GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

MonIKA

Monitoring durch **I**nformationsfusion und **K**lassifikation zur **A**nomalieerkennung

Rechtliche Herausforderungen der Informationsfusion und -klassifikation zur Erkennung von Anomalien in Internet-Infrastrukturen unter besonderer Berücksichtigung haftungs- und IT-rechtlicher Fragestellungen

Deliverable 5.1.

Editor: Philipp Roos, Philipp Schumacher

Institution: Insitut für Informations-, Telekommunikations- und Medienrecht
Zivilrechtliche Abteilung

Erstellt am: 28. Februar 2014

Projektpartner

Fraunhofer FKIE
Friedrich-Ebert-Allee 144
53113 Bonn
Dr. Michael Meier
Telefon +49 228 73-54249
Fax +49 228 73-54254
mm@cs.uni-bonn.de

Cassidian Cybersecurity
Willy-Messerschidt-Straße
5521 Ottobrunn
Dr. Tobias Kiesling
Telefon +49 89 3179 3807
Fax +49 89 3179 4031
helmut.kaufmann@eads.net

Westfälische Wilhelms-Universität
Institut für Informations-,
Telekommunikations-
und Medienrecht (ITM)
Zivilrechtliche Abteilung
Leonardo-Campus 9
48149 Münster
Prof. Dr. Thomas Hoeren
Telefon +49 251 83-38600
Fax +49 251 83-38601
hoeren@uni-muenster.de

Unabhängiges Landeszentrum für
Datenschutz (ULD)
Holstenstr. 98
24103 Kiel
Marit Hansen
Telefon +49 431 988 1214
Fax +49 431 1223
ULD6@datenschutzzentrum.de

Mitwirkende

Autor(en)	Institution	E-Mail
Philipp Roos	ITM	philipp.roos@uni-muenster.de
Philipp Schumacher	ITM	philipp.schumacher@uni-muenster.de

Über MonIKA

Die heutige Gesellschaft ist in hohem Maße auf sichere – insbesondere verlässliche und verfügbare – Infrastrukturen wie das Internet angewiesen. Aus diesem Grund sind diese Infrastrukturen nach der Definition des Bundesministerium des Innern als kritisch zu betrachten, d.h. sie haben eine wichtige Bedeutung für das Gemeinwesen, so dass ihr Ausfall oder Fehlverhalten nachhaltig wirkende ökonomische Schäden und soziale Beeinträchtigungen nach sich ziehen oder andere dramatische Auswirkungen zur Folge haben kann.

Der durch das Internet ermöglichte sog. Cyber-Raum lässt sich wegen seiner globalen und autonomen Charakteristika nicht auf territoriale Grenzen beschränken und umfasst alle weltweit erreichbaren Informationsinfrastrukturen und deren Dienste. In Deutschland nutzen alle Bereiche des gesellschaftlichen und wirtschaftlichen Lebens die vom Cyber-Raum zur Verfügung gestellten Dienste und werden damit ein Teil einer zunehmend vernetzten Welt. Die Verfügbarkeit des Cyber-Raums sowie die Integrität, Authentizität und Vertraulichkeit der darin vorhandenen Dienste sind auf Grund der Relevanz für Gesellschaft und Wirtschaft eine wesentliche Grundlage zukunftsweisender Innovationen und damit wirtschaftlicher Wettbewerbsfähigkeit. Dies erfordert eine Fokussierung auf Qualitätsziele wie Wirtschaftlichkeit und Sicherheit.

Das *Domain Name System* und das globale *Routing* stellen klassische Beispiele für kritische Internet-Infrastrukturen dar, die dezentral organisiert sind. Die koordinierte Verwendung einer Vielzahl von Internet-Endgeräten beispielsweise durch Botnetze weist ein erhebliches Schadpotential auf. Aus diesen Umständen resultiert, dass jegliche Formen von Anomalien in Internet-Infrastrukturen schwer frühzeitig zentral zu erkennen, zu erfassen und zu klassifizieren sind, um geeignet und effektiv auf die resultierende Bedrohungslage reagieren zu können.

Sowohl die zunehmende Komplexität und Verwundbarkeit der bereitgestellten Dienste als auch die vielfältigen Möglichkeiten des Missbrauchs lassen zukünftig ein gesamtheitlich hohes Sicherheitsrisiko erwarten. Dies gilt im Besonderen für das globale Umfeld des Cyber-Raums und der zugehörigen vernetzten Informations-infrastrukturen. Von gezielt herbeigeführten Angriffen oder anderweitig verursachten Ausfällen dieser Infrastrukturen sind Staat, Wirtschaft und Gesellschaft betroffen. Es ist notwendig, das resultierende Sicherheitsrisiko transparent darzustellen, um ökonomisch effizient und effektiv handeln zu können. Hierzu bedarf es rechtskonformer, dezentraler und kooperativer Verfahren, Modelle und Methoden zur Erkennung und Klassifizierung von Anomalien. Diese gilt es innerhalb des MonIKA-Projekts zu entwickeln, exemplarisch zu validieren und für eine adäquate systematische Risikobehandlung vorzubereiten.

