, wobei festzustellen ist, dass eine solche Trennung prinzipbedingt einer Prüfung auf Sicherheitslücken entgegensteht.

---

[54] *Klaas*, MMR 2022, 187 (189).

[55] Zu unterschiedlichen Methoden siehe: *Maier/Franzen/Wagner*, DuD 2020, 511 (512 f.).

[56] *Vettermann/Wagner*, InTeR 2020, 126 (129)

[57] *Ohly*, GRUR 2019, 441 (447).

[58] *Alexander*, AfP 2019, 1 (4 f.); *Hauck*, WRP 2018, 1032 (1033); *Dann/Markgraf*, NJW 2019, 1774 (1776).

[59] *Renner*, in: Borges/Hilber, BeckOK IT-Recht, § 2 GeschGehG Rn. 18.

[60] Vgl. § 3 Abs. 1 Nr. 2 b) GeschGehG.

[61] Insofern folgen Einschränkungen im Hinblick auf zwingend vorrangige Rechte, ob diese wirksam sind, soll an dieser Stelle nicht abschließend beurteilt werden.

[62] VG Wiesbaden, Urteil vom 17.1.2022 – 6 K 784/21.WI.

Insgesamt fehlen derzeit eindeutige Regelungen und einschlägige Präzedenzfälle in Deutschland, um die Rechtslage der IT-Sicherheitsforschung insgesamt oder zumindest bestimmter Formen von IT-Sicherheitsanalysen rechtssicher einschätzen zu können. Keinen Risiken setzen sich Forschende und ethische Hacker:innen hingegen aus, wenn es ihnen gelingt die jeweiligen Rechtsinhaber:innen zu identifizieren und eine (rechtswirksame) Erlaubnis entweder explizit zu erhalten oder sich im Rahmen einer Sicherheitsanalysen erlaubenden Responsible Disclosure Policy oder eines Bug-Bounty-Programms[63] zu bewegen. Solche Erlaubnisse sind aktuell eine Seltenheit. In der Praxis zeigen sich zudem auch hier sowohl rechtliche als auch tatsächliche Hürden.[64] Die unaufgeforderte Meldung des Funds von *proaktiv* gefundenen Sicherheitslücken geht somit oftmals mit dem Risiko einher, Ziel staatlicher Ermittlungen oder zivilrechtlicher Auseinandersetzungen zu werden.

2. Empfehlungen an Produktverantwortliche und Minimalkonsens zum Umgang mit Sicherheitslücken

Zu Verbesserung des Coordinated-Disclosure-Prozesses werden u.a. folgende Maßnahmen für Produktverantwortliche empfohlen:[65]

- Veröffentlichung einer Disclosure Policy.[66]
- Nennung eines:r Ansprechpartner:in für IT-Sicherheitsmeldungen und Bereitstellung eines Kommunikationskanals, der ausreichend abgesichert ist.
- Etablierung entsprechender unternehmensinterner Prozesse (inkl. Fristen bzgl. Reaktionszeiten für Antworten und Patchen).
- Verzicht gegenüber freiwilligen Melder:innen auf formelle Bedingungen oder vorab abzuschließende Vereinbarungen wie Non-Disclosure-Agreements.

[63] Unter „Bug Bounty" versteht man die Auslobung von Sach- oder Geldpreisen für die Entdeckung und Meldung von Fehlern in Software. Rechtliche Legitimation vermitteln diese allerdings nur, wenn sie von der Stelle ausgehen, die über das jeweils betroffene Rechtsgut verfügen kann.

[64] Whitepaper Rechtslage der IT-Sicherheitsforschung 2021, S. 16 mwN.

[65] BSI, Handhabung von Schwachstellen, BSI-CS 019 | Version 2.0 vom 11.07.2018 https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_019.pdf?__blob=publicationFile&v=1 (zuletzt abgerufen am 21.012.2021).

[66] Whitepaper Rechtslage der IT-Sicherheitsforschung 2021, S. 54 f.; *Woszczynski/Green/Dodson/Easton*, Government Information Quarterly 37(1) 2020, 101418 – DOI: https://doi.org/10.1016/j.giq.2019.101418.

Folgende fünf Grundregeln sollten als Minimalkonsens für Entdecker:innen/Melder:innen und Meldungsempfangende gelten:[67]

1. Schwachstellen sollten an die Stellen gemeldet werden, die sie beheben oder die Behebung erzwingen können – in der Regel sind dies die Hersteller:innen eines Produkts/Systems oder die Stelle, bei der die Schwachstelle oder auch eine Fehlkonfiguration auftritt oder die sie verursacht hat.
2. Die Meldung sollte so schnell wie möglich erfolgen und insbesondere dürfen keine unsachgemäßen Interessen insb. Dritter die Ursache für eine Verzögerung der Meldung durch die Entdeckende sein.
3. Die Stelle, an die die Schwachstellen gemeldet wurden, sollte Abhilfemaßnahmen so schnell wie möglich entsprechend dem Risiko bereitstellen.[68] Insbesondere sollten keine unsachgemäßen Interessen Dritter (z.B. Vermeidung negativer Presseberichte) der Grund für eine Verzögerung bei der Suche nach der Behebung oder Entschärfung sein.
4. Die Abhilfemaßnahmen sollten so einfach wie möglich anzuwenden und leicht zugänglich sein.
5. Die Entdeckenden dürfen Informationen zur Schwachstelle nach einer angemessenen Zeitspanne nach der Meldung zur Anerkennung ihrer Leistung und/oder Forschungszwecken veröffentlichen. Bug Bounties dürfen verwendet werden, solange sie den vorherigen Aussagen nicht widersprechen.

III. Hintergrund zu den Entdecker:innen von Schwachstellen

1. IT-Sicherheitsforschung im engeren Sinne

Forschung wird aus rechtlicher Sicht definiert als 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.[69] IT-Sicherheitsforschung findet an Hochschulen und Forschungseinrichtungen statt, ist allerdings nicht auf diese beschränkt.[70] Ihre moderne

[67] Whitepaper Rechtslage der IT-Sicherheitsforschung 2021, S. 38.

[68] Rechtspflichten hierzu bestehen allerdings nicht in jedem Fall, siehe hierzu Kapitel 2 zur allgemeinen Interessenlage produktverantwortlicher Unternehmen und Kapitel 4 zur End-of-Life-Problematik.

[69] BVerfGE 35, 79 (113); 47, 327 (367).

[70] Etwa Forschung durch Einzelpersonen oder Kollektive (z.B. im Rahmen zivilgesellschaftlichen Engagements) oder in Unternehmen, die (IT-Sicherheits-)Soft-/Hardware entwickeln oder oder dienstleistend/beratend tätig sind, aber auch durch staatliche Einrichtungen, wie etwa Streitkräfte, Sicherheitsbehörden oder Nachrichtendienste samt deren Dienstleister.

Ausprägung betrachtet ganzheitlich die **Informationstechnologie aus Sicht von Angreifer:innen und Verteidiger:innen**. Ein festes Methodik-Set der IT-Sicherheitsforschung gibt es nicht.[71] Im Fokus steht hier die **anwendungsorientierte Forschung**, also die Überprüfung der Ingenieur- und Programmierleistung des Herstellers sowie des Betriebs und der Nutzung mit Blick auf Sicherheit. Dies kann einerseits im Rahmen eines konkreten Auftrags erfolgen. Andererseits ist eine bezüglich der zu untersuchenden Systeme offene, experimentelle und in ihren Maßstäben dynamische Herangehensweise ohne Auftrag möglich. Hinzu kommen Untersuchungen zu Präventionsmöglichkeiten,[72] Ursachen für Schwachstellen[73] sowie im Vorfeld oder Nachgang von Ein- bzw. Angriffen[74] und an den Schnittstellen zur grundlegenderen Forschung[75].

Während sich Sicherheitsforschung im engeren Sinne durch ein methodisches Vorgehen auszeichnet, finden Laien wie Fachleute oftmals zufällig in Alltagssituationen Verdachtsfälle unzureichender IT-Sicherheit. Um diesem Verdacht nachzugehen und anschießend ein Coordinated-Vulnerability-Disclosure-Verfahren (nachfolgend auch CVD-Prozess) durchzuführen, kann es erforderlich werden in ein System einzudringen, um die vermutete Sicherheitslücke zu bestätigen (dies wird mitunter auch als „ethisches Hacken" bezeichnet).[76]

2. Ethisches Hacken

Die Bedeutung ethischen Hackens für die Gesamtsituation der IT-Sicherheitslandschaft kann mit einigen Zahlen und Beispielen belegt werden. So hat eine Umfrage ergeben, dass 37% der befragten Organisationen einer repräsentativen Stichprobe von 1.000 Befragten aus verschiedenen IT-Branchen und Unternehmensgrößen in den USA, Deutschland, Frankreich, Italien und dem Vereinigten Königreich innerhalb von 12 Monaten (im Zeitraum 2018/2019) unaufgeforderte Meldungen über Sicherheits-

[71] Zu Systematisierungsansätzen vgl. *Edgar/Manz*, Research Methods for Cyber Security, S. 63 ff.

[72] *Anderson*, Security Engineering, S. 3 ff.

[73] Vgl. für eine empirische Untersuchung unter Programmierern etwa *Naiakshina/Danilova/Gerlitz/von Zezschwitz/Smith,* „If you want, I can store the encrypted password" – A Password-Storage Field Study with Freelance Developers, abrufbar unter https://doi.org/10.1145/3290605.3300370.

[74] Etwa Bedrohungsanalysen oder Priorisierung von Schutzmaßnahmen, Attribution von Tätern oder Nachverfolgung von Datenflüssen.

[75] Etwa zum Chiffren Design *Schmeh*, Kryptografie, S. 97 ff.

[76] Zum Begriff: *Peeters*, Strengthening the digital Achilles heel of the European Union: Make use of ethical hackers to find vulnerabilities in information systems?, S. 9 m.w.N. – abrufbar unter: https://openaccess.leidenuniv.nl/handle/1887/55426.

lücken erhielten, von denen 90% koordiniert nach dem CVD-Prozess abgearbeitet wurden.[77] 90 % der Befragten IT-Expert:innen, die mit Vulnerability Disclosure Prozessen durchschnittlich bis gut vertraut sind, bestätigten, dass die Offenlegung von Schwachstellen dabei einem allgemeineren Zweck dient, nämlich der Verbesserung der Art und Weise, wie Software entwickelt, verwendet und Fehler behoben werden.[78] Die Zustimmung zu unaufgeforderten Sicherheitsprüfungen variierte hingegen in verschiedenen Branchen und Regionen.[79] Laut Angaben von *Bugcrowd*, einer Crowdsourcing-Sicherheitsplattform[80], habe allein im Zeitraum von Mai 2020 bis August 2021 die Mithilfe ethischer Hacker:innen zur Abwehr von Cyberangriffen einen Wert von 27 Mrd. US-Dollar beigetragen.[81] Die Daten des Security Reports der Plattform *Hackerone* zeigen eine Zunahme der Schwachstellenmeldungen in den letzten Jahren.[82] In Deutschland machte besonders das Hackerkollektiv *zerforschung*[83] Schlagzeilen[84] und bietet mit einem humorvollen Tutorial Einblicke in ihr Vorgehen.[85] Dieser zeigt anschaulich im Vergleich zur institutionalisierten Sicherheitsforschung: Nicht das systematische Vorgehen beim Aufspüren einer Sicherheitslücke unterscheidet sich wesentlich bei ethischen Hacker:innen, sondern vielmehr nur der Kontext – Freizeitaktivität einerseits

[77] *Kennedy*, in: 451 Research, Black & White Paper, Exploring Coordinated Disclosure, S. 4, 11. Die Studie differenziert allerdings nicht nach Sicherheitsforschenden im engeren Sinne und ethischen Hacker:innen, sondern benennt diese als „thrid party security researcher". Zudem mussten die Befragten bereits mit den Modellen zur Offenlegung von Schwachstellen durchschnittlich bis gut vertraut sein, um teilnehmen zu können.

[78] *Kennedy*, in: 451 Research, Black & White Paper, Exploring Coordinated Disclosure, commissioned by Veracode, 2019, S. 8.

[79] *Kennedy*, in: 451 Research, Black & White Paper, Exploring Coordinated Disclosure, S. 9. Insgesamt zeigten sich 62% der Befragten aufgeschlossen.

[80] Vermittlungsplattform zwischen (freischaffenden) IT-Sicherheitsforscher:innen bzw. ethischen Hacker:innen und produktverantwortlichen Unternehmen für Sicherheits-Analysedientsleistungen (insbesondere zum Auffinden von Sicherheitslücken).

[81] *Bugcrowd*, Inside the Mind of a Hacker 2021, abrufbar unter: https://www.bugcrowd.com/resources/report/inside-the-mind-of-a-hacker/.

[82] *hackerone*, Hacker-Powered Security Report, Industry Insights 2021, abrufbar über https://www.hackerone.com/resources/reporting/hacker-powered-security-report-industry-insights-21?ungated=.

[83] https://zerforschung.org/.

[84] Siehe bspw. *Kruse*, „Gravierende Sicherheitslücke bei Corona-Testzentren" in: Süddeutsche Zeitung, 22.06.2021, abrufbar unter: https://www.sueddeutsche.de/politik/datenschutz-testzentren-1.5330068.

[85] *Zerforschung*, „Deine Software, die Sicherheitslücke und ich", abrufbar unter: https://zerforschung.org/posts/rc3-2021/.

und berufliche (Auftrags-)Arbeit andererseits. Im Englischen werden ethische Hacker:innen oftmals ebenfalls unter den Begriff der „security researcher" gefasst.[86]

a) Definition der „Hacker:in"

Der Begriff des Hackens ist im allgemeinen Sprachgebrauch mittlerweile eher negativ konnotiert und wird regelmäßig für Kriminelle verwendet, die illegal in IT-Systeme eindringen.[87] Hacken kann aber auch viel allgemeiner für den Weg der Entwicklung einer kreativen Lösung für ein ungewöhnliches Problem genutzt werden (vgl. auch den Begriff „Life-Hacks").[88] So war der Begriff in seinen Ursprüngen zu den Anfängen des Internets noch neutral bis positiv belegt und wurde für Bastler:innen, Tüftler:innen oder Computerspezialist:innen verwendet, bis sich die Gleichsetzung mit illegalen IT-Angriffen im allgemeinen Sprachgebrauch wie auch in der juristischen Betrachtung durchsetzte.[89] Hervorgehoben wird die spielerische Ausrichtung in der „Hacker-Szene" sowie der Wunsch herausragende Fähigkeiten zu demonstrieren.[90] „Hacking" kann somit definiert werden als „users' unconventional, playful mastery and unique, outsider expertise".[91] Bezogen auf die IT-Sicherheit lässt sich ein „hack" als etwas beschreiben, das die Regeln eines Systems zulässt, das aber von seinen Entwickler:innen nicht vorhergesehen und nicht gewollt war.[92]

Für eine Differenzierung etablierten sich sodann die Begriffe „Black Hat", „Grey Hat" und „White Hat". White Hat Hacker studieren die Technologien, Methoden und

---

[86] Vgl. *Bugcrowd*, Inside the Mind of a Hacker 2021, S. 5; *Woszczynski/Green/Dodson/Easton*, Government Information Quarterly 37(1) 2020, 101418 – https://doi.org/10.1016/j.giq.2019.101418; *Eichensehr*, Public-private cybersecurity, Texas Law Review, 95(3) 2017, 467 (486).

[87] *Ernst*, NJW 2003, 3233 (3233); vgl. auch *Denker*, in: Alberts/Oldenziel (Hrsg.), Hacking Europe. From Computer Cultures to Demoscenes, History of Computing, S. 168; Barber, Computer Fraud & Security 2001, 14 (14).

[88] Zur Historie: Alberts/Odenziel, in: Alberts/Oldenziel (Hrsg.), Hacking Europe. From Computer Cultures to Demoscenes, History of Computing, S. 2; Erdogan, Avantgarde der Computernutzung: Hackerkulturen der Bundesrepublik und DDR, S. 27 ff. Siehe bspw.auch: *Kargl*, „Hacker" – Vortrag CCC-Ulm 2003, abrufbar unter: http://web.archive.org/web/20130116013524/http://ulm.ccc.de/old/chaos-seminar/hacker/hacker.pdf zum Selbstverständnis und Anfängen des CCC.

[89] *Ernst*, NJW 2003, 3233 (3233); *Alberts/Odenziel*, in: Alberts/Oldenziel (Hrsg.), Hacking Europe. From Computer Cultures to Demoscenes, History of Computing, S. 2; *Erdogan*, Avantgarde der Computernutzung: Hackerkulturen der Bundesrepublik und DDR, S. 27 ff. Im englischsprachigen Raum wurden Kriminelle dagegen als „Cracker" bezeichnet, siehe hierzu *Gleb*, „Computerkids als mimetische Unternehmer: die Cracker-Szene zwischen Subkultur und Ökonomie (1985-1995)", WerkstattGeschichte 2016, (74):49-66.

[90] *Alberts/Odenziel*, in: Alberts/Oldenziel (Hrsg.), Hacking Europe. From Computer Cultures to Demoscenes, History of Computing, S. 2 f.; *Barber*, Computer Fraud & Security 2001, 14 (15).

[91] *Alberts/Odenziel*, in: Alberts/Oldenziel (Hrsg.), Hacking Europe. From Computer Cultures to Demoscenes, History of Computing, S. 3.

[92] *Anderson*, Security Engineering, S. 15.

Praktiken des Hackens und setzen die so gewonnenen Fähigkeiten ein, um Sicherheitslücken zu identifizieren und zu melden, damit diese geschlossen werden können.[93] Aufgrund ihrer Stellung außerhalb der für das untersuchte Produkt oder System zuständigen Organisation und Tätigwerden oftmals ohne explizite Beauftragung setzen sie sich allerdings einem Strafbarkeitsrisiko aus und agieren in rechtlicher Grauzone.[94] Dabei kann diese Form des Hackens auch als „wichtiger Baustein einer funktionierenden IT-Sicherheitslandschaft" bezeichnet werden.[95] Anstelle des stereotypen Bildes eines „Hackers", handelt es sich laut Studien bei ethischen Hacker:innen zumeist um hoch qualifizierte Expert:innen mit nachweisbaren sowie einschlägigen beruflichen Erfahrungen in verschiedenen Fachgebieten der Informationstechnologie.[96] Dagegen wird der Begriff des „Scriptkiddie" für solche Personen genutzt, die über keine tiefen Grundlagenkenntnisse verfügen.[97] Je ausgeprägter die Unerfahrenheit, desto eher steigen Befürchtungen unbeabsichtigter Schädigungen.[98]

Ethische Hacker:innen nutzen dabei oftmals Plattformen wie HackerOne, BugCrowd, Cobalt, etc., welche bspw. die Auszahlung bei Bug Bounty-Programmen verwalten und als Anlaufstelle bei Konflikten dienen.[99] Erste Zertifizierungen als ethische Hacker:innen werden für „legales Hacken" angeboten.[100] Abzugrenzen sind diese Plattformen und Initiativen von sog. Bug-Bounty-Plattformen, die Informationen über Sicherheitslücken ankaufen, ohne dass Transparenz darüber besteht, wie diese Informationen anschließend genutzt werden.[101] Diese richten ihr Angebot zwar auch an „Security Researchers" und „Ethical Hackers", sind aber wohl eher dem Bereich der Black und Grey Hats zuzuordnen.

---

[93] *Barber*, Computer Fraud & Security 2001, 14 (16).

[94] *Wagner*, DuD 2020, 111; *Klaas*, MMR 2022, 187 (188).

[95] *Klaas*, MMR 2022, 187 (187).

[96] *Bugcrowd*, Inside the Mind of a Hacker 2021, S. 5, 10 ff.; *Woszczynski/Green/Dodson/Easton*, Government Information Quarterly 37(1) 2020, 101418, siehe https://doi.org/10.1016/j.giq.2019.101418.

[97] *Barber*, Computer Fraud & Security 2001, 14 (15); *Sheenan/Dunckley*, Computer Viruses and Younger Users – who are the script kiddies?.

[98] *Barber*, Computer Fraud & Security 2001, 14 (15).

[99] *Laszka/Zhao/Malbari/Grossklags*, „The rules of engagement for bug bounty programs" In International Conference on Financial Cryptography and Data Security 2018, 138 (139).

[100] Siehe hierzu bspw. die Angebote des EC-Council unter: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/.

[101] Siehe bspw. die Plattform „Zerodium" für Zero-Day-Schwachstellen unter: https://zerodium.com/.

b) Ethische Grundsätze

Das zentrale Merkmal *ethischer* Hacker:innen ist die Notwendigkeit einen Ethikkodex zu befolgen.[102] Erste Grundsätze der Hackerethik finden sich in dem Werk von Steven Levy aus den 80er Jahren zurück.[103] In Deutschland hat der CCC diese übernommen und erweitert, weist aber auch darauf hin, dass sich die Hackerethik in ständiger Fortentwicklung befindet, die aufgestellten Regeln daher eher Diskussionsgrundlage und Orientierung bieten sollen:[104]

- unbegrenzter und vollständiger Zugang zu IT und Wissen, um zu lernen und Technologie weiterzuentwickeln;
- Freiheit der Information, Austausch von Ideen und Transparenz zur Stärkung der Kreativität;
- Misstrauen gegenüber Autoritäten – Förderung von Dezentralisierung;
- Beurteilung von Hacker:innen leistungsorientiert nach Taten / Fähigkeiten (nicht nach Äußerlichkeiten);
- IT-Nutzung für Kunst und Schönheit;
- Vertraulichkeit privater Daten und nicht-öffentlicher Daten Dritter;
- „Öffentliche Daten nützen, private Daten schützen".

Insofern haben sich international weitere Codes of Ethics herausgebildet.[105] Auch hier finden sich Elemente wieder, wie Vertraulichkeit, Schutz geistigen Eigentums, der sinnvolle Einsatz der eigenen Kompetenzen und Qualifikationen, Warnung und Risikominimierung, keine absichtlichen Gefährdungen Dritter, keine Vermarktung von Sicherheitslücken oder Teilnahme an betrügerischen Finanzpraktiken sowie das Aufzeigen von Interessenkonflikten.

Die Tätigkeit ethischer Hacker:innen dürfte von einem Bündel an Motiven getragen werden, wobei das Agieren zum Wohle der Allgemeinheit einen möglichen, aber nicht zwangsläufig den ausschlaggebenden Faktor ausmachen muss, wie die in Abbildung 1 gezeigte Erhebung einer Hackerplattform unter ihren Mitgliedern aus dem Jahr 2021 andeutet. Einer anderen Umfrage zufolge gab die Mehrheit an, nach einer Meldung vor allem Rückmeldungen zum Behebungsprozess zu erwarten. Danach hätten nur 18 % der unabhängigen Sicherheitsforscher:innen angegeben, dass sie eine Art von

---

[102] *Woszczynski/Green/Dodson/Easton*, Government Information Quarterly 37(1) 2020, 101418; Takanen/Vuorijärvi/Laakso/Röning, „Agents of responsibility in software vulnerability processes", Ethics and Information Technology, 6(2) 2004, 93.

[103] *Levy*, Hackers: Heroes of the Computer Revolution.

[104] Hackerethik – siehe https://www.ccc.de/de/hackerethics.

[105] Siehe bspw. die 19 Kriterien des EC-Councils, abrufbar unter: https://www.eccouncil.org/code-of-ethics/.

Bezahlung und nur 16 % eine ausdrückliche Anerkennung erwarten.[106] Eine nicht-repräsentative Erhebung der National Telecommunications and Information Administration (NTIA) unter ethischen Hacker:innen, Zufallsfinder:innen und Mitgliedern von Non-Profit sowie For-Profit Organisationen von 2016 ergab ebenfalls, dass eine überwiegende Mehrheit (95%) der Befragten eine aktive Kommunikation in der Form erwarteten, dass die Sicherheitsforscher:in benachrichtigt wird, wenn das Problem behoben ist.[107] Wurden diese Erwartungen enttäuscht, sahen viele die Offenlegung von Schwachstellen (auch Full Disclosure) als Abhilfe.[108] Eine knappe Mehrheit der Befragten (53 %) erwartete zudem als „Gegenleistung" für die Meldung einer Sicherheitslücke zumindest eine Anerkennung ihres Beitrags.[109]

[106] *Kennedy*, in: 451 Research, Black & White Paper, Exploring Coordinated Disclosure, S. 13.

[107] *National Telecommunications and Information Administration (NTIA)*, Vulnerability disclosure attitudes and actions: A research report, S. 5.

[108] *National Telecommunications and Information Administration (NTIA)*, Vulnerability disclosure attitudes and actions: A research report, S. 6.

[109] *National Telecommunications and Information Administration (NTIA)*, Vulnerability disclosure attitudes and actions: A research report, S. 7.

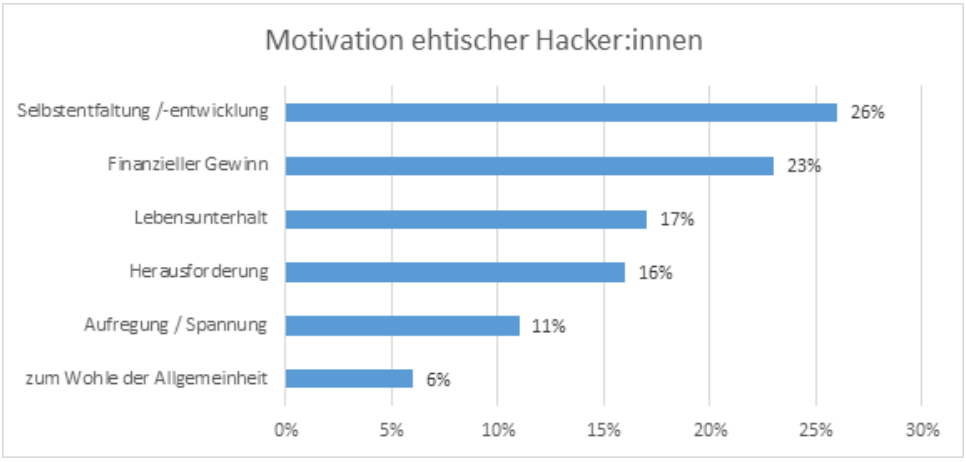

Abbildung 1: Ergebnis einer Befragung unter ethischen Hacker:innen der Bugcowd-Plattform[110]

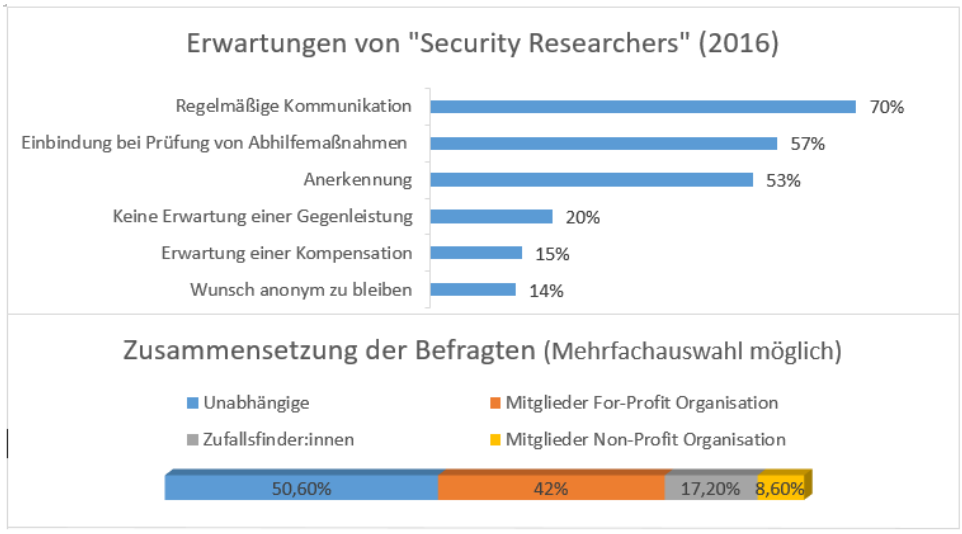

Abbildung 2: Ergebnis einer internationalen Befragung der National Telecommunications and Information Administration (NTIA)[111]

[110] *Bugcrowd*, Inside the Mind of a Hacker, S. 24.

[111] *National Telecommunications and Information Administration (NTIA)*, Vulnerability disclosure attitudes and actions: A research report.

3. IT-Sicherheitsanalysen im Rahmen der Aufgabenwahrnehmung des BSI

Um zweifelsfrei Strafbarkeitsrisiken bei Untersuchungen des/für das BSI auszuschließen, wurde § 7a BSIG geschaffen.[112] Erfasst sind alle Untersuchungsgegenstände, die für das BSI zur Erfüllung seiner Aufgaben herangezogen werden können. Dabei darf das BSI für die Untersuchung Dritte (bspw. Forschungseinrichtungen) beauftragen, wobei schutzwürdige Interessen der Hersteller:innen zu berücksichtigen sind. Im Rahmen des IT-SiG 2.0 wurde nochmals unterstrichen, dass das Responsible-Disclosure-Verfahren, d.h. die Einbindung der Hersteller vor der Veröffentlichung einer Sicherheitslücke, Anwendung findet.[113]

IV. Fazit

Die Bewertung der „IT-Sicherheit" ist eine Momentaufnahme nach dem jeweils aktuellen Stand der Technik, sodass in der Praxis regelmäßig nur kontinuierliche, dynamische Prozesse die Wahrung eines gewünschten Sicherheitsniveaus von Informationstechnologie ermöglichen. Mit der Vernetzung der IT-Landschaft steigt die Komplexität dieser Prozesse und die Gefahr des Auftretens von Sicherheitslücken. Solche Schwachstellen zu entdecken, wird somit immer bedeutsamer. Die Suche erfolgt dabei nicht nur durch Personen, die für Produkte und Systeme verantwortlich sind, sondern auch durch unabhängige, externe Akteure, zu denen Forscher:innen, ethische Hacker:innen und staatliche Stellen, wie das BSI, gezählt werden können. Der Begriff der „Sicherheitsforscher:in" (engl. „security researcher") ist dabei nicht klar definiert und sollte neben Wissenschaftler:innen an Hochschulen und Forschungseinrichtungen, ehrenamtlich in ihrer Freizeit Nachforschenden, Zufallsfinder:innen, auch Mitgliedern von gewerblichen und Non-Profit-Organisationen umfassen. Um die Interessenlage besser zu verstehen, wurden in diesem Kapitel die Hintergründe der IT-Sicherheitsforschung an Hochschulen und Forschungseinrichtungen sowie das Phänomen der ethischen Hacker:innen vorgestellt. Sofern diese auf Sicherheitslücken stoßen, hat sich international ein Prozess etabliert, um diese zu melden und so zur Behebung beizutragen: Coordinated Vulnerability Disclosure (CVD). „Coordinated" bzw. „Koordiniert" bezieht sich dabei auf die Kommunikation zwischen meldender Person und Empfänger:in der Meldung (in der Regel die Hersteller:in oder Betreiber:in/Nutzer:in eines

[112] BT-Drs. 18/4096, S. 25.
[113] BT-Drs. 19/28844, S. 40.

