

CAROLIN KEMPER

Cybergefahrenabwehrrecht

*Beiträge zum Sicherheitsrecht
und zur Sicherheitspolitik*

20

Mohr Siebeck

Beiträge zum Sicherheitsrecht und zur Sicherheitspolitik

herausgegeben von

Jan-Hendrik Dietrich, Klaus Ferdinand Gärditz
und Kurt Graulich

20



Carolin Kemper

Cybergefahrenabwehrrecht

Die staatliche Abwehr von Gefahren
für die Cybersicherheit privater IT-Systeme

Mohr Siebeck

Carolin Kemper, geboren 1993; Studium zur Unternehmensjuristin (LL.B.) an der Universität Mannheim und der Jagiellonen-Universität Krakau; 2018 Erste Juristische Prüfung (Mannheim); Rechtsreferendariat und 2020 Zweites Staatsexamen am Landgericht Mannheim; Forschungsreferentin am Deutschen Forschungsinstitut für öffentliche Verwaltung Speyer; 2025 Promotion (Speyer); Postdoktorandin am Hasso-Plattner-Institut in Potsdam.
orcid.org/0000-0003-1790-0710

ISBN 978-3-16-200479-6 / eISBN 978-3-16-200480-2
DOI 10.1628/978-3-16-200480-2

ISSN 2568-731X / eISSN 2569-0922
(Beiträge zum Sicherheitsrecht und zur Sicherheitspolitik)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind über <https://dnb.dnb.de> abrufbar.

© 2026 Mohr Siebeck Tübingen.

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für die Verbreitung, Vervielfältigung, Übersetzung und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Das Recht einer Nutzung der Inhalte dieses Werkes zum Zwecke des Text- und Data-Mining im Sinne von § 44b UrhG bleibt ausdrücklich vorbehalten.

Gedruckt auf alterungsbeständiges Papier.

Mohr Siebeck GmbH & Co. KG, Wilhelmstraße 18, 72074 Tübingen, Deutschland
www.mohrsiebeck.com, info@mohrsiebeck.com

Für Steve Blum

Vorwort

Die vorliegende Dissertation entstand zwischen 2021 und 2024 während meiner Tätigkeit als Forschungsreferentin am Deutschen Forschungsinstitut für öffentliche Verwaltung in Speyer und wurde im September 2025 von der Deutschen Universität für Verwaltungswissenschaften Speyer angenommen.

Die Arbeit berücksichtigt die aktuelle Rechtslage, insbesondere die Neufassung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik seit der Umsetzung der NIS-2-Richtlinie. Literatur und Rechtsprechung habe ich bis zur Abgabe der Arbeit im Jahr 2024 ausgewertet. Wesentliche Quellen, insbesondere solche, die sich mit der NIS-2-Umsetzung befassen, sind seit der Abgabe ergänzt worden. Außerdem erfuhr die Arbeit einiges an Restrukturierung, um die Vorschläge des Zweitgutachtens aufzugreifen.

Herrn Professor Dr. Mario Martini danke ich vielmals dafür, dass er die Arbeit betreut und mich im Rahmen meiner Tätigkeit als Forschungsreferentin gefördert hat.

Herrn Professor Dr. Stefan Korte danke ich für die zügige Erstellung des Zweitgutachtens und ausdrücklich für seine hilfreichen Anmerkungen und weiterführenden Ideen, die das vorliegende Werk prägen und verbessert haben.

In diese Arbeit sind die Ideen, Gedanken und Impulse zahlreicher Personen eingeflossen, denen mein Dank für den inspirierenden fachlichen Austausch sowie die mentale Unterstützung gilt:

Besonders möchte ich meinen (ehemaligen) Kolleginnen und Kollegen am Forschungsinstitut für öffentliche Verwaltung danken, insbesondere Jonas Botta, Luci Haspinger, Martin Feldhaus, Rene Hermann, Thomas Kienle, Inken Kramme, Jonas Lange, Luise Lautenbach, Paul Seeliger und David Wagner. Danken möchte ich auch meiner ehemaligen Kollegin Beate Bukowski, insbesondere für das Lektorat dieser Arbeit.

Herzlich danken möchte ich auch Steve Ritter für die zahlreichen Ratschläge und kritischen Hinweise, die bis zum Schluss in die Arbeit eingeflossen sind.

Für die inhaltliche Unterstützung und wertvolle Expertise sei auch Sven Herpig (Interface) besonders hervorgehoben. Durch ihn erhielt ich Zugang zu interdisziplinären Perspektiven der aktiven Cyberabwehr.

Von besonderer Bedeutung war auch die Zusammenarbeit mit Nicolas Ziegler: Als Sparringpartner konnte ich mit ihm zentrale Denkansätze weiterentwickeln.

Mein Dank gebührt auch Max Petras und Victoria Guijarro Santos für das inspirierende Miteinander und den ständigen fachlichen wie persönlichen Rückhalt in unserer Promotionsgruppe.

Ebenso möchte ich Professorin Dr. Hannah Ruschemeier für ihre wertvollen Ratschläge in Karriere- und Fachfragen danken.

Nicht zuletzt danke ich auch meinem früheren Chef Herrn Professor Dr. Hans-Joachim Cremer. Er hat mich das „juristische Handwerkszeug“ gelehrt und meine Leidenschaft für die Rechtswissenschaft geweckt.

Mein tiefer Dank richtet sich an Michael Kolain, der mich in den letzten fünf Jahren beruflich begleitet und geprägt hat.

An letzter – und wichtigster – Stelle möchte ich meiner Familie danken: Meine Eltern, Gabriele und Dr. Bernd-Michael Kemper, haben mich auf vielfältige Weise unterstützt, indem sie u. a. nach thematisch relevanten Fachartikeln Ausschau gehalten haben, von denen viele Eingang in diese Arbeit fanden. Die Promotionsphase war zudem intensiv geprägt von der Schwangerschaft und den ersten Lebensjahren meiner Tochter, Luna. Sie macht den Abschluss dieser Arbeit umso besonderer.

Diese Arbeit ist meinem Partner Steve Blum gewidmet: Er hat sie wie kein Zweiter geprägt – durch zahlreiche Diskussionen, Korrekturlesen, aber auch durch seine emotionale Unterstützung und Bestärkung.

Speyer, im November 2025

Carolin Kemper

Inhaltsverzeichnis

Vorwort	vii
Inhaltsverzeichnis	ix
Abbildungsverzeichnis	xix
Abkürzungsverzeichnis	xx

Teil I

Cybergefahrenabwehr als Staatsaufgabe

§ 1 Einleitung	4
A. Allgegenwärtige Gefahren für unsere Gesellschaft	9
I. Log4Shell	10
II. Colonial Pipeline	13
III. Microsoft Exchange Server	15
IV. Emotet	19
B. Staatliche Cyberabwehr als Lösungsweg?	23
I. Cybersicherheit als technische, rechtliche und gesellschaftliche Herausforderung	23
II. Cybergefahrenabwehr als Notwendigkeit	26
C. Fragestellung: Der Staat als Schutzschild gegen Cyberangriffe?	31
§ 2 Die Gewährleistung von Cybersicherheit als Staatsaufgabe.....	35
A. Cybersicherheit	38
I. Schutzziele der IT-Sicherheit	40
1. Vertraulichkeit von Daten bzw. Informationen	41
2. Integrität von Daten und IT-Systemen	42
3. Verfügbarkeit von Daten und IT-Systemen	42
4. Verhältnis der Schutzziele zueinander	43
II. Schutzobjekte der IT-Sicherheit	44
III. Von der IT-Sicherheit zur Cybersicherheit	46
IV. Bewältigungsstrategien der Cybersicherheit	47
B. Nationale Sicherheit und Cybersicherheit	50
I. Sicherheit als Staatsaufgabe	51
II. Der staatliche Sicherheitsauftrag im Cyberraum	52

III.	Die „Versicherheitlichung“ des Cyberraums	56
C.	Die staatliche Verantwortung für Cybersicherheit	59
I.	Staatsaufgabe Cybersicherheit?	59
II.	Die staatliche Sicherheitsgewährleistungsverantwortung	61
1.	Von der Staatsaufgabe zur Gewährleistungsverantwortung	61
2.	Sicherheitsverantwortung zwischen grundrechtlichen Abwehrrechten und Schutzpflichten	62
3.	Zwischenfazit: Gestaltungsspielraum zwischen den Grund- rechtsdimensionen	66
III.	Die Schutzpflicht für Cybersicherheit	67
1.	Grundrechte mit Cybersicherheitsbezug im Grundgesetz ..	68
2.	Grundrechtlicher Schutz von Cybersicherheit auf EU-Ebene	75
3.	Bedürfnis eines Grundrechts auf Cybersicherheit?	78
IV.	Die Cybersicherheit Kritischer Infrastrukturen als staatlicher Verantwortungsbereich	80
1.	Der Begriff der Kritischen Infrastrukturen	81
2.	Kritische Infrastrukturen und Cybersicherheit	84
3.	Die staatliche Gewährleistungsverantwortung für (privat getragene) Kritische Infrastrukturen	85
V.	Zwischenfazit: Cybersicherheit als staatliche Gewährleistungsverpflichtung	87
D.	Gefahrenabwehr als Teil der staatlichen Verantwortung für Cybersicherheit	89
I.	Cybersicherheitsrecht als Gefahrenabwehrrecht	89
1.	Das öffentliche Cybersicherheitsrecht	90
2.	Cybersicherheit als Gegenstand des Technikrechts	94
3.	Das Polizei- und Ordnungsrecht als Basis des Gefahrenabwehrrechts	96
4.	Zwischenfazit: Cybergefahrenabwehr zwischen Polizei-, Ordnungs- und Technikrecht	99
II.	Der Wirkbereich der Gefahrenabwehr	99
1.	Der personelle Wirkbereich: Private oder staatliche Schutzobjekte	99
2.	Der räumliche Wirkbereich: Innere Sicherheit	100
3.	Der zeitliche Wirkbereich: Die Abgrenzung von Prävention und Strafverfolgung	101
4.	Der epistemische Wirkbereich: Gefahr und Risiko	102
III.	Staatliche und private Verantwortlichkeit für die Cybersicher- heit privater IT-Systeme	104
1.	Private und staatliche Verantwortlichkeit für Sicherheit	105
2.	Gefahrenabwehr zum Schutz privater IT-Systeme	106