Ziel des MonIKA-Projekts ist dabei die Entwicklung wissenschaftlich fundierter Verfahren der Informationsfusion und Klassifikation, so dass einerseits rechtliche Aspekte und Datenschutz durch geeignete Aggregation, Anonymisierung und Reduzierung berücksichtigt, andererseits eine effiziente Erkennung von Anomalien gewährleistet werden kann. Die Nutzbarmachung sonst nicht verwertbarer Einzeldaten und der damit zu erwartende Effizienzgewinn führen aus Sicht der MonIKA-Projektpartner zu einem hohen wirtschaftlichen Potenzial der entwickelten Konzepte und Verfahren.

Inhaltsverzeichnis

1 Überblick

Im Folgenden soll ein Überblick über die Inhalte des vorliegenden Deliverables 5.1 gegeben werden, das sich mit haftungs- und IT-rechtlichen Fragestellungen auseinandersetzt, die für das MonIKA-Projekt von Relevanz sind.

1.1 Einführung

IT-Sicherheit ist in aller Munde. Die stetig wachsende Vernetzung führt neben den zahlreichen Vorteilen für Unternehmen und private Anwender aber auch dazu, dass sich kriminelle Handlungen vermehrt im Cyber-Raum abspielen. Dies wird bei einem Blick auf die Kriminalitätsstatistiken deutlich, die – trotz der Bekanntheit des Problems und entsprechender Gegenmaßnahmen – immer noch Zuwächse bei der Anzahl von dem Cybercrime zugehörigen Delikten verzeichnen können. Ein Beispiel bietet der jährlich vom Bundeskriminalamt veröffentlichte Bericht „Cybercrime – Bundeslagebild 2012“, der eine Steigerung von 8 % der Anzahl begangener Cybercrime-Fälle vermelden muss.[1]

Entsprechend hoch sind die Bemühungen von Politik und Forschung, dass Möglichkeiten gefunden werden, durch die die Gefahren aus dem Cyber-Raum eingedämmt werden. Besonderes Potenzial weisen dabei solche Verfahren auf, die einen kooperativen Ansatz enthalten. An dieser Stelle setzt das MonIKA-Projekt an, das Kooperationen zwischen möglichen Betroffenen ermöglichen will, sodass ein höheres Maß an IT-Sicherheit generiert werden kann.

Neben den technischen Herausforderungen spielen hierbei auch rechtliche Fragen eine besondere Rolle.

[1] *Bundeskriminalamt*, Bundeslagebild Cybercrime 2012, S. 3.

1.2 Abgrenzung

Durch die Ergebnisse des MonIKA-Projekts soll eine Datenfusion und –klassifikation zur Erkennung von Anomalien ermöglicht werden. In rechtlicher Hinsicht wirft dies zahlreiche datenschutzrechtliche Probleme auf, die in Deliverable 5.2 behandelt werden. Damit ein Verfahren zur Datenfusion und –klassifkation aber auch praktische Anwendung findet, sind potenzielle Anwender nicht nur an der Datenschutzkonformität der Verfahren interessiert, sondern stellen sich auch die Frage, welche haftungsrechtlichen Risiken bestehen und wie sich das Verfahren in sonstige rechtliche Rahmenbedingungen einfügt. Das vorliegende Deliverable 5.1 widmet sich diesen haftungs- und rahmenrechtlichen Fragestellungen.

Die Betrachtung haftungsrechtlicher Risiken benötigt Handelnde. Im Mittelpunkt steht daher der innerhalb der Laufzeit des MonIKA-Projekts gebildete Anwendungsfall „Enterprise-Monitoring“ (Kapitel 4). Dieser gibt wieder, wie sich die Projektpartner die praktische Umsetzung der Ergebnisse des MonIKA-Projekts vorstellen. Auf den Anwendungsfall „Botnetz-Monitoring“ soll am Beispiel des Spam-Szenarios jedoch ebenso eingegangen werden, wie auf die globale Routenüberwachung als weiteren Anwendungsfall.

1.3 Vorgehensweise

Das Gutachten erarbeitet zunächst relevante Bestimmungen im deutschen Recht, die die IT-Sicherheit betreffen. Sodann erfolgt eine Untersuchung, ob und bejahendenfalls warum die Notwendigkeit besteht, an rechtskonformen präventiven Lösungen – wie es maßgebliches Ziel des MonIKA-Projekts ist – zu arbeiten. Hierfür werden die Risiken validiert, die bei der Bekämpfung von Botnetzen durch sog. Desinfektionsmaßnahmen von Internet-Service-Providern (ISP) auftreten. Die Frage nach möglichen anderweitigen – rechtskonformen – Vorgehensweisen trat innerhalb der Projektlaufzeit auf.