Produkts/Systems). Der Prozess ist darauf ausgelegt, das Risiko, welches von einer Sicherheitslücke ausgeht, bestmöglich zu minimieren. Allerdings zeigen sich in der Praxis zahlreiche praktische sowie rechtliche Probleme. Zahlreiche Empfehlungen als auch elementare Grundregeln für einen erfolgreichen CVD-Prozess wurden bereits erarbeitet, um die praktischen Herausforderungen zu adressieren. Den skizzierten rechtlichen Hürden und Rahmenbedingungen zum Umgang mit Sicherheitslücken sowie möglichen Lösungsansätzen widmet sich das folgende Kapitel.

Kapitel 2

Problemlagen und Lösungsansätze für einen verantwortungsbewussten Umgang mit Sicherheitslücken

Ein kooperatives Zusammenwirken von Produkt- bzw. Systemverantwortlichen und externen Sicherheitsexpert:innen, die als IT-Sicherheitsforschende oder ethische Hacker:innen ihre Fähigkeiten einsetzen um Sicherheitslücken aufzudecken, wird entscheidend durch Anreize als auch Hemmnisse im Rechtsrahmen geprägt. Wesentliche Weichenstellungen folgen hier aus der Grundrechtsperspektive, insbesondere dem Schutzauftrag zur Gewährleistung von IT-Sicherheit im Spannungsverhältnis zur öffentlichen Sicherheit und Grundrechtskonflikten im Dreiecksverhältnis zwischen Produktverantwortlichen, Produktnutzenden und IT-Sicherheitsforschenden. Anschließend soll nochmals ein vertiefter Blick auf das Strafrecht eingenommen werden, welches mit seiner Strafandrohung besonders in der Lage ist, abschreckende Wirkung zu entfalten. Auf der anderen Seite können Compliance-Anforderungen[1] Unternehmen direkt oder indirekt dazu anreizen, ein auf Zusammenwirken mit externen Sicherheitsforschenden und ethischen Hacker:innen basierendes IT-Schwachstellenmanagement aufzubauen.[2] Insofern werden aktuelle Reformen und Novellierungen vorgestellt, welche neue Impulse auch im Hinblick auf eine erfolgreiche Implementierung von CVD-Prozessen setzen könnten.

[1] Vgl. allgemein hierzu: *Schmidl/Tannen*, in: Kipker, Cybersecurity, Kap. 6.

[2] Unter IT-Schwachstellenmanagement werden vorliegend unternehmerische Prozesse zum Umgang mit Schwachstellen von der Entdeckung/Meldung, über die Aufklärung des technischen Hintergrunds, Ermittlung der Kritikalität, Bewertung/Priorisierung und Kommunikation/den Umgang mit den Beteiligten/Betroffenen/(Aufsichts-)Behörden bis zur Beseitigung/anderweitigen Mitigation und Dokumentation verstanden.

I. Schutzauftrag zur Gewährleistung von IT-Sicherheit im Spannungsverhältnis zur öffentlichen Sicherheit und privater Interessen

1. Rechtsprechung des Bundesverfassungsgerichts zum verantwortungsbewussten Umgang mit Sicherheitslücken durch staatliche Stellen

Mit der Entscheidung zum behördlichen Umgang mit Schwachstellen bestätigte das Bundesverfassungsgerichts (BVerfG) eine aus dem Grundrecht der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme folgende staatliche Schutzpflicht mit weitreichenden Konsequenzen.[3] Die wegen fehlender Darlegung der Beschwerdebefugnis und Einhaltung des Subsidiaritätsprinzips letztendlich abgewiesene Verfassungsbeschwerde[4] richtete sich gegen die Regelung im Polizeigesetz Baden-Württemberg zur Quellen-Telekommunikationsüberwachung (Quellen-TKÜ).[5] Die Beschwerdeführer monierten fehlende Regelungen zur Erstellung/Beschaffung und zum konkreten Einsatz von Software zum Mitschneiden und Exfiltrieren von Daten auf/von Systemen der Zielperson (umgangssprachlich als „Staatstrojaner" bezeichnet). Die grundrechtliche Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verlange zwar nicht die Quellen-TKÜ „durch Nutzung unerkannter Schwachstellen vollständig" zu unterlassen und auch nicht „jede unerkannte Sicherheitslücke sofort und unbedingt dem Hersteller zu melden".[6] Die grundrechtliche Schutzpflicht gebiete jedoch kontinuierliche Abwägungsentscheidungen zwischen dem Nutzen und den Risiken der Geheimhaltung der Sicherheitslücke. Schon wenn ersteres nicht überwiege, sei eine Meldung an den Hersteller abzugeben.[7]

Die Dynamik der IT-Landschaft mit häufigen Veränderungen durch etwa neue Hard-/Software, Updates/Patches, Modifikation der Netzwerktopologie oder an der Konfiguration von Systemen führt zu sehr unterschiedlichen Lebenszeiten von Schwachstellen und Exploits. Die besonders langlebigen Schwachstellen sind aber eine latente Bedrohung für Hersteller:innen, Betreiber:innen und Nutzer:innen der vulnerablen Hard- und Software. Diese wissen nichts von dem Risiko und können ohne forensische Anhaltspunkte eine Ausnutzung nur schwerlich detektieren. Es gibt keine

---

[3] BVerfG BeckRS 2021, 19234 (Rn. 27, 32 ff.).

[4] Zur kontextualen Einbettung vgl. *Büring*, c't 18/2021, 172.

[5] § 23b Abs. 2 PolG BW in der Fassung des Gesetzes zur Änderung des Polizeigesetzes vom 28.11.2017 (GBl. S. 6124). Danach geändert mit der Neuverkündung des PolG BW vom 06.10.2020 (GBl. 2020, 735, ber. S. 1092). Die Regelung findet sich jetzt in § 54 Abs. 2 PolG BW.

[6] BVerfG BeckRS 2021, 19234 (Rn. 43). Besprechung bei *Dickmann/Vettermann*, MMR 2022, 740 ff.

[7] BVerfG BeckRS 2021, 19234 (Rn. 44).

sichere Möglichkeit der Feststellung, dass Sicherheitslücken nicht ausgenutzt werden.[8] Angriffe auch auf Nachrichtendienste mit Abfluss von Exploits und Angriffssoftware wurden schon mehrfach bekannt.[9] Wenn die Entwendung, ein Reverse Engineering oder eine Parallel-/Wiederentdeckung aber von den Sicherheitsbehörden nicht bemerkt oder diese trotz Kenntnis mit Blick auf den weiterhin bestehenden Nutzen geheim gehalten werden, besteht die Bedrohung schlimmstenfalls unbegrenzt fort. Bedienen sich Sicherheitsbehörden (offensiver) Angriffsmethoden, um Sicherheitslücken aufrecht zu erhalten, bringt dies einen nicht unerheblichen Grad an IT-Unsicherheit mit sich. Diese betrifft etwa bei Standardsoftware auch die Sicherheitsbehörden und staatliche Stellen als IT-Betreiber/Nutzer:innen.[10] Wenn man nun diesen Hoheitsträgern eine Abwägungsentscheidung zwischen dem Schließen und Geheimhalten von Schwachstellen abverlangt, sind nicht ausräumbare Interessen- und Zielkonflikte augenscheinlich.[11] Zudem zu beachten sind die durch die Geheimhaltung verletzten staatlichen Schutzpflichten insbesondere gegenüber den Bürger:innen und Unternehmen sowie die internationale Dimension. Der Versuch, in den USA einen entsprechenden Abwägungs- und Kontrollprozess diensteübergreifend zu etablieren, wird als gescheitert bezeichnet.[12]

Der „verantwortungsvolle Umgang mit Schwachstellen" durch „zügiges Schließen erkannter Sicherheitslücken" wurde in Deutschland zum Strategieziel erhoben.[13] Einen „allgemein gültigen Rahmen, der beschreibt, welche Akteure in welchem Umfang und

[8] *Derin/Golla*, NJW 2019, 1111 (1115).

[9] Zum bekanntesten Fall „Shadow Brokers" *Buchanan*, The Hacker and the State, S. 242 ff.; *Perlroth*, This is how they tell me the world ends, S. 320 ff.

[10] Zu den Wechselwirkungen *Pohlmann/Riedel*, DuD 2018, 37 (40 ff.).

[11] Zum Lying-Endpoint-Problem *Pohlmann/Riedel*, DuD 2018, 37 (43 f.).

[12] Zum Scheitern des Vulnerabilities Equities Process (VEP) *Perlroth*, This is how they tell me the world ends, S. 304 ff., 360. Das VEP-Dokument kann unter https://www.eff.org und ein Update per Blogpost von Joyce vom 15.11.2017 unter https://trumpwhitehouse.archives.gov abgerufen werden. Aus Sicht der Obama-Administration *Schwartz/Knake*, Governments's Role in Vulnerability Disclosure, Juni 2016, abrufbar unter https://www.belfercenter.org; aus europäischer Sicht *CEPS Task Force*, Software Vulnerability Disclosure in Europe, S. 61 ff. abrufbar unter https://www.ceps.eu; zu einem am VEP orientierten Vorschlag zu einem Kernprozess auf Behördenseite *Herpig*, Governmental Vulnerability Assessment and Management, August 2018, abrufbar unter https://www.stiftung-nv.de. Leider ist er nicht ganzheitlich (vgl. S. 11) und die grundrechtliche Dimension bleibt unterbelichtet.

[13] Vgl. Cybersicherheitsstrategie 2021 der Bundesregierung, S. 46 f. – abrufbar unter https://www.bmi.bund.de.

mit welchen Methoden und Instrumenten Sicherheitslücken finden und den Herstellern melden dürfen", gebe es nicht.[14] (Zwischen-)Ergebnisse wurden bislang nicht veröffentlicht oder gar in Gesetzesform gegossen. Daher muss davon ausgegangen werden, dass bislang keine entsprechenden Prozesse implementiert worden sind.

Das BVerfG stellt nun fest, dass mit der Kenntnis staatlicher Stellen von einer Sicherheitslücke ein staatlicher Schutzauftrag entsteht.[15] Dieser münde jedoch nicht in einem grundrechtlich fundierten Verbot der Quellen-TKÜ unter Ausnutzung von Sicherheitslücken.[16] Vielmehr komme es zu einem Zielkonflikt zwischen dem Schutz vor Infiltration durch Dritte einerseits und der Ermöglichung einer Quellen-TKÜ mittels unbekannter Sicherheitslücken zum Zwecke der Gefahrenabwehr andererseits.[17] Dieser ist durch eine Abwägung aufzulösen, die der Gesetzgeber verpflichtend durch die Regelung des Umgangs von (Polizei-)Behörden mit Sicherheitslücken, die den Herstellern nicht bekannt sind, vorbereiten müsse.[18] Dabei sei von dem Grundsatz auszugehen, dass bislang unveröffentlichte Sicherheitslücken den Herstellern von der Behörde zu melden seien.[19] Die Ermächtigung zur Quellen-TKÜ erlaube zwar hiervon abzuweichen, aber nur nach entsprechender Abwägung, wobei im Zweifel das Interesse an der Erfüllung der Schutzpflicht durch Meldung an die Hersteller überwiege. Die Aufstellung und normative Umsetzung eines entsprechenden Schutzkonzepts sei Sache des Gesetzgebers.[20]

Wesentliche Detailfragen sind dabei offengeblieben, wie konkret ein „verantwortungsbewusster" Umgang geregelt werden müsste, u.a. zu folgenden Fragestellungen, welche wiederum zahlreiche Folgefragen aufwerfen, die hier nicht im Detail betrachtet werden sollen:

- Will der Gesetzgeber grundsätzlich die Geheimhaltung von Informationen zu Schwachstellen verbieten oder erlauben?
- Bei Erlaubnis: Wie wird entsprechendes Know-How bei den Entscheidungsträger:innen sichergestellt, um den potenziellen Nutzen, aber auch die Gefährlichkeit einer Schwachstelle technisch einschätzen zu können?

[14] Vgl. Cybersicherheitsstrategie 2021 der Bundesregierung, S. 46 – abrufbar unter https://www.bmi.bund.de.

[15] BVerfG BeckRS 2021 19234 (Rn. 34).

[16] BVerfG BeckRS 2021 19234 (Rn. 43); hierzu kritisch *Derin/Golla,* NJW 2019, 1111 (1114).

[17] BVerfG BeckRS 2021 19234 (Rn. 34).

[18] BVerfG BeckRS 2021 19234 (Rn. 41).

[19] BVerfG BeckRS 2021 19234 (Rn. 42); vgl in diese Richtung auch die Cybersicherheitsstrategie 2021 der Bundesregierung, S. 46, abrufbar unter https://www.bmi.bund.de.

[20] BVerfG BeckRS 2021 19234 (Rn. 49).

- Nach welchen Kriterien und Referenzen werden dabei Schwachstellen etwa mit Blick auf ihre Ausnutzbarkeit, ihre Kritikalität, ihre Verbreitung und die Möglichkeiten zu ihrer Beseitigung evaluiert?
- Wie wird sichergestellt, dass bei Entscheidungen potenziell betroffene Gruppen (IT-Nutzer:innen insbesondere kritische Infrastrukturen und von besonders schadensrelevanten Anwendungen etc.) ausreichend beachtet werden? Welche Prozess, Kontroll- /Prüfmechanismen wirken Fehlentscheidungen entgegen? Wie wird Kontrolle durch Rechts- und Fachaufsicht sichergestellt? In welchen zeitlichen Abständen müssen Re-Evaluationen durchgeführt werden?
- Welche Quellen dürfen für die Beschaffung von Schwachstellen genutzt werden? Ist wirksamer Grundrechtsschutz beim Zusammenwirken mit (privaten) Dienstleistern noch ausreichend möglich?
- Wie wird die Geheimhaltung sichergestellt? Mit welchen Akteuren (national/EU/international) dürfen Informationen geteilt werden?
- Wie werden Zielkonflikte gelöst, wenn Behörden auf Bundes- bzw. Landesebene zur Gefahrenabwehr im Rahmen ihrer gesetzlich definierten Aufgaben sowohl aus Geheimschutzgründen zum Zurückhalten von Erkenntnissen zu Sicherheitslücken als auch zum Offenlegen mit dem Ziel schnellstmöglicher Schließung der Lücke angehalten werden können.

Als Fazit kann festgehalten werden: Aktuell bestehen weder Regelungen, die die angerissenen Fragestellungen in ausreichender Tiefe materiell-rechtlich beantworten, noch gewährleisten ein klarer Zuschnitt von Zuständigkeiten und Aufgaben von IT-Sicherheitsbehörden als Meldestellen für Sicherheitslücken auf Bundes- oder Landesebene derzeit prozessual, dass Entscheidungen über den Umgang mit Sicherheitslücken stets unter Vermeidung bzw. nach Ausräumen von Interessen- und Zielkonflikten, transparent und nachprüfbar erfolgen.[21]

2. Grundrechtskonflikte bei der verantwortungsbewussten Offenlegung von Schwachstellen durch Sicherheitsforschende

Bei der durch unabhängige Sicherheitsforschende erfolgenden Suche, dem Finden und Melden von Sicherheitslücken durch unabhängige Sicherheitsforschende in IT-techni-

[21] Ausführlich: *Dickmann/Vettermann*, MMR 2022, 740 ff.; vgl. auch *Herpig/Rupp*, Deutschlands staatliche Cybersicherheitsarchitektur, dort insbesondere das Poster auf Seite 15. Zum Normendschungel siehe *bitkom*, Regulierungsmapping IT-Sicherheit, Stand Juli 2020, abrufbar unter https://www.bitkom.org.

schen Produkten und Systemen besteht regelmäßig eine Dreieckskonstellation grundrechtlich geschützter Positionen tangiert, welche im Rahmen einer gesetzlichen Regelung austariert werden müssten. Hierbei können sowohl gegensätzliche als auch überlappende Interessen festgestellt werden (vgl. Abb. 3).

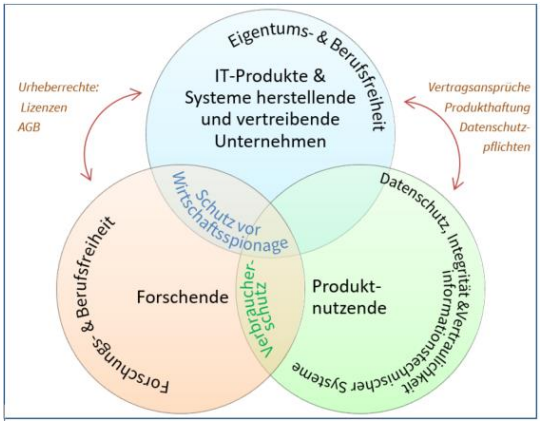

Abbildung 3: Interessen- und Grundrechtskollisionen

a) Perspektive der Produkt-/Systemnutzenden

Auf der Seite der Nutzer:innen greift das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG, ggf. bei juristischen Personen nur Art. 2 Abs. 1 i.V.m. Art. 19 Abs. 3 GG[22]) einerseits im Hinblick auf die Gefahr, welche von IT-Sicherheitslücken ausgeht, und andererseits gegenüber Zugriffen durch Forschende. Beeinträchtigungen durch die Forschung werden aber mangels ausreichender staatsähnlicher Handlungsweise durch einfache Gesetze und grundrechtliche „Einfallstore" geregelt (z.B. §§ 823 Abs. 1, 1004 BGB). Daneben besteht das Bedürfnis auf Schutz der Unternehmensdaten und Geschäftsgeheimnisse (wahlweise aus Art. 12 Abs. 1, 14 Abs. 1 GG oder zumindest Art. 2 Abs. 1 i.V.m. Art. 19 Abs. 3 GG)[23] sowie Schutz personenbezogener Daten der Produktnutzenden (Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG bzw. Art. 7, 8 EU-GrCh) bei etwaigem Zugriff auf existente Systeme. Die Forschung könnte kurzzeitig die Interessen von Privatpersonen tangieren, insbesondere wenn Zugriffe auf personenbezogene Daten

[22] Hierzu *Vettermann*, Der grundrechtliche Schutz der digitalen Identität, S. 260 ff – abrufbar unter https://doi.org/10.5445/KSP/1000148103.

[23] Vgl. *Vettermann*, Der grundrechtliche Schutz der digitalen Identität, S. 220 ff. – abrufbar unter https://doi.org/10.5445/KSP/1000148103.

beim Untersuchen von Sicherheitslücken ermöglicht werden.[24] Insgesamt könnte sie aber zu einem höheren Verbraucherschutzniveau beitragen, wenn IT-Produkte und Systeme durch Forschungserkenntnisse sicherer bzw. gegen Angriffe robuster werden.

b) Perspektive der Produkt-/Systemverantwortlichen

Das Interesse der Urheber:innen an der ungehinderten wirtschaftlichen Verwertung ihrer kreativen Schöpfungsleistung und der Schutz ihres Urheberpersönlichkeitsrechts sind ebenfalls grundrechtlich geschützt (Art. 12 Abs. 1, 14 Abs. 1, 2 Abs. 1 GG)[25]. Zudem stehen auch hier Zugriffsmöglichkeiten auf Unternehmensdaten und Geschäftsgeheimnisse im Raum, welche die Eigentums- und Berufsfreiheit tangieren könnten.

Überlappende Interessen der Erforschung von Sicherheitslücken sind ggü. Sicherheitslücken verantwortenden Unternehmen gegeben, wenn diese durch deren Schließung vor Wirtschaftsspionage oder Sanktionsdrohungen[26] und Haftungsrisiken geschützt werden.

c) Perspektive der Forschung

Die Forschung tritt in der betrachteten Dreieckskonstellation jedoch in zweierlei Form auf: Zum einen zeigt sich die Forschung in ihrer institutionellen Form an Universitäten und öffentlich-rechtlichen Forschungseinrichtungen, die einem bestimmten Forschungsauftrag folgen. Zum anderen besteht die Möglichkeit der privaten Forschung, entweder in privatrechtlichen Unternehmen (z.B. zur Verbesserung der eigenen Produkte oder zur Erhöhung des IT-Sicherheitsniveaus im Umfeld um die eigene Wertschöpfung) oder aus reiner Neugier der Privatperson oder von Kollektiven (z.B. Aktivist:innen). Im Hinblick auf die Forschung ergeben sich aber im Rahmen der Forschungs- und Wissenschaftsfreiheit des Art. 5 Abs. 3 GG keine Unterschiede; als Jedermann-Grundrecht schützt es sowohl Lehrpersonen von Universitäten[27] wie auch jede Person, die außeruniversitär wissenschaftlich tätig ist[28].

Da in beiden Fällen jede Tätigkeit geschützt ist, die „nach Inhalt und Form als ernsthafter planmäßiger Versuch zur Ermittlung der Wahrheit“[29] anzusehen ist, kommt es in beiden Fällen zu der erwähnten Grundrechtskollision in Form von Zugriffen auf

[24] Siehe hierzu Whitepaper zur Rechtslage der IT-Sicherheitsforschung 2021, S. 17 ff.

[25] Zum Trias ausführlich *Vettermann*, Der grundrechtliche Schutz der digitalen Identität, S. 220 ff. – abrufbar unter https://doi.org/10.5445/KSP/1000148103.

[26] Z.B. aufgrund von Datenschutzverstößen, vgl. Art. 83 DSGVO.

[27] BVerfGE 35, 79.

[28] *Kempen* in: Epping/Hillgruber, BeckOK Grundgesetz, Art. 5 Rn. 184 aE.

[29] BVerfGE 35, 79.

Hard- und Software in der Form, dass in nicht für die Öffentlichkeit vorgesehene Bereiche vorgedrungen wird. Dementsprechend können bestehende Regelungen im Licht der Forschungsfreiheit des Art. 5 Abs. 3 GG verstanden werden, jedoch in den Grenzen der kollidierenden Grundrechte.

3. Zwischenfazit

Die grundrechtliche Konfliktlage zeigt sich also sowohl im Verhältnis IT-Sicherheitsforschende – Staat sowie zwischen den (privatrechtlichen) Akteuren im Umgang mit den IT-Sicherheitslücken selbst. In erster Hinsicht hat das BVerfG einen groben Rechtsrahmen gesteckt, indem es in die grundrechtliche Gefährdungslage bei gefundenen IT-Sicherheitslücken im Zweifel eine staatliche Meldepflicht annimmt. Nutzenden von betroffenen Produkten ist es insoweit nicht zumutbar, dass die eigenen Produkte durch staatliche Kenntnis einer Sicherheitslücke unsicher bleiben. Eine Nutzung für staatliche Zwecke kann im Übrigen erst dann möglich sein, wenn ein entsprechendes Konzept im Umgang mit IT-Sicherheitslücken gesetzlich verankert ist. Diese gesetzliche Verankerung käme theoretisch auch den Sicherheitsforschenden in der aufgezeigten Dreieckskonstellation zugute, schon um der Rechtssicherheit Willen. Grundrechtlich gegenläufige Positionen können so durch die Gesetzgebung austariert werden. Dies adressiert auch das erwähnte Vorhaben im Koalitionsvertrag. Die Notwendigkeit, konfligierende grundrechtliche Interessen in Einklang zu bringen, ergibt sich aber schon aus den jeweiligen Positionen und in Rekurs auf die Rechtsprechung des BVerfG. Eine zentrale Melde- und Koordinierungsstelle sowie ein klarer Rechtsrahmen wären ein erster Anfang. Bis dahin müssen die grundrechtlichen Positionen in Generalklauseln und Einzelfallabwägungen einbezogen werden, bspw. ob die Forschungstätigkeit „sozial adäquat“ ist.

II. Das Strafrecht als Hemmnis für proaktive, unabhängige Sicherheitsüberprüfungen

Das Thema proaktiver Sicherheitstests ist mittlerweile auf der politischen Ebene angekommen. Nachdem bei der verfassungsrechtlichen Bewertung des sog. „Hackerparagraphen“[30] und im Rahmen der Novelle des Computerstrafrechts 2007[31] im Hinblick

[30] So war die Strafbarkeit des Verfassungsbeschwerde führenden Pentesters bereits ausgeschlossen, da dieser dank Beauftragung nicht die Absicht verfolgte, eine Computerstraftat zu begehen: BVerfGK 15, 491.

[31] Vgl. die Formulierung in BT-Drs. 16/3656, S. 19.

auf erlaubtes „Hacken“ noch das Bild der Beauftragung des:der „Hacker:in“ (bspw. als Pentester) im Vordergrund der juristischen Betrachtung stand, scheinen die Koalitionsparteien Handlungsbedarf für nicht-beauftragte Sicherheitsanalysen erkannt zu haben.[32] Mit Fokus auf die Rechtslage im Strafrecht soll dieser Abschnitt beleuchten, welche rechtlichen Risiken unter dem aktuellen Rechtsrahmen bestehen und wie das Anliegen des Koalitionsvertrags, das Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren, z. B. in der IT-Sicherheitsforschung, legal durchführbar zu gestalten, umgesetzt werden könnte.

1. Aktueller Rechtsrahmen – Strafrechtliche Risiken und Abschreckungseffekte[33]

Um Sicherheitslücken aufzudecken, muss sich die angewandte IT-Sicherheitsforschung trotz völlig anderer Zielsetzung oftmals der gleichen Methoden und technischen Vorgehensweisen bedienen wie Cyberkriminelle.[34] Daraus resultieren Strafbarkeitsrisiken.

Beispiel: Ein:e Hersteller:in hinterlegt in einem Produkt ein Passwort, das explizit nicht zum Auslesen und zur Verwendung durch Nutzer:innen 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 in IT-Systemen und IT-Netzwerken Sicherheitslücken aufzuspüren, besteht insbesondere die Sorge, dass sie sich nach § 202a Abs. 1 StGB (Ausspähen von Daten) strafbar machen können. Dieser Tatbestand ist erfüllt, wenn die Handelnde unter Überwindung einer Zugangssicherung Zugang zu Daten, die nicht für ihn bestimmt sind, erlangt. Das ist etwa in dem beschriebenen Beispiel der Fall.

Der Wortlaut der Vorschrift differenziert nicht zwischen kriminellen und anderen Zielrichtungen der Handlung. Unbeschadet früherer Erwägungen, „einfaches Hacking“ nicht unter Strafe zu stellen,[35] besteht inzwischen ein erhebliches Risiko, dass

---

[32] Bundesregierung, Koalitionsvertrag 2021-2025, S. 13.

[33] Wir greifen nachfolgend in erheblichem Umfang und in teils wörtlicher Übernahme (vgl. VVdStRL 72 [2012], 701 [707 Nr. 48]) auf das Whitepaper zur Rechtslage der IT-Sicherheitsforschung 2021, insb. S. 9 ff., zurück.

[34] 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.

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

aus Sicht der Strafverfolgungsbehörden und Gerichte Forschende den Tatbestand erfüllen, wenn sie IT-Sicherheitsforschung betreiben. Die Überwindung einer Zugangssicherung ist – vor allem in der weiten Interpretation, den dieses Tatbestandsmerkmal in der Rechtsprechung gefunden hat[36] – 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.

Um eine Strafbarkeit nach § 202a Abs. 1 StGB sicher auszuschließen, müssen Forschende das Einverständnis sämtlicher Berechtigter an den getesteten IT-Systemen erlangen.[37] Dies kann praktisch schwierig sein und ist vom Willen der Hersteller:innen abhängig, die häufig kein Interesse daran haben, dass Schwachstellen an ihren Produkten gefunden oder publik gemacht werden. Auf anderen Wegen 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. So wies das Bundesverfassungsgericht kürzlich zu § 202d Abs. 1 StGB darauf hin, dass die subjektiven Voraussetzungen nicht vorschnell unterstellt werden dürfen: „Die Schädigung beziehungsweise der Vorteil müssen vom Täter als Erfolg gewollt werden, es muss ihm gerade darauf ankommen. Steht die Aufklärung von Missständen im Vordergrund, richtet sich die Absicht des Täters hierauf, nicht aber auf die Schädigung." Daher wird zwar im Regelfall keine Bereicherungs- oder Schädigungsabsicht, aber auch kein Handeln aus Eigennutz[38] vorliegen – so etwa in dem oben beschriebenen Beispiel. Jedoch lässt sich diese subjektive Tatseite vor allem in frühen Stadien straf-

[36] 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.

[37] Vgl. auch RL (EU) 2013/40 EG 17.

[38] Ein wissenschaftliches Interesse ist hiervon nicht erfasst.

rechtlicher 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.[39]

Für IT-Sicherheitsforschende ist es zudem unverzichtbar, sich über aktuelle Angriffsmethoden zu informieren, Schadsoftware zu analysieren und Evidenzen für die Ausnutzbarkeit von Sicherheitslücken (sogenannte „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",[40] auch i.V.m. §§ 303a Abs. 3, 303b Abs. 5 StGB sowie § 263a Abs. 3 StGB. Zwar hat hierzu das Bundesverfassungsgericht schon früh die restriktive Auslegung des Tatbestands betont, was die Strafbarkeit von Forschenden weitgehend ausschließen dürfte,[41] 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.

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.[42] Wenngleich es praktisch unwahrscheinlich ist, dass in naher Zukunft IT-Sicherheitsforschende nach § 202a Abs. 1 StGB oder § 202c StGB verurteilt werden,[43] sind die durch eine mögliche Strafbarkeit und Ermittlungsverfahren drohenden Abschreckungseffekte ernst zu nehmen. Staatsanwaltschaften

[39] Vgl. BGHSt 58, 268 (Rn. 49 ff.) zum gleichlautenden Merkmal bei § 44 Abs. 1 BDSG a.F.

[40] Vgl. statt vieler *Brodowski*, in: Kipker, Cybersecurity, Kap. 13 Rn. 42, 48.

[41] BVerfGK 15, 491.

[42] Hierzu *Brodowski*, it – Information Technology 57 (2015), 357.

[43] 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.

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*verfolgung*srisiken zu minimieren, sollten die Tatbestände des IT- und Datenschutzstrafrechts die Interessen der IT-Sicherheitsforschung ausdrücklich berücksichtigen; dies ist ein wesentlicher Baustein für einen rechtssicheren Rahmen für die IT-Sicherheitsforschung, wie ihn der Koalitionsvertrag fordert:

Koalitionsvertrag 2021–2025[44], Zeilen 445–446: „Das Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren, z. B. in der IT-Sicherheitsforschung, soll legal durchführbar sein".

Bezogen auf das Strafrecht wäre dies etwa durch die Einfügung eines Tatbestandsausschlusses für Handlungen im 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. Die Kooperation mit einer Meldestelle ist hingegen kein hinreichender Anknüpfungspunkt für eine Straffreistellung, da diese zeitlich erst nach Auffinden einer IT-Sicherheitslücke und daher im Nachgang zu demjenigen Verhalten erfolgt, das Anlass für strafrechtliche Ermittlungen geben kann. Allerdings muss durch Verwendungsregelungen sichergestellt werden, dass Meldungen an eine Meldestelle nicht zum Auslöser für strafrechtliche oder bußgeldrechtliche Ermittlungen *gegen* den Meldenden werden dürfen.

2. Grundsätzliche Erwägungen zu Reformoptionen in Deutschland

Um die Arbeit von Sicherheitsforschenden und das zivilgesellschaftliche Engagement ethischer Hacker:innen für eine praxisorientierte Verbesserung der IT-Sicherheit besser nutzbar zu machen und Abschreckungseffekte der aktuellen Rechtslage zu minimieren, sollte wie im Koalitionsvertrag angekündigt eine Gesetzesanpassung vorgenommen werden. Anstatt Meldende von Sicherheitslücken dem Risiko einer strafrechtlichen

[44] *Bundesregierung*, Koalitionsvertrag 2021-2025.