3. Grundrechte als Maßstab für die Abgrenzung zwischen privater und staatlicher Sicherheitsverantwortung	109
E. Fazit: Cybergefahrenabwehr als Teil des staatlichen Cybersicherheitsauftrags	110

Teil II Cybersicherheit durch Gefahrenabwehr

§ 3 Cybersicherheit als Teil der öffentlichen Sicherheit	113
A. Unversehrtheit der Rechtsordnung	114
I. Cyberkriminalität	114
1. Angriffe auf die IT-Sicherheit	115
2. Folgestraftaten	119
3. Keine Strafbarkeit für unsichere IT-Systeme	121
4. Zwischenfazit: Strafrechtlicher Fokus auf Cyberangriffe	122
II. IT-Sicherheitspflichten	122
1. Anforderungen für Hersteller	123
2. Verpflichtung zur Datensicherheit (Art. 32 DSGVO)	123
3. Sicherungspflichten für bestimmte Betreibergruppen	123
III. Zwischenfazit: Cybersicherheit als Schutzgut der Rechtsordnung	125
B. Kollektive Rechtsgüter	125
I. Cybersicherheit als kollektives Rechtsgut?	125
1. Allgemeine „Cyberhygiene“	126
2. IT-Sicherheit weitverbreiteter Anwendungen und Systeme	128
II. Kritische Infrastrukturen als Gemeinschaftsrechtsgut	129
III. Zwischenfazit: Das öffentliche Interesse an Cybersicherheit ...	130
C. Individualrechtsgüter	131
I. Betroffene Rechtsgüter bei Cyberangriffen	131
II. Betroffene Rechtsgüter bei unsicherer IT-Systemen	131
III. Grenzen des Individualrechtsgüterschutzes	132
D. Fazit: Cybersicherheit als Teil der öffentlichen Sicherheit	133
§ 4 Gefahren für die Cybersicherheit	135
A. Die allgemeine Bedrohungslage	138
I. Die Bedrohungslage als Risiko	138
II. Cybersicherheitsbedrohungen als abstrakte Gefahren?	139
B. Gefahren durch Cyberangriffe	140
I. Typischer Ablauf eines Cyberangriffs	141
1. Auskundschaftung (Reconnaissance)	143
2. Bewaffnung (Weaponization)	145
3. Auslieferung (Delivery)	146

4.	Kompromittierung des Systems (Command and Control)	147
5.	Schadensausübung (Actions on Objectives)	148
II.	Cyberangriffe zwischen Gefahrenvorfeld und Störung	148
III.	Erhöhung der Gefahrenstufe bei besonderen Gefahrenlagen	149
1.	Anpassung der Prognose bei Advanced Persistent Threats	149
2.	Anpassung der Prognose nach der Je-desto-Formel	150
IV.	Zwischenfazit: Cyberangriffe als Herausforderung für die Dogmatik des Gefahrenabwehrrechts	151
C.	Gefahren durch Schwachstellen in IT-Produkten	151
I.	Schwachstellen in IT-Produkten als abstrakte Gefahren?	152
II.	Zero-Day-Schwachstellen als Risiko	153
D.	Gefahren unsicherer IT-Systeme	154
I.	Gefahrenverdacht bei Schwachstellen	154
II.	Konkrete Gefahren bei strategischen Zielen?	155
III.	Unsichere IT-Systeme als Störung	156
IV.	Zwischenfazit: Unsichere IT-Systeme zwischen Risiko und Gefahr	157
E.	Qualifizierte Cybergefahren für besondere Schutzgüter	158
I.	Hochrangige Schutzgüter und erhebliche Störungen	159
1.	Schadenspotenziale einzelner IT-Systeme	159
2.	Kollektive Schadenspotenziale	159
II.	Qualifikation der Erheblichkeit von Cybergefahren	160
1.	Allgemeine Bedrohungslage: Warnstufen des BSI	160
2.	Bewertung von Schwachstellen	161
3.	Die Kategorisierung von Vorfällen	162
III.	Zwischenfazit: Erheblichkeitsabhängige Cybergefahrenabwehr	166
F.	Fazit: Cybergefahrenabwehr zwischen Gefahrenvorfeld und Störungsbewältigung	167

Teil III

Maßnahmen der Cybergefahrenabwehr

§ 5	Systematisierung von Cybergefahrenabwehrmaßnahmen	171
A.	Genese potenzieller Maßnahmen zur Cybergefahrenabwehr	171
I.	Maßnahmen der aktiven Cyberabwehr	172
1.	Aktive Cyberabwehr zwischen Defensive und Offensive	173
2.	Informationsbeschaffung und -austausch	176
3.	Denial and Deception (Verweigerung und Täuschung)	177
4.	Eindämmung von Bedrohungen	178
5.	Infiltration und Übernahme von Angriffssystemen	179

6.	Die Eignung aktiver Cyberabwehrmaßnahmen zur Gefahrenabwehr	181
7.	Die Eignung des Gefahrenabwehrrechts als Rahmen für die aktive Cyberabwehr	184
II.	Maßnahmen des Vorfallmanagements	185
1.	Erkennung, Identifikation und Analyse	186
2.	Eindämmung	187
3.	Entfernen schädlicher Komponenten	188
4.	Wiederherstellung	188
5.	Die ganze Zeit: Business Continuity	189
6.	Vorfallbewältigung und Gefahrenabwehr	189
B.	Einordnung der Cybergefahrenabwehrmaßnahmen	190
I.	Verortung in der gefahrenabwehrrechtlichen Dogmatik	190
1.	Rechtsform der Maßnahmen und Vollstreckung	190
2.	Aktionelle und informationelle Maßnahmen	192
3.	Selbstvornahme oder Anordnung	193
4.	Gebundene oder Ermessensentscheidungen	193
5.	Verfahrensanforderungen	195
II.	Maßnahmenadressaten	195
III.	Eingriffstiefe	198
IV.	Zeitlicher Anknüpfungspunkt und Zielrichtung von Maßnahmen	199
1.	Gefahrenvorsorge	199
2.	Abwehr von Cyberangriffen	200
3.	Bewältigung von Gefahren unsicherer IT-Produkte und IT-Systeme	201
C.	Fazit: Das Maßnahmenportfolio einer effektiven Cybergefahrenabwehr	201
§ 6	Cybergefahrenabwehr durch Informationsvorsorge	203
A.	Generieren von Informationen über Cybergefahren	204
I.	Informationen über Cyberbedrohungen	204
1.	Bezugsobjekte von Informationen	204
2.	Quellen von Informationen zur Cybergefahrenabwehr	208
II.	Beschaffung allgemeiner Informationen über Bedrohungen für die Cybersicherheit	211
1.	Befugnisse des BSI für die Beschaffung von Informationen	211
2.	Gefahrenabwehrrechtliche Informationsbeschaffung im Internet	216
3.	Zwischenfazit: Geringfügige Grundrechtseingriffe durch die Beschaffung allgemeiner Informationen	220

III.	Erforschen von Angriffsmethoden durch den Einsatz von Honeypots	220
1.	Technische Vorgehensweise	221
2.	Befugnis des BSI zum Betrieb von Honeypots (§ 15 Abs. 5 BSIG)	222
3.	Rechtsgrundlagen aus dem allgemeinen Gefahrenabwehrrecht	226
IV.	Entgegennahme von Informationen durch Meldungen	226
1.	Meldepflichten für regulierte Einrichtungen (§ 32 BSIG)	227
2.	Meldepflichten für Hersteller	228
3.	Freiwillige Meldungen	228
4.	Einrichtung einer bundesweiten, zentralen Meldestelle	228
5.	Weitere Möglichkeiten zum Austausch von Informationen über Cyberbedrohungen	229
B.	Staatliches Bereitstellen von Informationen über Cybersicherheit	230
I.	Formen des Bereitstellens von allgemeinen Informationen über Cybersicherheit	233
1.	Öffentlichkeitsarbeit	234
2.	Informationen und Hinweise	234
3.	Empfehlungen	235
4.	Warnungen	236
II.	Veröffentlichen von allgemeinen Informationen über Cyberbedrohungen	236
1.	Die Veröffentlichung allgemeiner Informationen durch das BSI	236
2.	Informationen über Schwachstellen in Datenbanken	237
3.	Pflicht des BSI zur Bereitstellung von Informationen an bestimmte Adressatenkreise	239
III.	Informationen über spezifische Vorfälle	239
IV.	Rückmeldungen des BSI gegenüber meldenden Einrichtungen	240
C.	Fazit: Informationsvorsorge als Voraussetzung für eine effektive Cybergefahrenabwehr	240
§ 7	Abwehr von gegenwärtigen Cyberangriffen	243
A.	Maßnahmen gegen Angriffssystemen	244
I.	Angreifende als Verhaltensverantwortliche	244
1.	Technische Attribution von Cyberangriffen	245
2.	Attribution von Cyberangriffen in der Gefahrenabwehr ..	247
II.	Gegenangriffe	248
1.	Bestehende Befugnisse des BSI	249
2.	Vorschläge einer Befugnis zu digitalen Gegenschlägen für die Bundespolizei	250
3.	Invasive Operationen, hohe Risiken	251