Besondere Aufmerksamkeit verlangt die Betrachtung der Anwendungsfälle, auf deren Basis die typischen Haftungsrisiken bei dem Einsatz eines Verfahrens zur Erkennung von Anomalien durch eine Datenfusion und –klassifikation in verschiedenen Konstellationen ermittelt werden.

Zudem erscheint es notwendig, das im Rahmen des MonIKA-Projekts entwickelte Verfahren für ein kooperatives Monitoring in die derzeitigen Pläne der Europäischen Kommission, des Bundesministeriums des Innern und der Bundesregierung für eine staatliche Regulierung auf dem Gebiet der IT-Sicherheit einzuordnen.

Abschließend werden die Ergebnisse des Gutachtens zusammengetragen.

2 Rechtliche Rahmenbedingungen bezüglich IT-Sicherheit

Die derzeitigen rechtlichen Rahmenbedingungen für die IT-Sicherheit ergeben sich nicht aus einem einheitlichen Gesetz, sondern aus den einzelnen Normen verschiedener Gesetze. Der IT-sicherheitsrechtliche Bezug kann anhand der Ziele von IT-Sicherheit ermittelt werden, die der Gesetzgeber in § 2 Abs. 2 BSIG[2] nennt. Danach ist es das Ziel von IT-Sicherheit, durch Sicherheitsvorkehrungen technischer, organisatorischer und rechtlicher Art, die Verfügbarkeit, Unversehrtheit und Vertraulichkeit von Informationen (Daten) zu gewährleisten. Im Folgenden sollen die wichtigsten Normen, die zumindest Berührungen mit dem MonIKA-Projekt haben, aufgezeigt werden.

2.1 Gesetzliche Verpflichtungen

Zunächst sind die gesetzlichen Verpflichtungen zu beachten.

2.1.1 § 9 BDSG i. V. m. der Anlage

Aus § 9 BDSG[3] i. V. m. Anlage ergeben sich IT-sicherheitsrechtliche Anforderungen für den Schutz personenbezogener Daten. Nach § 9 BDSG müssen bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten die technischen und organisatorischen Maßnahmen getroffen werden, die erforderlich sind, um die Ausführung des BDSG und die in der Anlage genannten Anforderungen zu gewährleisten. Für die Bestimmung der Erforderlichkeit müssen der (wirtschaftliche) Aufwand und der angestrebte Schutzzweck miteinander verglichen und in ein angemessenes Verhältnis zueinaner gebracht werden. Es gilt somit der Grundsatz der Verhältnismäßigkeit.[4]

Die Anlage des BDSG schreibt vor, dass (überhaupt) bestimmte Maßnahmen getroffen werden müssen: Dazu gehören eine Zutrittskontrolle bzgl. der

[2] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009, BGBl. I S. 2821.
[3] Bundesdatenschutzgesetz (BDSG) in der Fassung der Bekanntmachung vom 14. Januar 2003, BGBl. I S. 66.
[4] *Gola/Schomerus*, in: Gola/Schomerus, BDSG, § 9 Rn. 7.

Datenverarbeitungsanlagen, die Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle bzgl. der Daten sowie das Gebot zur Datentrennung. Der Umfang der zu treffenden Maßnahmen wird durch den Erforderlichkeitsvorbehalt beschränkt. Der Gesetzgeber hat sich damit für ein flexibles System entschlossen, bei dem eine Vielzahl von Maßnahmen möglich ist und es dem einzelnen Unternehmen überlassen bleibt, auf welche Weise es den Anforderungen nachkommt. Die Unternehmen sollten auf Basis einer Risikoanalyse ermitteln, welche konkreten Schutzmaßnahmen der Schutzbedürftigkeit der Daten gerecht werden.[5]

Relevanz weisen diese Regeln für das MonIKA-Projekt insofern auf, als dass stets auch personenbezogene Daten von den Vorgängen betroffen sind oder sein können. Insofern müssen diese Anforderungen von allen beteiligten Unternehmen (oder öffentlichen Stellen) stets berücksichtigt werden. Des Weiteren wird bezüglich spezifischer datenschutzrechtlicher Normen auf die Ausführungen in Deliverable 5.2 verwiesen.