Verfolgung auszusetzen, können sowohl Staat als auch Wirtschaft davon profitieren, wenn sie mit IT-Sicherheitsforschenden und ethischen Hacker:innen zur Behebung der Schwachstelle und bei der Warnung von Betroffenen zusammenarbeiten.[45] Der regulatorische Rahmen sollte Anreize setzen, ein auf Kooperation basierendes Zusammenwirken zu fördern und gleichzeitig „rote Linien" klar und eindeutig definieren, welche Verhaltensweisen weiterhin mit Strafe bewehrt sein sollten.

a) Ergänzung der Tatbestände der §§ 202a ff., 303a f. StGB

Bereits im Jahr 2019 forderte ein Antrag der FDP-Fraktion, dass die Strafbarkeit der §§ 202a ff. StGB an die Intention der Handlung geknüpft wird, „(...) um sicherzustellen, dass Maßnahmen, die mit dem Ziel der Schließung von Sicherheitslücken oder zu Zwecken der Fort- und Weiterbildung erfolgen, nicht strafbar sind."[46] Eine vergleichbare Konstruktion eines Delikts mit „überschießender Innentendenz" findet sich im österreichischen Strafrecht in § 118a öStGB. Die erhebliche Kritik wegen verbleibender Strafbarkeitslücken sowie beweistechnischer Schwierigkeiten deutet allerdings eher auf ein Negativbeispiel, welches sich nicht als Modell für eine Reform eignet.[47] Die Argumente dürften sowohl für die Aufstellung weiterer Strafbarkeitsmerkmale im objektiven wie im subjektiven Tatbestand gelten: Zum einen sind die objektiven Handlungen bei der Überwindung einer Zugangssicherung einer redlich agierenden Sicherheitsforscher:in oftmals kaum von denen einer kriminellen Hacker:in zu unterscheiden.[48] Zum anderen lassen sich Verkettungen mehrerer Vorsatzarten wie die Kombination aus bedingtem Vorsatz und (Nachteilszufügungs- bzw. Kenntnisverschaffungs-)Absicht wie im österreichischen Modell in der Praxis nur schwer beweisen.[49]

b) Erweiterung der Sozialadäquanzklauseln als Tatbestandsausschluss für Sicherheitsforschung

Als weitere Möglichkeit böte sich an, sich an vergleichbaren Regelungen zu Forschungsausnahmen zu orientieren, die sich bereits im StGB befinden. Zu nennen sind

[45] *Woszczynski/Green/Dodson/Easton*, Government Information Quarterly 37(1) 2020, 101418, https://doi.org/10.1016/j.giq.2019.101418 m.w.N.

[46] BT-Drs. 19/7698, S. 8.

[47] *Zech/Wagner*, in: Golla/Brodowski (Hrsg.), IT-Sicherheit und Strafrecht 2022 – im Erscheinen mwN.

[48] Ethisch Handelnde unterliegen zwar oftmals (selbstgesteckten) Grenzen, der technische Beleg einer Schwachstelle kann aber (derzeit) mit einer strafrechtlichen Grenzüberschreitung einhergehen. Die Rücknahme einer „Vorfeldkriminalisierung" im Hinblick darauf, dass bereits die Zugriffsmöglichkeit und nicht erst ein Schadenseintritt als strafauslösend gilt, sollte Forschende und ethisch Handelnde, aber nicht kriminelle Hacker:innen privilegieren.

[49] *Schmölzer,* ZStW 123 (2011), 709 (727 f).

hier die Sozialadäquanzklauseln der §§ 86 Abs. 4, 86a Abs. 3, 91 Abs. 2 Nr. 1, 130a Abs. 3, 201a Abs. 4 StGB sowie § 184k Abs. 3 StGB, die nach herrschender Meinung als Tatbestandsausschluss gewertet werden.[50] Diese enthalten auch eine Privilegierung von Wissenschaft und Forschung. Allerdings bleiben auch diese Ansätze nicht ohne Kritik, da mit der schillernden Bedeutungsfülle des Etiketts „sozial adäquat" sowie der Formulierung „überwiegender berechtigter Interessen" die Umsetzung in der Praxis auf eine Einzelfallabwägung hinausläuft.[51] Mit Blick auf die in § 201a StGB erfasste Verletzung des höchstpersönlichen Lebensbereichs sind bereits Anhaltspunkte und Hilfestellungen für eine Rechtsgüterabwägung vorhanden: So kann man sich an der Rechtsprechung zu § 193 StGB oder § 23 KUG orientieren,[52] Gutachten zu Forschungsprojekten bei Ethik-Kommissionen einholen oder aufgrund des persönlichkeitsrechtlichen Einschlags auch Stellungnahmen zum Datenschutzrecht als eng verwandte Thematik heranziehen.[53] Dagegen fehlen sowohl ein ausdifferenziertes Fallrecht zu Kollisionen von Forschungsfreiheit mit Computerdelikten als auch institutionelle Hilfestellungen, insbesondere wenn es sich um kleinere Forschungseinrichtungen oder ethischer Hacker:innen handelt.[54] Zudem würde eine Regelung, die nur eindeutig wissenschaftlich begründete Funde privilegiert, im Hinblick auf ethisches Hacken und Zufallsfunde zu kurz greifen. In einigen Fällen werden Schwachstellenfunde zufällig gemacht.[55] Für diese Fälle sind Anforderungen unpraktikabel, welche die vorherige Einholung einer Erlaubnis oder Anhörung eines Gremiums vorgeben.[56]

Eine eigenständige Formulierung eines Tatbestandsausschlusses könnte nach dem Vorbild der USA auf „redliche" oder „in gutem Glauben" durchgeführte Sicherheitsuntersuchungen rekurrieren. In diesem Jahr wurde eine Strafverfolgungsbehörden bindende Auslegungsregelung des Department of Justice (DOJ) zum Computer Fraud and Abuse Act (CFAA) veröffentlicht,[57] wonach ein strafbarer „*Access without autho-*

[50] BGH Urteil v. 6.4.2000 – 1 StR 502/99, BGHSt 46, 36 (43f.) = NJW 2000, 2217 (2218).

[51] *Becker*, in: Matt/Renzikowski, StGB, § 86 Rn. 15; *Paeffgen*, in: NK-StGB, § 86 Rn. 38.

[52] *Eisele*, in: Schönke/Schröder, StGB, § 201a Rn. 53.

[53] *Zech/Wagner*, in: Golla/Brodowski (Hrsg.), IT-Sicherheit und Strafrecht 2022 – im Erscheinen.

[54] Zwar bildeten sich erste Ethikkommissionen auch für den Fachbereich Informatik, allerdings noch nicht flächendeckend. Siehe hierzu auch: *Krüger/Sorge/Vorgelsang,*IRIS 2018, 529 (535).

[55] *Weulen Kranenbarg/Holt/van der Ham*, Crime Science 2018 7:16 – https://doi.org/10.1186/s40163-018-0090-8; National Telecommunications and Information Administration (NTIA), Vulnerability disclosure attitudes and actions: A research report, 2016, S. 4 – abrufbar unter https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf.

[56] *Woszczynski/Green/Dodson/Easton*, Government Information Quarterly 37(1) 2020, 101418 – https://doi.org/10.1016/j.giq.2019.101418

[57] *United States Department of Justice*, Policy 1 9-48.000, Mai 2022 – abrufbar unter https://www.justice.gov/opa/press-release/file/1507126/download.

rization" nach 18 U.S.C. §§ 1030(a)(1), (a)(2), (a)(3), (a)(4), oder (a)(5)(B)-(C) nur vorliegt, wenn die Strafverfolgung auch den Zielen des Ministeriums zur Durchsetzung des CFAA dient.[58] Diese Ziele sind die Förderung des Datenschutzes und der Cybersicherheit durch die Wahrung des Rechts von Einzelpersonen, Netzwerkbetreiber:innen und anderen Personen, die Vertraulichkeit, Integrität und Verfügbarkeit der in ihren Informationssystemen gespeicherten Informationen zu gewährleisten. Zeigen verfügbare Beweise, dass es sich um gutgläubige Sicherheitsforschung („*good-faith security research*") i.S.d. der vom Register of Copyrights empfohlenen Definition[59] handelt, soll die Staatsanwaltschaft von Strafverfolgung absehen. „Gutgläubige Sicherheitsforschung" bedeutet danach, dass der Zugriff auf einen Computer ausschließlich zu Zwecken des gutgläubigen Testens, der Untersuchung und/oder der Behebung eines Sicherheitsmangels bzw. Schwachstelle erfolgt, wenn diese Tätigkeit in einer Weise durchgeführt wird, die darauf abzielt, Schaden für Einzelpersonen oder die Öffentlichkeit zu vermeiden, und wenn die aus der Tätigkeit gewonnenen Informationen in erster Linie dazu verwendet werden, die Sicherheit der Klasse von Geräten, Maschinen oder Online-Diensten, zu denen der Computer, auf den zugegriffen wird, gehört, oder derjenigen, die diese Geräte, Maschinen oder Online-Dienste nutzen, zu fördern. Sicherheitsforschung, die nicht in gutem Glauben durchgeführt wird – wie das Aufdecken von Sicherheitslücken um die Eigentümer betroffener Geräte, Maschinen oder Dienste zu erpressen – kann als „Forschung" bezeichnet werden, ist aber nicht in gutem Glauben.[60] Kritisiert wird, dass die DOJ Policy offen lässt, ob auch in Fällen einer anschließenden Bezahlung, einer Veröffentlichung bspw. auf einer Konferenz oder Vorliegen anderer begleitender Motive die Strafverfolgung ausgeschlossen bleibt.[61] Auch der Verweis auf die im Rahmen der urheberrechtlichen Problematik zum Digital Millennium Copyright Act (DMCA) getroffene Definition sei zu eng und gleichzeitig zu vage.[62]

[58] Diese Anforderung soll auch im Hinblick auf „exceeding authorized access" geprüft werden.

[59] United States Copyright Office, Section 1201 Rulemaking: Eighth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention (Okt. 2021), S. 258, abrufbar unter: https://cdn.loc.gov/copyright/1201/2021/2021_Section_1201_Registers_Recommendation.pdf.

[60] *United States Department of Justice*, Policy 1 9-48.000, Mai 2022, S. 4.

[61] *Electronic Frontier Foundation*, DOJ's New CFAA Policy is a Good Start But Does Not Go Far Enough to Protect Security Researchers, 19.05.2022, abrufbar unter: https://www.eff.org/deeplinks/2022/05/dojs-new-cfaa-policy-good-start-does-not-go-far-enough-protect-security.

[62] *Electronic Frontier Foundation*, DOJ's New CFAA Policy is a Good Start But Does Not Go Far Enough to Protect Security Researchers, 19.05.2022 – abrufbar unter: https://www.eff.org/deeplinks/2022/05/dojs-new-cfaa-policy-good-start-does-not-go-far-enough-protect-security.

c) Schaffung einer IT-sicherheitsspezifischen Ausnahmeregelung

Wie auch der Koalitionsvertrag andeutet, könnte zur Differenzierung zwischen kriminellen Handlungen und redlichen Sicherheitsuntersuchungen ein „verantwortliches Verfahren“,[63] womit sicherlich der CVD-Prozess gemeint ist, das maßgebliche Unterscheidungsmittel sein. Einem solchen Ansatz folgt die niederländische Rechtsprechung, die basierend auf einem Leitfaden des Nationalen Zentrums für Cybersicherheit[64] sowie eines Grundsatzschreibens der Staatsanwaltschaft (Openbaar Ministerie)[65] Kriterien entwickelte, die als außergesetzlicher Grund zum Fehlen einer materiellen Rechtswidrigkeit und damit zum Ausschluss von der Strafverfolgung führt.[66] Die Tat ist danach nicht strafbar, wenn die Täter:in:

1. in Erfüllung eines ***öffentlichen Interesses*** durch verantwortungsbewusste Offenlegung einer Sicherheitslücke handelt (Absicht[67] der Durchführung eines CVD-Prozesses),
2. den Grundsatz der ***Verhältnismäßigkeit*** beachtet, d.h. 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 Sicherheitslücke.[68]

---

[63] *Bundesregierung*, Koalitionsvertrag 2021-2025, S. 13.

[64] *National Cyber Security Centre, Ministry of Justice and Security Netherlands*, Coordinated Vulnerability Disclosure: the Guideline, October 2018.

[65] *Openbaar Ministerie,* Beleidsbrief vom 14.12.2020 – abrufbar unter: https://www.om.nl/documenten/richtlijnen/2020/december/14/jurisprudentie-en-praktijkvoorbeelden; Openbaar Ministerie, Coordinated Vulnerability Disclosure: de Leidraad (Stand: Oktober 2018) – abrufbar unter: https://www.om.nl/documenten/brochures/cybercrime/map/map1/coordinated-vulnerability-disclosure.

[66] Rechtbank Den Haag, Urteil vom 17.12.2014, Nr. 09/748019-12, (ECLI:NL:RBDHA:2014:15611); Rechtbank Oost-Brabant, Urteil vom 19.02.2013, Nr. 01/820892-12, (ECLI:NL:RBOBR:2013:BZ1157).

[67] *Dick van der Reijden,* Biedt Art. 10 EVRM de ethisch hacker bescherming tegen onduidelijkheden en onvolkomenheden in de Leidraad Responsible Disclosure?, S. 35 – abrufbar unter: https://www.maesoever.nl/files/scriptie-dick-van-der-reijden-v1-0p.pdf.

[68] Zur Rechtslage und Aktivitäten in den Niederlanden siehe auch: *Harms,* Netherlands Journal of Legal Philosophy 2017 (46) 2, 196 (200); *CEPS Task Force*, Software Vulnerability Disclosure in Europe, S. 27; *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.

Wenn eine Schwachstelle gemeldet wird und es Anzeichen dafür gibt, dass die Offenleger:in mehr getan hat, als unbedingt notwendig war, um die Schwachstelle aufzudecken, wird dies von den zuständigen Behörden weiter untersucht.69 So wurde ein Hacker wegen „Computervredebreuk" (Ausspähen von Daten) verurteilt, obwohl das Gericht davon ausging, dass er keine böswillige Absicht hatte und ein Fehlverhalten – nämlich ein Sicherheitsleck – aufdecken wollte.70 Der Täter hatte allerdings mehrmals auf das System zugegriffen und mehr Informationen gesammelt, als notwendig gewesen wäre.71 Dagegen ging das Gericht davon aus, dass der Nachweis von Mängeln bei der Sicherheit vertraulicher, medizinischer und persönlicher Daten einem erheblichen gesellschaftlichen Interesse dienen kann.72 Auch das Aufspielen von Malware auf dem fremden Server und der Zugriff ohne Erlaubnis auf hochsensible Daten können notwendige Handlungen darstellen, um die Mängel der IT-Sicherheit aufzudecken. Der Ansatz differenziert nicht nach institutionalisierter Sicherheitsforschung im engeren Sinne und ethischem Hacken durch Privatpersonen. So profitierten bereits Sicherheitsexperten von den in der Rechtsprechung entwickelten Kriterien.[73]

Im Hinblick auf diesen Ansatz wird noch zu diskutieren sein, wie die Grundsätze der Verhältnismäßigkeit und Subsidiarität ohne Fallbeispiele rechtssicher belegbar wären und ob eine ex ante oder ex post Betrachtung ausschlaggebend sein sollte.

d) Ausnahmen auf strafprozessualer Ebene

Einen anderen Weg scheint Frankreich zu gehen: Nach Art. 47 des Rechts für eine digitale Republik 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. Würde man in Deutschland eine entsprechende Regelung in die Strafprozessordnung (StPO) einführen, verbliebe allerdings die Problematik, dass es sich selbst bei redlichen Sicherheitsanalysen um eine rechtswidrige und schuldhafte Straftat handelt,

---

[69] *Openbaar Ministerie*, Coordinated Vulnerability Disclosure: de Leidraad (Stand: Oktober 2018) – abrufbar unter https://www.om.nl/documenten/brochures/cybercrime/map/map1/coordinated-vulnerability-disclosure; *CEPS Task Force*, Software Vulnerability Disclosure in Europe, S. 27.

[70] Rechtbank Den Haag, Urteil vom 17.12.2014, Nr. 09/748019-12.

[71] Zu den Prinzipien siehe auch: Rechtbank Oost-Brabant, Urteil vom 19.02.2013, Nr. 01/820892-12.

[72] Rechtbank Den Haag, Urteil vom 17.12.2014, Nr. 09/748019-12; Rechtbank Oost-Brabant, Urteil vom 19.02.2013, Nr. 01/820892-12.

[73] Siehe bspw. den Fall des Eindringens in den Twitter-Account von Donald Trump: Openbaar Ministerie, Inlog Twitter-account Trump niet strafbaar, Nieuwsbericht 16.12.2020 11:38, abrufbar unter: https://www.om.nl/actueel/nieuws/2020/12/16/inlog-twitter-account-trump-niet-strafbaar.

was z.B. für Schadensersatzforderungen (§ 823 Abs. 2 BGB) ausreichen kann. Zudem verbleiben erhebliche Bedenken, ob eine solche rechtswidrige, bloß nicht verfolgte Tat mit den Grundsätzen der Redlichkeit der Forschung vereinbar wäre.[74]

e) Diskussion zur konkreten Gestaltung eines Strafausschlusses

Um dem Ziel verbesserter Rechtssicherheit näher zu kommen, erscheint eine explizite Ausnahmeklausel für Sicherheitsforschung, welche sowohl institutionalisierte Forschung im engeren Sinne als auch ethisches Hacken umfasst und Kriterien des CVD-Prozesses mit einbezieht, eine sinnvolle Lösung. Diese könnte als Tatbestandsausschluss oder Rechtfertigungsgrund konzipiert werden. Im vergleichbaren Fall der Ausgestaltung einer Erlaubnis zur Offenlegung von Geschäftsgeheimnissen im Rahmen berechtigter Interessen[75] in § 5 GeschGehG wurde bewusst vom ursprünglichen Plan, einen Rechtfertigungsgrund zu schaffen, Abstand genommen, und eine Tatbestandsausnahme kodifiziert. Hauptargument hierfür war der abschreckende Effekt, den das Erfüllen einer Verbotsnorm haben kann, „unabhängig davon wie weit ein dann eingreifender Rechtfertigungsgrund gefasst sei".[76] Dagegen kann aus rechtlicher Sicht festgehalten werden, dass die Einordnung weder aus rein dogmatischer Sicht noch im Hinblick auf Aspekte wie Irrtum, Täterschaft und Teilnahme oder Notwehrrechte eine erhebliche Bedeutung entfaltet, da für das Unrechtsurteil nicht entscheidend ist, ob ein Verhalten schlussendlich bereits nicht tatbestandsmäßig oder nur gerechtfertigt ist.[77]

Auf inhaltlicher Ebene gilt zu berücksichtigen, dass die Umsetzung einer Coordinated Disclosure erst nach Abschluss der Tathandlungen der §§ 202a ff., 303a f. StGB mit der Meldung der Sicherheitslücke sichtbar nach außen wird.[78] Für das Vorliegen einer entsprechenden Absicht könnten allerdings bereits Indizien vorliegen, sodass den Strafverfolgungsbehörden insofern Möglichkeiten verbleiben, eine reine Schutzbehauptung zu entlarven.[79] Eingrenzende Merkmale könnten zudem die vom niederländischen Modell bekannten Grundsätze der Verhältnismäßigkeit und Subsidiarität bilden, die dem Gedanken der Risikominimierung und Schadensbegrenzung folgen. Zudem könnte die Einführung eines den im 1. Kapitel vorgestellten CVD-Grundsätzen entsprechenden Kriteriums wie der unverzüglichen Meldung die Fälle in der Praxis minimieren, in

[74] Whitepaper zur Rechtslage der IT-Sicherheitsforschung 2021, S. 45 f.

[75] Hierzu zählen: die Ausübung u.a. journalistischer Tätigkeiten, das Whistleblowing oder die Wahrnehmung von Arbeitnehmerrechten.

[76] BT-Drs. 19/4742, S. 28; BT-Drs. 19/8300, S. 15.

[77] Vgl. zur behördlichen Genehmigung *Winkelbauer,* NStZ 1988, 201 (201). Ausführlich in: *Zech/Wagner*, in: Golla/Brodowski (Hrsg.) IT-Sicherheit und Strafrecht 2022 – im Erscheinen.

[78] Vgl. auch: *Dick van der Reijden,* Biedt Art. 10 EVRM de ethisch hacker bescherming tegen onduidelijkheden en onvolkomenheden in de Leidraad Responsible Disclosure?, S. 35.

[79] *Zech/Wagner*, in: Golla/Brodowski (Hrsg.) IT-Sicherheit und Strafrecht 2022 – im Erscheinen.

denen eine Entdeckung der Tat bereits vor Absendung der Schwachstellenmeldung erfolgt. Um die notwendige Flexibilität bei einer risikoadäquaten Umsetzung des CVD-Prozesses zu gewährleisten,[80] sollte die Regelung allerdings nur die groben Rahmenbedingungen beschreiben und bspw. keine starren Fristen vorgeben. Des Weiteren sollte von einer zwingenden Meldung an eine bestimmte Stelle abgesehen werden, da wie im folgenden 3. Kapitel erörtert wird, neben der direkten Meldung an den:die Produktverantwortlichen auch die Einbeziehung einer Meldestelle einen sinnvollen – aber nicht zwingenden – Weg darstellt.

3. Zwischenfazit zum Strafrecht

Die sog. Computerdelikte im Strafrecht beinhalten derzeit abschreckende Faktoren insbesondere gegenüber proaktiv durchgeführten Sicherheitsanalysen, die oftmals im Rahmen von Forschungsarbeiten an Hochschulen und Forschungseinrichtungen, aber auch durch unabhängige, ethische Hacker:innen durchgeführt werden. Selbst bei einer unverzüglichen Meldung der gefundenen Schwachstelle an die hierfür verantwortlichen Personen oder eine den Meldeprozess koordinierende Meldestelle, besteht keine Sicherheit vor Strafverfolgung. Daher wurden konkrete Möglichkeiten für eine Gesetzesänderung betrachtet, um Handlungen im wissenschaftlichen und gesellschaftlichen Interesse von Strafbarkeit auszunehmen. Dabei sollten die verschiedenen Facetten der Sicherheitsforschung im weiteren Sinne abgedeckt und gleichzeitig ein hohes Maß an Rechtssicherheit gewährleistet werden. Eine Orientierung am CVD-Prozess beinhaltet die Problematik, das die Umsetzung erst im Nachgang einer ggf. tatbestandsmäßigen Sicherheitsanalyse erfolgt. Nichtsdestotrotz können Indizien herangezogen werden, um festzustellen, ob die Täter:in im Sinne der Risikominimierung agierte und dabei die Zielsetzung der Verbesserung der IT-Sicherheit verfolgte.

III. Impulse für ein koordiniertes IT-Schwachstellenmanagement aus Compliance-Erwägungen

Wie haben Hersteller:innen mit Meldungen sicherheitsrelevanter Schwachstellen durch Endkund:innen oder IT-Sicherheitsforscher:innen umzugehen? Zwar wurden zumindest in größeren Unternehmen Prozesse hierfür entwickelt und ein ISO-Standard für Coordinated Vulnerability Disclosure (CVD) abgeleitet.[81] Dies geschah

[80] *ENISA*, Good Practice Guide on Vulnerability Disclosure, S. 56.
[81] ISO/IEC 29147:2018 sowie für Prozesse mit mehreren Parteien ISO/IEC TR 5895.

(auch), um Compliance-Anforderungen[82] Genüge zu tun. Bis heute sind die Einzelheiten der oftmals rein unternehmensinternen Vorgänge für die Melder:innen von Sicherheitslücken mangels Transparenz allerdings vielfach vage geblieben und es kann sich nicht immer darauf verlassen werden, dass sich Hersteller:innen überhaupt bzw. zeitnah der Sache samt tatsächlicher Beseitigung der Schwachstelle annehmen.[83] Zudem besteht bisher kein Anspruch der Endkund:innen auf ein (wirksames) IT-Schwachstellenmanagement. Im Folgenden wird gezeigt, welchen Einfluss insbesondere zivilrechtliche Haftungsrisiken auf den Umgang mit Schwachstellen haben könnten.

1. IT-Schwachstellenmanagement zur Umsetzung neuer Pflichten bei Consumer-Products

Das Ziel, die Qualität digitaler Produkte in Sachen Sicherheit zu verbessern, verfolgen die jüngst in nationales Recht umgesetzten Digitale-Inhalte-[84] und Warenkauf[85]-Richtlinien, die IT-Sicherheit erstmals gesetzlich als wesentliche objektive Eigenschaft von digitalen Produkten und Diensten sowie Waren mit digitalen Elementen für Verbrauchergeschäfte fixieren. Mit § 327e Abs. 3 S. 1 Nr. 2 BGB und §§ 475b Abs. 4 Nr. 1, 434 Abs. 3 S. 2 BGB ist klargestellt, dass ausnutzbare Sicherheitslücken Mängel im Sinne des Schuldrechts sind, was in Kombination mit Aktualisierungspflichten die Bereitschaft zur Vermeidung und Beseitigung durch Produktverantwortliche erhöhen könnte. Allerdings sind zur Anwendung der Normen noch viele Fragen ungeklärt. So wurde IT-Sicherheit nicht definiert. Für das anzulegende Sicherheitsniveau wurde auf das bei digitalen Produkten derselben Art übliche und vom Verbraucher unter Berücksichtigung der Art des digitalen Produkts erwartbare abgestellt.[86] Wie diese Erwartung zu ermitteln ist, erwähnen die Richtlinien wie auch die jeweilige Umsetzung in deutsches Recht nicht.[87] Hierzu müssen Rechtsprechung und weitere Harmonisierungen

[82] Zur Produkt-Compliance *Wagner/Ruttloff/Miederhoff,* CCZ 2020, 1 und im Bereich IT-Sicherheit an sich *Schmidl,* in: Hauschka/Moosmayer/Lösler (Hrsg.), Corporate Compliance, 2. Abschnitt, 4. Kap., § 28, Rn. 1 ff.; *Bertsch/Fortmann,* r+s 2021, 549 (552).

[83] Vgl. ETSI/EN 303645 V2.1.1 (2020-06), S. 14: „In the IoT industry, CVD is currently not well-established as some companies are reticent about dealing with security researchers."

[84] RL (EU) 2019/770. Zu dieser ausführlicher *Spindler/Sein,* MMR 2019, 415 sowie MMR 2019, 488; *Staudenmayer,* NJW 2019, 2497. Umsetzung bis zum 01.07.2021 und Anwendung ab dem 01.01.2022, Art. 24.

[85] RL (EU) 2019/771. Zu dieser ausführlicher *Bach,* NJW 2019, 1705; *Zöchling-Jud*, GPR 2019, 115 insbesondere zur Einrede der absoluten Unverhältnismäßigkeit.

[86] §§ 327 Abs. 3 S. 1 Ziff. 2; § 434 Abs. 3 S. 2 BGB sowie zur Auslegung im Lichte der RL (EU) 2019/770 EG 45 ff. und RL (EU) 2019/771 EG 24 ff.

[87] Man könnte an eine Kombination von z.B. Umfragen, Markterhebungen (Empirie zur Marktdurchdringung von Sicherheitsfeatures, zu Werbenhalten und Produktbeschreibungen), Gefährdungs-

abgewartet werden.[88] Auch werden Hersteller:innen teilweise nur indirekt adressiert, da Primärverpflichtete die „Bereitsteller:innen" oder Verkäufer:innen sind.[89] Für ein IT-Schwachstellenmanagement ist dies misslich, da die Hersteller:innen dieses implementieren müssten und es die gesamte Produktpalette umfassen sollte.

Gerade nicht triviale Software ist oft fehlerbehaftet.[90] Ein verantwortungsbewusster Umgang mit ihr als Produkt(-Komponente) erfordert das Anerkennen von Sicherheit als wichtigem Faktor im Entwicklungs- und Lebenszyklus[91] sowie die Bereitschaft zur Beseitigung von Sicherheitslücken mit entsprechender Transparenz gegenüber Betreiber:innen und Verwender:innen. Das Verbraucherschutzrecht verfolgt nun das Ziel, die Erhaltung der Vertragsmäßigkeit - insbesondere im Hinblick auf Kompatibilität, Interoperabilität und Sicherheit durch funktionserhaltende Updates und Sicherheits-Updates - zu gewährleisten, sofern es sich um Austauschverhältnisse handelt (Zahlung eines Preises, digitales Äquivalent oder Bereitstellung von Daten). Dies gilt allerdings nicht bei kostenlosen Leistungen. Nach Kritik von Datenschützer:innen wird im Hinblick auf das Modell „Bezahlen mit Daten" nicht mehr von einer „Gegenleistung" gesprochen, um Konflikte synallagmatischer Pflichten mit datenschutzrechtlichen Schutzmechanismen zu vermeiden.[92] Unerheblich ist, ob Daten aktiv bereitgestellt werden, oder nur passiv in die Erhebung eingewilligt wird.[93] Rein werbefinanzierte Angebote sollen aber nicht unter die Regelungen fallen, sofern kein Vertragsschluss vorliegt (umstritten bei Einsatz von Trackingtechnologien, personalisierter Werbung).[94] Insofern bleibt die Frage komplex, wann tatsächlich von „kostenlosen" Angeboten gesprochen werden kann. Die Regelungen unterscheiden des Weiteren zwischen digitalen Produkten (Bereitstellung digitaler Inhalte oder digitaler Dienstleistungen) und Waren mit digitalen Elementen. Letztere adressieren die Verbindung zwischen körperlichen Gegenständen und unkörperlichen, digitalen Leistungen. In beiden Konstellationen folgen aus der Richtlinienumsetzung Pflichten zur Aktualisierung, wobei bewusst

/Schadenanalysen und Studien zum Entwicklungsstand in der Sicherheitstechnik denken. Die Perspektive ist initial aber jeweils die des Kunden und nicht die des Herstellers/Händlers.

[88] RL (EU) 2019/771 EG 25 verlangt für Klarheit nach Vollharmonisierung.

[89] Vgl. *Dickmann*, International Cybersecurity Law Review – DOI: https://doi.org/10.1365/s43439-022-00064-9.

[90] Statt vieler *Spindler*, NJW 2004, 3145 (3147).

[91] Vgl. *Anderson*, Security Engineering, S. 985 ff.

[92] *Pech*, MMR 2022, 516 (518); zum Konflikt: *EDSB*, Stellungnahme 4/2017 zu dem Vorschlag für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, 2017; ausführlich: *Wagner*, Datenökonomie und Selbstdatenschutz, 2020, S. 281 ff. m.w.N.

[93] *Spindler*, MMR 2021, 451 (452).

[94] Vgl. Erwägungsgrund 25 RL (EU) 2019/770; str. *Pech*, MMR 2022, 516 (518); *Spindler*, MMR 2021, 451 (453).

keine Konkretisierung des Aktualisierungszeitraums erfolgte. Vielmehr wird auf berechtigte Erwartungen abgestellt, welche sich am Zeitraum der üblichen Nutzungs- und Verwendungsdauer der Sache bzw. des Produkts richten könnte.[95] Anwendbar sind diese Regelungen somit nur bei:

1. Verbraucherverträgen (Verträge zwischen Verbraucher:innen iSd § 13 BGB und Unternehmern iSd § 14 BGB) und
2. Zahlung eines Preises bzw. digitaler Darstellung eines Wertes oder Bereitstellung personenbezogener Daten, die über das zur Diensterbringung zwingend erforderliche Maß hinausgehen (Modell „Bezahlen mit Daten").