III.	Kollateralschäden: Die Problematik der Inanspruchnahme Unbeteiligter	253
IV.	Stilllegen von Angriffssystemen	254
V.	Zerschlagen von Angriffsstrukturen	257
B.	(Wieder-)Herstellung der IT-Sicherheit angegriffener Systeme	259
I.	Die Verantwortlichkeit von Betreibern	259
II.	Die Sicherung betroffener Systeme	260
1.	Anordnung von Sicherheitsmaßnahmen	261
2.	Unterstützung durch das BSI auf Ersuchen (§ 11 BSIG) ..	268
3.	Angebot des BSI zur Unterstützung bei der Behebung von meldepflichtigen Sicherheitsvorfällen (§ 36 Abs. 1 BSIG)	274
4.	Selbsteintritt im Wege der Ersatzvornahme?	274
5.	Zwischenfazit: Staatliche Hilfe bei der Vorfallsbewälti- gung	275
III.	Entfernen von Schadsoftware	276
1.	Anordnung der Bereinigung von Schadprogrammen durch das BSI (§ 16 Abs. 1 S. 1 Nr. 2 BSIG)	277
2.	Bereinigung infizierter Systeme direkt durch Behörden ..	283
3.	Zwischenfazit: Staatliche Zugriffe auf private IT-Systeme zur Abwehr von Cyberangriffen?	286
IV.	Zwischenfazit: Begrenzte staatliche Verantwortung für infizierte IT-Systeme Privater	287
C.	Datenverkehrsbezogene Maßnahmen	287
I.	Technische Durchführung	288
II.	Befugnis zur Anordnung datenverkehrsbezogener Maßnah- men durch das BSI (§ 16 Abs. 1 S. 1 Nr. 1 BSIG)	290
1.	Voraussetzungen	291
2.	Rechtsfolge: Anordnung der Maßnahmen nach § 169 Abs. 6 und 7 TKG	291
3.	Begleitbefugnisse zur Datenverarbeitung	293
4.	Verhältnismäßigkeit der Grundrechtseingriffe	294
III.	Polizeirechtliche Befugnisse zur Unterbrechung der Telekommunikation	295
D.	Fazit: Die Notwendigkeit von Maßnahmen zur Abwehr von Cyberangriffen	297
§ 8	Abwehr von Gefahren durch unsichere Produkte	299
A.	Die Verantwortlichkeit der Hersteller	299
B.	Untersuchung der Sicherheit von IT-Produkten	301
I.	Untersuchungsbefugnis des BSI (§ 14 Abs. 1 S. 1 BSIG)	302
II.	Mitwirkungspflichten der Hersteller	303
III.	Grundrechtseingriffe und Verhältnismäßigkeit	304

C. Veröffentlichung von Informationen über die IT-Sicherheit von Produkten	304
D. Warnungen vor Schwachstellen in IT-Produkten und IT-Systemen	306
I. Warnungen und Responsible Disclosure	307
II. Warnung vor unsicheren IT-Produkten (§ 13 BSIG).....	310
1. Warnungsgegenstände	310
2. Anforderungen an das Vorgehen.....	313
3. Veröffentlichung der Warnung	314
III. Warnungen im Rahmen der Marktüberwachung.....	318
E. Anordnungen und Maßnahmen gegenüber Herstellern	318
I. Marktüberwachungsbefugnisse	319
1. Allgemeine Marktüberwachungsbefugnisse	319
2. Marktüberwachungsbefugnisse nach der Cyberresilienz-VO.....	320
II. Anordnung der Mitwirkung an der Beseitigung von Sicherheitsvorfällen (§ 18 BSIG)	321
F. Fazit: IT-Produkte als Gefahrenursache.....	321
§ 9 Abwehr von Gefahren für unsichere IT-Systeme	325
A. Verantwortlichkeit von Betreibern für unsichere IT-Systeme	325
I. Verantwortlichkeit für unsichere IT-Systeme?	325
1. Betreiber als Verantwortliche?	325
2. Inanspruchnahme als Nichtverantwortliche	327
3. Inanspruchnahme von Privatpersonen	327
II. Verantwortlichkeit durch Sicherungspflichten.....	328
1. Eigensicherungspflichten für Betreiber	328
2. Eingrenzung der pflichtigen Betreiber in Befugnisnormen zur Wahrung der Verhältnismäßigkeit	329
III. Zwischenfazit: Verantwortlichkeit nur bei verletzten Cybersicherheitspflichten	331
B. Detektion von Sicherheitsrisiken	331
I. Technische Vorgehensweise	332
II. Detektion von Sicherheitsrisiken durch das BSI (§ 15 Abs. 1 bis 4 BSIG)	335
1. Detektionsmaßnahmen als Informationsvorsorge und Voraussetzung zur Gefahrenabwehr	335
2. Voraussetzungen und Handlungsfeld der Detektionsmaßnahmen	336
3. Prüftiefe der Detektionsmaßnahmen	337
4. Datenverarbeitungsbefugnisse	338
5. Grundrechtseingriffe und Verhältnismäßigkeit	339
6. Zwischenfazit: Milde bis keine Grundrechtseingriffe.....	340
III. Gefahrenabwehrrrechtliche Befugnisse	341

C. Benachrichtigung über konkrete Bedrohungen	342
I. Benachrichtigung Betroffener durch Behörden	342
1. Ermittlung der Betroffenen: Auskunft über Telekommunikationsdaten.....	342
2. Informationspflicht des BSI bei Auffinden einer Schwachstelle (§ 15 Abs. 2 BSIg)	343
3. Gefahrenabwehrrechtliche Benachrichtigung	344
4. Die Betroffenenbenachrichtigung als Grundrechtseingriff	344
5. Zwischenfazit: Die behördliche Pflicht zur Benachrichtigung über Sicherheitsrisiken	345
II. Anordnung der Benachrichtigung Dritter über Vorfälle	346
D. Maßnahmen zur Herstellung der IT-Sicherheit	346
I. Anordnung von Sicherheitsmaßnahmen	346
1. Anordnung von Maßnahmen gegenüber besonders wichtigen und wichtigen Einrichtungen	346
2. Anordnung von Maßnahmen gegenüber Anbietern von digitalen Diensten (§ 17 BSIg)	347
3. Anordnungen von Sicherungsmaßnahmen auf der Grundlage polizeilicher Generalklauseln?	349
4. Zwischenfazit: Gefahrenabwehr durch Anordnung von Sicherheitsmaßnahmen	349
II. Installieren von Sicherheitsupdates (§ 16 Abs. 1 S. 1 Nr. 2 BSIg)	349
III. Absicherung unsicherer IT-Systeme	352
IV. Zwischenfazit: Die individualbezogene Cybergefahrenabwehr	353
E. Fazit: Unsichere IT-Systeme als Anknüpfungspunkt einer Cybergefahrenabwehrstrategie	352

Teil IV

Organisation der Cybergefahrenabwehr

§ 10 Die staatliche Cybergefahrenabwehrarchitektur.....	357
A. Staatliche Einrichtungen der Cybergefahrenabwehr	359
I. Die Cybergefahrenabwehrbehörden	360
1. Das Bundesamt für Sicherheit in der Informationstechnik als zentrale IT-Sicherheitsbehörde	361
2. Das Bundeskriminalamt und seine Zuständigkeit für die Verhütung von Cyberkriminalität	376
3. Die Bundespolizei als moderne Grenzschutzbehörde	379
4. Die Cybergefahrenabwehr durch die Länder	381
5. Die Zuständigkeit der Katastrophenschutzbehörden im Cyber-Katastrophenfall	384

6.	Zwischenfazit: Myriaden von Cybergefahrenabwehr-	
	behörden	386
II.	Notfallteams für die Bewältigung von Sicherheitsvorfällen	386
III.	Informelle und ergänzende Einrichtungen	389
1.	Das Nationale Cyber-Abwehrzentrum	390
2.	Die Agentur der Europäischen Union für Cybersicher-	
	heit	391
3.	Die Netzwerke der Notfallteams	393
4.	Weitere Einrichtungen und Strukturen	394
IV.	Cybergefahrenabwehr im Netzwerk	396
B.	Grundkonflikte der Cybergefahrenabwehrrordnung	399
I.	Der horizontale Grundkonflikt zwischen polizeilichen und	
	regulierenden Behörden	400
II.	Der vertikale Grundkonflikt zwischen Ländern, Bund und EU	401
III.	Unsicherheiten der Attribution und Klassifizierung von	
	Cyberbedrohungen	404
1.	Militärische Zuständigkeit für Cyberangriffe?	405
2.	Nachrichtendienstliche Zuständigkeit für Cyberangriffe?	407
3.	Attributionskompetenz oder Zweifelsregelung?	409
C.	Fazit: Der Fortbestand der bisherigen cybersicherheitsrechtlichen Ord-	
	nung als Problem	412