2.1.2 § 109 TKG

Weiterhin zu beachten ist § 109 TKG[6], der besondere Anforderungen für die Anbieter von Telekommunikationsdienstleistungen normiert. § 109 TKG weist inhaltliche Berührungspunkte mit § 9 BDSG i. V. m. Anlage auf, aber geht in persönlicher und sachlicher Hinsicht noch über diesen hinaus.[7] § 109 TKG gilt dennoch nicht als reine Spezialvorschrift zu § 9 BDSG, sondern ergänzt dessen Schutz- und Regelungsbereich vielmehr.[8] Mit § 109 TKG wurden die Vorgaben aus der RL 2009/140/EG umgesetzt, die zuverlässige und sichere Kommunikation über elektronische Kommunikationsnetze für Wirtschaft und Gesellschaft bezweckt.[9]

Nach § 109 Abs. 1 TKG hat jeder Diensteanbieter erforderliche technische Vorkehrungen und sonstige Maßnahmen zum Schutz des Fernmeldegeheimnisses und personenbezogener Daten zu treffen, die dem Stand der Technik entsprechen. Damit wird der Gesetzgeber dem Umstand gerecht, dass bei Telekommunikationsdienstleistungen große Datenmengen anfallen.

---

[5] *Gola/Schomerus*, in: Gola/Schomerus, BDSG, § 9 Rn. 9.
[6] Telekommunikationsgesetz (TKG) vom 22. Juni 2004, BGBl. I S. 1190.
[7] *Eckhardt*, in: Geppert/Schütz, TKG, § 109 Rn. 8 f.
[8] *Klesczewski*, in: Säcker, TKG, § 109 Rn. 11.
[9] Vgl. Erwägungsgrund 44 der Richtline 2009/140/EG vom 25. November 2009 zur Änderung der Richtlinien 2002/21/EG, 2002/19/EG und 2002/20/EG.

Aus § 109 Abs. 2 TKG ergibt sich für Betreiber eines öffentlichen Telekommunikationsnetzes und die Erbringer öffentlich zugänglicher Telekommunikationsdienste (TK-Unternehmen) die Pflicht, angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen, um Störungen mit Beeinträchtigungspotenzial für die Telekommunikationsnetze und –dienste zu verhindern und sonstige Sicherheitsrisiken zu beherrschen.

Ferner ergeben sich aus § 109 Abs. 4 bzw. Abs. 5 TKG noch weitere Pflichten für TK-Unternehmen, die öffentlich zugängliche Dienste erbringen. Dazu zählen die Pflicht zur Ernennung eines Sicherheitsbeauftragten, die Erstellung eines Sicherheitskonzeptes, das der Bundesnetzagentur (BNetzA) vorgelegt wird, und eine Meldepflicht gegenüber der BNetzA, sofern Sicherheitsverletzungen festgestellt wurden, die Störungen mit beträchtlichen Auswirkungen bedingen.

Auch TK-Unternehmen sind potentielle Betreiber eines Verfahrens wie MonIKA, sodass sich das Verfahren in diese Rahmenbedingungen einfügen wird.

2.1.3 Branchenspezifische Regelungen

Nicht unmittelbar das MonIKA-Projekt betreffend, aber dennoch im Rahmen der Darstellung einzelner Normen, die sich mit IT-Sicherheit befassen, anzuführen, sind die branchenspezifischen Regelungen. Letztlich kommen sämtliche der durch die jeweiligen Normen verpflichteten Unternehmen auch als Betreiber eines kooperativen Verfahrens wie MonIKA in Betracht.

Für Unternehmen aus dem Finanzsektor gelten § 25a KWG[10] und § 33 WpHG[11]. Das KWG bezieht sich auf Kreditinstitute und Finanzdienstleistungsunternehmen, wie sich aus § 1 KWG ergibt. Das WpHG verpflichtet Unternehmen, die Wertpapierdienstleistungen erbringen und sonstigen Handel an der Börse betreiben (vgl. § 1 Abs. 1 WpHG). Nach § 25a Abs. 1 KWG, der über § 33 Abs. 1 Satz 1 WpHG auch für die in den Anwendungsbereich des WpHG fallenden Unternehmen gilt, ist es für eine ordnungsgemäße Geschäftsorganisation erforderlich, dass ein angemessenes und wirksames Risikomanagement betrieben wird. Dieses Risikomanagement umfasst u. a. auch ein Notfallkonzept für IT-Systeme (s. § 25a Abs. 1 Satz 3 Nr. 3 KWG), an das mittels

[10] Gesetz über das Kreditwesen (Kreditwesengesetz – KWG) in der Fassung der Bekanntmachung vom 9. September 1998, BGBl. I S. 2776.
[11] Gesetz über den Wertpapierhandel (Wertpapierhandelsgesetz – WpHG) in der Fassung der Bekanntmachung vom 9. September 1998, BGBl. I S. 2708.

des von der Bundesanstalt für Finanzdienstleistungsaufsicht veröffentlichten Rundschreibens (MaRisk)[12] bestimmte Anforderungen gestellt werden.