Ausgenommen sind zudem bestimmte Verträge, wie bspw. im Bereich der Telekommunikation, Behandlungsverträge, Glücksspielleistungen, Finanzdienstleistungen und die kostenlose Bereitstellung von Software unter freier und quelloffener Lizenz.

Tabelle 2 skizziert die unterschiedliche Umsetzung je nachdem ob es sich um ein Digitales Produkt oder eine Ware mit digitalem Element handelt.

[95] BT-Drs. 19/27653, S. 59.

	Digitales Produkt	Ware mit digitalem Element
Kriterien	Trennbarkeit zwischen körperlicher Sache und digitalem Produkt (Inhalt / Dienstleistung)[96] Abgrenzung problematisch bei „hybriden Produkten“[97]	Funktionales Kriterium: ohne digitales Element ist die Produktfunktion nicht erfüllbar Vertragliches Kriterium: Funktion ist nach Kaufvertrag geschuldet[98]
Vertragsart	Alle Vertragstypen (Kauf, Leasing, Miete, etc.)	Kaufverträge
Folge für Sicherheitsupdates	Pflicht zur Bereitstellung für den Erhalt der Vertragsmäßigkeit des digitalen Produkts erforderlicher Aktualisierung nach § 327f BGB: - bei einem Vertrag über die dauerhafte Bereitstellung eines digitalen Produkts der **Bereitstellungszeitraum**, - in allen anderen Fällen der Zeitraum, den der Verbraucher aufgrund der Art und des Zwecks des digitalen Produkts und unter Berücksichtigung der Umstände und der Art des Vertrags **erwarten** kann.	Ware entspricht nach § 475b BGB den **subjektiven** Anforderungen, wenn [...] für die digitalen Elemente die im Kaufvertrag vereinbarten Aktualisierungen während des nach dem Vertrag maßgeblichen Zeitraums bereitgestellt werden; und den **objektiven** Anforderungen, wenn dem Verbraucher während des Zeitraums, den er aufgrund der Art und des Zwecks der Ware und ihrer digitalen Elemente sowie unter Berücksichtigung der Umstände und der Art des Vertrags erwarten kann, Aktualisierungen bereitgestellt werden, die für den Erhalt der Vertragsmäßigkeit der Ware erforderlich sind [...].
verpflichtete Person	Unternehmer, der digitales Produkt **bereitstellt**	**Verkäufer:in** (mit Regressanspruch ggü. Hersteller:in)[99]

Tabelle 2: Überblick über neue Verbraucherschutzregelungen mit Bezug zur IT-Sicherheit

[96] *Dubovitskaya*, MMR 2022, 3.
[97] *Wendehorst*, in: Wendehorst/Zöchling-Jud, Ein neues Vertragsrecht für den digitalen Binnenmarkt?, S. 45.
[98] *Felsch/Kremer/Jacoby*, MMR 2022, 18.
[99] Zur Kritik *Dubovitskaya*, MMR 2022, 3.

Die Pflichten zur Aktualisierung sind zentral für die Gewährleistung der Funktionsfähigkeit und Sicherheit digitaler Inhalte und Dienste sowie digitaler Elemente in Kombination mit körperlichen Waren. Bezüglich Letzterer sind Aktualisierungen nicht explizit als Pflicht, sondern Konkretisierung des Mangelbegriffs geregelt. Im Ergebnis dürfte der Pflichtenkanon aus Praxissicht über das Recht auf Nachbesserung vergleichbar ausfallen. Den:die Unternehmer:in treffen Erstellungs-, Informations- und Bereitstellungspflichten, jedoch nicht die Pflicht Updates auch zu installieren.[100] Dies verbleibt im Verantwortungsbereich der Verbraucher:innen. Geschuldete Updates sind zudem nur solche, die die vertragsgemäß geschuldete Leistung erhalten (nicht erweitern) – wozu Sicherheitsupdates regelmäßig zählen dürften, selbst wenn Sicherheitsmängel keine Auswirkung auf die Funktionsfähigkeit des digitalen Produkts bzw. der Ware selbst haben sollten.[101]

Zusammenfassend lässt sich festhalten, dass die Regelungen Impulse setzen dürften, dass Unternehmen – soweit sie tatsächlich verpflichtet werden – Prozesse für regelmäßige Aktualisierungen der IT-Sicherheit vorhalten. Allerdings verbleiben gewisse Unsicherheiten und Limitierungen, die diese Impulse wiederum einschränken können. Dies betrifft im Besonderen die berechtigten Sicherheitserwartungen, Erfassung gesamter Lieferketten, Abgrenzung vertraglicher und nicht-vertraglicher sowie kostenloser Leistungen, sowie im Hinblick auf den Zeitraum, ob der gesamte Produktlebenszyklus abgedeckt ist.

2. IT-Schwachstellenmanagement zur Reduktion von Haftungsrisiken im B2B-Bereich

In Zuge der Novellierung wurde der Sachmangelbegriff des § 434 BGB auch mit Folgen für den B2B-Bereich angepasst. Neu ist die explizite Aufnahme von Faktoren wie Funktionalität, Kompatibilität, Interoperabilität und Sicherheit. Ansprüche können gegenüber der Verkäufer:in geltend gemacht werden. Insofern besteht das Problem des Auseinanderfallens zwischen den für den Sicherheitsmangel verantwortlichen Hersteller:innen und den rechtlich verpflichteten Händler:innen.[102] Anders als die verbraucherschützenden Regelungen, die nun auch Nutzungszeiträume nach Übergabe/Installation erfassen, bezieht sich die klassische Sachmangelhaftung nur auf den Zeitpunkt der Übergabe der Kaufsache. Vertragsbeziehungen mit Dauerschuldcharakter

[100] *Spindler*, MMR 2021, 451 (455).
[101] BT-Drs. 19/27653, 58 f.; *Spindler*, MMR 2021, 451 (455).
[102] Siehe hierzu: *Dickmann*, International Cybersecurity Law Review – DOI: https://doi.org/10.1365/s43439-022-00064-9.

(bspw. Cloud-Nutzungsverträge) wurden hingegen auch unter das Mietrecht subsumiert.[103] Insoweit bestehen ebenfalls Pflichten zur Aufrechterhaltung des zum vertragsgemäßen Gebrauch geeigneten Zustands. Ein gesetzliches Mindestniveau an IT-Sicherheit ist allerdings (auch hier) nicht festgelegt. Unklarheiten verbleiben bei der Übernahme des Leitbilds des Mietvertrags in Bezug auf Aktualisierungspflichten von Software, d.h. inwieweit diese dem neuesten Stand der Technik entsprechen oder auf der Version zum Zeitpunkt des Vertragsschlusses verbleiben müssen bzw. dürfen.[104] Abreden zum IT-Schwachstellenmanagement waren (und sind) als sehr spezielle Unterkategorie der IT-Sicherheit die große Ausnahme und höchstens in Selbstverpflichtungen großer (IT-)Unternehmen oder in Lieferketten über Zertifizierungsanforderungen zu finden. Faktoren wie fehlendes Technikverständnis und Gefahrenbewusstsein, Informationsasymmetrien oder Intransparenz führen oft zum Ausbleiben vertraglicher Fixierungen.

Seitens der Hersteller:innen bestehen grundsätzlich auch deliktische Pflichten, wie bspw. die Produktbeobachtungspflicht als Unterfall der Produzentenhaftung nach § 823 Abs. 1 BGB.[105] Erlangen Produktverantwortliche Kenntnis von ausnutzbaren Sicherheitslücken, besteht je nach Kritikalität Handlungsbedarf: In erster Linie die Warnung betroffener Betreiber:innen und Nutzer:innen, bei höheren Risiken auch Empfehlungen zu (vorläufigen) Absicherungs- bzw. Abhilfemaßnahmen bis hin zur Entwicklung und dem Ausrollen von Updates bzw. bereinigter Versionen.[106] Allerdings greifen die deliktischen Haftungsrisiken aus dem Produkthaftungsgesetz sowie der Produzentenhaftung nur im Fall der Verletzung bestimmter Rechtsgüter.[107] Produkthersteller:innen haften insofern im Gegensatz zum Vertragsrecht für die Gebrauchs*sicherheit*, nicht die Gebrauchs*tauglichkeit*.[108] Eine umfassende Pflicht zur Gewährleistung eines bestimmten IT-Sicherheitsniveaus lässt sich daraus nicht ableiten. Denn das auf EU-Ebene harmonisierte Produkthaftungsrecht stammt noch aus einer Zeit, als es vornehmlich um den Schutz vor analogen Mängeln in Betrieb und Steuerung bzw. ungewolltem Fehlgebrauch ging. Die entsprechende Richtlinie verschließt sich zwar der digitalen Welt nicht völlig, aber Daten haben regelmäßig keine Sachqualität und sind damit nur nachrangig erfasst.[109] Beim Vergleich der Sprachfassungen harmonisierten EU-

---

[103] BGH, Urteil vom 15.11.2006 – XII ZR 120/04.

[104] *Faust*, Digitale Wirtschaft – Analoges Recht: braucht das BGB ein Update?, S. 34.

[105] Vgl. zur Produzentenhaftung: BGH, NJW 1990, 906 (907), NJW 1990, 2560, NJW 1981, 1603 (1604).

[106] Vgl. *Rockstroh/Kunkel*, MMR 2017, 77 (81).

[107] Siehe hierzu § 1 Abs. 1 ProdHaftG, § 823 Abs. 1 BGB.

[108] *Staudinger/Czaplinski*, JA 2008, 401 (405).

[109] Vgl. zum Meinungsstand *Wagner,* in: MüKoBGB, ProdHaftG § 2 Rn. 21 ff.; *Lenz*, Produkthaftung, § 3, Rn. 298; *Förster,* in: BeckOK BGB, ProdHaftG § 2 Rn. 22 ff. mwN.

Sekundärrechts wie auch in der Praxis zeigen sich Unschärfen bei den Begrifflichkeiten und ihrer Verwendung bzw. ein unterschiedliches Verständnis etwa von Jurist:innen, Programmierer:innen und Hardware-Ingenieur:innen. Im angloamerikanischen Raum wird zwischen „Safety" und „Security" unterschieden.[110] Die deutsche Sprache kennt hingegen nur den (Sammel-)Begriff der „Sicherheit", dessen Abgrenzung und Schutzrichtung vielfach unklar bleiben. Mit der zunehmenden Digitalisierung und Vernetzung geht es immer mehr um den Schutz vor Missbrauch von Hard- und Software, wobei die gewählten Schutzziele noch herauszuarbeiten sind. Absoluten Schutz gibt es ebenso wenig wie (ab einem schnell erreichten Komplexitätslevel) fehlerfreie Software. Relative Sicherheit bedarf also der Einigung über ein anvisiertes Sicherheitsniveau, das es mit den vereinbarten Mitteln und entsprechenden Produktbeschaffenheiten zu erreichen gilt.

3. IT-Schwachstellenmanagement als Konformitätserfordernis für das Anbringen des CE-Kennzeichens an Funkanlagen

Impulse für ein höheres IT-Sicherheitsniveau könnten aus dem Produktsicherheitsrecht herrühren.[111] Als eine regulatorische Eingriffsmöglichkeit zur Erzielung eines Mindestsicherheitsniveaus und zur Schadenprävention wird als Voraussetzung des Inverkehrbringens von Waren in der EU mit Kennzeichnungspflichten gearbeitet.[112] Diese sollen die Konformität mit technischen Vorgaben im Hinblick auf die Rechtslage zum Zeitpunkt des Inverkehrbringens für die Kund:innen verständlich bestätigen.[113] Eine Konformitätserklärung ist das CE-Kennzeichen.[114] Bei Konformität ist es nur auf Produkten mit spezifischen Harmonisierungsanforderungen anzubringen. An das Kennzeichen ist ggf. die produktsicherheitsrechtliche Vermutung[115] für die Einhaltung der Vorgaben geknüpft, die etwa bei Non-Compliance wie Zurückfallen hinter den

[110] Funktionale Betriebssicherheit (Schutz der Umgebung vor dem Objekt) einerseits und Schutz vor An-/Eingriffen (Schutz des Objekts) andererseits. Vgl. *Anderson*, Security Engineering, S. 16.; *Hornung/Schallbruch*, IT-Sicherheitsrecht, 2021, § 1, Rn. 12; *Schucht*, NVwZ 2021, 532.

[111] Zu diesem Komplex insgesamt *Dickmann*, International Cybersecurity Law Review – DOI: https://doi.org/10.1365/s43439-022-00064-9.

[112] Adressaten sind vor allem (Komponenten-)Hersteller und Importeure. Zur Stellung des Händlers im Produktsicherheitsrecht *Schucht,* CCZ 2020, 322.

[113] Nachfolgende Verschärfungen der Anforderungen führen per se nicht zu einem nachträglich unzulässigen Einbringen in den Markt.

[114] Vgl. Art. 30 VO (EG) 765/2008 sowie für Funkanlagen RL (EU) 2014/53 EG 43 ff. Mithin handelt es sich um eine (behördlich ungeprüfte) Behauptung des Herstellers. Zur Wahrnehmung am Markt *Lenz*, Produkthaftung, § 8, Rn. 68 ff.

[115] Ggf. in Verbindung mit einer beizulegenden EU-Konformitätserklärung. Vgl. für Funkanlagen RL (EU) 2014/53 EG 38; § 17 FuAG. Vgl. VO (EU) 2022/30 EG 17. Dazu *Schucht*, NVwZ 2021, 532 (533).

Stand der Technik widerlegt werden kann.[116] In Zukunft wird mit der Aktivierung der Art. 3 Abs. 3 S. 1 d) bis f) der Funkanlagenrichtlinie mit Anwendungspflicht zum 01.08.2024 zumindest für kabellos (mittels Funktechnologie) erreichbare und ggf. mit dem Internet verbundene Geräte IT-Sicherheit als Kategorie für die Konformitätsprüfung an Relevanz zunehmen.[117] Auch der aktuelle Entwurf des Cyber Resilience Acts[118] – namentlich Art. 18 ff. – intensiviert die Relevanz der Konformitätsprüfung für Produkte mit digitalen Elementen.[119] Explizit von der Funkanlagenrichtlinie bzw. der delegierten Verordnung 2022/30 erfasste Funkanlagen sind bspw. solche, die (direkt oder indirekt) mit dem Internet verbunden sind und/oder personenbezogene Daten oder Verkehrs-/Standortdaten verarbeiten, die ausschließlich für die Kinderbetreuung konzipiert/bestimmt oder Komponenten von oder Spielzeug oder Wearables sind und personenbezogene Daten oder Verkehrs-/Standortdaten verarbeiten, sowie die mit dem Internet verbunden sind und die Übertragung von Geld, monetäre Werte oder virtuelle Währungen ermöglichen.[120] Nicht erfasst sind Anlagen, die (auch) der Medizinprodukteverordnung, In-vitro-Diagnostika-Verordnung, Flugsicherheits-Verordnung, Kfz-Typengenehmigungs-Verordnung oder Mautsysteme-Richtlinie unterliegen.Die Funkanlagenrichtlinie ist im Gesetz über die Bereitstellung von Funkanlagen auf dem Markt (FuAG) in Deutschland umgesetzt.[121] Die Sicherheitsanforderungen betreffen dabei nicht nur funkspezifische Funktionen, sondern erfassen die Produkte ganzheitlich.[122]

a) Konkretisierung des Stands der Technik durch technische Standards

Grundsätzlich sind Hersteller:innen frei in der Wahl der Mittel. Der Bericht der EU-Kommission über die vorausgehende Folgenabschätzung fordert als grundsätzliche Schutzmaßnahme von den Herstellern ein Schwachstellenmanagement, wobei Mel-

[116] Zu den Folgen siehe *Kapoor/Klindt,* NVwZ 2012, 719; *Schucht,* NVwZ 2015, 852.

[117] Zur Entwicklungsgeschichte siehe die Dokumentation unter https://ec.europa.eu/growth/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en.

[118] Siehe https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

[119] Zu weiteren Inhalten des Entwurfs vgl. Kapitel 2.III.5.

[120] Der Anwendungsbereich ist nicht auf Produkte für Verbraucher:innen begrenzt, vgl. Art. 1 Abs. 1 RL (EU) 2014/53.

[121] BGBl. 2017 I 1947 ff. vom 27.06.2017. Dazu im Überblick *Lenz*, Produkthaftung, 2. Aufl. 2022, § 9, Rn. 92 ff.; *Wagner/Ruttloff,* CB 2017, 234; *Schucht*, BePr 2017, 474.

[122] VO (EU) 2022/30 EG 8.

dungen insbesondere durch IT-Sicherheitsforscher explizit als integrale Bestandteile genannt werden.[123] Die Anforderungen in Harmonisierungsvorschriften bedürfen regelmäßig noch der Konkretisierung durch technische Standards. Dies sind solche, die auf Ersuchen der Kommission von einem europäischen Normungsgremium erarbeitet und im Amtsblatt der EU veröffentlicht werden.[124] Auf EU-Ebene gibt es schon Vorarbeiten des Europäischen Instituts für Telekommunikationsnormen (ETSI), welches die ETSI/EN 303645 erarbeitet hat.[125] Zentral ist dabei die Forderung nach einem IT-Schwachstellenmanagement.[126] Hierzu bedarf es der Veröffentlichung einer selbstbindenden Erklärung der Hersteller:in über den Umgang mit Meldungen von Schwachstellen (Disclosure Policy). Inhaltlich werden Pflichten zu einer zeitnahen Reaktion und einer selbstauferlegten Frist zur Bereitstellung einer Abhilfe gefordert. Hinzu kommt die Überwachung unterstützter Produkte auf Schwachstellen. Werden solche etwa von IT-Sicherheitsforscher:innen entdeckt, sollen diese freiwillig vorrangig direkt an den:die Hersteller:in oder (falls nicht möglich) an nationale Behörden gemeldet werden.[127]

Zudem müssen nach ETSI/EN 303645 unternehmensintern Vorbereitungen etwa durch Schulungen, Auswahl der (technischen) Ansprechpartner und Dokumentation der verwendeten Hard- und Software in Produkten getroffen werden.[128] Damit wäre eine Basis geschaffen, auf der man sich dann mit Folgeproblemen wie einer großen Zahl von Beteiligten etwa in vielgliedrigen Lieferketten,[129] Schwachstellen in ganzen Klassen von Produkten, nicht (mehr) zugänglichem Quellcode, Verantwortlichkeiten im Bereich Open Source, Insolvenzen oder Konflikten wegen Verschwiegenheitspflichten, öffentlich-rechtlichen Meldepflichten oder Lizenzrechten widmen kann.

Wie mit der Reform im Schuldrecht durch die Update-Pflicht wird durch die Aktivierung in der Funkanlagenrichtlinie eine dynamische Komponente implementiert, die mehr einfordert als eine bloße Produktbeobachtung. Nicht mit Blick auf Funktionali-

[123] *Whittle u.a.*, Final Report, April 2020, S. 25 f. abrufbar unter https://ec.europa.eu/docsroom/documents/40763.

[124] Eine Auflistung findet sich unter https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards_de.

[125] Aktuell ist der finale Entwurf in Version 2.1.0 aus Juni 2020, Cyber Security for Consumer Internet of Things: Baseline Requirements, abrufbar unter https://www.etsi.org.

[126] ETSI/EN 303645 V2.1.1 (2020-06), S. 14 f. (Provision 5.2-1 ff.).

[127] ETSI/EN 303645 V2.1.1 (2020-06), S. 15.

[128] ETSI/EN 303645 V2.1.1 (2020-06), S. 15 (Provision 5.2-3; Software Bill of Materials (SBOM)).

[129] Vgl. ISO/IEC TR 5895.

täten, wohl aber auf IT-Sicherheit wird hiermit eine Produktpflege innerhalb des Lebenszyklus abverlangt. Dessen Dauer kann die Hersteller:in selbst bestimmen, muss aber bei Inverkehrbringen die Mindestunterstützungszeit mitteilen.[130]

b) Haftungsrisiken als Motor für die Etablierung von Coordinated-Disclosure-Prozessen

Ein zu Unrecht angebrachtes CE-Kennzeichen dürfte einen Sachmangel iSv § 434 Abs. 1 BGB darstellen, wenn das Produkt harmonisierte sicherheitstechnische Anforderungen nicht erfüllt.[131] Zudem ist § 7 Abs. 2 ProdSG als Schutzgesetz iSv § 823 Abs. 2 BGB auszulegen.[132] Dies gilt spätestens mit Inkrafttreten der Aktivierung der Anforderungen zur IT-Sicherheit in der Funkanlagenrichtlinie und deren neuen Schutzzielen.[133] Dies sind die Protektion vor missbräuchlicher Nutzung von Netzwerkressourcen, der Privatsphäre, von personenbezogenen Daten und vor Betrug. Sie zielen nicht nur als Reflex auf die Nutzer und Teilnehmer ab, die damit in den Schutzbereich fallen.

Eine unterbliebene Einrichtung eines IT-Schwachstellenmanagements trägt allerdings nicht die Vermutung in sich, dass ein Produkt selbst mangelhaft ist und etwa eine Schwachstelle enthält. Das Unterlassen kommt vielmehr erst zum Tragen, wenn eine Sicherheitslücke bekannt wird und deren Ausnutzung einen Schaden auslöst. Dann stellt sich die Frage, ob ein ordnungsgemäßes Schwachstellenmanagement nicht zu einer Beseitigung der Lücke vor der schadensstiftenden Ausnutzung geführt hätte. Dem Geschädigten wird es meist schwerfallen, den Beweis für die Kausalkette zu führen. Allerdings können sich etwa bei Ransomware-Kampagnen (auch IT-forensisch) Erleichterungen ergeben, wenn die durch die verwendete Schadsoftware ausgenutzten Schwachstellen im anvisierten System dem Hersteller vor Ausnutzung bekannt waren. Letzteres kann etwa durch Presseberichte, ungewollte Informationsabflüsse, Informationsschreiben an Betroffene, behördliche Ermittlungen oder durch Antworten auf Auskunftsansprüche bekannt werden. Hatte die Herstellerin zuvor angemessen Zeit z. B. für die Entwicklung und das Bereitstellen eines Updates bzw. anderweitige Abhilfemaßnahmen (wenigstens aber eine Warnung) zu sorgen und hat dies nicht getan, kann sich hieraus eine Haftung ergeben.

---

[130] Benennung des Zeitpunkts, bis zu dem/ab dem (keine) Sicherheitsupdates bzw. entsprechende anderweitige Lösungen (mehr) für ein spezifisches Produkt erbracht werden.

[131] So auch *Schütte,* in: Ehring/Taeger, Produkthaftungs- und ProduktsicherheitsR (2022), § 7 ProdSG, Rn. 46.

[132] Anders (wohl noch zur alten Rechtslage) *Schütte,* in: Ehring/Taeger, Produkthaftungs- und ProduktsicherheitsR, 2022, § 7 ProdSG, Rn. 43 mwN.

[133] Vgl. RL (EU) 2014/53 EG 44: „wichtig für die Information der Verbraucher und der Behörden".

4. IT-Schwachstellenmanagement als Bestandteil der DSGVO-Compliance

Neben Verpflichtungen zur Produktbeobachtung ist auch das Datenschutzrecht seit der Anwendung der DSGVO – bereits aufgrund der dort regulierten Bußgeldhöhe – ein wesentlicher Grund für die Verbesserung von Compliance-Prozessen. IT-Sicherheit ist dabei ein zentraler Bestandteil des Datenschutzes. In der DSGVO wird dies insbesondere durch sog. technische und organisatorische Maßnahmen festgehalten, welche ein angemessenes Schutzniveau für die Rechte und Freiheiten von Betroffenen sicherstellen müssen. Adressiert werden diese Aspekte v.a. in den

- Art. 5 Abs. 1 lit. f DSGVO (Grundsatz der Integrität und Vertraulichkeit),
- Art. 25 Abs. 1, 2 DSGVO (Grundsätze des Privacy by Design, Privacy by Default),
- Art. 32 DSGVO (Sicherheit der Verarbeitung),
- Art. 33 DSGVO (Meldepflicht bei sog. Datenschutzverletzungen)
- sowie in Art. 35 DSGVO (Datenschutz-Folgeabschätzung).[134]

So normiert Art. 32 Abs. 1 DSGVO etwa das Ziel, ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau zu erreichen. Um zu bestimmen, welche technischen und organisatorischen Maßnahmen hierfür geeignet sind, zählt Art. 32 Abs. 1 DSGVO einige zu berücksichtigende Abwägungskriterien, wie etwa den Stand der Technik oder die Implementierungskosten auf. Exemplarisch nennt die Norm als konkrete Maßnahme: „ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung".

Um aus einer organisatorischen Perspektive die DSGVO-Compliance sicherzustellen, ist die Einführung eines sog. Datenschutz-Managementsystems (DSMS) üblich.[135] Im Rahmen dieses DSMS müssen dann auch Informationen über (potenzielle) Schwachstellen Berücksichtigung finden. Dies gilt etwa für die Beurteilungen über

- die (andauernde) Wirksamkeit der implementierten technischen und organisatorischen Schutzmaßnahmen i. S. d. Art. 32 Abs. 1 DSGVO
- das mögliche Vorliegen von sog. Datenschutzverletzungen bei Bekanntwerden einer Sicherheitslücke (Art. 33 DSGVO)
- die zu treffenden Risikobewertungen (z.B. in Art. 32 Abs. 1 oder in Art. 35 Abs. 1 DSGVO) im Hinblick auf die Rechte und Freiheiten betroffener Personen.

---

[134] Vgl. statt vieler: *Voskamp*, in: Kipker, Cybersecurity, Kap. 5 Rn. 5 ff.

[135] Teilweise wird die Einführung eines DSMS auch als verpflichtend angesehen, dies ist jedoch im Einzelfall zu prüfen, vgl. *Lang*, in: Taeger/Gabel, DSGVO, Art. 24 Rn. 28, 81.

Unmittelbar aus der DSGVO verpflichtet werden Hersteller:innen zwar nur, wenn sie entweder als Verantwortliche i. S. d. Art. 4 Nr. 7 DSGVO oder als Auftragsverarbeiter i. S. d. Art. 4 Nr. 8 DSGVO eingeordnet werden können – also auch an der Verarbeitung personenbezogener Daten beteiligt sind oder ihre Produkte selbst entsprechend einsetzen. Doch auch mittelbar sind diese Anforderungen für Hersteller:innen relevant, nämlich dann, wenn diese ihre Produkte im Geltungsbereich der DSGVO vertreiben.

Obwohl technische und organisatorische IT-Sicherheit(-smaßnahmen) und rechtliche Datenschutzanforderungen eng zusammenhängen, verfolgen sie im Kern unterschiedliche Ziele. Dadurch ergeben sich Zielkonflikte, die in der Literatur verschiedentlich diskutiert werden.[136] Diese können auch bei der Implementierung eines IT-Schwachstellenmanagements relevant werden, etwa wenn es für Mitigationsmaßnahmen erforderlich ist, personenbezogene Daten (etwa der Melder:innen der Schwachstelle oder weiterer Dritter) zu verarbeiten.[137] Hierbei können sich Verantwortliche dennoch das oben skizzierte enge Verhältnis zwischen IT-Sicherheit und Datenschutzrecht zu Nutze machen: Da die DSGVO selbst IT-Sicherheitsmaßnahmen fordert und diese denknotwendig auch Datenverarbeitungen zu Zwecken der IT-Sicherheit zur Folge hat, können mögliche Rechtsgrundlagen auch in diesem Lichte gelesen werden. Dies gilt insbesondere für die Datenverarbeitung auf Grundlage einer Interessenabwägung (Art. 6 Abs. 1 lit. f DSGVO)[138] sowie für die Datenverarbeitung auf Grundlage einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c DSGVO). Im Ergebnis kann daher auch im Kontext der DSGVO-Compliance ein Impuls für IT-Schwachstellenmanagement entstehen.

5. Impulse aus dem IT-Sicherheitsrecht

Aktuelle Impulse für ein Schwachstellenmanagement könnten sich darüber hinaus sowohl aus der kürzlich verabschiedeten NIS2-Richtlinie (NIS2-RL) als auch aus dem Entwurf des Cyber Resilience Act (CRA) ergeben.

Ziel der NIS2-RL[139] ist nach aktuellem Stand die einheitlichere Regulierung der IT-Sicherheit dadurch, dass die Verpflichtung zur Einbindung geeigneter Schutzmaßnahmen nun ein breiteres Spektrum von Anwendungen bzw. Entitäten betreffen soll. Auf diese Weise soll das Ungleichgewicht der Vorgänger-Richtlinie EU (RL)

---

[136] Statt vieler vgl. nur: *Jandt,* in: Hornung/Schallbruch, IT-Sicherheitsrecht, § 17 Rn. 45 ff.

[137] Einführend zu möglichen Rechtsgrundlagen für IT-Sicherheitsforscher vgl. auch Whitepaper zur Rechtslage der IT-Sicherheitsforschung 2021, S. 18 f. Vorliegend ist jedoch die Perspektive von Hersteller:innen als verantwortliche Stelle relevant.

[138] Hierzu: *Voskamp,* in: Kipker, Cybersecurity, Kap. 5 Rn. 43.

[139] Abrufbar unter https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022L2555 .

2016/1148 (NIS-Richtlinie) ausgeglichen werden. In der Tiefe greift die NIS2-Richtlinie auf eine Mischung aus einem breiteren Anwendungsbereich durch die Auflösung der Kernbegriffe „Kritische Infrastruktur" und „Digitale Dienste" und die Implementierung vertrauensbildender Maßnahmen zurück. Zur Vertrauensbildung etabliert die Richtlinie unmittelbar die Implementierung des CVD-Prozesses in Art. 12 und 21 Abs. 2 lit. e NIS2-RL. Im Rahmen der nationalen Cybersicherheits-Strategien sind u.a. Konzepte für die koordinierte Offenlegung von Schwachstellen nach Art. 12 Abs. 1 NIS2-RL vorzusehen (Art. 7 NIS2-RL). Die Koordination obliegt laut der Kernnorm Art. 12 NIS2-RL einem nationalen CSIRT (eng. Cyber Security Incident Response Team), das als vertrauenswürdiger Mittler zwischen der meldenden Institution/Person und dem Hersteller agiert. Auch eine Schwachstellen-Meldung bezüglich mehrerer Hersteller im Sinne einer „multi-party vulnerability disclosure" ist möglich. Ergänzend hierzu wird die ENISA eine europäische Schwachstellendatenbank entwickeln und pflegen (Art. 12 Abs. 2 NIS2-RL), bei der das bestehende System der CVE-Nummern aufgegriffen werden sollte. Hierauf wird zumindest indirekt verwiesen, wenn das CSIRT bei seiner Arbeit – also auch der Bearbeitung von Schwachstellen-Meldungen – gem. Art. 11 Abs. 5 lit. c NIS2-RL die Annahme und Anwendung gemeinsamer oder standardisierter Vorgehensweisen, Klassifizierungssysteme und Taxonomien fördern soll. auf etablierte Standards zurückgreifen soll. Nach Art. 12 Abs. 1 UAbs. 2 NIS2-RL soll eine Schwachstelle auch anonym gemeldet werden können.