Schluss

Cybergefahrenabwehr als Teil der Cybersicherheitsarchitektur

§ 11	Gefahrenabwehr in der Cybersicherheitsarchitektur	417
A.	Das Cybersicherheitsrecht – Mosaik oder Flickenteppich?	418
B.	Der Fokus der Gefahrenabwehr auf Schadensverhinderung und -min-	
	derung	420
C.	Die Adressaten von Gefahrenabwehrmaßnahmen	421
D.	Die staatliche Verantwortung für private IT-Systeme	422
E.	Cybergefahrenabwehr im Netzwerk	423
F.	Ausblick	424
§ 12	Thesen der Arbeit	427
	Glossar	433
	Literaturverzeichnis	441
	Stichwortverzeichnis	495

Abbildungsverzeichnis

Abbildung 1 – Kategorisierung von Cybervorfällen	165
Abbildung 2 – Spektrum möglicher Gefahrenabwehrmaßnahmen	199

Abkürzungsverzeichnis¹

a. a. O.	am angegebenen Ort
a. E.	am Ende
a. F.	Alte Fassung
ABl.	Amtsblatt
AG KRITIS	Arbeitsgruppe Kritische Infrastrukturen
APT	Advanced Persistent Threat
ASOG Bln	Allgemeines Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung in Berlin
AtG	Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren
Aufl.	Auflage
AusschussDrs.	Ausschussdrucksache
AVwVMeldeVf	Allgemeine Verwaltungsvorschrift über das Meldeverfahren
AWV	Außenwirtschaftsverordnung
BaFIN	Bundesanstalt für Finanzdienstleistungsaufsicht
Bay., bay.	Bayern, bayerisch
Bbg., bbg.	Brandenburg, brandenburgisch
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BeckOK	Beck'scher Online-Kommentar
BfDI	Bundesbeauftragte(r) für Datenschutz und Informationsfreiheit
BfV	Bundesamt für Verfassungsschutz
BGB	Bürgerliches Gesetzbuch
BGBL.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BImSchV	Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes
BKA	Bundeskriminalamt
Bln, bln.	Berlin, berlinerisch
BMI	Bundesministerium des Innern
BND	Bundesnachrichtendienst
BNDG	Gesetz über den Bundesnachrichtendienst
BNetzAG	Gesetz über die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BNetzAgentur	Bundesnetzagentur
BPolG	Gesetz über die Bundespolizei (Bundespolizeigesetz)

¹ Vgl. auch *Kirchner*, Abkürzungsverzeichnis der Rechtssprache (11. Aufl. 2024).

BR	Bundesrat
Brem, brem.	Bremen, bremisch
BSH	Bundesamt für Seeschifffahrt und Hydrographie
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BStatG	Gesetz über die Statistik für Bundeszwecke
BT	Bundestag
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen der amtlichen Sammlung des Bundesverfassungsgerichts
BVerfSchG	Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz
BVerwG	Bundesverwaltungsgericht
BW, bw.	Baden-Württemberg, baden-württembergisch
CER-Richtlinie	Richtlinie über die Resilienz kritischer Einrichtungen (EU) 2022/2557
CERT	Computer Emergency Response Team
CIR	Cyber- und Informationsraum (militärischer Organisationsbereich der Bundeswehr)
CISA	Cybersecurity and Infrastructure Security Agency
C&C-Server	Command-and-Control-Server
CRA, Cyberresilienz-VO	Cyberresilience Act, Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (EU) 2024/2847
CSA	Cybersecurity Act, Rechtsakt zur Cybersicherheit, Verordnung (EU) 2019/881
CSG BW	Gesetz für die Cybersicherheit in Baden-Württemberg
CSIRT	Computer Security Incident Response Team
CVD-Leitlinie	Leitlinie des BSI zum Coordinated Vulnerability Disclosure (CVD)-Prozess
DDG	Digitale-Dienste-Gesetz
DDoS-Angriff	„Distributed Denial of Service“-Angriff
DMA	Digital Markets Act, Verordnung über bestreitbare und faire Märkte im digitalen Sektor (EU) 2022/1925
DORA	Verordnung über die digitale operationale Resilienz im Finanzsektor (EU) 2022/2554
DoS-Angriff	„Denial of Service“-Angriff
DRDoS-Angriff	„Distributed Reflected Denial of Service“-Angriff
Drs.	Drucksache
DSGVO	Datenschutz-Grundverordnung
DVO	Durchführungsverordnung
E	Entwurf
ebd.	ebenda
EGMR	Europäischer Gerichtshof für Menschenrechte
ehem.	ehemalig, ehemalige, ehemaliger, ehemaliges
Einf.	Einführung
Einl.	Einleitung

engl.	englisch
ENISA	Die Agentur der Europäischen Union für Cybersicherheit
ENISA-VO	Verordnung zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit (EG) Nr. 460/2004
EnWG	Gesetz über die Elektrizitäts- und Gasversorgung
Erwgr.	Erwägungsgrund
EuGH	Europäischer Gerichtshof
f., ff.	folgende Seite bzw. Seiten
FBI	Federal Bureau of Investigation
FS	Festschrift
Fn.	Fußnote
FS	Festschrift
G	Gesetz
gem.	gemäß
GeschGehG	Geschäftsgeheimnisgesetz
GPSR	General Product Safety Regulation, Verordnung über die allgemeine Produktsicherheit (EU) 2023/988
GRCh	Europäische Grundrechtecharta
HdB	Handbuch
Hervorh.	Hervorhebung
Hess., hess.	Hessen, hessisch
HITSiG	Hessisches IT-Sicherheitsgesetz
Hmb., hmb.	Hamburg, hamburgisch
Hrsg., hrsg.	Herausgeber, herausgegeben
Hs.	Halbsatz
HStR	Handbuch des Staatsrechts, hrsg. v. Josef Isensee und Paul Kirchhof
i. e. S.	im engeren Sinne
i. R. v.	im Rahmen von
i. S. v.	im Sinne von
i. Ü.	im Übrigen
i. V. m.	in Verbindung mit
i. H. v.	in Höhe von
IoT	Internet of Things bzw. Internet der Dinge
IP-Adresse	Internet-Protocol-Adresse
IT	Informationstechnik
IT-Sicherheit	Sicherheit von Informationstechnik
IT-Sicherheitsgesetz 2.0	Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (BGBl. 2021 I, S. 1122)
ITSiV-PV	Verordnung zur Gewährleistung der IT-Sicherheit der im Portalverbund und zur Anbindung an den Portalverbund genutzten IT-Komponenten (BGBl. 2022 I, S. 18)
IT-System	informationstechnisches System
IuK-Technik	Informations- und Kommunikationstechnik
Jg., Jge.	Jahrgang, Jahrgänge
JI-RL,	Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Ver-
JI-Richtlinie	

	folgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (EU) 2016/680
KRITIS	Kritische Infrastrukturen
KRITIS-Betreiber	Betreiber Kritischer Infrastrukturen bzw. Betreiber kritischer Anlagen
lit.	litera
LSA	Sachsen-Anhalt
LT	Landtag
LVerfGSchG	Landesverfassungsschutzgesetz
LVwG	Landesverwaltungsgesetz
m. Anm.	mit Anmerkung
MAC-Adresse	Media Access Control-Adresse
MAD	Militärischer Abschirmdienst
MEPolG	Musterentwurf eines einheitlichen Polizeigesetzes
MIRT	Mobile Incident Response Team
MüG	Marktüberwachungsgesetz
MÜ-VO	Verordnung über Marktüberwachung und die Konformität von Produkten (EU) 2019/1020
MV, mv	Mecklenburg-Vorpommern, mecklenburg-vorpommersch
n. F.	Neue Fassung
NCSC	National Cyber Security Centre
Nds., nds.	Niedersachsen, niedersächsisch
NIS2-RL,	Richtlinie über Maßnahmen für ein hohes gemeinsames Cyber-
NIS-2-Richtlinie	sicherheitsniveau in der Union (EU) 2022/2555
NIS-2-Umsetzungs-	Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung
gesetz	wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung
NIS-RL,	Richtlinie über Maßnahmen zur Gewährleistung eines hohen
NIS-Richtlinie	gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (EU) 2016/1148
NPOG	Niedersächsisches Polizei- und Ordnungsbehördengesetz
NRW, nrw.	Nordrhein-Westfalen, nordrhein-westfälisch
NSA	National Security Agency
OSINT	Open Source Intelligence
OT	Operational Technology
OVG	Oberverwaltungsgericht
OZG	Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz)
PAG	Polizeiaufgabengesetz
PC	Personal Computer
POG	Polizei- und Ordnungsbehördengesetz
PolG	Polizeigesetz
PolR	Polizeirecht
PrALR	Preußisches Allgemeines Landrecht
ProdHaftG	Produkthaftungsgesetz
ProdSG	Produktsicherheitsgesetz
R	Recht
RefE	Referentenentwurf
RFC	Request for Comments