Mit § 11 Abs. 1a EnWG[13] existiert eine sicherheitsspezifische Norm für die Energiebranche. § 11 Abs. 1a EnWG verpflichtet die Betreiber von Energieversorgungsnetzen dazu, angemessene Schutzvorkehrungen gegenüber Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die der Netzsteuerung dienen, zu treffen. Dafür erstellen BNetzA und das Bundesamt für Sicherheit in der Informationstechnik (BSI) einen Katalog, der Sicherheitsanforderungen enthält, bei deren Einhaltung ein angemessener Schutz vermutet wird.

Erwähnt werden kann ferner § 13 Abs. 4 Nr. 1 – 6 TMG[14], der für die Diensteanbieter i. S. d. TMG gilt. Danach haben Diensteanbieter bestimmte technische und organisatorische Vorkehrungen (Systemdatenschutz) zu treffen, die insbesondere dem Datenschutz dienen.[15]

Alle diese Sektoren und Branchen können nach der Definition des Bundesministerium des Innern (BMI) zu kritischen Infrastrukturen gezählt werden, also eine Organisation oder Einrichtung mit wichtiger Bedeutung für das staatliche Gemeinwesen sein, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen einträten.[16] Insbesondere diese kritischen Infrastrukturen sind erhöhten Gefährdungen aus dem Cyber-Raum ausgesetzt und könnten aus der Teilnahme an einem kooperativen Verfahren zur Datenfusion und –klassifikation zur Erkennung von Anomalien erhebliche Vorteile schöpfen.

2.1.4 IT-Sicherheitsgesetz

Es ist davon auszugehen, dass der Gesetzgeber in absehbarer Zeit ein IT-Sicherheitsgesetz verabschiedet, das als Kernpunkte die branchenübergreifende Einhaltung von Mindestanforderungen verlangt und Meldepflichten für eingetretene

[12] Bundesanstalt für Finanzdienstleistungsaufsicht, Rundschreiben 10/2013 (BA) – Mindestanforderungen an das Risikomanagement (MaRisk), abrufbar unter http://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/rs_1210_marisk_ba.html.
[13] Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz – EnWG) vom 7. Juli 2005, BGBl. I S. 1970, ber. S. 3621).
[14] Telemediengesetz (TMG) vom 26. Februar 2007, BGBl. I S. 179.
[15] Vgl. *Müller-Broich*, TMG, § 13 Rn. 6.
[16] *BMI*, Nationale Strategie zum Schutz kritischer Infrastrukturen (KRITIS-Strategie), S. 3. S. auch die Übersicht unter http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/BevoelkerungKrisen/Sektoreneinteilung.pdf?__blob=publicationFile.

Sicherheitsvorfälle begründet. Dazu hat das Bundesministerium des Innern im März 2013 einen Referentenentwurf[17] vorgelegt, der auf den Richtlinienvorschlag der Europäischen Kommission für eine Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union[18] zurückgeht. Wie sich das MonIKA-Verfahren in diese rechtlichen Rahmenbedingungen einfügen kann, wird in Kapitel 8 erarbeitet.

2.2 Zivilrechtliche Verpflichtungen

Neben den öffentlich-rechtlichen bestehen auch zivilrechtliche Verpflichtungen zur Schaffung von IT-Sicherheit, deren Missachtung zu einer Haftung führen kann. Die IT-Sicherheit stellt einen wesentlichen Aspekt der sog. IT-Compliance im Unternehmen dar, unter der die Einhaltung rechtlicher Anforderungen bei dem Einsatz von Informationstechnologie zu verstehen ist.[19] Auch zum Aspekt der IT-Compliance existiert kein einheitliches Gesetz.[20]

Einen Ausgangspunkt bilden jedoch die aktienrechtlichen Vorschriften über die Pflicht des Vorstandes zur Einrichtung eines effektiven Risikomanagementsystems aus § 91 Abs. 2 AktG[21].[22] § 91 Abs. 2 AktG spricht davon, dass der Vorstand geeignete Maßnahmen wie insbesondere ein Überwachungssystem einzurichten hat, damit gesellschaftsgefährdende Entwicklungen früh erkannt werden können. Auch wenn diese Vorschrift selbst keine expliziten Vorgaben für die von den Unternehmen zu gewährleistende Sicherheit enthält, wurde durch das KonTraG[23] klargestellt, dass die „übliche Sorgfalt“ der Unternehmensführung auch das Erkennen und Bekämpfen von IT-Risiken beinhaltet und ferner die Einrichtung von Sicherheitsmaßnahmen für die IT

[17] Referentenentwurf für ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz).
[18] COM(2013) 48 final.
[19] *Beucher*/*Utzerath*, MMR 2013, 362 (367 f.); *Nolte*/*Becker*, BB Beilage 2008 Heft 5, 23.
[20] S. schon *Schmidl*, in: Hauschka, Corporate Compliance, § 29 Rn. 13; *Nolte/Becker*, BB Beilage 2008 Heft 5, 23.
[21] Aktiengesetz vom 6. September 1965, BGBl. I S. 1089.
[22] *Nolte*/*Becker*, BB Beilage 2008 Heft 5, 23.
[23] Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KontraG) in der Fassung der Bekanntmachung vom 27. April 1998, BGBl. I S. 786.