Der Entwurf des Cyber Resilience Acts fokussiert sich dagegen produktspezifisch nur auf Produkte mit „digitalen Elementen". Darunter versteht der CRA gem. Art. 3 Nr. 1 CRA jede Soft-, Hardware oder Remote-Anwendung einschließlich dazugehöriger technischer Komponenten. Ergibt sich aus der Verarbeitung der Daten durch die Anwendung ein besonderes Risiko für die Resilienz bzw. IT-Sicherheit, handelt es sich um ein kritisches Produkt (Art. 3 Nr. 3 CRA). Für beide Arten sieht der Entwurf besondere Vorgaben und Maßnahmen zum Erhalt der Resilienz im Hinblick auf IT- und Datensicherheit vor – hierzu Annex I – oder ergänzt diese durch spezifische Beschlüsse gem. Art. 50 CRA. Der CVD-Prozess findet im Entwurf aber nur am Rande seinen Platz: In Art. 10 Nr. 6 i.V.m. Annex I Abschnitt 2 und Art. 11 CRA findet sich lediglich die Vorgabe einer Coordinated Disclosure Policy, die besagter Annex I Abschnitt 2 inhaltlich spezifiziert. Ein Meldeprozess wird lediglich zwischen Hersteller:in und ENISA gem. Art. 11 Abs. 1 CRA etabliert; selbige Meldung ist an das zuständige CSIRT weiterzuleiten. Eine Einbeziehung Dritter – wie z.B. IT-Sicherheitsforschende – wird dabei ausgespart. Aus dem Gefälle zwischen NIS2-RL als Richtlinie und CRA als Verordnung kann sich schon nicht ergeben, dass die NIS2-RL die Verordnung inhaltlich ergänzt. Schließlich bedarf die Richtlinie erst der Umsetzung, wenngleich die Abweichungsmöglichkeiten der NIS2-RL recht schmal sind. Dennoch zeigt sich eine

enge Verzahnung beider Entwürfe beispielsweise darin, dass die Definition der Kritikalität zur Einschätzung kritischer Produkte mit digitalen Elementen aus der NIS2-RL übernommen wird (siehe Art. 6 Abs. 2 lit. b CRA).

Die Überarbeitung des IT-Sicherheitsrechts auf europäischer Ebene deutet entsprechend auf eine Implementierung des CVD-Prozesses hin, wenngleich dieser durch die Umsetzung der NIS2-RL zeitlich von den Mitgliedsstaaten abhängt. Zur vollen Geltung kann dann selbst der CRA erst kommen, wenn das Gesamtpaket der EU auf den Weg gebracht und umgesetzt wurde. Inwieweit der im Entwurf herausgearbeitete CVD-Prozess den Empfehlungen dieses Papiers entspricht und so erhalten bleibt, kann daher an dieser Stelle noch nicht abschließend beurteilt werden.

6. Zwischenfazit zu Impulsen der Compliance-Anforderungen für ein koordiniertes Schwachstellen-Management

Ob sich aus dem Zusammenspiel von Produktsicherheitsrecht, Zivilrecht und Datenschutzrecht mit Blick auf die IT-Sicherheit und das IT-Schwachstellenmanagement eine eigenständige Relevanz für die praktische Durchsetzung von Coordinated-Disclosure-Prozessen auf Augenhöhe zwischen Melder:innen und Meldungsempfänger:innen entfaltet, bleibt abzuwarten. Die Frage wird sich jedoch insbesondere dann stellen, wenn es zu unterschiedlicher Rechtsprechung zu einzufordernden IT-Sicherheitsmaßnahmen kommt. Sicherheitserwartungen im Markt tendieren jedoch dazu, über die Mindeststandards technischer Normen hinauszugehen. Dies bedeutet, dass Hersteller:innen, die die Mindeststandards unterlaufen, auch die Erwartungen des Marktes enttäuschen. Zu hoffen bleibt, dass die Hersteller:innen das IT-Schwachstellenmanagement nicht als bloßen administrativen Ballast sehen, sondern gerade die Meldung durch IT-Sicherheitsforscherinnen als Geschenk und Chance für mehr Produktsicherheit annehmen. Die jüngere Entwicklung – insbesondere im Kontext der Funkanlagenrichtlinie sowie des Entwurfs zum CRA – deutet jedoch darauf hin, dass das Unionsrecht zunehmend direkt Hersteller adressiert. Dies ist grundsätzlich als Schritt in die richtige Richtung zu werten. Ob die aktuell konkret vorliegenden Entwürfe ausreichen, bleibt – insbesondere wegen der fehlenden ausdrücklichen Berücksichtigung von IT-Sicherheitsforschenden im Entwurf des CRA – abzuwarten.

IV. Fazit

In diesem Kapitel konnte gezeigt werden, dass das Thema des verantwortungsbewussten Umgangs mit Sicherheitslücken noch nicht ausreichend Eingang in die Gesetzgebung gefunden hat. Dies gilt sowohl für den Umgang mit Schwachstellen durch staat-

liche Stellen als auch die Adressierung potenzieller Konflikte bei der Meldung von Sicherheitslücken durch unabhängige IT-Sicherheitsforschende. Die von den Gefahren durch Sicherheitslücken tangierten Grundrechte – insbesondere der vom BVerfG festgestellte Schutzauftrag zur Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – gebieten allerdings eine gesetzgeberische Befassung mit der Problematik. Die aktuelle Rechtslage bietet zudem kaum Rechtssicherheit für Sicherheitsforschung, unabhängig davon, ob Sicherheitsuntersuchungen an Hochschulen und Forschungseinrichtungen oder durch sog. ethische Hacker:innen erfolgen. Mit der Meldung einer Sicherheitslücke gegenüber den für ein Produkt bzw. System verantwortlichen Stellen, Organisationen und Unternehmen laufen Melder:innen Gefahr in den Fokus strafrechtlicher Ermittlungen oder zivilrechtlicher Verfahren zu geraten. Zwar setzen haftungs- und datenschutzrechtliche Compliance-Anforderungen Impulse für Unternehmen, Verantwortliche und Auftragsverarbeiter, Sicherheitsmeldungen im Rahmen eines koordinierten Schwachstellenmanagements einzubinden. Allerdings sind die Regelungen noch fragmentarisch, d.h. nur in bestimmten Fällen und Konstellationen anwendbar. Ohne gesetzliche Anpassungen bleibt die Umsetzung einer Coordinated Disclosure weitgehend freiwillig. Auch der Entwurf des CRA enthält in Annex I lediglich oberflächliche Anforderungen, sodass die Problematik hiermit noch nicht ausreichend adressiert ist. Um sowohl rechtliche als auch praktische Konflikte zu entschärfen, könnte die Einrichtung von Meldestellen dabei unterstützen, einen verantwortungsbewussten Umgang mit Sicherheitslücken besser zu koordinieren. Welche Anforderungen dabei zu bedenken sind, wird im folgenden Kapitel erörtert.

Kapitel 3

Konzept einer Melde- und Koordinierungsstelle zur Unterstützung von Coordinated-Disclosure-Prozessen

I. Motivation einer Melde- und Koordinierungsstelle für Coordinated-Disclosure-Prozesse

Dieser Beitrag propagiert eine zentrale Stelle zur Vereinfachung der Meldung von Sicherheitslücken, die die bereits im IT-Umfeld etablierten Melde-Verfahren unterstützt und dabei insbesondere unterschiedliche Grade der Koordinierung übernimmt. Dazu wird eingangs die aktuelle Rechtslage zu möglichen Melde- und Koordinierungsstellen erläutert. Anschließend wird auf die zentralen Ziele einer Melde- und Koordinierungsstelle eingegangen. Diese liegen primär im Ausgleich konfligierender Interessen der am CVD-Prozess Beteiligten bzw. von diesem Betroffenen. Daraus folgen funktionale und nicht-funktionale Anforderungen an eine solche Stelle. Abschließend wird die rechtliche Ausgestaltung einer zentralen Stelle zur Koordinierung der Meldevorgänge diskutiert und der Anpassungsbedarf in einschlägigen Gesetzen aufgezeigt.

II. Aktuelle Rechtslage zu möglichen Melde- und Koordinierungsstellen

Die bis hierhin aufgezeigten Probleme im Rahmen der Coordinated Disclosure werden durch die aktuelle Rechtslage bei der Meldung von IT-Sicherheitslücken und die unzureichend geregelte Zuständigkeit geeigneter Institutionen begünstigt. Hier eignet sich sowohl ein Blick in das geltende Datenschutz- wie IT-Sicherheitsrecht.

In seinem Beschluss vom 08.06.2021 hat das BVerfG hinsichtlich des Umgangs staatlicher Stellen mit Schwachstellen die Erstellung und Implementierung eines Managementprozesses gefordert.[1] Die „Aufstellung und normative Umsetzung eines Schutzkonzepts“ sei Sache des Gesetzgebers. Neben Prozessen für den (behördeninternen) Umgang bei und nach Erlangung von Informationen zu Schwachstellen gehört

[1] BVerfG NJW 2021, 3033, Rn. 49.

dazu auch die Einrichtung eines Meldewegs an die Verantwortlichen zur Beseitigung. Dies betrifft sowohl Informationen, die zielgerichtet von Behörden erlangt, wie auch solche die ihr zufällig angetragen werden. Ergibt sich aus einer der nach Kenntniserlangung notwendigen kontinuierlichen Abwägungsentscheidungen zum weiteren Umgang, dass die Geheimhaltung der Informationen zur Schwachstelle unverhältnismäßig ist, muss die Meldung an Verantwortliche zur Beseitigung erfolgen.[2] Es liegt nahe, mit dem Meldeprozess eine eigene Stelle zu betrauen.

1. Rechtliche Ausgestaltung des BSI

Institutionell eignen sich nach aktueller Gesetzeslage sowohl die Datenschutzaufsichtsbehörden als auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) als potenzielle, bereits existierende Kandidaten für die Melde- und Koordinierungsstelle (MKS). Eine Meldung beim BSI erscheint schon der Idee halber naheliegend, da die Eigenschaft als zentrale Meldestelle bereits in § 4b Abs. 1 BSIG verankert ist. Der Anwendungsbereich gem. §§ 3 Abs. 1 S. 1, 2 Abs. 1 BSIG beschränkt die Behörde auf die „Informationstechnik" (des Bundes, vgl. § 3 Abs. 1 S. 2 Nr. 1 BSIG). In § 4b Abs. 1 BSIG wird zwar bloß von der Entgegennahme und Auswertung von Informationen über Sicherheitsrisiken zur Wahrnehmung der Aufgaben aus § 3 BSIG gesprochen. In § 3 Abs. 1 S. 2 Nr. 14, 14a BSI-G wird „Beratung, Information und Warnung" genannt. Die Weiterleitung von Informationen an Verantwortliche explizit zur Beseitigung von Schwachstellen ist lediglich indirekt über § 4b Abs. 3 Nr. 1 BSIG als „Dritte" bzw. Nr. 2 i.V.m. § 7 Abs. 1 lit. a BSIG bei der Warnung der Öffentlichkeit sowie in § 4b Abs. 3 Nr. 4 bei Betreibern Kritischer Infrastrukturen aufgezählt, zumal die „Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen" (so § 3 Abs. 1 S. 2 Nr. 14, 14a BSIG) betont wird. Die Formulierung stellt sich nicht als ein Fokus der Tätigkeit auf der Beseitigung oder gar Prävention des Risikogrundes dar. Vielmehr wird als Zielrichtung auf die Erfüllung der Aufgaben nach § 3 BSIG verwiesen, indem mit dem Passus „in Fragen der Sicherheit in der Informationstechnik" letztlich auf § 3 Abs. 1 S. 1 BSIG Bezug genommen wird. Der dortige Katalog ist abschließend und lässt den Charakter des BSI als allgemeine Sicherheitsbehörde, die nicht ausschließlich der Verbesserung der IT-Sicherheit verpflichtet ist, nach der Reform noch klarer erkennen.

Die Meldung von IT-Sicherheitslücken reduziert sich damit auf die technischen, die Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit (§ 2 Abs. 2 BSIG) einbeziehenden Aspekte, wie sie z.B. für die Erstellung von Lagebildern (vgl. § 8b Abs. 2 Nr.

[2] BVerfG NJW 2021, 3033, Rn. 44. Vgl. zum Folgenden auch die Besprechung von *Dickmann/Vettermann*, MMR 2022, 740 ff.

3 BSIG) nötig ist. Eine proaktive Rolle zur Schließung von IT-Sicherheitslücken auf Basis der Meldungen sowohl in Hard- als auch Software ist mangels Regelung folglich nicht ausdrücklich umfasst. Schließlich ergeben sich aus dem Entgegennehmen (§ 4b Abs. 1 BSIG) und Weiterleiten von Informationen (§ 4b Abs. 3 BSIG) nicht auch eigene Forschungsbemühungen oder gar die Rolle als Mittler zwischen Produktherstellerin, Sicherheitsforscherin und ggf. Nutzenden. Weiterhin ist eine rein defensive – auf die Stärkung und Gewährleistung der Sicherheit bundesweiter IT-Systeme gerichtete – Ausrichtung des BSI nicht ausreichend gesetzlich verankert, da das BSI dem Bundesministerium des Inneren (BMI) unterstellt ist. Mehr noch könnten sich Risiken aus dem (Ver-)Teilen von Informationen zu Schwachstellen bei gegenseitiger Amtshilfe der unterstellten Stellen – Polizei, Geheimdienste und BSI – ergeben, entweder zu Ungunsten der Finderinnen oder Nutzerinnen von IT-Soft- oder Hardware; Schwachstellen können entsprechend bspw. zur Exploit-Entwicklung genutzt werden. Dieser Konflikt wird im Falle einer Ansiedlung der MKS beim BSI zu Akzeptanzproblemen bei der (deutschen) IT-Sicherheitscommunity führen.[3]

Besagte Unterstützung „anderer Stellen" (vor allem der Polizei und Nachrichtendienste) ist in §§ 3 Abs. 1 S. 2 Nr. 2 und Nr. 13, 13a BSIG zu finden, wonach insbesondere gewonnene Informationen und Erkenntnisse zur Erfüllung der Sicherheitsaufgaben der empfangenden Behörde zur Verfügung gestellt werden. Dies gilt also sowohl für den Bereich der Prävention wie auch den der Strafverfolgung und Spionage. Zwar findet sich in § 3 Abs. 1 S. 2 Nr. 13 BSIG aE die Einschränkung, dass die Unterstützung nur gewährt werden darf, wenn sie „erforderlich ist, um Tätigkeiten zu verhindern oder zu erforschen, die gegen die Sicherheit in der Informationstechnik gerichtet sind oder unter Nutzung der Informationstechnik erfolgen". Es erscheint jedoch fraglich, ob dies auf eine defensive Ausrichtung des BSI hindeuten soll. Jüngere politische Bestrebungen wie die Erweiterung von Ermittlungsbefugnissen des BSI durch das IT-Sicherheitsgesetz 2.0 oder die Verankerung der Behörde im Grundgesetz[4] lassen deutlich eine Tendenz weg von einer verbraucher- und infrastrukturschützenden Behörde hin zu einem Annex der Sicherheitsbehörden erkennen. Mit „Tätigkeiten" sind wohl nicht solche von Behörden, sondern solche von Dritten (also „externen Gefährderinnen der IT-Sicherheit") gemeint. Gewinnen also das BSI oder andere Sicherheitsbehörden Erkenntnisse über Schwachstellen ist unklar ob und wie das BSI für deren Beseitigung abseits der Informationstätigkeit des § 4b Abs. 3 BSIG verantwortlich ist. Denn eine Meldung etwa an Produktverantwortliche und eine Veröffentlichung insbesondere von solchen

[3] Siehe dazu auch Kapitel 4.2 des Konzepts zum Cyberhilfswerk der AG-Kritis (Version 1.0) – abrufbar unter https://ag.kritis.info/chw-konzept/.

[4] Siehe https://www.rnd.de/politik/cybersicherheit-faeser-will-grundgesetzaenderung-bundesamt-soll-anlaufstelle-sein-OCNEZZQBUNBRZENLEQSKDHGQQM.html.

Schwachstellen, die von Sicherheitsbehörden und ihren Dienstleistern z. B. für die Erstellung von Trojaner-Software oder die Infiltrierung von Netzwerken zur Aufklärung genutzt werden, laufen der Aufgabenerfüllung nach § 3 Abs. 1 S. Nr. 13 a) bis c) BSIG diametral entgegen. Zudem stellt sich für die zweite Alternative in § 3 Abs. 1 S. 2 Nr. 13 BSIG („oder unter Nutzung der Informationstechnik") die Frage, ob dies nicht eine generelle Öffnungsklausel ist, die ein Tätigwerden solange erlaubt, wie es um Informationstechnik geht.

Melder:innen von Schwachstellen an das BSI können jedenfalls nicht sicher sein, dass die entsprechenden Informationen nicht (auch) an Polizei und Nachrichtendienste zur offensiven Nutzung weitergeleitet werden. Die Vorgabe einer Information von Produktverantwortlichen als „Dritte" gem. § 4b Abs. 3 BSIG reicht zumindest nicht so weit, einen CVD-Prozess zu etablieren, zu begleiten und auf eine Beseitigung der Schwachstelle proaktiv hinzuwirken. Dabei ist zu bedenken, dass das BSI aktiv Unterstützung bei der Herstellung von Offensivmitteln wie Staats-Trojanern geleistet hat.[5] Dies schafft keine Vertrauensbasis, sondern hat eher abschreckende Wirkung auf potenzielle Melder:innen.

2. Kompetenzbeschreibung der Datenschutzaufsichtsbehörden

Andererseits sind Aspekte des Persönlichkeitsrechts und der Schutz der informationellen Selbstbestimmung dem Datenschutzrecht bei der Verarbeitung von personenbezogenen Daten durch Hard- und Software zuzuordnen. Interessen der IT-Sicherheitsforschung unterliegen damit einer strengeren unionsrechtlichen (Art. 89 DSGVO) wie nationalen (§ 27 BDSG) Regulierung. Die datenverarbeitende Informationstechnik betreffend sehen Art. 32, 25 DSGVO flexible Schutzmaßnahmen vor, die auf technischer und organisatorischer Ebene für datenschutzrechtlich Verantwortliche und ggf. Forscher:innen ansetzen. Hierzu könnte auch das Schließen von Sicherheitslücken als präventives Mittel zählen, soweit die Verantwortlichen selbst hierzu in der Lage sind. Hersteller:innen sind nicht primär von der Regelung umfasst; ein Hineinlesen in den „Stand der Technik" i.S.e. Update-Pflicht oder zur Gewährleistung der Systemsicherheit ist naheliegend, aber nach herrschender Auffassung vage.[6] Ebenfalls nicht dafür

[5] *Meister*, netzpolitik.org vom 16.03.2015 – abrufbar unter https://netzpolitik.org/2015/geheime-kommunikation-bsi-programmierte-und-arbeitete-aktiv-am-staatstrojaner-streitet-aber-zusammenarbeit-ab/.

[6] Siehe zum Streit über die Erstreckung auf Hersteller und Softwareproduzenten *Baumgartner/Gausling*, ZD 2017, 308 (311); *Schuster/Hunzinger*, CR 2017, 141 (146); *Dümeland*, K&R 2019, 22 (24). Umfänglich ablehnend dagegen *Jandt*, in: Kühling/Buchner, DS-GVO/BDSG, DS-GVO Art. 32 Rn. 4; *Martini*, in: Paal/Pauly, DS-GVO/BDSG, DS-GVO Art. 32 Rn. 27 mwN.

spricht die anderweitig in § 327f BGB geregelte Verpflichtung zur Aktualisierung digitaler Produkte – also Software —, da diese nur den Vertrieb erfasst[7]. In jedem Fall müsste die Gesetzeslage für diese Fälle die Datenschutzaufsichtsbehörden als unterstützende Institutionen bedingen. Dafür spricht der Warnmechanismus bei einer Beeinträchtigung der technischen – und personenbezogene Daten verarbeitenden – Infrastruktur gem. Art. 33 Abs. 1, 34 Abs. 1 DSGVO. Die Meldung gegenüber der Datenschutzbehörde dient jedoch nicht dazu, diese als universelle Meldestelle für IT-Sicherheitslücken zu erheben; vielmehr bezweckt sie die effektive Aufsicht und Durchsetzung der Betroffenenrechte.[8] Der Aufgabenkatalog des Art. 57 Abs. 1 DSGVO benennt diese ebenso wenig: Die Formulierung „jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten erfüllen" (Art. 57 Abs. 1 lit. v DSGVO) darf nicht als offene Generalklausel zur Aufgabenerfindung dienen, sondern bedarf einer hinreichenden Nähe zum behördlichen wie kodifizierten Tätigkeitsumfang. Völlig ausgeschlossen ist der Bezug der behördlichen Tätigkeit zur IT-Sicherheit bei der stetigen Einbeziehung technischer und organisatorischer Maßnahmen (TOM) aber nicht.[9] Entfernt wäre denkbar, das Beschwerderecht des Art. 77 Abs. 1 DSGVO zu nutzen, sofern die gefundene IT-Sicherheitslücke auf die mangelhafte Umsetzung der TOM i.S.d. Art. 25, 32 DSGVO hindeutet. Grundlage hierfür ist aber die eigene Betroffenheit der Melder:in bzw. Finder:in.[10] Ob trotz der gesetzlichen Regelung eines Rückkanals auch eine anonyme Beschwerde möglich ist, bleibt von der Notwendigkeit für die Prüfung der Beschwerde abhängig.[11] Im Umkehrfall könnte ein zufälliger Fund oder ein Eindringen in die Infrastruktur im Rahmen der Forschung als Gefahr für die personenbezogenen Daten wahrgenommen werden – dann würde sich das ehrbare Verhalten der Finder:in/Melder:in gegen sie selbst richten.

Im Ergebnis scheint es daher naheliegend, nicht auf die Datenschutzbehörden für die Errichtung der MKS zurückzugreifen; der gesetzliche Rahmen deckt dies aus dargelegten Gründen nicht hinreichend ab. Hinzu kommt die Differenzierung von Datenschutz und IT-Sicherheit: Die IT-Sicherheit dient u.a. auch dem Datenschutz, aber nicht allein. Zu schützen sind entsprechend gefährdete Produkte allgemein, unabhängig ihrer Verarbeitung personenbezogener Daten. Ansatzpunkt unter der aktuellen Rechtslage bliebe daher das BSI.

---

[7] Vgl. zum Anwendungsbereich § 327 BGB.

[8] ErwGr 85 S. 1 DSGVO.

[9] Hierzu im Detail *Hansen*, DuD 2021, 234 (235 f.).

[10] Statt vieler *Boehm*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 77 DSGVO, Rn. 5.

[11] *Bergt*, in: Kühling/Buchner, DS-GVO, Art. 77, Rn. 13.

III. Ziel: Ausgleich kollidierender Interessen

Finder:innen von Sicherheitslücken können Dienstleister der Verantwortlichen und/oder Produktnutzenden[12] oder IT-Sicherheitsforscher:innen, aber auch Personen sein, die zufällig auf diese etwa bei der Benutzung von Hard- und Software oder (Internet-)Diensten stoßen. Von ihnen sind bloße Melder:innen zu unterscheiden, die die Sicherheitslücke bei der geeigneten Stelle einreichen – diese können, müssen aber nicht personenidentisch mit den Finder:innen sein.[13] Sie verfolgen ein redliches, gesamtgesellschaftlich förderungswürdiges Ziel, wenn sie die Beseitigung von Sicherheitslücken vor allem zur Erhöhung der (eigenen und/oder fremden) IT-Sicherheit erreichen wollen. Vermieden werden soll hingegen, dass Sicherheitslücken in die Arsenale etwa von Geheimdiensten, Sicherheitsbehörden aber auch von Kriminellen zur Entwicklung von Exploits eingehen, nicht beseitigt und somit für eine unabsehbare Zeit ausgenutzt werden können. Gerade bei bislang (vermeintlich) unbekannten Sicherheitslücken (sog. „Zero-Days") besteht bei Einschaltung der Verantwortlichen die Hoffnung auf zügige Behebung. Mit der Kontaktaufnahme gilt es eine Vertrauensbasis zu schaffen und so einen einvernehmlichen Prozess auf Augenhöhe ohne unrealistische Erwartungen an das Gegenüber zu gestalten. Dabei sind auch die Hürden durch Unerfahrenheit, unterschiedliche (technische) Kenntnisse oder verschiedene Fach-/Muttersprachen der Beteiligten zu bewältigen. Hinzu treten technische Probleme etwa bei der Etablierung sicherer Kommunikationskanäle oder von Feedback-Schleifen bei Rückfragen bzw. Zusammenarbeit zum Ausräumen der Sicherheitslücken. Damit entsprechende Probleme und resultierende Konflikte nicht in jedem Fall von neuem entstehen und ausgeräumt werden müssen, bietet sich eine zentrale Stelle mit Erfahrung, Know-How und Akzeptanz unter den Beteiligten an.[14]

1. Interessen der Finder:innen von Schwachstellen

Finder:innen wird es zentral darum gehen, die Sicherheitslücken beseitigen zu lassen, um die IT-Sicherheit zu verbessern und andere vor Schäden zu bewahren. Bei selbst

[12] Siehe bspw. im Fall einer Hausdurchsuchung nach Meldung Tremmel, golem.de vom 14.10.2021 – abrufbar unter https://www.golem.de/news/nach-datenleck-hausdurchsuchung-statt-dankeschoen-2110-160269.html.

[13] Die Finder:in kann sich aus verschiedensten Gründen einer Melder:in als Mittler:in bedienen (etwa Wahrung der eigenen Anonymität, besseres Kommunikationsvermögen der Melder:in, hohes Ansehen der Melder:in am Markt; Expertise/Erfahrung der Melder:in).

[14] In der Forschung deuten erste empirische Erkenntnisse darauf hin, dass der Einbezug von Koordinierungsstellen wie das CERT/CC zu einem schnelleren Patchen beiträgt: Arora/Krishnan et al. (2005). An empirical analysis of vendor response to disclosure policy. The 4th annual workshop on economics of information security (WEIS05). Harvard University.

oder von der eigenen Organisation genutzter Hard-/Software ist ein weiteres Ziel die Produktverbesserung. Finder:innen haben ggf. nicht unerheblichen Aufwand samt entsprechendem Fachwissen in ihre Untersuchungen fließen lassen. In diesem Falle besteht ggf. der Wunsch nach Anerkennung, insbesondere da die wertvollen Ergebnisse den Produktverantwortlichen kostenlos und initiativ zur Verfügung gestellt werden. Gerade auch wegen des letzten Punktes wollen Finder:innen und (ggf. personenverschiedene) Melder:innen keiner zivil- und strafrechtlichen Inanspruchnahme ausgesetzt werden.[15] [16] Wie bereits in Kapitel 1 gezeigt, sind Erwartungen und Interessen durchaus heterogen – grundlegend ist daher die Koordination in Form von Kommunikation. Eine technisch qualifizierte, verantwortungsbewusste und an Kommunikation auf Augenhöhe interessierte Ansprechpartner:in aufseiten der Produktverantwortlichen erlaubt vertrauensvolle Zusammenarbeit und reduziert den weiteren eigenen Aufwand sowie die Gefahr von (technischen) Missverständnissen oder frustrierten Erwartungen.

2. Interessen der IT-Sicherheitsforscher:innen

Neben den gleich gelagerten Interessen der Finder:innen verfolgen IT-Sicherheitsforscher:innen meist das Ziel, die Früchte ihrer Arbeit durch wissenschaftliche Veröffentlichungen zu ernten. Die Möglichkeit dazu sollte ihnen spätestens nach Beseitigung der Sicherheitslücke eingeräumt werden, auch um Lernmöglichkeiten und Innovation zu fördern, sowie Hersteller:innen, Betreiber:innen und Nutzer:innen von (unsicherer) IT für Risiken zu sensibilisieren. Gerade IT-Sicherheitsforscher:innen wünschen keine Verwertung von Sicherheitslücken zu illegalen oder unethischen Zwecken. Vielmehr soll Wissen um sie möglichst geteilt werden, um sie in Zukunft zu vermeiden. Dafür wünschen sich die IT-Sicherheitsforscher:innen ein technologieoffenes und nicht durch rechtliche Hürden und Bedrohungen versperrtes Forschungsumfeld sowie die Entwicklung einer Fehlerkultur.

---

[15] Siehe bspw. die Reaktionen auf die Strafanzeige gegenüber einer Melder:in: *Wolfnagel*, Zeit vom 05.08.2021 – https://www.zeit.de/digital/datenschutz/2021-08/cdu-connect-app-it-sicherheit-lilith-wittmann-forscherin-klage; *Hurtz*, Süddeutsche vom 05.08.2021 – https://www.sueddeutsche.de/politik/cdu-connect-anzeige-wittmann-1.5373488; *Reuter*, Netzpolitik.org vom 04.08.2021 – https://netzpolitik.org/2021/cdu-connect-berliner-lka-ermittelt-gegen-it-expertin-die-sicherheitsluecken-in-partei-app-fand; *Holland*, heise vom 04.08.2021 – https://www.heise.de/news/Sicherheitsluecken-in-CDU-connect-App-Strafverfahren-gegen-Entdeckerin-6154663.html.

[16] Siehe bspw. die Reaktionen auf die Strafanzeige gegenüber einer Melder:in: *Wolfnagel*, Zeit vom 05.08.2021 — https://www.zeit.de/digital/datenschutz/2021-08/cdu-connect-app-it-sicherheit-lilith-wittmann-forscherin-klage; *Hurtz*, Süddeutsche vom 05.08.2021 — https://www.sueddeutsche.de/politik/cdu-connect-anzeige-wittmann-1.5373488; *Reuter*, Netzpolitik.org vom 04.08.2021 — https://netzpolitik.org/2021/cdu-connect-berliner-lka-ermittelt-gegen-it-expertin-die-sicherheitsluecken-in-partei-app-fand; *Holland*, heise vom 04.08.2021 — https://www.heise.de/news/Sicherheitsluecken-in-CDU-connect-App-Strafverfahren-gegen-Entdeckerin-6154663.html.

3. Interessen der Wirtschaft

Die Wirtschaft, seien es IT-Unternehmen oder Unternehmen mit IT, ist grundsätzlich an der Verbesserung der eigenen IT-Sicherheit sowohl bezüglich der von ihnen hergestellten Produkte, wie auch als Nutzende und Betreibende von Produkten interessiert.[17] Dabei besteht vielfach Unsicherheit insbesondere wegen fehlender Standards und Messbarkeiten, aber auch im kommunikativen, technischen und juristischen Umgang mit Sicherheitslücken. Die Produktverantwortlichen als Empfänger haben das berechtigte Interesse die Meldung zu evaluieren, um herausfinden zu können, ob überhaupt eine (ausnutzbare) Sicherheitslücke und wenn ja mit welcher Kritikalität vorliegt. Bei Existenz einer solchen sollte eine angemessene Zeitspanne zur Entwicklung und zum Ausrollen technischer Lösungen eingeräumt werden, um Risiken eines Full Disclosure (Veröffentlichung ohne vorher veröffentlichen Patch oder Mitigation)[18] zu vermeiden. So kann der Missbrauch der Sicherheitslücke ggf. verhindert und die Sicherheit des Produkts verbessert werden.