RhPf, rhpf.	Rheinland-Pfalz, rheinland-pfälzisch
RL	Richtlinie
Rn.	Randnummer
Rspr.	Rechtsprechung
Saarl., saarl.	Saarland, saarländisch
Sachs., sächs.	Sachsen, sächsisch
SächsISichG	Sächsisches Informationssicherheitsgesetz
SächsPVDG	Sächsisches Polizeivollzugsdienstgesetz
SCADA-System	„Supervisory Control and Data Acquisition“-System
SchlH, schlh.	Schleswig-Holstein, schleswig-holsteinisch
Slg.	Sammlung
SOG	Sicherheits- und Ordnungsgesetz
st.	ständig
StGB	Strafgesetzbuch
Störfall-VO	Zwölfte Verordnung zur Durchführung des Bundes-Immissions- schutzgesetzes (Störfall-Verordnung)
StPO	Strafprozessordnung
str.	streitig, strittig, umstritten
StVG	Straßenverkehrsgesetz
sublit.	Unterbuchstabe
TDDDG	Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten
Thür., thür.	Thüringen, thüringisch
TK-Anbieter	Anbieter von Telekommunikationsdiensten
TKG	Telekommunikationsgesetz
TM-Anbieter	Anbieter von Telemedienangeboten
TM-Angebot	Telemedienangebot
TMG	Telemediengesetz
TOR	The Onion Router
TTDSG	Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien
u. U.	unter Umständen
UAbs.	Unterabsatz
ÜAnlG	Gesetz über überwachungsbedürftige Anlagen
Urt.	Urteil
US	United States
USA	United States of America, Vereinigte Staaten von Amerika
Var.	Variante
VG	Verwaltungsgericht
VGH	Verwaltungsgerichtshof
VO	Verordnung
Vol.	Volume, Band
Vorb.	Vorbemerkung
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
Ziff.	Ziffer
ZKA	Zollkriminalamt

Teil I

Cybergefahrenabwehr als Staatsaufgabe

§ 1 Einleitung

Cybersicherheit ist eine grundlegende Voraussetzung für das Funktionieren unserer Gesellschaft, denn Informationstechnik ist allgegenwärtig und sie ist verletzlich.¹ Gefahren für die Cybersicherheit gehören längst zum Alltag. Maßgeblich sind dabei weniger die großen, katastrophalen Cyberangriffe, die Blackouts oder gar Unfälle in Atomkraftwerken verursachen könnten.² Denn tagtäglich richten unzählige Cyberangriffe Schäden an – und können jeden treffen.

Als Russland im Jahr 2022 seinen Angriffskrieg gegen die Ukraine begann, erwarteten viele einen „Cyberkrieg“.³ Tatsächlich legte ein Angriff auf den Satellitennetz-Provider Viasat den Internetzugang ukrainischer Kundinnen und Kunden – unter anderem auch den des ukrainischen Militärs – lahm.⁴ Der Angriff hatte europaweite Auswirkungen; zum Beispiel waren in Deutschland

¹ Vgl. *Roßnagel/Wedde/Hammer/Pordesch*, Die Verletzlichkeit der „Informationsgesellschaft“ (2. Aufl. 1989), S. 5 ff., 79 ff. Siehe auch BT-Drs. 11/7029, S. 1; *Hornung/Schallbruch*, in: *Hornung/Schallbruch/Bäcker*, IT-Sicherheitsrecht (2. Aufl. 2025), § 1 Rn. 1 ff.; *Leisterer*, Internetsicherheit in Europa (2018), S. 2 f.; *Olejnik/Kurasinski*, Philosophy of Cybersecurity (2024), S. 2 ff.; *Wischmeyer*, Informationssicherheit (2023), S. 3 ff.

² *Röhrlich*, Hackerangriffe auf Atomkraftwerke – Abwehrstrategien sind schwierig zu entwickeln, Deutschlandfunk vom 08.07.2016. Das Schreckensszenario wird z. T. auch als „Cyber Pearl Harbor“ bezeichnet: *Panetta*, Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security. Siehe auch *Bumiller/Shanker*, Panetta Warns of Dire Threat of Cyberattack on U.S., The New York Times vom 11.10.2012; *Goldman/Warner*, Why a Digital Pearl Harbor Makes Sense ... and Is Possible, in: *Perkovich/Levite* (Hrsg.), *Understanding Cyber Conflict* (2017), S. 147. Freilich ist das Gefahrenpotenzial für Kritische Infrastrukturen nicht auf Cyberangriffe begrenzt – Sabotageakte oder Fehler können ebenfalls zum Ausfall oder der Beeinträchtigung von Kritischen Infrastrukturen führen, vgl. *Nolte*, Flugausfälle durch gekapptes Glasfaserkabel: Der Fehler liegt bei der Lufthansa, heise Online vom 18.02.2023; *Sawall*, Glasfaser: Anschlag auf Bahn-Kabel erfolgte mit Insiderwissen, Golem.de vom 10.10.2022.

³ Vgl. bspw. *Knoll*, Streitkräfteeinsatz zur Verteidigung gegen Cyberangriffe (2020), S. 37 ff.; *Olejnik/Kurasinski*, Philosophy of Cybersecurity (2024), S. 141 ff. *Kello*, The Virtual Weapon and International Order (2017), S. 17.

⁴ *Der Spiegel*, „Cyber-Kollateralschaden“ auch in Deutschland: Satellitennetzwerk Viasat offenbar gezielt in Osteuropa gehackt, 05.03.2022, <https://www.spiegel.de/netzwelt/web/viasat-satellitennetzwerk-offenbar-gezielt-in-osteuropa-gehackt-a-afd98117-5c32-4946-ab8a-619f1e7af024>.

über 3.000 Windräder nicht mehr zur Fernwartung erreichbar.⁵ Außerdem trennte Ende 2023 ein Cyberangriff auf den Telekommunikationsdienstleister Kyivstar rund 24 Millionen ukrainische Kundinnen und Kunden vom Internet.⁶ Hinzu kommen zahlreiche, aber nur begrenzt effektive, Angriffe auf Banken und Verwaltungsbehörden mit sog. „Wiper“-Schadsoftware, die Daten befähigter Systeme löscht;⁷ ferner überlasteten sog. „Denial-of-Service“-Angriffe ukrainische Webseiten mit Anfragen, sodass diese nicht mehr abrufbar waren (sog. Web-Defacement).⁸ Ein Angriff auf ukrainische Umspannwerke, der zu Stromausfällen führen sollte, blieb dagegen erfolglos.⁹ Im Vergleich dazu konnte die russische Gruppe „Sandworm“ im Jahr 2015 einen mehrstündigen Blackout für ungefähr 80.000 ukrainische Kundinnen und Kunden erreichen¹⁰ und im Oktober 2023 gelang es russischen Angreifenden aber, (auch) durch einen Cyberangriff die Stromversorgung zu beeinträchtigen.¹¹ Größere strategische Erfolge durch Cyberoperationen gelangen Russland folglich nicht¹² – Russland führt den Krieg gegen die Ukraine hauptsächlich mit konventionellen Methoden und kinetischen Waffen; Cyberangriffe sollen diese nur ergänzen (sog. hybride Kriegsführung).¹³

Man könnte daher zu dem Schluss kommen, dass die Gefahren für die Cybersicherheit gar nicht so gravierend seien und physischen Bedrohungen nicht

⁵ *Biermann/Wolfangel*, Cyberkrieg: Angriff im Rücken der ukrainischen Armee, *Die Zeit* vom 23.02.2023.

⁶ *Stöckel*, Ukraine: Russische Hacker verbrachten wohl Monate im Kyivstar-Netz, *Golem.de* vom 05.01.2024.

⁷ *Holland*, Ukraine-Krieg: So viele Angriffe mit zerstörerischen Wipern wie nie zuvor, *heise Online* vom 24.02.2023; *Greenberg*, Ukraine Suffered More Wiper Malware in 2022 Than Anywhere, Ever, *WIRED* vom 22.02.2023.

⁸ *Conger/Sanger*, Hackers Claim to Target Russia With Cyberattacks and Leaks, *The New York Times* vom 22.04.2022; *Lindern/Polke-Majewski/Biermann*, Cyberangriff auf die Ukraine: Digitale Nadelstiche, *Die Zeit* vom 16.02.2022. vgl. auch *BSI*, Die Lage der IT-Sicherheit in Deutschland 2022, S. 11, 43 ff. Kritisch; *Brenner*, *J. Crim. L. & Criminology* 97 (2007), 379 (390 ff.).

⁹ Vgl. *ESET*, Industroyer2: Angriffe auf ukrainische Energiewirtschaft, 12.04.2022. Vgl. auch *Greenberg*, Pipedream Malware: Feds Uncover „Swiss Army Knife“ for Industrial System Hacking, *WIRED* vom 13.04.2022; *Dragos, Inc.*, Pipedream: Chernovite's Emerging Malware Targeting Industrial Control Systems (2022).

¹⁰ *Zetter*, Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, *WIRED* vom 03.03.2016.

¹¹ *Mäder*, Cyberattacke auf Stromnetz: Russische Hacker mit neuartigem Vorgehen, *NZZ* vom 09.11.2023.

¹² Siehe u. a. *Gibney*, Was ist mit Russlands Cyberwar?, *Spektrum.de* vom 02.04.2022; *Schmidt*, Russlands Krieg: Was droht uns im Cyberspace?, *heise Online* vom 16.03.2022.