sowie deren Kontrolle umfasst.[24] Diese Grundsätze aus § 91 Abs. 2 AktG sind auch auf andere Gesellschaftsformen wie z. B. die GmbH anwendbar.[25]

Über dieses Einfallstor sind auch die Gesetze und Normen von Bedeutung, die sich auf die Verwendung von Informationstechnologie beziehen.[26] Hierzu zählen die schon aufgezeigten Normen aus dem BDSG, TMG und dem TKG und darüber hinausgehend einschlägige nationale und internationale Qualitätsstandards für IT-Systeme oder auch die Grundschutzkataloge des BSI.[27] Zu beachten ist, dass die technischen Regelwerke wie ISO-Normen oder BSI-Grundschutzkataloge keine gesetzlichen Pflichten enthalten, sondern es sich um Empfehlungen handelt, an denen sich die Unternehmen orientieren können/sollen.[28] Eine unmittelbare Haftung ergibt sich aus ihrer Nichteinhaltung daher auch nicht. Dennoch ist ihre Bedeutung nicht zu unterschätzen, da es nahe liegt, dass ein Gericht bei einem möglichen Prozess die Maßstäbe heranziehen und ihre Einhaltung prüfen würde. Dadurch könnte ermittelt werden, ob die verkehrserforderliche Sorgfalt eingehalten wurde. Entsprechende Entscheidungen hierzu existieren derzeit – soweit ersichtlich – noch nicht.

2.2.1 Folgen der Nichteinhaltung für die Unternehmensleitung

Pflichten, die sich aus der IT-Compliance an Ausstattung und Betrieb der Unternehmens-IT ergeben – z. B. die Pflicht zur Einrichtung von Schutzmechanismen (Firewalls, aktuelle Antiviren-Software etc.) – stellen zunächst nur Organisationspflichten des Unternehmens dar. [29] Die Pflichten gelten somit im Innenverhältnis zwischen der Geschäftsführung und der Gesellschaft, was sich für Kapitalgesellschaften aus § 93 Abs. 2 Satz 1 AktG bzw. § 43 Abs. 2 GmbHG[30] ergibt. Ein Pflichtenverstoß stellt für die Leitungsebene ein persönliches Haftungsrisiko gegenüber der Gesellschaft dar.[31] So haften Vorstandsmitglieder nach § 93 Abs. 2 Satz 1 AktG gesamtschuldnerisch für entstandene Schäden gegenüber der Gesellschaft. § 43 Abs. 2 GmbHG sieht eine solidarische Haftung der Geschäftsführer gegenüber der Gesellschaft vor, sollten diese ihre Obliegenheiten

[24] *Schmidl*, in: Hauschka, Corporate Compliance, § 29 Rn. 37; *Beucher*/*Utzerath*, MMR 2013, 362 (367 f.).
[25] *Lensdorf*, CR 2007, 413 (414); *Spindler*, MMR 2008, 7 (10).
[26] *Nolte*/*Becker*, BB Beilage 2008 Heft 5, 23.
[27] *Nolte*/*Becker*, BB Beilage 2008 Heft 5, 23.
[28] *Schmidl*, in: Hauschka, Corporate Compliance, § 29 Rn. 97.
[29] *Nolte*/*Becker*, BB Beilage 2008 Heft 5, 23 (25).
[30] Gesetz betreffend die Gesellschaften mit beschränkter Haftung in der im BGBl. Teil III, Gliederungsnummer 4123-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 27 des Gesetzes vom 23. Juli 2013 (BGBl. I S. 2586) geändert worden ist.
[31] *Beucher*/*Utzerath*, MMR 2013, 362 (367 f.).

verletzen. Wichtig ist, dass § 93 Abs. 2 S. 1 AktG und § 43 Abs. 2 GmbHG ausschließlich für das Innenverhältnis zwischen Geschäftsführern und Gesellschaft gelten: Gesellschafter oder Dritte, die Ansprüche geltend machen wollen, sind auf die allgemeinen Normen verwiesen. Ferner muss beachtet werden, dass eine völlige Abwälzung des Haftungsrisikos für die Geschäftsführer durch eine Delegation der Aufgabe, für eine angemessene IT-Sicherheit Sorge zu tragen, nicht ohne Weiteres möglich ist, denn es besteht weiterhin die Anforderung, das entsprechende Personal sorgsam auszusuchen, zu überwachen und zu instruieren.[32]