Im Hinblick auf einen Ausgleich unterschiedlicher Interessen im Rahmen des Umgangs mit Sicherheitslücken sind aus rechtlicher Hinsicht die mit Sicherheitslücken verbundenen Haftungsrisiken zu bedenken.[19] Hierbei unterscheiden sich wie in Kapitel 2 gezeigt die Rahmenbedingungen je nachdem, ob es sich um den B2C oder B2B-Bereich handelt. Ein erfolgreicher CVD-Prozess vermeidet im besten Fall bereits die Entstehung von Schäden durch Sicherheitslücken, welche für das verantwortliche Unternehmen in Kostenbelastung durch Sanktions-, Haftungs- und Reputationsrisiken münden können. Meldungen von Schwachstellen stellen sich gewissermaßen als „Geschenk" dar, welches zu Gunsten bedrohter Kund:innen wie auch des eigenen Unternehmens schnellstmöglich als solches angenommen und in sicherheitsfördernde Problemlösungen umgesetzt werden sollte.[20] Erfolgt dies nicht, bleibt es aufgrund fehlender Rechtspflichten insbesondere im Hinblick auf die Aufrechterhaltung der Produkt- bzw. Sys-

---

[17] Laut BSI ist und bleibt der Umgang mit Schwachstellen eine der größten Herausforderungen der Informationssicherheit: *BSI*, Die Lage der IT-Sicherheit in Deutschland 2021, S. 87. Im Allianz Risk Barometer – Identifying the major Business Risks for 2021, stuften Unternehmen Cyber Incidents auf Rang 3 der bedeutendsten Unternehmensrisiken nach Betriebsunterbrechung und Pandemien ein: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2021.pdf.

[18] Zum Full Disclosure Whitepaper zur Rechtslage der IT-Sicherheitsforschung 2021, S. 29.

[19] Siehe Kapitel 2 Abschnitt II.

[20] Diese Sichtweise vertritt die Mehrzahl der befragten IT-Expert:innen im Rahmen der Studie: Kennedy, in: 451 Research, Black & White Paper, Exploring Coordinated Disclosure, S. 4 ff. Die Befragten mussten allerdings mit den Modellen zur Offenlegung von Schwachstellen durchschnittlich bis gut vertraut sein, um teilnehmen zu können. Es ist daher nicht auszuschließen, dass Unternehmen mit geringeren Erfahrungen zum CVD andere Antworten geben könnten.

temsicherheit allerdings oftmals bei bloßen Reputationsschäden für betroffene Unternehmen. Eine Veröffentlichung kann daher auch gerade nicht im Interesse der Wirtschaft sein. Insofern kann aus den Haftungsrisiken nicht zwangsläufig für die gesamte Wirtschaft geschlussfolgert werden, dass tatsächlich stets ein (wirtschaftliches) Interesse an der Offenlegung von Sicherheitslücken besteht.

4. Interessen der Allgemeinheit

Es liegt im gesamtgesellschaftlichen Interesse zur Erhöhung der IT-Sicherheit als Gemeinwert die Zahl der offenen Schwachstellen zu verringern und dauerhaft so gering wie möglich zu halten. Dies dient etwa dem digitalen Staats- und Zivilschutz, dem Schutz von Wirtschaft und Verbraucher:innen sowie der internationalen Friedenssicherung. Vor diesem Hintergrund sind das Geheimhalten und Horten von Schwachstellen samt des Risikos eines Abflusses entsprechender Informationen etwa an Kriminelle und fremde Staaten unerwünscht. Erreicht werden kann dies durch Anreize zur schnellstmöglichen Meldung und Beseitigung von Schwachstellen unter dem Leitgedanken des guten Samariters mit entsprechender Wertschätzung insbesondere der Melder:innen. Nachhaltigkeit wird ergänzend zu individuellen Schutzmaßnahmen u.a. durch kontinuierliches Monitoring von privat wie staatlich eingesetzter IT seitens unabhängiger und mit ausreichend finanziellen Mitteln versehener IT-Sicherheitsforschung erreicht. IT-Sicherheitsforschung und die Meldung von Schwachstellen sind dabei Motoren zur Vermeidung bzw. Minimierung externalisierter Schadenrisiken und Informationsasymmetrien, zur Steigerung des entsprechenden Wissens als Bildungsgrundlage sowie zur Etablierung einer Fehlerkultur für IT-Sicherheit. Dies erzeugt bzw. stärkt das Vertrauen in digitale Produkte (made in Germany) sowie in digitale Infrastruktur und Technik in Deutschland, Europa und der Welt.

IV. Anforderungen an eine Melde- und Koordinierungsstelle

Die Meldung einer Sicherheitslücke an die Produktverantwortlichen mag auf den ersten Blick trivial erscheinen, die in Kapitel 1 genannten praktischen Probleme führen aber zu einem nicht zu unterschätzenden Aufwand. Die Etablierung eines standardisierten Prozesses kann hier Abhilfe schaffen, indem er Melder:innen und Produktverantwortliche beim Coordinated-Disclosure-Verfahren unterstützt sowie Planungssicherheit, Verlässlichkeit und Transparenz schafft. Weiterhin kann er Rechtssicherheit

und Rechtsklarheit stärken, bspw. im Hinblick auf allgemein anerkannte Fristen.[21] Die Melde- und Koordinierungsstelle (MKS) muss eine kurzfristige Erreichbarkeit gewährleisten, um auch z.B. an Feiertagen auf (kritische) Sicherheitslücken schnell reagieren zu können.

1. Funktionale Anforderungen

Der Prozess sollte sich dabei an den folgenden Schritten orientieren:

1. Entgegennahme der Meldung von der Melder:in
2. Prüfung der Meldung auf Plausibilität (s.u.)
3. (Ggf.) Klärung von Unklarheiten in der Meldung
4. Identifikation der Produktverantwortlichen und ggf. dazugehörigen Ansprechpartner:innen
5. Übermitteln der Informationen zur Sicherheitslücke an die Produktverantwortlichen
6. (Ggf.) Herstellung eines sicheren Kommunikationskanals zwischen Melder:in und Produktverantwortlichen
7. Nach Fristablauf: Veröffentlichung der Informationen zur Sicherheitslücke (ggf. in Absprache mit der Melder:in)
8. (Ggf.) Löschkonzept bezüglich der Details zur Sicherheitslücke und rechtlich geschützter Daten

Abhängig von der Art der jeweiligen Sicherheitslücke und den Anforderungen der Melder:in muss der Prozess mehrere Gestaltungsoptionen vorsehen. Die folgenden Anforderungen muss der Prozess erfüllen:

a) Option zur anonymen Meldung

Die Melder:in kann die Meldung wahlweise unter Angabe des Klarnamens samt Kontaktdaten oder anonym abgeben. Die Melder:in kann Merkmale hinterlegen, mit denen sie sich auch nachträglich einseitig als Melder:in authentisieren bzw. das Einreichen nachträglich beweisen kann. Dies können Benutzername und Passwort sein, oder der öffentliche Schlüssel zu einem kryptografischen Schlüsselpaar, zu dem sie den privaten

[21] Vgl. die unterschiedlichen Ansätze bei CERT, Vulnerability Disclosure Policy, FAQ – abrufbar unter: https://vuls.cert.org/confluence/display/Wiki/Vulnerability+Disclosure+Policy; Project Zero – abrufbar unter: https://googleprojectzero.blogspot.com/2015/02/feedback-and-data-driven-updates-to.html; 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; *Shepherd*, How do we define Responsible Disclosure?, SANS Institute Information Security Reading Room (2003), S. 9.

Schlüssel kennt. Durch diese Optionen ergeben sich drei Arten von Kommunikationskanälen:

- Mit Klarnamen und bidirektional: die Melder:in kann sich gegenüber der MKS als Melder:in der betroffenen Lücke authentisieren und (weitere) Informationen mitteilen; die MKS kann die Melder:in kontaktieren und antworten.
- Anonym und bidirektional: die Melder:in kann sich gegenüber der MKS als Melder:in der betroffenen Lücke authentisieren und (weitere) Informationen mitteilen; die MKS kann Rückfragen und Informationen für die Melder:in verschlüsselt hinterlegen, die Melder:in aber nicht aktiv kontaktieren.
- Anonym und einmalig: die Melder:in kontaktiert die MKS anonym und hinterlegt lediglich Informationen bzgl. der Sicherheitslücke. Die MKS kann die Melder:in nicht kontaktieren und nicht antworten.

Die Option zur anonymen Meldung ist technisch so auszugestalten, dass die Melderin:in durch technische Maßnahmen vor einer De-Anonymisierung geschützt ist, beispielsweise durch das Anbieten eines Meldeinterfaces über das TOR-Netzwerk. Technische Lösungen sind bereits vorhanden und werden beispielsweise für die sichere Kommunikation zwischen Journalist:innen und deren Quellen (z.B. Whistleblower) verwendet.[22]

In jedem Fall wird einer Meldung eine eindeutige ID zugewiesen, die der Melder:in mitgeteilt wird und als Referenz für weitere Kommunikation aller beteiligten Parteien dient.

Die Option zur anonymen Meldung senkt die Hürde, eine Sicherheitslücke zu melden. Finder:innen, die sich bei der Entdeckung einer Sicherheitslücke ggf. strafbar gemacht haben (könnten), oder Angst vor zivilrechtlichen Konsequenzen haben, können so trotzdem Sicherheitslücken melden. Die große Spanne der Möglichkeiten von einfachen Meldungen unter Klarnamen bis hin zu kryptografisch gesicherten anonymisierten Meldungen deckt die Interessenlagen des gesamten Spektrum der von potenziellen Melder:innen gewünschten Optionen ab. Insbesondere die Akzeptanz des Meldeverfahrens bei sehr sicherheitsbewussten und IT-affinen Personen ist für den Erfolg maßgeblich.

Auch bei Meldungen mit Klarnamen, muss die MKS die Möglichkeit bieten, auf Wunsch der Melder:in, deren Identität gegenüber der Produktverantwortlichen zu Beginn oder dauerhaft geheim zu halten. Dies kann insbesondere dann notwendig sein, wenn (unberechtigte) Rechtsstreite oder Einschüchterungsversuche von Seiten der Produktverantwortlichen befürchtet werden. Um dies zu gewährleisten, darf die MKS auch nicht einer behördlichen Ermittlungs- oder Anzeigepflicht unterliegen und muss

[22] Siehe z.B. „SecureDrop“.

für die relevanten Themen (z.B. Computerstrafrecht, Urheberrecht) von der Pflicht zur Übermittlung der Daten an Ermittlungsbehörden entbunden werden.

b) (Mindest-)Umfang einer Meldung und Standardisierung

Welche Informationen im Rahmen der Meldung von Sicherheitslücken erforderlich sind, ist inzwischen recht gut erforscht. Es existieren mehrere Empfehlungen.[23]

Da die Ausgestaltung eines standardisierten Meldesystems den Meldeprozess strukturell vorgibt, sollten sämtliche Herausforderungen im Vorhinein bedacht werden. Eine davon stellt die Meldung von umfangreichen Datensätzen aus automatisierten Massenscans dar.[24] Eine öffentliche Anwendungsschnittstelle (API) würde einen solchen Meldeprozess erleichtern. Webformulare, bei denen jede Schwachstelle einzeln eingetragen werden müssten, würden hingegen die Einreichung (auch ungefilterter) Massendaten effektiv verhindern, da der Aufwand einer manuellen Übernahme seitens der Meldenden kaum handhabbar wäre. Hierbei ist zu bedenken, dass IT-Sicherheitsforschende insbesondere im akademischen Umfeld, z.B. im Rahmen einer Promotion, bereits einer erheblichen Arbeitsbelastung unterliegen, und die verfügbare Kapazität für Meldeprozesse entsprechend begrenzt ist. Zu hohe Hürden, gerade im Bereich von Massendaten, können dazu führen, dass Lücken – obwohl bekannt –, nicht mehr gemeldet werden.

Gleichzeitig verlagert die Auswahl an Pflichtfeldern den Aufwand zwischen Melder:in und Meldestelle. Ist beispielsweise eine erste Abschätzung zur Kritikalität, z.B. mittels CVSS-Scores erforderlich, muss die Melder:in diese Daten erst erarbeiten. Dies erleichtert jedoch die Priorisierung auf Seiten der Meldestelle. Hierbei ist zu bedenken, dass auch standardisierte Metriken wie CVSS auf dem aktuellen Wissensstand zu einer Schwachstelle basieren, und oftmals Schätzungen über das Risiko erforderlich machen[25]. Somit bleibt es eine offene Frage, ob und in welchem Ausmaß sich die Meldestelle auf die Einschätzungen der Meldenden verlassen sollte.

Sinnvoll wäre eine standardisierte Erfassung der betroffenen Software, damit durch die Meldenden in einer einheitlichen Taxonomie Hersteller:in, Produkt und Version

---

[23] CERT Guide to CVD (https://vuls.cert.org/confluence/display/CVD): Unter 4.3. zu Risiko (Validation and Triage), bezieht sich aber hauptsächlich auf CVSS, Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure (https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.1). Verschiedene Varianten von komplexen, multi-party Disclosure (Users do not deploy remediation immediately...) UK National Cyber Security Centre – Guidance Vulnerability Management – https://www.ncsc.gov.uk/guidance/vulnerability-management.

[24] Für eine ausführliche Darstellung siehe Kapitel 4.

[25] Der von manchen Organisationen vertretene Ansatz, CVSS-Scores rein nach technischer Art der Schwachstelle (z.B. SQL Injection) zu vergeben, bildet nur einen Teil der Metrik ab (Base Score) und ist mit Verweis auf die Gewichtung, z.B. des Environmental Scores in der CVSS-Formel, abzulehnen.

angegeben werden. Betrachtet die Meldestelle alle Meldungen zu einem Produkt gemeinsam, reduziert dies den Aufwand für die manuelle Erkennung doppelter oder ähnlicher Meldungen.

Eine Integration in bestehende Schwachstellendatenbanken wie CVE ist dabei anzuraten, da CVE-Nummern international anerkannt werden. Zudem können CVE-Nummern gleichzeitig als Eingabe für Prüfungen dienen, mit denen Unternehmen bekannte Schwachstellen bei sich identifizieren können, z.B. die Nutzung von veralteten Softwareversionen mit bekannten CVE-Einträgen.

c) Meldung ohne Details

Es ist im Normalfall nicht notwendig, dass die MKS alle (technischen) Details einer Sicherheitslücke durch eine Meldung erhält. Insbesondere bei besonders kritischen Sicherheitslücken kann es auf Basis des Need-to-Know-Prinzips sinnvoll sein, die Details der MKS nicht zukommen zu lassen, sondern lediglich Hilfe beim Kontaktaufbau oder bei der Kommunikation mit den Produktverantwortlichen anzufordern. Die MKS benötigt dann nur so viele Details, dass eine grundlegende Prüfung (siehe nächste Anforderung) möglich ist. Der MKS keine Details melden zu müssen, ermöglicht es auch Melder:innen, die der Stelle gegenüber wenig Vertrauen haben, Sicherheitslücken über diese abzuwickeln. Je mehr Details über Sicherheitslücken bei der MKS liegen, umso höher ist das Risiko, dass die MKS selbst zu einem lukrativen Angriffsziel wird und hierdurch Sicherheitslückenmeldungen und Details frühzeitig bekannt werden. Details, die der MKS nicht vorliegen, können in diesem Fall nicht an unbefugte Dritte gelangen.

d) Prüfung der Meldung

Vor der Weiterverarbeitung muss die MKS die Meldung auf Plausibilität prüfen. Für diese Prüfung muss sie nicht alle Details einer Sicherheitslücke vollumfänglich nachvollziehen können. Bei besonders komplexen Sicherheitslücken wird dies auch regelmäßig aus technischen Gründen nicht möglich sein. Die Prüfung kann anhand der technischen Beschreibung der gemeldeten Lücke erfolgen. Außerdem können die Angaben zur Person der Melder:in in die Prüfung einbezogen werden. Gegebenenfalls können Rückfragen an die Melder:in gestellt werden. Offensichtlich unplausible Meldungen werden nach diesem Schritt verworfen. Dies wird an die Melder:in zurückgemeldet, oder, bei einer anonymen Meldung, die ID der Meldung mit dem Hinweis, dass sie verworfen wurde, veröffentlicht um die Melder:in zu informieren.

e) Bereitstellen von sicheren Kommunikationskanälen

Für die Kontaktaufnahme der Melder:in mit der MKS, stellt die MKS geschützte Kommunikationskanäle zur Verfügung, die entsprechend den Anforderungen auch anonym genutzt werden können. Hierfür kommen insbesondere das TOR-Netzwerk sowie Dienste wie SecureDrop in Betracht. Für Produktverantwortliche, die die üblichen sicheren Kanäle, wie z.B. S/MIME oder PGP geschützte E-Mails nicht unterstützen, stellt die MKS geeignete Kanäle zur Verfügung.

Um es der Produktverantwortlichen zu ermöglichen, technische Rückfragen an die Melder:in zu stellen, stellt die MKS direkt Kommunikationskanäle zwischen Melder:in und der Produktverantwortlichen zur Verfügung. Je nach Anforderung der Melder:in laufen diese über die MKS oder direkt zwischen der Produktverantwortlichen und der Melder:in. Die Kommunikationskanäle sind Ende-zu-Ende gesichert, die MKS wird nur auf expliziten Wunsch der Melder:in oder der Produktverantwortlichen in die Kommunikation mit einbezogen. Dabei wird die Forward-Secrecy der bisherigen Kommunikation gewahrt. Allerdings kann es hierfür auch genügen, die Melder:in bei der Identifikation der Ansprechpartner:in bei der Produktverantwortlichen zu unterstützen.

Ebenso erwarten gerade Forscher:innen für ihre unentgeltliche Meldung oftmals eine immaterielle Kompensation, z.B. durch Namensnennung (teilweise unter Pseudonym). Dies kann durch Hersteller:innen als Danksagung auf der Webseite erfolgen, z.B. als Liste der „besten" Einreichenden, oder durch Nennung in den Schwachstelleninformationen für die eigenen Kund:innen. Eine entsprechende „Hall of Fame" ist auch bei der Meldestelle denkbar. Gerade im Bereich der Softwaresicherheit sind entsprechende Referenzen relevant für die Publikation von wissenschaftlichen Arbeiten, sei es als Beleg für mit dem neuen Ansatz gefundene Schwachstellen, oder für die Effektivität der eigenen Arbeit bei Bewerbungen.

f) Vermittlung bei Streit

Die MKS kann bei Streitigkeiten zwischen Melder:in und der Produktverantwortlichen angerufen werden und vermittelt dann zwischen beiden. Dabei sind ein etwaiges Ungleichgewicht der beiden Positionen – z.B. unternehmerischer Reputationsschutz versus altruistische Interessen der Melder:in – sowie der gesellschaftliche Nutzen der Forschung besonders zu berücksichtigen. Ein möglicher und in der Praxis oft vorkommender Streitpunkt ist die Fristsetzung für die Veröffentlichung einer Sicherheitslücke. Da Kritikalität sowie technische Details für die Fristsetzung eine entscheidende Rolle spielen, kann die MKS nur als vermittelnde Instanz agieren und Lösungen vorschlagen. Eine Fristsetzungskompetenz der MKS sollte nicht vorgesehen werden.

Für den Fall einer juristischen Auseinandersetzung soll das Verhalten von Melder:in und Produktverantwortlicher belastbar dokumentiert werden. Dafür gibt die MKS z.B. für die Einreichung einer Meldung eine Quittung aus. Diese Quittung lässt sich über kryptografische Hashverfahren und eine digitale Signatur der MKS eindeutig den übermittelten Inhalten samt Zeitstempel zuordnen und ist fälschungssicher. Somit kann die Melder:in selbst dann noch ihre Kommunikation zweifelsfrei belegen, wenn die MKS die entsprechenden Daten bereits gelöscht hat. Im Einzelfall könnte die MKS auch als neutrale Zeugin auftreten und Angaben zum Ablauf des Verfahrens machen und somit helfen, eine Aussage-gegen-Aussage Situation zu klären.

2. Nicht-funktionale Anforderungen

Ferner sind nicht-funktionale, organisatorische bzw. institutionelle Anforderungen an die Melde- und Koordinierungsstelle zu erörtern.

a) Zentrale oder dezentrale Struktur

Die Vermittlung zwischen Melder:in und Produktverantwortlichen bei Sicherheitsmeldungen könnte durch eine einzelne, zentrale Anlaufstelle organisiert werden oder geeignete, dezentrale Stellen könnten sich bspw. als Nebenaufgabe im Wege einer Zertifizierung bzw. Akkreditierung als MKS etablieren. Vorteile eines zentralen Ansprechpartners lägen in einer einfacheren Möglichkeit, einen standardisierten, transparenten Meldeprozess sowie standardisierte Formulare bereitzustellen. Dies könnte bei dezentralen Strukturen aufwendiger ausfallen. Bei dezentralen Strukturen könnte dagegen die Expertise bspw. aus der Forschung eingebracht und Aufgaben auf viele Schultern verteilt werden. Nachteile wären dagegen die schwierigere Standardisierung sowie die Gefahr der Voreingenommenheit, wenn die Stelle einer bestimmten „Seite“ (Forschung/Industrie/Verwaltung) zugehörig ist. Bei dezentralen Stellen ist darüber hinaus ein deutlich höherer Koordinationsaufwand zur Vernetzung und des Datenaustauschs zwischen den Stellen selbst notwendig, um eine mit einer zentralen Stelle vergleichbare Leistung bereitstellen zu können. Dies gilt auch für die internationale Vernetzung. Potenzielle Probleme einer zentralen Stelle hingegen sind neben der Überforderung durch zu viele Meldungen, die Gefahr einer zentralen Sammlung von Sicherheitslücken sowie ein Single-Point-of-Failure, womit neue Sicherheitsrisiken entstehen könnten im Hinblick auf die Attraktivität für illegale Zugriffsversuche von außen wie auch die Weiternutzung von Daten für sachfremde Zwecke. Insofern ist die organisatorische Ansiedelung als auch die konkrete Ausgestaltung für die Akzeptanz und damit die Unterstützungswirkung entscheidend.

Im Hinblick auf die beschriebenen funktionalen Anforderungen wären beide Konzepte durchaus realisierbar. Daher soll zunächst auch in praktischer Hinsicht erörtert

werden, bei welchen bereits existenten Stellen eine organisatorische Ansiedlung denkbar oder ausgeschlossen wäre.

b) Organisatorische Ansiedelung

In der wissenschaftlichen Diskussion[26] stellt die Unabhängigkeit der Meldestelle den wesentlichen Vertrauensanker dar. Ohne ihn erscheint die Ausrichtung der Stelle allein auf die Beseitigung von Schwachstellen nicht sichergestellt. Vorbild ist insoweit das Modell der Datenschutzaufsichtsbehörden, die gemäß der Vorgabe des Art. 52 Abs. 1 DSGVO unabhängig von staatlicher Beeinflussung zu sein haben. Ihre Begründung findet sie vor allem darin, die Betroffenenrechte und damit (Unions-)Grundrechte der Art. 7, 8 EU-GrC sowie Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG zu gewährleisten bzw. durchzusetzen. Entsprechend benennt Art. 8 Abs. 2 EU-GrC ausdrücklich die Unabhängigkeit dieser Stelle. Würde man diese Behörden in einem bestimmten Lager verorten wollen, so wäre dieses das der Betroffenen – ggf. als Verbraucher:innen. Seiner Natur nach vorwiegend für die IT-Sicherheit des Bundes zuständig, untersteht das BSI jedoch wie erläutert dem Bundesministerium des Innern (BMI) und damit entsprechender Kontrolle in der Tätigkeit – z.B. mittels Weisungsbefugnis (Art. 65 S. 2 GG). Ersichtlich wird diese Abhängigkeit auch in der Ausstattung der Behörde durch das BMI und auf Basis der Berichtspflichten des § 13 BSIG. Ebenfalls dem BMI unterstellt sind u.a. Bundespolizei, BKA und Bundesamt für Verfassungsschutz. Diese Verbindung erzeugt unauflösliche Interessen- und Zielkonflikte, denn für diese Behörden stellt die Ausnutzung von Schwachstellen ein wichtiges Mittel zur Erstellung von Werkzeugen zur Aufgabenerfüllung insbesondere in den Bereichen Nachrichtengewinnung und Telekommunikationsüberwachung dar.[27] Ferner richtet sich die finanzielle Ausstattung der Behörden nach dem zugeordneten Bundesministerium und dessen Haushaltsführung; hier haben die Bundesminister:innen entsprechend ihrer Ressortkompetenz gem. Art. 62, 65 S. 2 GG ausreichend Spielraum hinsichtlich Sach-, Organisations-, Personal- und Haushaltsfragen.[28] Insofern ist nicht abzustreiten, dass die personelle/finanzielle Ausstattung der Behörde im Ermessen der Bundesminister:in und damit in einem Abhängigkeitsverhältnis resultiert. Dieser Umstand wurde bereits im Hinblick auf die Kon-

[26] *Kipker/Scholz*, DuD 2021, 40 (44); *Schallbruch*, DuD 2021, 229 (231 ff).
[27] BVerfG NJW 2021, 3033 (Rn. 42 f).
[28] Vgl. *Epping* in: Epping/Hillgruber, BeckOK GG, Art. 65, Rn. 6.

zeptionierung eines dem THW nachempfundenen Cyber-Hilfswerks (CHW) kritisiert.[29] Insofern könnte die Etablierung einer rein defensiven Cybersicherheitsstrategie Mitvoraussetzung für ein aktives Mitwirken ehrenamtlich Engagierter werden.[30]

Organisatorisch bedarf es daher einer eigenständigen, vom Ministerialapparat der Art. 62, 65 S. 2 GG losgelösten Institution. Innerhalb der EU findet sich kein ähnliches Modell, das die aufgezeigten Ansätze aufgreift – wenngleich z.B. die Nationale Behörde für Cybersicherheit in Holland zumindest Leitlinien für CVD-Prozesse formuliert.[31] Zum Zwecke einer harmonisierenden Wirkung empfiehlt sich, die MKS auf europäischer Ebene anzusiedeln. Hinsichtlich der CVD-Prozesse enthält Art. 6 NIS2-RL-Entwurf[32], bereits die Grundlagen hierfür. Parallel dazu bedarf es geeigneten Stellen auf mitgliedsstaatlicher Ebene, die im Fall von Deutschland allerdings nicht auf Ebene der Bundesländer angesiedelt werden sollten. Nicht nur spricht die Gefahr eines IT-sicherheitsrechtlichen Flickenteppichs dagegen, sondern auch die mangelnde Gesetzgebungskompetenz der Länder: Regelmäßig folgt die Regelung der IT-Sicherheit auf Bundesebene aus dem Recht der Wirtschaft gem. Art. 72, 74 Abs. 1 Nr. 11 GG unter Verweis auf die Wahrung der Rechts- und Wirtschaftseinheit gem. Art. 72 Abs. 2 GG.[33] Ansonsten könnte die bereits für die IT-Sicherheitsbehörden der Länder geschehene Verschmelzung mit dem Datenschutzbeauftragten ausgeweitet werden. Neue, in der Materie begründete Abhängigkeiten und Konflikte entstehen; eine Unabhängigkeit wäre auch dann nicht gewahrt. Weiterhin bestünde durch die einzelnen Regelungsniveaus der Länder die Gefahr eines Forum Shopping, das dem Ziel der Harmonisierung entgegenwirkt.

c) Ausrichtung auf defensive Sicherheit

Daneben ist hervorzuheben, dass eine unabhängige, staatlich finanzierte Stelle nicht das Sammeln von Sicherheitslücken parallel betreiben darf, um die Zielsetzungen des Meldeprozesses nicht zu konterkarieren. Ebenso ist zu befürchten, dass Tätigkeiten, die im Konflikt zur schnellstmöglichen Behebung von Sicherheitslücken stehen, zu einem Vertrauensverlust gegenüber Melder:innen wie auch Produktverantwortlichen führen

---

[29] AG KRITIS, Das Cyber-Hilfswerk, Version 1.0 – veröffentlicht am 07.02.2020, S. 23 f.

[30] Chaos Computer Club, Stellungnahme zum Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) Linus Neumann, 17. April 2015, S. 12 f.

[31] Siehe https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline.

[32] Zum Entwurf der Richtlinie: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72166.

[33] So zuletzt auch der Entwurf des IT-Sicherheitsgesetzes 2.0, S. 35 f - https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/it-sicherheitsgesetz.pdf;jsessionid=B341CA1BEEB88013EABD239BB4CFD401.1_cid295?__blob=publicationFile&v=2.

könnte. Die Funktion als Vermittler kann nur eine Vertrauensinstanz erfüllen, deren Aufgaben und Ziele nicht im Widerspruch stehen.

V. Fazit

Die Finder:innen von Sicherheitslücken haben aktuell das Problem, dass sie einen Weg zur Meldung an die richtigen Ansprechpartner:innen bei dem oder den Verantwortlichen finden müssen. Schon die Identifikation von Letzteren aber auch die Organisation sicherer Kommunikationswege und die Vermittlung der technischen Details bergen erhebliche Herausforderungen. Warum sollen die entsprechenden Hürden immer wieder neu gemeistert werden müssen? Es bietet sich die Schaffung einer Melde- und Koordinierungsstelle an, die Kontakte zu Produktverantwortlichen knüpft, aufrecht erhält und diese im konkreten Fall mit den Melder:innen verbindet. Eine solche MKS sollte den folgenden Anforderungen genügen:

Zuständigkeit und Organisation:
- Klare singuläre gesetzliche Aufgabenstellung (Beseitigung von Sicherheitslücken)
- Unabhängigkeit
- Schaffung von (sicheren) Kommunikationskanälen zwischen Melder:innen und Produktverantwortlichen
- Mediation im Konfliktfall: ggf. Vermittlung zwischen Melder:innen und Produktverantwortlichen in Konfliktfällen

Grundsatz der Freiwilligkeit:
- Einschaltung der MKS ist ebenso freiwillig wie das Mitwirken der Melder:in am weiteren Prozess mit dem oder den Produktverantwortlichen
- Schaffung von Anreizen für Coordinated Disclosure

Grundsatz der Vertraulichkeit:
- Im Rahmen der Meldeprozesse von der MKS gewonnene Erkenntnisse und Informationen werden nicht weitergegeben (es sei denn für den Disclosure-Prozess relevant, z.B. Veröffentlichung von Produktwarnungen)
- Geheimhaltung der Identität der Melder:in bei gewünschter Anonymität auch gegenüber Behörden.

Kapitel 4

Grenzen einer Meldestelle aus Praxissicht der Forschung

Nachdem in Kapitel 3 das Grobkonzept einer problemlösungsorientierten Meldestelle und entsprechender Meldewege skizziert wurde, widmet sich dieses Kapitel verbleibenden Herausforderungen beim Umgang mit Sicherheitslücken aus der Praxiserfahrung. Dabei wird zu zeigen sein, dass eine Meldestelle wie nach dem aufgezeigten Modell nicht als alleiniges Mittel zur Problemlösung dienen kann. Vielmehr sollten andere Mittel wie ein Rechtsrahmen für Hersteller:innen ergänzend hinzutreten.