¹³ *Burt*, The hybrid war in Ukraine, *Microsoft On the Issues* vom 27.04.2022; *Hartmann*, Hybride und konventionelle Kriegsführung in der Ukraine vom 19.11.2023; *Knoll*, Streitkräfteeinsatz zur Verteidigung gegen Cyberangriffe (2020), S. 59 ff.; *Schmidt*, Russlands Krieg: Was droht uns im Cyberspace?, *heise Online* vom 16.03.2022; *Taminga*, *SWP-Aktuell* 2015 Nr. 27, S. 1 ff.

einmal im Ansatz gleichkämen. Allerdings muss das auch nicht das Ziel sein: Cyberangriffe können ein zweckmäßiges Mittel sein, um gegnerischen Staaten zu schaden, ohne die Intensität eines bewaffneten Angriffs (und damit den Kriegszustand) zu erreichen. Russland führt schon seit Jahren digitale Feldzüge gegen die Ukraine – immer unter dem Deckmantel der Cyberkriminalität. Am 27. Juni 2017 löschte das Schadprogramm „NotPetya“ die Daten zahlreicher IT-Systeme in der Ukraine (und weltweit).¹⁴ Der Name „NotPetya“ rührt daher, dass IT-Sicherheitsexpertinnen und -experten zu Beginn des Angriffs dachten, es handle sich um die Ransomware Petya. Später stellte sich heraus, dass NotPetya keine Ransomware, sondern ein Wiper war: Das Programm verschlüsselte die Daten, um sie zu zerstören; die Erpressungsnachrichten waren lediglich eine Finte.¹⁵ NotPetya ist ein Wurm, d. h. ein Schadprogramm, das sich selbstständig verbreitet.¹⁶ Diese Schadsoftware infizierte zunächst eine ukrainische Buchhaltungssoftware, breitete sich dann aber rasch aus und setzte die IT-Systeme in Krankenhäusern, Banken und der Verwaltung außer Betrieb – und traf schätzungsweise zehn Prozent der Computer des Landes.¹⁷ Die Anlage des ehemaligen Atomkraftwerks Tschernobyl war ebenso betroffen wie Geldautomaten und Kartenzahlungssysteme.¹⁸ Zum Beispiel waren das deutsche Pharma- und Chemieunternehmen Merck,¹⁹ die dänische Reederei Maersk und das russische Staatsunternehmen Rosneft betroffen.²⁰ Allein der Schaden von Maersk soll im neunstelligen Bereich liegen.²¹ Dieses Schadensausmaß dürften von den Angreifenden nicht beabsichtigt gewesen sein.

¹⁴ Vgl. u. a. *Bendiek/Schulze*, Attribution als Herausforderung für EU-Cybersanktionen (Oktober 2021), S. 26 ff.; *Perlroth*, This Is How They Tell Me The World Ends (2021), S. 339 ff.; *Rhysider*, NotPetya, Darknet Diaries Episode 54 vom 24.12.2019.

¹⁵ Vgl. *Greenberg*, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, WIRED vom 21.08.2018; *Schmidt*, Petya/NotPetya: Kein Erpressungstrojaner, sondern ein „Wiper“, heise Online vom 29.06.2017.

¹⁶ *BKA*, Bundeslagebild Cybercrime 2017, S. 14.

¹⁷ *BKA*, Bundeslagebild Cybercrime 2017, S. 14; *Greenberg*, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, WIRED vom 21.08.2018.

¹⁸ *Greenberg*, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, WIRED vom 21.08.2018; *Perlroth*, This Is How They Tell Me The World Ends (2021), S. 339.

¹⁹ Merck schätzte seinen Schaden auf ca. 870 Millionen US-Dollar, *Greenberg*, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, WIRED vom 21.08.2018.

²⁰ *Greenberg*, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, WIRED vom 21.08.2018. Siehe auch *U.S. Department of Justice*, Six Russian GRU Officers Charged, 19.10.2020 sowie *Auchard*, New computer virus spreads from Ukraine to disrupt world business, Reuters vom 27.06.2017.

²¹ *Perlroth*, This Is How They Tell Me The World Ends (2021), S. 140. Der komplette Betrieb des Unternehmens kam zum Erliegen, *Auchard*, New computer virus spreads from Ukraine to disrupt world business, Reuters vom 27.06.2017.

Die USA und die EU schreiben NotPetya russischen Akteuren zu, allerdings bestehen hierfür lediglich Indizien; eine eindeutige Attribution ist nicht möglich.²² Jedenfalls scheint klar, dass es sich angesichts der Komplexität des Angriffs um einen staatlichen Akteur handeln muss.²³ Das Schadprogramm nutzte u. a. EternalBlue, ein von der US-amerikanischen National Security Agency (NSA) entwickeltes Werkzeug, um eine Sicherheitslücke in Windows zu nutzen und sich volle Kontrolle über betroffene Systeme zu verschaffen.²⁴

NotPetya veranschaulicht das große Schadenspotenzial von Cyberangriffen und nähert sich der Schwelle zum „Cyberkrieg“ an.²⁵ Es handelt sich jedoch nur um *einen* Vorfall – Cyberangriffe und Schadprogramme wüten indessen permanent. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt seit Jahren vor einer angespannten Bedrohungslage.²⁶ Eine besonders große Bedrohung stellt Ransomware dar: Der Begriff Ransomware setzt sich aus *ransom* (engl. für Lösegeld) und *ware* (von Software) zusammen; es handelt sich um Schadsoftware, die Daten verschlüsselt und diese den Betroffenen entzieht, um Lösegeld zu erpressen.²⁷ Sie nimmt pandemische Ausmaße an²⁸

²² U.S. Department of Justice, Six Russian GRU Officers Charged, 19.10.2020; Rat der Europäischen Union, EU verhängt erstmals Sanktionen als Reaktion auf Cyberangriffe, 30.07.2020; siehe den der DurchführungsVO (EU) 2020/1125. Vgl. auch Auchard, New computer virus spreads from Ukraine to disrupt world business, Reuters vom 27.06.2017.

²³ NATO Cooperative Cyber Defence Centre of Excellence, NotPetya and WannaCry Call for a Joint Response from International Community, <https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/>. Siehe auch Bendiek/Schulze, Attribution als Herausforderung für EU-Cybersanktionen (Oktober 2021), S. 27 f.; Scherschel, 3 Jahre NotPetya: Der Erpressungstrojaner, der keiner war, heise Online vom 27.06.2020.

²⁴ Greenberg, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, WIRED vom 21.08.2018.

²⁵ Von Cyberkrieg sprechen u. a. Greenberg, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, WIRED vom 21.08.2018; Moore, Offensive Cyber Operations (2022), S. 163 f. Dagegen entschied ein US-amerikanisches Gericht, dass NotPetya keinen Kriegsfall darstelle, vgl. Krempl, Kein Kriegsfall: Versicherung muss für Ransomware-Schaden durch NotPetya zahlen, heise Online vom 05.05.2023.

²⁶ BSI, Die Lage der IT-Sicherheit in Deutschland 2024, S. 8 ff.; BSI, Die Lage der IT-Sicherheit in Deutschland 2023, S. 11; BSI, Die Lage der IT-Sicherheit in Deutschland 2022, S. 11; BSI, Die Lage der IT-Sicherheit in Deutschland 2021, S. 9 f.; BSI, Die Lage der IT-Sicherheit in Deutschland 2020, S. 9; BSI, Die Lage der IT-Sicherheit in Deutschland 2019, S. 7 f. Siehe ferner das Lagebild der Agentur der Europäischen Union für Cybersicherheit: ENISA, Threat Landscape 2023, S. 6.

²⁷ Büchel/Hirsch, Internetkriminalität (2. Aufl. 2020), S. 87 ff.; Kochheim, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik (2. Aufl. 2018) Rn. 445.

²⁸ Vgl. zur Verbreitung Atug, Ransomware als Business Case in der organisierten Kriminalität, in: Rüdiger/Bayerl (Hrsg.), Handbuch Cyberkriminalologie 2, S. 345 ff.; Kropotov u. a., What Decision-Makers Need to Know About Ransomware Risk, Trend Micro Research (2023), S. 16 ff.

und trifft Unternehmen wie staatliche Stellen.²⁹ Zudem akquirieren Botnetze Hunderttausende unsichere IoT-Geräte.³⁰ Sicherheitslücken in weitverbreiteter Software gefährden Millionen von Nutzenden.³¹ Krankenhäuser müssen die medizinische Versorgung einschränken, was das Leben und die Gesundheit von Patientinnen und Patienten gefährdet – insbesondere in Notfällen.³² Sind Verwaltungsbehörden betroffen, gefährdet dies die Funktionsfähigkeit des Staates und beeinträchtigt Menschen, wenn sie z. B. keine Sozialhilfe mehr ausgezahlt bekommen.³³ Angriffe auf große Unternehmen, staatliche Stellen oder Kritische Infrastrukturen sind aber zusätzlich attraktiv, da sich höhere Lösegelder bzw. Verkaufspreise für gestohlene Daten erzielen lassen (sog. „Big Game Hunting“).³⁴ Auch Privatpersonen sind exponiert, wenn Cyberkriminelle Daten abgreifen: In Finnland verschafften sich Angreifende Zugriff auf die Daten psychotherapeutischer Praxen und drohten, diese zu veröffentlichen.³⁵ Nach einem Datenleck der Online-Plattform Ashley Madison, einer Dating-Webseite für Seitensprünge, wurden Informationen über außereheliche Affären veröffentlicht.³⁶

²⁹ *Stöckel*, Südwestfalen IT: Cyberangriff legt IT-Dienste vieler deutscher Kommunen lahm, Golem.de vom 30.10.2023. Siehe auch den Podcast „You are fucked – Deutschlands erste Cyberkatastrophe“ vom MDR zum Ransomwarevorfall des Landkreis Anhalt-Bitterfeld, <https://www.mdr.de/mdr-sachsen-anhalt/podcast/you-are-fucked/index.html>.