Bei einer Personengesellschaft (GbR, oHG, KG) gelten die allgemeinen zivilrechtlichen Haftungsgrundsätze und auch hier besteht die Möglichkeit, dass die Gesellschaft oder Mitgesellschafter Ansprüche auf Grund der Verletzung von Geschäftsführungspflichten – wie der Sicherheit der verwendeten IT – geltend macht bzw. machen.[33]

Überdies kann es aber auch zu einer Außenhaftung kommen, wenn die Geschäftsführung schuldhaft Organisationspflichten wie die IT-Compliance verletzt.[34] Dritte können in diesem Fall über allgemeine zivilrechtliche Haftungsnormen unmittelbar gegen die Geschäftsführung vorgehen, wobei vornehmlich an deliktsrechtliche Tatbestände zu denken ist.[35] Bei Personengesellschaften wird die persönliche Haftung der Gesellschafter gegenüber Dritten über § 128 HGB[36] (KG), § 128 HGB analog (GbR) bzw. § 128 i. V. m. § 161 Abs. 2 HGB für Komplementäre und § 171 HGB für Kommanditisten (KG) begründet.[37]

2.2.2 Folgen der Nichteinhaltung für das Unternehmen

Bei einer Verletzung von IT-Sicherheitspflichten entsteht nicht nur für die Unternehmensleitung, sondern ebenfalls für das Unternehmen in Gestalt von vertraglichen oder deliktischen Schadensersatzansprüchen gegenüber Dritten eine Haftung. Insbesondere Kunden könnten Schadensersatzansprüche geltend machen,

[32] *Sundermann*, in: Reinhard/Pohl/Capellaro, IT-Sicherheit und Recht, Rn. 211.
[33] Dazu *Sundermann*, in: Reinhard/Pohl/Capellaro, IT-Sicherheit und Recht, Rn. 224 ff.
[34] *Lensdorf*, CR 2007, 413 (415).
[35] *Sundermann*, in: Reinhard/Pohl/Capellaro, IT-Sicherheit und Recht, Rn. 219.
[36] Handelsgesetzbuch in der im BGBl. Teil III, Gliederungsnummer 4100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 4. Oktober 2013 (BGBl. I S. 3746) geändert worden ist.
[37] *Sundermann*, in: Reinhard/Pohl/Capellaro, IT-Sicherheit und Recht, Rn. 223.

wenn es auf Grund des Ausfalls der IT-Infrastruktur zu einer Verzögerung der vertraglichen Leistungen kommt.[38]

Bei bestehenden vertraglichen Beziehungen stellt § 280 Abs. 1 BGB die mögliche Haftungsgrundlage dar.[39] Eine Haftung besteht dann, wenn die Gewährleistung von IT-Sicherheit eine Hauptleistungspflicht darstellt.[40] Es kann sich jedoch auch um eine aus § 241 Abs. 2 BGB ableitbare Nebenpflicht handeln, für eine sichere IT-Infrastruktur zu sorgen.[41]

Eine lückenhafte IT-Sicherheit kann ferner zu einer deliktischen Haftung aus §§ 823 ff. BGB führen.[42] Sollte eines der dort geschützten Rechtsgüter auf Grund von IT-Sicherheitsmängeln verletzt werden, besteht das Haftungsrisiko gegenüber dem jeweiligen Rechtsinhaber.

Mögliche Anspruchsgrundlagen für einen Schadensersatz ergeben sich zudem aus § 7 BDSG sowie § 44 Abs. 1 TKG. In § 43 BDSG und § 149 TKG sind Bußgelder normiert, sofern bestimmte Maßnahmen (nicht) getroffen werden.

2.3 Ergebnis

Festhalten lässt sich, dass im deutschen Recht bereits Normen existieren, die einen Bezug zu Fragen der IT-Sicherheit aufweisen. Ein übergreifendes Gesetz ist jedoch nicht vorhanden. Die Verletzung von IT-Sicherheit stellt für die Unternehmen und deren Führung auch ein Haftungsrisiko dar, sodass die Thematik auf der Agenda der Unternehmen stehen sollte.

Mit Spannung abzuwarten bleibt die Ausgestaltung der in Planung befindlichen (derzeit ein Kommissionsvorschlag) Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union[43] und ihre entsprechende Umsetzung in deutsches Recht.

[38] *Schmidl*, in: Hauschka, Corporate Compliance, § 29 Rn. 104; *Heckmann*, MMR 2006, 280 (282).
[39] Einzelheiten zu § 280 Abs. 1 BGB als Haftungsgrundlage in Kapitel 4.5.2.1.1.
[40] *Beucher*/*Utzerath*, MMR 2013, 362 (367).
[41] *Beucher*/*Utzerath*, MMR 2013, 362 (367).
[42] Einzelheiten zu §§ 823 ff. BGB als Haftungsgrundlage in Kapitel 4.5.2.1.2.
[43] COM(2013) 48 final.