I. Zahnloser Tiger: Schwachstellenmeldungen nach End-of-life

Das primäre Ziel der Coordinated Vulnerablity Disclosure sowie der Einrichtung einer Meldestelle ist die Behebung von Sicherheitslücken, was regelmäßig die Mitwirkung der Produktverantwortlichen bedingt. Eine offene Frage bleibt allerdings der Umgang mit Fällen, in denen eine Überarbeitung des fehlerbehafteten Produkts bzw. Systems nach dem Ende eines Produktzyklus‘ (sog. End-of-life) verweigert wird.

Beispiel: Nachdem ein Forscherteam des Fraunhofer SIT gravierende Sicherheitslücken im TwitterKit für iOS 3.4.2 fanden, warnten das Team davor, dieses und dessen ältere Versionen weiter zu benutzen und empfahlen das TwitterKit auszutauschen. Durch die Schwachstelle können Angreifer:innen über einen Man-in-the-middle-Angriff private Daten wie geschützte Tweets und Direktnachrichten fremder Twitter-Accounts einsehen oder im Namen der Nutzer:innen twittern, Tweets liken und retweeten. Darüber hinaus kann jede App angegriffen werden, die das schadhafte TwitterKit dafür nutzt, einen Login via Twitter anzubieten. Unter Ausnutzung der Verwundbarkeit[1] sind demnach Identitätsdiebstahl, Account-Missbrauch sowie Datenverluste möglich. Nach vertraulicher Information an Twitter wurde mitgeteilt, dass eine Schließung der Sicherheitslücke durch einen Patch nicht erfolgen wird, da der Support für den TwitterKit bereits Ende Oktober 2018 ausgelaufen sei. Beim TwitterKit für iOS 3.4.2 handelt sich um eine End-of-life-Softwarebibliothek von Twitter, die nicht mehr

[1] Technische Details zur gefundenen Sicherheitslücke finden sich unter www.sit.fraunhofer.de/cve.

aktualisiert wird, aber noch in Apps im Oktober 2019 zum Einsatz kam. Es wurden lediglich Alternativen benannt.[2] App-Entwickler:innen wurden dringend dazu aufgerufen, den TwitterKit für iOS-App-Entwicklungen nicht mehr einzusetzen und in bestehenden Apps durch Alternativen zu ersetzen.

Dieses Beispiel TwitterKit zeigt exemplarisch die Problematik von End-of-life auf. Hersteller:innen sehen sich häufig nicht verpflichtet nach einem End-of-life ihre digitalen Produkte wie IT-Dienste, IT-Systeme, Hardware und Software weiter mit Sicherheitsupdates zu versorgen – selbst dann, wenn diese eine weite Verbreitung haben und die Sicherheitslücke schwerwiegend ist. Dass dies kein Einzelfall ist, zeigen systematische Studien mit teilweise besorgniserregenden Ergebnissen[3]. Ebenso besteht bei Bibliotheken wie TwitterKit nicht nur Handlungsbedarf für die Hersteller:in der Bibliothek, sondern auch für die Hersteller:innen der Anwendungen, welche die Bibliothek einsetzen. Auch diese können eine Anwendung bereits abgekündigt haben und sich folglich ggf. weigern, den Austausch oder auch nur Update der Bibliothek in ihrer Software vorzunehmen.

In rechtlicher Hinsicht zeigen sich hier mehrere Konfliktlagen:

Das **Zivilrecht** sieht keine Regelungen vor, die einheitlich im B2B- und B2C-Bereich auf digitale Produkte, Hardware und Software zur Festlegung des End-of-life Anwendung finden. Einen gesetzlichen Anhaltspunkt zur Bestimmung des End-of-life bieten die bereits thematisierten Regelungen zur Mängelhaftung für Waren mit digitalen Elementen sowie digitalen Produkten, welche allerdings nur im Bereich der Verbraucherverträge Anwendung finden. Demnach besteht für die Hersteller:innen eine Aktualisierungspflicht für den Zeitraum, den die Verbraucher:innen „aufgrund der Art und des Zwecks der Ware und ihrer digitalen Elemente sowie unter Berücksichtigung der Umstände und der Art des Vertrags erwarten“ können (§ 475b Abs. 4 Nr. 2 BGB, vgl. auch § 327f Abs. 1 Nr. 2 BGB). Der Aktualisierungszeitraum richtet sich also nach dem Erwartungshorizont der Durchschnittsverbraucher:innen.[4] Im Fall des TwitterKit wäre dann diskutabel, inwieweit Twitter als verantwortliches Unternehmen nach Eintritt des End-of-life die Verantwortung für eine Nachsorge trägt oder die Hersteller:innen der Anwendungen, welche TwitterKit als Komponente in ihrer Software

[2] https://blog.twitter.com/developer/en_us/topics/tools/2018/discontinuing-support-for-twitter-kit-sdk.

[3] Siehe beispielsweise https://arxiv.org/pdf/2105.14298; https://www.rand.org/pubs/research_reports/RR1751.html; https://cve.mitre.org/cve/cna/CVE_Program_End_of_Life_EOL_Assignment_Process.html; https://cve.mitre.org/cve/cna/CVE_Program_End_of_Life_EOL_Assignment_Process_v1-1.pdf mit dem Zitat: "There are no expectations of vendors to either investigate or correct vulnerabilities reported in EOL products."

[4] Vgl. *Dickmann*, International Cybersecurity Law Review – DOI: https://doi.org/10.1365/s43439-022-00064-9.

einsetzen. Allein die behördliche Warn- und Mediationsfunktion vermag da – unabhängig von der letztlichen Zuständigkeit für die Aktualisierung oder den Ersatz der betroffenen Komponente – nicht auszureichen. Hier stünde es der Gesetzgebung zu, zum Schutz von Verbraucher:innen und mittelbar auch der IT-Sicherheit insgesamt auf eine zahlenmäßige Mindestgrenze festzulegen. Einen ersten Grundstein legt die genannte Dauer von 5 Jahren im Entwurf des Cyber Resilience Acts[5], konkret Art. 10 Abs. 6 CRA-Entwurf – zugleich stellt der Absatz aber auch auf die Produktlebenszeit ab. Im Ergebnis wird diese Problematik daher auch nicht durch den CRA-Entwurf – zumindest nicht in der derzeitigen Fassung – gelöst.

Datenschutzrechtlich könnten die allgemeinen Regelungen der Art. 25, 32 DSGVO Anwendung finden. Es erscheint plausibel, dass die Auswahl technischer und organisatorischer Maßnahmen auch das Schließen von Sicherheitslücken via Updates als Mitigation einbezieht. Auch als Maßnahme zur Risikominderung im Rahmen einer Datenschutz-Folgenabschätzung des Art. 35 DSGVO erscheint ein Update als effektives Mittel. Konkrete Rechtspflichten benennt die DSGVO allerdings nicht; es gilt das zum Zivilrecht Gesagte. In die Warnung und Information betroffener Personen sollten dann auch die Datenschutzbehörden einbezogen werden. Im Übrigen sei auf die obigen Ausführungen in Kapitel 2 verwiesen.

Für den Bereich des **IT-Sicherheitsrecht**s sei auf die obigen Ausführungen in Kapitel 2 verwiesen, insbesondere im Hinblick auf die Funkanlagenrichtlinie.

II. Überlastung: Massenfindings und Mehrfachnennungen

Für die Konzeption der Beziehung zwischen Meldenden und Meldestelle ist die Frage relevant, ob Entdecker:innen von Sicherheitslücken dazu verpflichtet sein sollten, sämtliche potenziellen Sicherheitslücken zu melden – also, ob eine faktische Meldepflicht etabliert werden sollte. Auch erhöhte Haftungsrisiken könnten sich indirekt zu einer Meldeobliegenheit auswachsen. Des Weiteren sollte der rechtliche Rahmen einer staatlich organisierten Meldestelle reflektieren, wie diese mit eingegangenen Meldungen zu verfahren hat. Eine Pflicht *sämtliche* Meldungen zu sichten, auszuwerten und weiterzuleiten könnte auf beiden Seiten – in einer MKS sowie bei den IT-Sicherheitsforschenden – an technische, organisatorische und personelle Grenzen stoßen. Erhebliche Praxisprobleme zeigen sich bspw. im Fall von statischen als auch dynamischen Massenscans, deren Problematik im Folgenden skizziert wird. So kann es für Sicherheitsforschende bspw. angezeigt sein, nur die wahrscheinlichsten oder kritischsten potenziellen Fehler detailliert zu analysieren und ggf. zu melden.

[5] Siehe https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

1. Zur Funktionsweise automatisierter Testverfahren

Schwachstellen in Software werden nicht nur durch manuelle Tests identifiziert. Aufgrund der Größe und Komplexität moderner Software ist die Arbeit an automatisierten Testverfahren ein wesentlicher Bestandteil der Software-Sicherheitsforschung. Hierbei unterscheidet man zwischen statischen und dynamischen Analysen. Statische Analysen betrachten den (Binär-)Code einer Anwendung und gleichen ihn mit bekannten Schwachstellenmustern ab. Ein solches Muster kann z.B. ein Aufruf einer veralteten Verschlüsselungsfunktion sein, welche einen Algorithmus verwendet, der nicht mehr als sicher anzusehen ist.

Dynamische Analysen auf der anderen Seite beobachten die Zielanwendung während der Ausführung. Hierfür werden automatisiert Eingaben erzeugt, welche an die Anwendung übergeben werden. Dabei wird meist der Angriffsweg nachgestellt, bei welchem ein Nutzender eine Datei aus einer nicht vertrauenswürdigen Quelle öffnet. Fehler in der Dateiverarbeitung zeigen sich im einfachsten Fall durch einen Crash der Zielanwendung. Ein solcher Crash weist darauf hin, dass die Verarbeitung der Eingabedatei zu einem ungültigen Zustand im Arbeitsspeicher geführt hat, wodurch die Ausführung der Anwendung aufgrund falscher Rücksprungadressen nicht fortgesetzt werden konnte.[6] Anders ausgedrückt: Die Angreifer:in, die die nicht vertrauenswürdige Eingabedatei erzeugt, kann den Speicher auf dem Zielsystem manipulieren. Hieraus lassen sich dann Exploits erzeugen, wenn statt eines Crashs eine bewusste Manipulation des Speichers angestrebt wird, z.B. durch Injektion von Schadcode oder durch Umschreiben des Programmablaufs auf Basis vorhandener Codefragmente (z.B. Return-oriented-Programming).

Gemein ist beiden automatisierten Testansätzen die Vielzahl an Ergebnissen, die sie liefern. Bei Mobilapps sind dutzende bis hunderte Ergebnisse keine Seltenheit, bei größeren Unternehmensanwendungen ist von hunderten bis tausenden Ergebnissen auszugehen. Diese Ergebnisse erfordern jedoch eine Nachbearbeitung. Insbesondere statische Analysen können falsch-positive Ergebnisse liefern, bei denen es sich nicht um eine real ausnutzbare Schwachstelle handelt. So kann eine veraltete Verschlüsselung bspw. bewusst genutzt werden, wenn diese aus Gründen der Rückwärtskompatibilität explizit von Benutzer:innen aktiviert wurde. Solche Zusammenhänge sind für statische Scanner oft nicht zu erkennen und werden wie eine „echte" Sicherheitslücke gemeldet. Ebenso analysieren statische Scanner den gesamten Code, auch wenn beispielsweise von einer ins Programm eingebundenen Bibliothek gar nicht alle Funktionen genutzt

[6] Auf kompliziertere Abbruchbedingungen, z.B. überschriebene Stack Canaries, soll hier nicht eingegangen werden, da sie zu denselben Schlussfolgerungen führen.

werden. Schwachstellen im nicht genutzten Code sollten zwar im Sinne von „Codehygiene“ ebenfalls vermieden werden, lassen sich aber nicht unmittelbar von einem:r Angreifer:in ausnutzen.

Durch Verwendung qualitativ hochwertiger statischer Scanner kann die Quote an Falschmeldungen zwar reduziert werden, es verbleibt jedoch eine signifikante Anzahl an nicht relevanten Meldungen. Hierdurch ergibt sich die Notwendigkeit einer manuellen Nachkontrolle. Bei hunderten oder tausenden von Ergebnissen nimmt diese Nachkontrolle signifikant Zeit von Experten:innen in Anspruch. Forscher:innen könnten eine solche Tätigkeit fachlich leisten, jedoch steht der wissenschaftliche Erkenntnisgewinn in keinem akzeptablen Verhältnis zur aufgewendeten Zeit. Für die wissenschaftliche Evaluation neuer Verfahren der statischen Analyse werden daher bei größeren Datensätzen (z.B. die automatische Analyse hunderter Anwendungen zur Erprobung neuer Scanner) lediglich Stichproben realistischer Größe betrachtet. Im industriellen Kontext ist die Prüfung der Scanergebnisse begrenzt auf eigene Produkte. Selbst dafür werden oftmals dedizierte Stellen im Test- oder Entwicklungsteam geschaffen.

Dynamische Analysen vermeiden Falschmeldungen in dem Sinne, dass jeder Crash tatsächlich zur Laufzeit beobachtet wurde. Je nach Testverfahren bedeutet dies jedoch auch nicht, dass im realen Einsatz eine Sicherheitslücke bestehen würde, insbesondere, wenn Teile des Codes isoliert in einer künstlichen Umgebung getestet wurden. In diesem Fall kann die reale Umgebung zusätzliche Prüfungen enthalten, die den Crash vermieden hätten. Die Extraktion relevanten Codes und Testung außerhalb der Ursprungsanwendung ist z.B. dann populär, wenn die Interaktion mit der Originalanwendung zu kompliziert zu simulieren wäre.

Zudem können mehrere unterschiedliche Eingabedateien aufgrund derselben Sicherheitslücke zu Crashes führen. Der dynamische Scanner meldet dann beispielsweise mehrere dutzende Crashes, obwohl es sich nur um einige einzige Sicherheitslücke handelt. Die automatische Deduplizierung von Crashes ist ein aktives Forschungsfeld. Auch hier kann die Verwendung neuer Verfahren das Problem reduzieren, aber nicht lösen. Die Identifikation der ursächlichen Fehler hinter den Crashes verbleibt als manuelle Aufgabe.

Bei statischen und dynamischen Analysen muss überdies die Relevanz der Schwachstelle eingeschätzt werden. Wird zum Beispiel die Verwendung eines veralteten kryptografischen Algorithmus erkannt, ist dies nicht zwingend eine Sicherheitslücke. Wird durch einen MD5-Hash beispielsweise nur eine eindeutige ID-Nummer für abzuspeichernde Daten generiert, wird der Algorithmus gar nicht für eine sicherheitsrelevante Aufgabe eingesetzt.

In Summe bleibt festzuhalten, dass sowohl statische als auch dynamische Analysen mit einem signifikanten Nachbereitungsaufwand einhergehen. Dieser ist im prakti-

schen Einsatz, wenn z.B. Unternehmen ihre eigenen Anwendungen scannen, wirtschaftlich abbildbar. Für Forschende, insbesondere im Kontext von statistischen Evaluationen auf Massendaten (z.B. mehrere tausend Apps für eine Analyse des Sicherheitsniveaus in App-Märkten) jedoch nicht.

2. Optionen zum Umgang mit Massenfindings

Geht man von davon aus, dass eine vollständige Nachkontrolle der Scanergebnisse durch die Wissenschaftler:innen nicht realistisch ist, verbleiben drei Optionen für die Weiterverwendung der potenziellen Schwachstellen:

1. Weiterleitung der geprüften Stichprobe an die Meldestelle
2. Ungeprüfte Weiterleitung aller Ergebnisse an die Meldestelle
3. Keine Weiterleitung der Ergebnisse

Option 3 ist eine nicht unübliche Wahl, sollte der Meldeaufwand sich als zu hoch erweisen, so dass die Meldetätigkeit in Konkurrenz zur wissenschaftlichen Tätigkeit tritt. Hierdurch wird der relevante Teil der Schwachstellen jedoch ebenfalls nicht behoben.

Die Stichprobe an die Meldestelle weiterzuleiten (**Option 1**) führt zu ähnlichen Schwierigkeiten. Die zufällige Stichprobe muss nicht zwingend die relevantesten Schwachstellen enthalten und ist im Regelfall nicht vollständig. Somit gehen auch bei dieser Option reale Schwachstellen verloren.

Option 2 vermeidet den Aufwand der manuellen Nachbereitung auf Seiten des:der Forscher:in. Hierdurch entfällt der Aufwand jedoch nicht, sondern wird lediglich zur Meldestelle bzw. MKS verschoben. Geht man von zahlreichen Wissenschaftler:innen aus, die – teilweise auf denselben, teilweise auf unterschiedlichen Anwendungen – Scans durchführen und die Ergebnisse melden, wären auf Seiten der Meldestelle erhebliche Kapazitäten erforderlich. Dieser Effekt wird dadurch verstärkt, dass die Erkennung von Duplikaten in den Schwachstellenmeldungen nur zu einem begrenzten Grad automatisierbar ist. Für die Meldestelle verbleibt neben dem eigenen Aufwand noch die Möglichkeit, die jeweiligen Hersteller:innen zu einer Kommentierung aller Meldungen zu verpflichten, d.h. die Massendaten ungefiltert weiterzureichen. In Anbetracht doppelter Meldungen und Falschmeldungen kollidiert dieser Ansatz jedoch erkennbar mit den Interessen der beteiligten Akteure.

Um die Menge an Schwachstellen bewältigen zu können, wäre eine Priorisierung denkbar. Hierfür müssten jedoch gesellschaftlich akzeptierte Kriterien entwickelt werden. Die Häufigkeit der Meldung einer bestimmten potenziellen Schwachstelle ist offenbar kein valides Kriterium für die Priorisierung einer Meldung durch die Meldestelle. Möglich wäre stattdessen die Priorisierung nach Nutzungszahlen oder Kritikali-

tät bzw. Risiko für die IT-Sicherheit der betroffenen Anwendung, die in kritischen Infrastrukturen verwendet wird. Eine solche Priorisierung scheint sich insoweit in den Entwürfen des Cyber Resilience Acts und der NIS2-Richtlinie abzuzeichnen.

In Summe verbleibt eine nur durch Abwägungen lösbare Situation für den Umgang mit den Ergebnissen wissenschaftlicher Massenanalysen. Notwendig ist eine gesellschaftliche Diskussion über die Chancen und Risiken der vorgestellten Ansätze, wobei kein Ansatz in allen Kriterien besser als die anderen ist.

III. Ineffektive Maßnahmen: Risikoeinschätzung trotz lückenhafter Informationen

Organisatorische und personelle Engpässe sowie ein erhöhtes Meldeaufkommen vorausgesetzt, müssten die Relevanz einer Schwachstelle für die IT-Sicherheit und die Allgemeinheit sowie der daraus entstehende Handlungsbedarf stetig überprüft werden. Besteht keine Möglichkeit die Sicherheitslücke zu beheben, muss entschieden werden, ob und in welcher Form öffentliche Warnungen ausgesprochen werden. Für die Einschätzung ist nicht nur ein detailliertes Verständnis der Schwachstelle, sondern auch des Nutzungskontexts erforderlich: Wer hat Zugang zu der betroffenen Anwendung, welche Daten werden verarbeitet, welche Prozesse ausgelöst (z.B. Kraftwerkssteuerung)? Gleichzeitig ergeben sich Risiken nicht nur aus dem Weiterbetrieb, sondern auch aus einer (partiellen) Abschaltung, z.B. wenn relevante Dienste nicht mehr erbracht werden können oder wirtschaftliche Schäden entstehen.

Um die Einschätzung treffen zu können, muss die Meldestelle somit Analyseaufwand in jede (potenzielle) Schwachstelle investieren. Hierbei ist zu bedenken, dass die Einschätzung und Weitergabe der Meldung durch die Meldestelle mit einem Zeitverzug einhergehen. Sinnvoll wäre zudem in Abstimmung mit den jeweiligen Hersteller:innen den Zeitplan für die Behebung der Lücke abzustimmen, ggf. muss eine Zwischenlösung bis zur Behebung gefunden werden, und Nachkontrollen der Maßnahmen zeigen, ob Risiken angemessen reduziert werden konnten. Aus diesem Aufwand und der Anzahl der gemeldeten Schwachstellen ergibt sich die notwendige Personalausstattung der Meldestelle. Bei inkorrekter Einschätzung einer Schwachstelle und unterlassener Weiterleitung an Produktverantwortliche sowie daraus entstehenden Schäden stellt sich zudem die Frage der Verantwortlichkeit. Schwierigkeiten für die Meldestelle ergeben sich aus einer limitierten Informationslage, wenn kein Zugang zum Quellcode und der Dokumentation der Systemlandschaft besteht – was über eine verpflichtende Offenlegung solcher Dokumente gegenüber der Meldestelle lösbar wäre.

Es sollte allerdings keine Übertragung von Aufgaben und Verantwortung von Unternehmen (Hersteller:innen, Betreiber:innen) an eine staatliche, mit öffentlichen Mitteln finanzierten Meldestelle wie die MKS erfolgen. Denkbar wäre ein Finanzierungsbeitrag der betroffenen Unternehmen ähnlich eines Haftungsfonds, wenn Kosten einer Überprüfung der Schwachstelle und ihrer Kritikalität praktisch an die Meldestelle ausgelagert werden. Diese Problematik bietet letztlich auch die Chance, das Verhältnis zwischen der Verantwortung der einzelnen Unternehmen und ihre jeweiligen Risikobewertungen und den Risikobewertungen staatlicher Einrichtungen neu auszubalancieren.

IV. Fazit

Anhand der wenigen Beispiele zeigt sich: Die MKS kann bei der Koordinierung und Orientierung für geeignete Maßnahmen zur Risikominderung bzw. Resilienzerhöhung (in Anlehnung an den kommenden Cyber Resilience Act) dienen. Dennoch bleiben gewisse Verantwortungsanteile stets bei Hersteller:innen oder IT-Sicherheitsforscher:innen, die durch eine zentrale Meldestelle wie die MKS nicht aufgelöst werden können und sollen. Im Einzelfall könnten Eingriffs- und Abhilfebefugnisse die Verantwortung erleichtern, dennoch sollte damit ein gewisser Sanktionsapparat einhergehen. Gerade aus diesem Grund empfiehlt sich die Unabhängigkeit der MKS, um Vorwürfen einer Begünstigung aus politischen oder finanziellen Gründen vorzubeugen. Im Hinblick auf IT-Sicherheitsforscher:innen und Hersteller:innen sei deshalb auf einen grundlegenden Rechtsrahmen für Meldeverfahren und Mediation hingewiesen. Dabei sei die erwähnte Priorisierung anhand Kritikalität bzw. Risiko für die IT-Sicherheit einzubinden, um Massenfindings wie Verantwortlichkeiten entsprechend aufzuteilen. Die Beteiligung der MKS könnte dann dynamisch entlang am Risiko erfolgen; weniger „relevante“ IT-Sicherheitslücken könnten auch eigenständig durch die Beteiligten bewältigt werden. Entsprechend muss der Rechtsrahmen abseits der MKS die einzelnen Rollen und damit verbundene Rechte und Pflichten klären. Inwieweit IT-Sicherheitsforschende wegen ihrer Tätigkeit zugunsten der Allgemeinheit tendenziell besser zu stellen sind, bliebe an anderer Stelle zu diskutieren.

Damit lässt sich festhalten, dass für Regelungen zum Rahmen einer Melde- und Koordinierungsstelle weitere Punkte bedacht werden sollten – unter anderem:

- Staatlich stärkere Ausrichtung auf Open-Source Software als Teil einer sichereren und autonomen Infrastruktur, dabei Einbeziehung der MKS bei einer Art Bug-Bounty-Programm
- Bildung eines Haftungs- und Rechtsrahmens für die Beteiligten eines IT-Sicherheitslücken-Fundes

- Meldestelle als Lernmaterialersteller zur Etablierung einer Fehlerkultur in der IT-Sicherheit für private und öffentliche Institutionen
- Vorbildfunktion der zentralen Melde- und Koordinierungsstelle für den kooperativen und integrativen Ansatz im europäischen Raum

Zusammenfassung

Ziel dieses Whitepapers war es, einen Überblick über die bestehenden Probleme im verantwortungsvollen Umgang mit IT-Sicherheitslücken zu geben und einen Lösungsansatz aufzuzeigen.

Grundlage dafür ist die Problemlage in gesellschaftlicher wie wissenschaftlicher Hinsicht: Die Einblicke in die wissenschaftliche und politisch-gesellschaftliche Diskussion (**Kapitel 1**) verdeutlichen die Relevanz der IT-Sicherheit in der fortschreitenden Digitalisierung und Vernetzung, und damit auch die Bedeutung von Schwachstellen bei der Bewertung der IT-Sicherheit. Die daran beteiligten Personen sowie Prozesse sind allerdings nur mäßig definiert bzw. überwiegend international etabliert. So ist der Begriff der IT-Sicherheitsforscher:in nicht klar und einheitlich definiert; oft schließt er ethische Hacker:innen und unabhängige Akteur:innen nicht ein. Die Meldung bzw. koordinierte Offenlegung von IT-Sicherheitslücken nach dem Schema des international etablierten Coordinated -Disclosure-Prozesses hat sich dagegen national bislang mäßig durchgesetzt.

Grund dafür mögen die zahlreichen rechtlichen Probleme sein, die **Kapitel 2** in dieser Hinsicht aufzeigt. Die Betrachtung des Prozesses aus verschiedenen rechtswissenschaftlichen Blickwinkeln bzw. Disziplinen zeigt zunächst grundrechtliche Konflikte im Dreieck IT-Sicherheitsforscher:in – Nutzer:in – Hersteller:in auf. Das Austarieren dieser Positionen gelingt auch nicht über die in der Untersuchung vertieften Betrachtungen u.a. im Datenschutz-, Straf- und Produktsicherheitsrecht. Auch aktuelle europäische Entwürfe wie jene der NIS2-Richtlinie und des Cyber Resilience Acts enthalten nur oberflächliche Lösungsvorschläge, die ein Austarieren kaum einbeziehen. Damit deuten die Ergebnisse dieses Kapitels darauf hin, dass bisheriges gesetzgeberisches Handeln die Konfliktlage nicht ausreichend berücksichtigt hat.

Im Zuge der Umsetzung europäischer Regelungsvorhaben sowie des Gesetzgebungsauftrags in der Rechtsprechung des Bundesverfassungsgerichts eröffnet sich jedoch eine Chance, die einzelnen Positionen gesetzgeberisch zu würdigen. Hierfür bietet **Kapitel 3** die Grundlage in Form einer unabhängigen Melde- und Koordinierungsstelle zur Unterstützung von CVD-Prozessen. Aufgabe der Stelle ist es, die vermittelnde Position zwischen Hersteller:in und Finder:in (z.B. IT-Sicherheitsforscher:innen) einzunehmen und im Interesse der Allgemeinheit das Schließen der IT-Sicherheitslücke bzw. Schwachstelle zu begleiten. Im Einzelnen sei auf die Ausführungen im Kapitel selbst verwiesen.

Dennoch sei zu betonen, dass die Umsetzung des Vorschlags aus Kapitel 3 nicht dazu führt, dass sämtliche Probleme im Umgang mit IT-Sicherheitslücken gelöst würden. Aus rechtlicher Sicht verbleiben stets Verantwortungsanteile bei Hersteller:innen bzw. Produzent:innen und Melder:innen. Es ist daher notwendig, begleitende staatliche Maßnahmen – wie in **Kapitel 4** ausgeführt – im Zuge des Aufbaus einer Melde- und Koordinierungsstelle zu treffen.

Ein verantwortungsvoller Umgang mit IT-Sicherheitslücken kann folglich nur durch ein Zusammenspiel aus institutioneller Lösung in Form (freiwillig eingeschalteten) der Melde- und Koordinierungsstelle (Kapitel 3) und Begleitmaßnahmen zur Stärkung der Rechtssicherheit für Melder:innen von Schwachstellen und Hersteller:innen (Kapitel 4) gelingen.

Literaturverzeichnis

Abelson, Harold/Anderson, Ross/Bellovin, Steven M./Benaloh, Josh/Blaze, Matt/Diffie, Whitfield "Whit"/Gilmore, John/Green, Matthew/Landau, Susan/Neumann, Peter G./Rivest, Ronald L./ Schiller, Jeffrey I./Schneier, Bruce/Specter, Michael A./Weitzner, Daniel J., Keys under doormats: mandating insecurity by requiring government access to all data and communications, in: Journal of Cybersecurity, Volume 1, Issue 1, September 2015, S. 69–79.

AG KRITIS – Arbeitsgruppe Kritische Infrastrukturen, Das Cyber-Hilfswerk. Konzept zur Steigerung der Bewältigungskapazitäten in Cyber-Großschadenslagen, Version 1.0 v. 07.02.2020, abrufbar: https://ag.kritis.info/wp-content/uploads/2020/02/chw-konzept_v1.0.pdf (zit. Konzept zum Cyberhilfswerk der AG-Kritis).

Albert, Gleb J., Computerkids als mimetische Unternehmer: die Cracker-Szene zwischen Subkultur und Ökonomie (1985-1995), WerkstattGeschichte 2016, S.49-66.

Alberts, Gerard/Oldenziel, Ruth, Hacking Europe. From Computer Cultures to Demoscenes, London 2014 (zit. *Bearb*., in: Alberts/Oldenziel (Hrsg.), Hacking Europe. From Computer Cultures to Demoscenes, History of Computing, 2014).

Alexander, Christian, Geheimnisschutz nach dem GeschGehGE und investigativer Journalismus, AfP 2019, S. 1-11.

Allianz, Allianz Risk Barometer identifying the major business risks for 2021, abrufbar: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2021.pdf.

Amberg, Eric/Schmid, Daniel, Hacking. Der umfassende Praxis-Guide, 1. Aufl., Frechen 2020.

Anderson, Ross, Security Engineering. A Guide to Building Dependable Distributed Systems, 3. Aufl., Indianapolis 2020.

Arora, Ashish/Krishnan, Ramayya/Telang, Rahul/Yang, Yubao, An Empirical Analysis of Vendor Response to Disclosure Policy, in: Workshop on economics of information security 2005 (WEIS05), 2005, abrufbar: http://infosecon.net/workshop/pdf/41.pdf.

Bach, Ivo, Neue Richtlinien zum Verbrauchsgüterkauf und zu Verbraucherverträgen über digitale Inhalte, NJW 2019, S. 1705-1711.

Balaban, Silvia/Boehm, Franziska/Brodowski, Dominik/Dickmann; Roman/Franzen, Fabian/ Goerke, Niklas/Golla, Sebastian/Koloßa, Stephan/Kreutzer, Michael/Krüger, Jochen/Leicht, Maximilian/Obermaier, Johannes/Pieper, Maria/Schink, Marc/Schreiber, Linda/Schuster, Dieter/ Sorge, Christoph/Tran, Hoa/Vettermann, Oliver/Vogelgesang, Stephanie/Vonderau, Daniel/Wagner, Manuela: Whitepaper zur Rechtslage der IT-Sicherheitsforschung. Reformbedarf aus Sicht der angewandten Sicherheitsforschung, abrufbar: https://sec4research.de/assets/Whitepaper.pdf; (zit. Whitepaper Rechtslage der IT-Sicherheitsforschung 2021).