³⁰ Internet of Things bzw. Internet der Dinge, d. h. vernetzte Geräte. Vgl. bspw. *Goodin*, New, more-powerful IoT botnet infects 3,500 devices in 5 days, *Ars Technica* vom 01.11.2016. Siehe allgemein zur Unsicherheit von IoT-Geräten: *Heckmann/Paschke*, in: Bräutigam/Kraul/Bauer, *Internet of Things* (2021), § 10 Rn. 21 ff.; *Kleinhans*, *Internet of Insecure Things* (07.12.2017), S. 5 ff.; *Sohr/Kemmerer*, in: Kipker u. a., *Cybersecurity* (2. Aufl. 2023), Kapitel 3 Rn. 2421 ff.

³¹ Siehe u. a. *Knop*, Kritische Word-Lücke: Proof-of-Concept-Code veröffentlicht, heise Online vom 07.03.2023.

³² *Knop*, Ransomware-Angriff: Krankenhaus muss hunderte Operationen absagen, heise Online vom 07.03.2023; *Krempf*, Bundesregierung: Deutlich mehr Cyberangriffe auf Kliniken und Versorger, heise Online vom 26.11.2020; *Spinnler*, Kliniken im Visier der Hacker, tagesschau.de vom 28.06.2021; *Stock*, Missing Link: Ransomware-Angriffe auf Krankenhäuser gefährden Menschenleben, heise Online vom 28.01.2024. Siehe auch *Olejnik/Kurasinski*, *Philosophy of Cybersecurity* (2024), S. 96 ff.

³³ *dpa*, Nach Cyberangriff: Rhein-Pfalz-Kreis erwartet Normalbetrieb im Frühsommer, heise Online vom 12.01.2023, <https://www.heise.de/news/Nach-Cyberangriff-Rhein-Pfalz-Kreis-erwartet-Normalbetrieb-im-Fruhsommer-7457667.html>; *Heidmann*, Ransomware-Angriffe: Landkreis Anhalt-Bitterfeld wird erpresst, *Süddeutsche Zeitung* vom 15.07.2021.

³⁴ *Aug*, Ransomware als Business Case in der organisierten Kriminalität, in: Rüdiger/Bayerl (Hrsg.), *Handbuch Cyberkriminalologie* 2, S. 345 (355 f.); *BSI*, *Die Lage der IT-Sicherheit in Deutschland* 2022, S. 11.

³⁵ *Holland*, Psychotherapeuten gehackt: Finnische Patienten und Praxen werden erpresst, heise Online vom 27.10.2020.

³⁶ *Schirmmacher*, Nach Ashley-Madison-Hack: Erbeutete Daten veröffentlicht, heise Online vom 19.08.2015; siehe auch *Segall*, Pastor outed on Ashley Madison commits suicide, *CNN* vom 11.03.2023.

Wer findet nicht mindestens eine eigene E-Mail-Adresse in geleakten Datensätzen mithilfe der Webseite *haveibeenpwned.com*?

Bedrohlich sind daher nicht einzelne Staaten oder Cyberkriminellen-Gruppen, entscheidend ist weniger der *eine* große Konflikt. Auch wenn die großen Cyberangriffe von Antagonisten wie den USA, Russland, China, Nordkorea oder dem Iran als die primäre Bedrohung im Cyberraum erscheinen, rührt die kritische Cybersicherheitslage von vielen verschiedenen Akteuren her, die alle unterschiedliche Interessen verfolgen.

Sobald Sicherheitslücken öffentlich oder in kriminellen Kreisen bekannt werden, wittern Cyberkriminelle rentable Angriffsmöglichkeiten – und ihre Angriffszyklen verkürzen sich.³⁷ Dienste wie Shodan finden automatisiert geeignete Angriffsziele. Werkzeuge und Baukästen wie Metasploit ermöglichen es, den passenden Exploit (die Schadsoftware zum Ausnutzen einer Sicherheitslücke) mit der gewünschten Payload (die Transportlast, die das eigentliche Angriffsziel verfolgt, z. B. Ransomware)³⁸ zu verbinden, sodass selbst Amateure Schaden anrichten können.

Angesichts dessen kann kein IT-System als sicher gelten: Die Frage ist nicht, *ob* ein System über Sicherheitslücken verfügt – sondern *welche* Schwachstellen existieren.³⁹ Wer lange und intensiv genug sucht, wird Schwachstellen finden; meistens reicht jedoch der Blick in frei zugängliche Schwachstellen-Datenbanken, fachspezifische Nachrichten oder Handelsforen für bislang unbekannte Sicherheitslücken (sog. Zero-Day-Schwachstellen, die dem Hersteller „null Tage“ bekannt sind).⁴⁰ Ein erklärter Cyberkrieg ändert an dieser Bedrohungslage nur wenig,⁴¹ denn dieses Gefahrenpotenzial besteht für alle IT-Systeme – permanent.

Diese Gefahrenlage für die IT-Sicherheit verlangt nach einer kohärenten, multidimensionalen und nationalen Cybersicherheitspolitik, die Cybersicherheit nicht den Kräften des Marktes oder den einzelnen Nutzenden überlässt. Das Recht kann an mehreren Stellschrauben drehen, um die Cybersicherheit zu verbessern: Notwendig sind vertragliche und deliktische Haftungs- und Einstandspflichten der Hersteller von IT-Produkten, die strafrechtliche Sanktionierung von Cyberangriffen und (die dafür erforderlichen) Ermittlungsbefugnisse, sowie eine öffentlich-rechtliche Risikoregulierung. Doch diese Bausteine verhindern nicht alle Cyberangriffe – sie können lediglich die allgemeine

³⁷ BSI, IT-Grundschutz-Kompodium (2023), IT-Grundschutz – Basis für Informationssicherheit, S. 2.

³⁸ Siehe *Froehlich/Loshin*, payload (computing), TechTarget vom 2021.

³⁹ Wie Gene Spafford es einmal sagte: „The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards – and even then I have my doubts.“ (zitiert nach <https://spaf.cerias.purdue.edu/quotes.html>).

⁴⁰ BSI, Zero-Day-Exploit, <https://web.archive.org/web/20230526140324/https://www.bsi.bund.de/SharedDocs/Glossareintraege/DE/Z/Zero-Day-Exploits.html>.

⁴¹ BSI, Die Lage der IT-Sicherheit in Deutschland 2022, S. 22.

Grundsicherheit von IT-Systemen erhöhen oder Angreifende im Nachhinein bestrafen. Es bedarf aber auch Handlungsmöglichkeiten, um akuten Gefahren zu begegnen. Die Politik rekurriert regelmäßig auf die Forderung nach Befugnissen für das „Zurückhacken“ (sog. „Hackbacks“ oder digitale Gegenschläge).⁴² Die Abwehr von Gefahren für die Cybersicherheit kann jedoch mithilfe einer ganzen Reihe von Maßnahmen gelingen. Manche dieser Maßnahmen beschränken sich auf die Gewinnung von Informationen über Bedrohungen, manche unterstützen Betroffene eines Cyberangriffs oder geben Betreibern bei der Absicherung ihrer IT-Systeme Hilfestellung.

Im folgenden Abschnitt (A.) stellen vier vergangene Cyberangriffe exemplarisch dar, welche Auswirkungen möglich sind und welche Strategien Betroffene und staatliche Stellen zur Bewältigung von Vorfällen verfolgt haben. Dabei zeigt sich, dass Betroffene – wie auch die Allgemeinheit – auf staatliche Unterstützung bei der Bewältigung von Gefahren für die Cybersicherheit angewiesen sind (B.). Als Garant für Sicherheit ist der Staat gefragt: Die Abwehr von Gefahren für die Cybersicherheit fällt unter die staatliche Aufgabe der Gefahrenabwehr. Diese Arbeit erkundet, inwiefern die gefahrenabwehrrrechtliche Dogmatik auf die Abwehr von Gefahren für die Cybersicherheit anwendbar ist. Zugleich systematisiert sie die Befugnisse der Cybergefahrenabwehr.

A. Allgegenwärtige Gefahren für unsere Gesellschaft

Die folgenden vier Beispiele von Cybervorfällen dienen zum einen dazu, Angriffsvektoren und Vorgehensweisen der Angreifenden sowie (potenzielle) Auswirkungen dazustellen. Sie sollen aber auch zeigen, welche Gefahrenabwehrmaßnahmen staatliche Stellen ergriffen haben oder hätten ergreifen können, um die Vorfälle zu bewältigen.