Barber, Richard, Hackers Profiled — Who Are They and What Are Their Motivations?, Computer Fraud & Security, Volume 2001, Issue 2, 20021, S. 14-17.

Baumgartner, Ulrich/Gausling, Tina, Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen. Was Unternehmen jetzt nach der DS-GVO beachten müssen, ZD 2017, S. 308-313.

Bertsch, Sascha/Fortmann, Michael, Silent-Cyber-Risiken in konventionellen Unternehmensversicherungen (Teil 2), r+s 2021, S. 549-556.

Bitkom, Regulierungsmapping IT-Sicherheit. Gesetzliche Anforderungen auf nationaler und europäischer Ebene, Juli 2020, abrufbar: https://www.bitkom.org/sites/default/files/2020-09/200908_regulierungsmapping.pdf.

Borges, Georg/Hilber, Marc, BeckOK IT-Recht, 7. Edition, 01.07.2022 (zit. Bearb., in: Borges/Hilber, BeckOK IT-Recht).

Brodowski, Dominik, Hacking 4.0 – Seitenkanalangriffe auf informationstechnische Systeme. Zugleich ein Beitrag zur Theorie und Dogmatik des IT-Strafrechts, ZIS 2019, S. 49-61.

Brodowski, Dominik, (Ir-)responsible disclosure of software vulnerabilities and the risk of criminal liability, in: it – Information Technology, Volume 57, no. 6, 2015, S. 357-365.

Buchanan, Ben, The hacker and the state: cyber attacks and the new normal of geopolitics, Cambridge 2020 (zit. *Buchanan*, The Hacker and the State).

Bugcrowd, Inside the Mind of a Hacker Report, 2021, abrufbar: https://www.bugcrowd.com/resources/guides/inside-the-mind-of-a-hacker/.

Bundesamt für Sicherheit in der Informationstechnik (BSI), Die Lage der IT-Sicherheit in Deutschland 2021, abrufbar: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf?__blob=publicationFile&v=4.

Bundesamt für Sicherheit in der Informationstechnik (BSI), Handhabung von Schwachstellen. Empfehlungen für Hersteller, BSI-CS 019, Version 2.0 v. 11.07.2018, abrufbar: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_019.pdf?__blob=publicationFile&v=1.

Bundesregierung, Mehr Fortschritt wagen. Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit. Koalitionsvertrag zwischen SPD, BÜNDNIS 90/DIE GRÜNEN und FDP, 2021, abrufbar: https://www.bundesregierung.de/resource/blob/974430/1990812/04221173eef9a6720059cc353d759a2b/2021-12-10-koav2021-data.pdf?download=1 (zit. *Bundesregierung,* Koalitionsvertrag 2021-2025).

Büring, Harald, Doppelte Staatsverantwortung. Polizei muss bei Quellen-TKÜ auf IT-Sicherheit achten, c't 18/2021, S. 172.

Camp, L. Jean/Wolfram, Catherine, Pricing security, in: Proceedings of the CERT Information Survivability Workshop, S. 31--39, 2000.

Centre for European Policy Studies (CEPS) Task Force, Software Vulnerability Disclosure in Europe. Technology, Policies and Legal Challenges, Juni 2018, abrufbar: https://www.ceps.eu/wp-content/uploads/2018/06/CEPS%20TFRonSVD%20with%20cover_0.pdf.

Centre for Strategy & Evaluation Services (CSES), Final Report. Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment, April 2020 (zit. *Whittle* u.a., Final Report, April 2020).

CIO Platform Nederland/Rabobank, Coordinated Vulnerability Disclosure Manifesto, Juli 2016, abrufbar: https://www.cio-platform.nl/en/publications.

Dalg, Paul, „Bei Cybersicherheit gibt es keinen Königsweg", Tagesspiegel Background v. 18.11.2021, abrufbar: https://background.tagesspiegel.de/cybersecurity/bei-cybersicherheit-gibt-es-keinen-koenigsweg.

Dann, Matthias/Markgraf, Jochen W., Das neue Gesetz zum Schutz von Geschäftsgeheimnissen, NJW 2019, 1774-1779.

Derin, Benjamin/Golla, Sebastian J., Der Staat als Manipulant und Saboteur der IT-Sicherheit?. Die Zulässigkeit von Begleitmaßnahmen zu „Online-Durchsuchung" und Quellen-TKÜ, NJW 2019, S. 1111-1116.

Dickmann, Roman, Vulnerability management as compliance requirement in product security regulation—a game changer for producers' liability and consequential improvement of the level of security in the Internet of Things?, International Cybersecurity Law Review (ICLR) 2022.

Dickmann, Roman/Vettermann, Oliver, Geheimhaltung als Grundrechtsverletzung. Entscheidung des BVerfG zum Umgang von Behörden mit IT-Schwachstellen, MMR 2022, S. 740-745.

Dick van der Reijden, Biedt Art. 10 EVRM de ethisch hacker bescherming tegen onduidelijkheden en onvolkomenheden in de Leidraad Responsible Disclosure?, abrufbar: https://www.maesoever.nl/files/scriptie-dick-van-der-reijden-v1-0p.pdf.

Dubovitskaya, Elena, Kauf von Waren mit digitalen Elementen. Fortschritt und Rechtsunsicherheit im Verbrauchsgüterkaufrecht, MMR 2022, S. 3-8.

Dümeland, Malte, Sachmangelhaftigkeit von Software bei nicht DSGVO-konformer Entwicklung, K&R 2019, S. 22-25.

Eckert, Claudia, IT-Sicherheit: Konzepte – Verfahren – Protokolle, 10. Aufl., Berlin 2018 (zit. *Eckert*, IT-Sicherheit).

EDSB, Stellungnahme 4/2017 zu dem Vorschlag für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, 2017, abrufbar:

https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_de.pdf.

Edgar, Thomas W./Manz, David O., Research Methods for Cyber Security, 1. Aufl., Cambridge 2017.

Ehring, Philipp/Tager, Jürgen, Produkthaftungs- und Produktsicherheitsrecht, BGB | ProdHaftG | ProdSG MÜ-VO | MüG | ÜAnlG, 1. Aufl., Baden-Baden 2022.

Eichensehr, Kristen E., Public-Private Cybersecurity, Texas Law Review, Volume 95, Issue 3, 2017, S. 467-538.

Eisenbarth, Thomas/Kasper, Timo/Paar, Christof, Sicherheit moderner Funktüröffnersysteme, DuD 2008, S. 507-510.

Electronic Frontier Foundation, DOJ's New CFAA Policy is a Good Start But Does Not Go Far Enough to Protect Security Researchers, 19.05.2022, abrufbar: https://www.eff.org/deeplinks/2022/05/dojs-new-cfaa-policy-goodstart-does-not-go-far-enough-protect-security.

Epping, Volker/Hillgruber, Christian, BeckOK Grundgesetz, 52. Edition, Stand 15.08.2022 (zit. *Bearb.,* in: Epping/Hillgruber, BeckOK Grundgesetz).

Erdogan, Julia Gül, Avantgarde der Computernutzung. Hackerkulturen der Bundesrepublik und der DDR, Göttingen 2021.

Ermert, Monika: Offenlegung von Softwarelücken: Rechtsstreit endet mit Vergleich, heise online v. 06.09.2018, abrufbar: https://www.heise.de/newsticker/meldung/Offenlegung-von-Softwareluecken-Rechtsstreit-endet-mit-Vergleich-4156393.html.

Ernst, Stefan, Hacker und Computerviren im Strafrecht, NJW 2003, S. 3233-3239.

European Union Agency for Cybersecurity (ENISA), Glossary, abrufbar: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/glossary#G52.

European Union Agency for Cybersecurity (ENISA), Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations, November 2015, abrufbar: https://www.enisa.europa.eu/publications/vulnerability-disclosure.

Faust, Florian, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?. Gutachten zum 71. Deutschen Juristentag, München 2016.

Felsch, Johannes Claudio/Kremer, Julian/Wagener, Jonas, Handhabung der neuen Aktualisierungspflicht bei digitalen Produkten. Anwendungsbereich, Inhalt und Dauer anhand zweier konkreter Beispiele, MMR 2022, S. 18- 23.

Forum of Incident Response and Security Teams (FIRST), Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure, Version 1.1, Spring 2020, abrufbar: https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRST-Multiparty-Vulnerability-Coordination.pdf.

Franzen, Fabian/Maier, Dominik/Wagner, Manuela, Mehr schlecht als Recht: Grauzone Sicherheitsforschung. Reverse Engineering vor Gericht, DuD 2020, S. 511-517.

Gamero-Garrido, Alexander/Savage, Stefan/Levchenko, Kirill/Snoeren, Alex C., Quantifying the Pressure of Legal Risks on Third-party Vulnerability Research, in: CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, S. 1501-1513.

Golla, Sebastian: IT-Sicherheit und Strafrecht – Neukalibrierung eines belasteten Verhältnisses, JZ 2021, S. 985-990.

Golla, Sebastian/Brodowski, Dominik, IT-Sicherheit und Strafrecht – im Erscheinen.

Gebeshuber, Klaus/Teiniker, Egon/Zugaj, Wilhelm, Exploit!. Code härten, Bugs analysieren, Hacking verstehen. Das Handbuch für sichere Softwareentwicklung, 1. Aufl., Bonn 2019.

Hackerone, Hacker-Powered Security Report: Industry Insights '21, 09.03.2022, abrufbar: https://www.hackerone.com/resources/reporting/hacker-powered-security-report-industry-insights-21?ungated=.

Hansen, Marit, Informationssicherheit: Aufgabe für die Datenschutzaufsicht?, DuD 2021, S. 234-238.

Harms, Karel, Positieve uitlokking van ethisch hacken, Netherlands Journal of Legal Philosophy, Volume 2, 2017, S. 196-207.

Hau, Wolfgang/Poseck, Roman, BeckOK BGB, 61. Edition, 01.02.2022 (zit. *Bearb.,* in: BeckOK BGB).

Hauck, Ronny, Grenzen des Geheimnisschutzes, WRP 2018, S. 1032-1037.

Hauschka, Christoph E./Moosmayer, Klaus/Lösler, Thomas, Corporate Compliance. Handbuch der Haftungsvermeidung im Unternehmen, 3. Aufl., München 2016 (zit. *Bearb.,* in: Hauschka/Moosmayer/Lösler (Hrsg.), Corporate Compliance).

Herpig, Sven, Governmental Vulnerability Assessment and Management. Weighing Temporary Retention versus Immediate Disclosure of 0-Day Vulnerabilities, Stiftung Neue Verantwortung, August 2018, abrufbar: https://www.stiftung-nv.de/sites/default/files/vulnerability_management.pdf.

Herpig, Sven/Rupp, Christina, Deutschlands staatliche Cybersicherheitsarchitektur, 9. Aufl. September 2022, abrufbar: https://www.stiftung-nv.de/sites/default/files/cybersicherheitsarchitektur_neunteauflage0922.pdf.

Holland, Martin, Sicherheitslücken in CDU-connect-App: Strafverfahren gegen Entdeckerin, heise online, 04.08.2021 10:31 Uhr, abrufbar: https://www.heise.de/news/Sicherheitsluecken-in-CDU-connect-App-Strafverfahren-gegen-Entdeckerin-6154663.html.

Hornung, Gerrit/Schallbruch, Martin, IT-Sicherheitsrecht, 1. Aufl., Baden-Baden 2021 (zit. *Hornung/Schallbruch*, IT-Sicherheitsrecht).

Hunzinger, Sven/Schuster, Fabian, Pflichten zur Datenschutzeignung von Software. Wie die Pflichten zur Verwendung datenschutzkonformer IT-Lösungen auf die vertragliche Sollbeschaffenheit von Software durchschlägt, CR 2017, S. 141-148.

Hurtz, Simon, CDU blamiert sich mit Anzeige gegen IT-Expertin, 05.08.2021, Süddeutsche Zeitung, abrufbar: https://www.sueddeutsche.de/politik/cdu-connect-anzeige-wittmann-1.5373488.

IoT Security Foundation, Understanding the Contemporary Use of Vulnerability Disclosure in Consumer Internet of Things Product Companies, abrufbar: https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/Vulnerability-Disclosure-Design-v4.pdf.

Kapoor, Arun/Klindt, Thomas, Das neue deutsche Produktsicherheitsgesetz (ProdSG), NVwZ 2021, S. 719-724.

Kennedy, Dan, Exploring Coordinated Disclosure. Shedding Light on Perceptions and Experiences in how Software Vulnerabilities are reported, 2019, abrufbar: https://www.veracode.com/sites/default/files/pdf/resources/surveyreports/451-research-exploring-coordinated-disclosure-veracode-survey-report.pdf.

Kidwell, Peggy Aldrich, Stalking the Elusive Computer Bug, in: IEEE Annals of the History of Computing, Volume 20, Issue 4, 1998, S. 5-9.

Kindhäuser, Urs/Neumann, Ulfrid/Paeffgen, Hans-Ullrich, Strafgesetzbuch, 5. Aufl., Baden-Baden, 2017 (zit. *Bearb.*, in: NK-StGB).

Kipker, Dennis-Kenji, Cybersecurity, 1. Aufl., München 2020 (zit. *Bearb.,* in: Kipker, Cybersecurity).

Kipker, Dennis-Kenji/Scholz, Dario E., Das IT-Sicherheitsgesetz 2.0. Eine kritische Analyse, DuD 2021, S. 40-45.

Klaas, Arne, „White Hat Hacking" – Aufdecken von Sicherheitsschwachstellen in IT-Strukturen. Grenzen der Strafbarkeit von ethischen Hacking-Angriffen, MMR 2022, S. 187-192.

Kofler, Michael/Gebeshuber, Klaus/Kloep, Peter/Neugebauer, Frank/Zingsheim, André/Hackner, Thomas/Widl, Markus/Aigner, Roland/Kania, Stefan/Scheible, Tobias/Wübbeling, Matthias, Hacking & Security. Das umfassende Handbuch, 2. Aufl., Bonn 2020 (zit. *Kofler* et al., Hacking & Security).

Kruse, Berit, Gravierende Sicherheitslücke bei Corona-Testzentren, 22.06.2021, Süddeutsche Zeitung, abrufbar: https://www.sueddeutsche.de/politik/datenschutz-testzentren-1.5330068.

Krüger, Jochen/Sorge, Christoph/Vogelgesang, Stephanie, IT-Forscher als potentielle Straftäter? – IT-Sicherheitsforschung zwischen Wissenschaftsfreiheit und Strafrecht, in: Datenschutz/LegalTech – Tagungsband des 21. Internationalen Rechtsinformatik Symposions IRIS 2018: Data Protection/LegalTech – Proceedings of the 21st International Legal Informatics Symposium, 2018, S. 529-536 (zit. *Krüger/Sorge/Vogelgesang*, IRIS 2018, 529).

Kühling, Jürgen/Buchner, Benedikt, Datenschutz-Grundverordnung BDSG, 3. Auflage, München 2020 (zit. *Bearb.,* in: Kühling/Buchner, DS-GVO/BDSG).

Laszka, Aron/Zhao, Mingyi/Malbari, Akash/Grossklags, Jens, The rules of engagement for bug bounty programs, in: International Conference on Financial Cryptography and Data Security, 2018, S. 138-159.

Lenz, Tobias, Produkthaftung, 2. Aufl., München 2022.

Levy, Steven, Hackers: heroes of the computer revolution, London 1984.

Magnusson, Andrew, Practical Vulnerability Management, San Francisco 2020.

Matt, Holger/Renzikowski, Joachim, Strafgesetzbuch, 2. Auflage, München 2020 (zit. *Bearb.,* in: Matt/Renzikowski, StGB).

Mangel, Marcel/Bicchi, Sebastian, Praktische Einführung in Hardware Hacking. Sicherheitsanalyse und Penetration Testing für IoT-Geräte und Embedded Devices, 1. Aufl., Frechen 2020.

Meister, Ander, BSI programmierte und arbeitete aktiv am Staatstrojaner, streitet aber Zusammenarbeit ab, netzpolitik.org, 16.03.2015 15:40 Uhr, abrufbar: https://netzpolitik.org/2015/geheime-kommunikation-bsi-programmierte-und-arbeitete-aktiv-am-staatstrojaner-streitet-aber-zusammenarbeit-ab/#netzpolitik-pw.

Müller, Jens/Noss, Dominik/Mainka, Christian/Mladenov, Vladislav/Schwenk, Jörg, Processing Dangerous Paths – On Security and Privacy of the Portable Document Format, in: 28th Annual Network and Distributed System Security Symposium (NDSS), 2021.

Myers, Glenford J./Badgett, Tom/Thomas, Todd M./Sandler, Corey, The art of software testing, 2. Aufl., Hoboken 2004.

Naiakshina, Alena/Danilova, Anastasia/Gerlitz, Eva/von Zezschwitz, Emanuel/Smith, Matthew; "If you want, I can store the encrypted password": A Password-Storage Field Study with Freelance Developers, in: CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, no. 140, S. 1-12.

National Cyber Security Centre, Coordinated Vulnerability Disclosure: the Guideline, Oktober 2018, abrufbar: https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline.

National Telecommunications and Information Administration (NTIA), Vulnerability disclosure attitudes and actions: A Research Report from the NTIA Awareness and Adoption Group, 2016, abrufbar: https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf.

Neumann, Linus, Chaos Computer Club. Stellungnahme zum Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 17.04.2015, abrufbar: https://www.ccc.de/system/uploads/186/original/ITSG_Stellungnahme.pdf.

Ohly, Angsar, Das neue Geschäftsgeheimnisgesetz im Überblick, GRUR 2019, S. 441-451.

Openbaar Ministerie, Bijlage 2 – Jurisprudentie en praktijkvoorbeelden bij de OM-beleidsbrief Coordinated Vulnerability Disclosure December 2020, 14.12.2020, abrufbar:
https://www.om.nl/documenten/richtlijnen/2020/december/14/jurisprudentie-en-praktijkvoorbeelden.

Openbaar Ministerie, Coordinated Vulnerability Disclosure: de leidraad, 01.10.2018, abrufbar: https://www.om.nl/documenten/brochures/cybercrime/2018/oktober/coordinated-vulnerability-disclosure-de-leidraad.

Openbaar Ministerie, Inlog Twitter-account Trump niet strafbaar, Nieuwsbericht 16.12.2020 11:38, abrufbar: https://www.om.nl/actueel/nieuws/2020/12/16/inlog-twitter-account-trump-niet-strafbaar.

Paal, Boris P./Pauly, Daniel A., Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. Aufl., München 2021 (zit. *Bearb.,* in: Paal/Pauly DS-GVO/BDSG).

Pech, Sebastian, Widerrufsrecht bei kostenloser Bereitstellung digitaler Inhalte. Auswirkungen der Mod-RL und DID-RL, MMR 2022, S. 516-521.

Peeters, Gijs, Strengthening the digital Achilles heel of the European Union: Make use of ethical hackers to find vulnerabilities in information systems?, 2017, abrufbar: https://hdl.handle.net/1887/55426.

Perlroth, Nicole, This Is How They Tell Me the World Ends: The Cyberweapons Arms Race, New York 2021.

Pohlmann, Norbert/Riedel, Rene, Strafverfolgung darf die IT-Sicherheit im Internet nicht schwächen. Die Quellen-TKÜ bringt mit dem Bundestrojaner große Risiken für eine dringend notwendige vertrauenswürdige IT-Sicherheit und nachhaltige Digitalisierung, DuD 2018, S. 37-44.

RedaktionsNetzwerk Deutschland, Innenministerin will Grundgesetzänderung: Bund soll für Cybersicherheit sorgen, 12.07.2022 10:42 Uhr, abrufbar: https://www.rnd.de/politik/cybersicherheit-faeser-will-grundgesetzaenderung-bundesamt-soll-anlaufstelle-sein-OCNEZZQBUNBRZENLEQSKDHGQQM.html.

Reuter, Markus, Berliner LKA ermittelt gegen IT-Expertin, die Sicherheitslücken in Partei-App fand, 04.08.2021 10:48 Uhr, abrufbar: https://netzpolitik.org/2021/cdu-connect-berliner-lka-ermittelt-gegen-it-expertin-die-sicherheitsluecken-in-partei-app-fand/.

Ries, Uli, Büro-Drucker mit löcheriger Firmware – Sicherheitsniveau wie vor Jahrzehnten, heise security v. 12.8.2019, abrufbar: https://www.heise.de/security/meldung/Buero-Drucker-mit-loecheriger-Firmware-Sicherheitsniveau-wie-vor-Jahrzehnten-4490944.html.

Rockstroh, Sebastian/Kunkel, Hanno, IT-Sicherheit in Produktionsumgebungen. Verantwortlichkeit von Herstellern für Schwachstellen in ihren Industriekomponenten, MMR 2017, S. 77-82.

Säcker, Franz Jürgen/Rixecker, Roland/Oetker, Hartmut/Limpberg, Bettina, Münchener Kommentar zum Bürgerlichen Gesetzbuch, 8. Aufl., München 2020 (zit. *Bearb.,* in: MüKoBGB).

Schallbruch, Martin, Mehr Unabhängigkeit für das BSI?. Aufgaben und Steuerung des Bundesamtes für Sicherheit in der Informationstechnik, DuD 2021, S. 229-233.

Schmeh, Klaus, Kryptografie. Verfahren, Protokolle, Infrastrukturen, 6. Auflage, Heidelberg 2016.

Schmidt, Jürgen, l+f: Selbstbedienungsladen NSA, heise security v. 24.02.2021, abrufbar: https://www.heise.de/news/l-f-Zero-Day-Exploits-Selbstbedienungsladen-NSA-5064197.html.

Schmölzer, Gabriele: Straftaten im Internet: eine materiell-rechtliche Betrachtung, ZStW 2011, S. 709-736.

Schneier, Bruce, Click here to kill everybody, 1. Aufl., New York 2018.

Schneier, Bruce, Full Disclosure of Security Vulnerabilities a 'Damned Good Idea', 2007, abrufbar: https://www.schneier.com/essays/archives/2007/01/schneier_full_disclo.html.

Schneier, Bruce, Secrets & Lies. Digital Security in a Networked World, 15th Anniversary Edition, 2000.

Schönke, Adolf/Schröder, Horst, Strafgesetzbuch, 30. Auflage, München 2019 (zit. *Bearb.*, in: Schönke/Schröder, StGB).

Schucht, Carsten, Das neue Funkanlagengesetz (FuAG), BePr 2017, S. 474-478.

Schucht, Carsten, Safety & Security bei smarten Produkten. Weichenstellungen zur IT-Sicherheit durch den Ausschuss für Produktsicherheit, NVwZ 2021, S. 532-535.

Schuster, Heidi, Der Hackerparagraph – ein kurzes Intermezzo?. Bundesverfassungsgericht schränkt Anwendungsbereich des § 202c Abs. 1 Nr. 2 StGB ein, DuD 2009, S. 742-746.

Schwartz, Ari/Knake, Robert, Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process, Juni 2016, abrufbar: https://www.belfercenter.org/publication/governments-role-vulnerability-disclosure-creating-permanent-and-accountable.

Shane, Scott/Perlroth, Nicole/Sanger David E., Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core, The New York Times v. 12.11.2017, abrufbar: https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html.

Sheenan, John/Dunckley, Lynne, Computer Viruses and Younger Users – who are the script kiddies?, abrufbar: http://www.agentabuse.org/jsheenanA2.pdf.

Shepherd, Stephen, How do we define Responsible Disclosure?, SANS Institute Information Security Reading Room, 2003.

Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra, Datenschutzrecht. DSGVO mit BDSG, 1. Aufl., Baden-Baden 2019 (zit. *Bearb.,* in: in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht).

Spindler, Gerald, IT-Sicherheit und Produkthaftung - Sicherheitslücken, Pflichten der Hersteller und der Softwarenutzer, NJW 2004, S. 3145-3150.

Spindler, Gerald, Umsetzung der Richtlinie über digitale Inhalte in das BGB. Schwerpunkt 1: Anwendungsbereich und Mangelbegriff, MMR 2021, S. 451-457.

Spindler, Gerald/Sein, Karin, Die endgültige Richtlinie über Verträge über digitale Inhalte und Dienstleistungen. Anwendungsbereich und grundsätzliche Ansätze, MMR 2019, S. 415-420.

Spindler, Gerald/Sein, Karin, Die Richtlinie über Verträge über digitale Inhalte. Gewährleistung, Haftung und Änderungen, MMR 2019, S. 488-493.

Statistisches Bundesamt, Rechtspflege. Strafverfolgung, Fachserie 10, Reihe 3, 2020, abrufbar: https://www.destatis.de/DE/Themen/Staat/Justiz-Rechtspflege/Publikationen/Downloads-Strafverfolgung-Strafvollzug/strafverfolgung-2100300197004.pdf?__blob=publicationFile.

Stock, Ben/Pellegrino, Giancarlo/Rossow, Christian/Johns, Martin/Backes, Michael, Hey, You Have a Problem: On the Feasibility of Large-Scale Web Vulnerability Notification, in: Proceedings of the 25th USENIX Security Symposium, 2016, S. 1015-1032.

Staudenmayer, Dirk, Auf dem Weg zum digitalen Privatrecht – Verträge über digitale Inhalte, NJW 2019, S. 2497-2501.

Staudinger, Angsar/Czaplinski, Paul, Rückruf- und Kostentragungspflicht des Produzenten bei In- wie Auslandssachverhalten, JA 2008, S. 401-408.

Speit, Julian/Becker, Steffen/Ender, Maik/Puschner, Endres/Paar, Christof, Hardware-Trojaner. Die unsichtbare Gefahr, DuD 2020, S. 446-450.

Takanen, Ari/Vuorijärvi, Petri/Laakso, Marko/Röning, Juha, Agents of responsibility in software vulnerability processes, Ethics and Information Technology, Volume 6, Issue 2, 2004, S. 93-110.

Taeger, Jürgen/Gabel, Detlev, DSGVO – BDSG – TTDSG, 4. Auflage, Frankfurt am Main 2022 (zit. *Bearb.,* in: Taeger/Gabel, DSGVO).

Tremmel, Moritz, Hausdurchsuchung statt Dankeschön, golem.de v. 14.10.2021 7:00 Uhr, abrufbar: https://www.golem.de/news/nach-datenleck-hausdurchsuchung-statt-dankeschoen-2110-160269.html.

Tukey, John W., The Teaching of Concrete Mathematics, in: The American Mathematical Monthly, Volume 65, Issue 1, S. 1-9.

United States Copyright Office, Section 1201 Rulemaking: Eighth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Oktober 2021, abrufbar: https://cdn.loc.gov/copyright/1201/2021/2021_Section_1201_Registers_Recommendation.pdf.

United States Department of Justice, Policy 1 9-48.000, C omputer Fraud and Abuse Act, Mai 2022, abrufbar: https://www.justice.gov/opa/press-release/file/1507126/download.

Vettermann, Oliver, Der grundrechtliche Schutz der digitalen Identität unter Berücksichtigung von Datenschutz- und IT-Sicherheitsrecht, Karlsruhe 2022 (zit. *Vettermann*, Der grundrechtliche Schutz der digitalen Identität).

Vettermann, Oliver/Wagner, Manuela, Broken by Design? Rechtlicher Schutz und Schranken der IT-Sicherheitsforschung, InTeR 2020, S. 126-134.

Vogelgesang, Stephanie/Möllers, Frederik/Potel, Karin, Strafrechtliche Bewertung von „Honeypots" bei DoS-Angriffen. Strafbarkeit bei der digitalen Spurensuche, MMR 2017, S. 291-295.

Vonderau, Daniel/Wagner, Manuela: Vom Hörsaal in den Gerichtssaal – IT-Sicherheitsforschung als rechtliches Risiko, DSRITB 2020, S. 525- 543.

Wagner, Eric/Ruttloff, Marc, Das neue Funkanlagengesetz: Compliance-Herausforderung für Mobiltelefone, Bluetooth-Geräte und WLAN-Router, CB 2017, S. 234-239.

Wagner, Manuela, Datenökonomie und Selbstdatenschutz. Grenzen der Kommerzialisierung personenbezogener Daten, 1. Auflage, Köln 2020.

Wagner, Manuela, Hacken im Dienst der Wissenschaft: Proaktive IT-Sicherheitstests im Angesicht des Strafrechts. Strafbarkeitsrisiken und Rechtfertigungsmöglichkeiten der IT-Sicherheitsforschung, PinG 2020, S. 66-77.

Wagner, Manuela, IT-Sicherheitsforschung in rechtlicher Grauzone. Lizenz zum Hacken, DuD 2020, S. 111-120.

Wagner, Eric/Ruttloff, Marc/Miederhoff, Rebecca, Product Compliance – Ein wesentlicher Baustein für Compliance-Organisationen, CCZ 2020, S. 1-7.

Welp, Jürgen, Datenveränderung (§ 303a StGB) – Teil 1, IuR 1988, S. 443-449.

Wendehorst, Christiane/Zöchling-Jud, Brigitta, Ein neues Vertragsrecht für den digitalen Binnenmarkt?. Zu den Richtlinienvorschlägen der Europäischen Kommission vom Dezember 2015, Wien 2016 (zit. *Bearb.,* in: Wendehorst/Zöchling-Jud, Ein neues Vertragsrecht für den digitalen Binnenmarkt?).

Winkelbauer, Wolfgang, Die behördliche Genehmigung im Strafrecht, NStZ 1988, S. 201-206.

Wolfnagel, Eva, Danke für den Hinweis, Anzeige ist raus, Zeit Online v. 5.8.2021, abrufbar: https://www.zeit.de/digital/datenschutz/2021-08/cdu-connect-app-it-sicherheit-lilith-wittmann-forscherin-klage/komplettansicht.

Woszczynski, Amy/Green, Andrew/Dodson, Kelly/Easton, Peter, Zombies, Sirens, and Lady Gaga – Oh My! Developing a Framework for Coordinated Vulnerability Disclosure for U.S. Emergency Alert Systems, Government Information Quarterly, Volume 37, Issue 7, 2020, 101418.

Weulen Kranenbarg, Marleen/Holt, Thomas J./van der Ham, Jeroen, Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure, in: Crime Science, Volume 7, Issue 16, 2016, S. 1-9.

Zöchling-Jud, Brigitta, Das neue Europäische Gewährleistungsrecht für den Warenhandel, GPR 2019, S. 115-133.

digital | recht

Staat und digitale Gesellschaft

Autor:innen:
Manuela Wagner, Oliver Vettermann, Steven Arzt, Dominik Brodowski, Roman Dickmann, Niklas Goerke, Sebastian Golla, Michael Kreutzer, Maximilian Leicht, Johannes Obermaier, Marc Schink, Linda Schreiber, Christoph Sorge

Verantwortungsbewusster Umgang mit IT-Sicherheitslücken

IT-Sicherheitslücken in Hard- und Software betreffen private, unternehmerische und auch staatliche Systeme. Sobald eine Ausnutzung der Lücken technisch möglich ist, stellen sie eine Bedrohung für die IT-Sicherheit aller Beteiligten dar. Konkret betroffen sind Bürger:innen und Unternehmen als Nutzende, 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. Dieses Whitepaper führt in die rechtlichen und praktischen Probleme der IT-Sicherheitsforschung ein. Zugleich zeigt es vor allem rechtliche Auswege auf, die perspektivisch zu einer rechtssicheren IT-Sicherheitsforschung führen.