Die Sicherheitslücke *Log4Shell* (I.) verdeutlicht die Komplexität moderner Software: Die Unsicherheit einer Komponente reicht aus, um unzählige Systeme zu gefährden. Dass auch ein relativ banaler Ransomware-Angriff gravierende Auswirkungen für die Versorgung der Bevölkerung haben kann, zeigt der Colonial-Pipeline-Vorfall (II.). Das dritte Beispiel veranschaulicht den Ablauf eines klassischen Cyberangriffs: Angreifende suchen eine Sicherheitslücke und nutzen diese aus, um sich möglichst umfassend Zugriff auf das Ziel-

⁴² *Greis*, Cyberabwehr: Faeser will Grundgesetz für Hackbacks ändern, Golem.de vom 03.04.2023; *Metzger/Stoll*, Faeser: BKA muss Putins Hacker stoppen können, ZDF vom 31.03.2023; siehe auch ein Jahr zuvor *Krempl*, Cyberverteidigung: EU-Kommission fordert Hackbacks zum digitalen Gegenschlag, heise Online vom 11.11.2022; siehe aber auch *Grüner/dpa*, IT-Sicherheit: Faeser lehnt Hackbacks offenbar doch ab, Golem.de vom 01.05.2022. Hackbacks forderte auch die vorherige Bundesregierung: *Biselli*, Hackback im Bundespolizeigesetz: Seehofer wollte den digitalen Gegenangriff starten, netzpolitik.org vom 29.01.2020.

system zu verschaffen. Die Sicherheitslücke betraf eine häufig eingesetzte Anwendung und exponierte zahlreiche Unternehmen weltweit (*Microsoft Exchange Server*, III.). Angreifende können aber auch komplexe Angriffsstrukturen aufbauen, indem sie IT-Systeme übernehmen, in eine Befehlsstruktur einbinden und ein sog. Botnetz aufbauen. Ein Beispiel hierfür ist *Emotet* (IV).

I. *Log4Shell*

Im November 2021 versetzte eine bislang unbekannte Sicherheitslücke in der weitverbreiteten Open-Source-Bibliothek Log4j die IT-Branche in Angst und Schrecken:⁴³ Log4j bietet ein Paket mit Programmcode für die Programmiersprache Java und protokolliert Aktivitäten von Anwendungen.⁴⁴ Es lässt sich kostenlos und leicht in Anwendungen integrieren, ohne dass Entwicklerinnen oder Entwickler selbst Logging-Funktionalitäten erstellen müssen; dementsprechend findet sich Log4j in vielen Software-Architekturen wieder.⁴⁵

Die Sicherheitslücke – Log4Shell getauft – ermöglicht es Angreifenden, mit Log4j eine „Shell“ (eine Schnittstelle) auf dem Zielsystem zu etablieren und damit nicht nur Programmcode zu loggen, sondern auch auszuführen.⁴⁶ Dadurch lassen sich anfällige System kontrollieren.⁴⁷ Die Sicherheitslücke betraf Hunderte Millionen von IT-Systemen und IT-Produkten, da Java eine der am häufigsten verwendeten Programmiersprachen und Log4j in vielen Java-Anwendungen integriert ist.⁴⁸ Betroffene konnten aber nicht ohne Weiteres klären, ob ein Softwareprodukt oder ein konkretes IT-System betroffen ist, da

⁴³ Siehe hierzu Apache Log4j, <https://logging.apache.org/log4j/2.x/>. Vgl. auch die Berichterstattung: *Hunter/Vynck*, The „most serious“ security breach ever is unfolding right now. Here’s what you need to know, *The Washington Post* vom 20.12.2021; *Woodyard*, „Critical vulnerability“: Smaller firms may find it harder to stop hackers from exploiting Log4j flaw, *USA TODAY* vom 16.12.2021. Siehe auch *cy*, Log4Shell – Bug oder Feature, YouTube vom 21.05.2022, <https://media.ccc.de/v/gpn20-60-log4shell-bug-oder-feature>.

⁴⁴ *BSI*, Kritische „Log4Shell“ Schwachstelle in weit verbreiteter Protokollierungsbibliothek Log4j (CVE-2021-44228), 12.01.2022, S. 1.

⁴⁵ *BSI*, Warnstufe Rot: Schwachstelle Log4Shell führt zu extrem kritischer Bedrohungslage, 16.12.2021.

⁴⁶ <https://nvd.nist.gov/vuln/detail/CVE-2021-44228>; *Hunter/Vynck*, The „most serious“ security breach ever is unfolding right now. Here’s what you need to know, *The Washington Post* vom 20.12.2021; *Lim*, Apache Log4j Vulnerability Explained, *Swarmnetics* vom 05.02.2022.

⁴⁷ *Newman*, A Log4j Vulnerability Has Set the Internet „On Fire“, *WIRED* vom 10.12.2021.

⁴⁸ *statista*, Programmiersprachen weltweit laut PYPL-Index im März 2024, <https://de.statista.com/statistik/daten/studie/678732/umfrage/beliebteste-programmiersprachen-weltweit-laut-pypl-index/>. Siehe auch *Barrett*, The Next Wave of Log4J Attacks Will Be Brutal, *WIRED* vom 16.12.2021; *Hunter/Vynck*, The „most serious“ security breach ever is unfolding right now. Here’s what you need to know, *The Washington Post* vom 20.12.2021.

Stichwortverzeichnis

- abstrakte Gefahr 138, 140,
153 ff., 157, 339, 431
aktive Cyberabwehr 172 ff., 252,
299
Anordnung 194, 261 ff., 277 ff.,
290 ff., 318 ff., 346 ff.
Attribution 244 ff., 409
automatisierte Massenangriffe 8,
12, 16, 29, 31, 144, 146, 150,
153, 157, 247, 289
- Belastbarkeit 124, 342
Benachrichtigung 344
Betreiber 124, 261, 327
Botnetz 133, 143, 180, 259 f.,
279, 289, 292 f., 346
Bundesamt für Sicherheit in der
Informationstechnik 90 ff.,
364 ff.
Bundeskriminalamt 379 ff.
Bundespolizei 252 f., 382 ff.
Bundeswehr 212, 409 f.
- Colonial Pipeline 13 ff.
CSIRT 187 ff., 230, 320, 395 f.
Cyberangriff 141 ff, 245 ff.
Cyberhygiene 127 f.
Cyberkrieg 3, 6, 8, 57
Cyberkriminalität 31, 55 f., 102,
115, 122, 173, 219, 298, 361,
365, 372, 380, 386, 398, 400,
403, 412
Cyberresilienz-VO 25, 76, 93,
123, 130, 322 f., 421, 424
Cybersicherheit 38
CybersicherheitsVO 76, 93
- Cybersicherheitsvorfall 165 f.,
186, 216, 242, 270, 390, 395
CybersolidaritätsVO 165 f., 396
- Datenschutz 77, 229
Detektionsmaßnahmen 337 ff.
digitale Dienste 264, 332, 350
- Emotet 19 ff., 42, 101, 286, 316,
361, 381, 422
ENISA 394 ff.
- Gefahrenbegriff 136 ff.
Gefahrenverdacht 138, 145, 147,
152 ff., 169, 240, 314, 317,
339, 349 f.
Gefahrenvorfeld 103, 109, 138,
144 f., 150, 169, 194, 219, 329,
355 f., 380, 431, 433
Gefahrerforschung 137, 145, 210,
225, 337, 343
Gegenangriff 101, 184, 250 ff.
- Hackback 56, 174, 182, 185, 250,
252, 382
Hersteller 25, 45, 107, 123, 129,
230 f., 275, 301 ff.
- Incident Response 270
Indicators of Compromise 151
Informationsaustausch 56, 228,
231, 394, 407, 414
Informationshandeln 233, 235,
346, 369
Integrität 42, 71, 117, 200
IT-Produkt 45, 301 ff.

- IT-Sicherheit 40
IT-Sicherheitsgesetz 2.0 26, 33,
76, 88, 92, 217, 292, 331, 337,
367, 370, 415
IT-Sicherheitspflichten 122 ff.,
158, 331, 333
IT-System 44, 153, 155, 261
- konkrete Gefahr 137 f., 141,
145 ff., 150 ff., 156 ff., 257,
327, 343, 346, 350, 355
Kritische Infrastrukturen 15,
80 ff., 121, 130 f., 157, 161,
277, 387, 407, 411
- Log4Shell 10 ff.
- Marktüberwachung 320 f.
Meldepflichten 228 ff.
Microsoft Exchange 15 ff.
MIRT 274, 277 f., 371, 400
- Nachrichtendienst 98, 100,
410 ff.
NIS-2-Richtlinie 76, 87 ff., 332,
337, 405
NIS-2-Umsetzungsgesetz 352,
367, 424
Notfallteams 93, 206, 361, 389 ff.
- Patch 12, 17, 154, 157, 283, 319,
354
Portscan 154, 334, 342, 425
Produktsicherheitsrecht 25, 123,
306, 321
- Ransomware 5, 6, 120, 149, 179,
222, 247, 388
- Schwachstelle 153, 156, 304,
312, 337
Sicherheitsupdates 12, 129,
352 ff.
soziotechnische Systeme 47
Staatsaufgabe 37 ff.
Staatshaftung 198, 226, 256, 342
- Technikregulierung 94 ff.
- Versicherlichung 56, 58 ff.,
99, 255, 315
Vorfall 164 f.
Vorfallbewältigung 166, 183,
185, 190, 201, 205, 262, 263,
274, 276, 305, 391 ff., 398,
413, 426
- Warnung 238, 308 ff.
- Zero-Day 8, 15, 27, 29, 154 f.,
175, 211