3 Notwendigkeit rechtskonformer präventiver Methoden am Beispiel der Botnetzbekämpfung durch Internet-Service-Provider[44]

Nachfolgend wird untersucht, inwiefern es aus rechtlicher Sicht notwendig ist, überhaupt an präventiven Lösungen zu arbeiten.

3.1 Überblick

So ist zu fragen, ob überhaupt die Notwendigkeit besteht, Verfahren zur Datenfusion und -klassifikation zur Entdeckung von Anomalien zu entwickeln, oder ob bereits technisch effektives und zugleich rechtssicheres Instrumentarium besteht, das ausreichenden Schutz und ausreichende Möglichkeiten bietet, um sich gegen Botnetze zur Wehr zu setzen.

Der Beantwortung dieser Frage wurde im Rahmen des MonIKA-Projekts am Beispiel der Botnetzbekämpfung nachgegangen. Hierbei wurde die Maßnahme der Desinfektion und ihrer möglichen Folgen gewählt. Bei einer Desinfektion handelt es sich um eine der effektivsten Maßnahmen, um bestehende Botnetze zu beseitigen. Sie ist damit kein präventives, sondern ein reaktives Instrument. Bei ihrer Anwendung werden die Mechanismen des Botnetzes selbst genutzt. Über die bestehende Update-Funktionalität, die der Botmaster für die Kommunikation mit dem Botnetz nutzt, wird ein spezielles Update eingespielt. Dieses Update soll die Malware auf den betroffenen Systemen dazu veranlassen, sich selbst zu deinstallieren.

Der Vorteil einer Desinfektion liegt darin, dass sie geeignet ist, das komplette Botnetz zu beseitigen. Jeder infizierte Rechner kann mittels der Uptdate-

[44] Die Ausführungen in diesem Kapitel wurden im Rahmen des 13. Deutschen IT-Sicherheitskongresses vorgestellt (Bonn, Mai 2013) und publiziert: *Roos/Schumacher/Elsner/Meier/Wübbeling*, Rechtliche Betrachtung von Desinfektionsmaßnahmen zur Botnetzbekämpfung durch Internet-Service-Provider, Informationssicherheit stärken – Vertrauen in die Zukunft schaffen (Tagungsband zum 13. Deutschen IT-Sicherheitskongress), S. 37.

Funktionaliät erreicht werden. Damit besteht eine hohe Effizienz. Der Nachteil ergibt sich jedoch daraus, dass die Folgen einer Desinfektion trotz intensiver Testläufe in abgeschlossenen Systemen kaum vorhersehbar sind. Damit wohnt einer Desinfektion stets das Risiko inne, dass Schäden an unbekannten Systemen mit unabsehbaren Folgen verursacht werden.

Aus diesem Grund erscheint es notwendig, eine rechtliche Analyse vorzunehmen. Als ausführende Instanz wurde hierfür ein ISP gewählt, der dem Nutzer bezüglich Schutzmaßnahmen gegen die Infektion mit Malware am nächsten steht. Dies belegen auch die Empfehlungen der Allianz für Cybersicherheit e. V. unter Mitwirkung von BSI und namhaften ISPs wie der 1&1 Internet AG, Deutschen Telekom und Vodafone, die u. a. vorsehen, dass der ISP den Kunden bei dem Verdacht auf eine Infektion vorwarnt, ihm Informationen über Schutzmaßnahmen an die Hand gibt und ihn bei der Entfernung der Schadsoftware unterstützt.[45] Überdies sieht der Entwurf für ein IT-Sicherheitsgesetz in § 109a TKG IT-SiG-E ebenfalls vor, dass der ISP den Nutzer über Störungen informiert (Satz 3) und ihn zusätzlich auf technische Mittel hinweist, mit denen er die Störungen erkennen und beseitigen kann (Satz 4). Insofern liegt es nahe, den ISP als potenziell Handelnden zu wählen.

3.2 Verpflichtungen zur Botnetzbekämpfung

Von erhöhter Relevanz ist zunächst die Frage, ob den ISPs generell eine Pflicht zur Botnetzbekämpfung zukommt. Eine derartige Pflicht könnte sich sowohl aus öffentlich-rechtlichen Normen als auch aus dem Vertrag mit dem jeweiligen Kunden ergeben.

3.2.1 Gesetzliche Verpflichtungen aus dem Telekommunikationsgesetz

Die öffentlich-rechtlichen Rahmenbedingungen werden durch das TKG vorgegeben. Hier sind die §§ 88 ff. TKG, die sich dem Fernmeldegeheimnis, dem Datenschutz und der Öffentlichen Sicherheit widmen, von besonderer Bedeutung.

§ 109 TKG bezweckt die Sicherstellung, dass Telekommunikationsdienstleister angemessene Vorkehrungen zum Schutz vor

[45] *BSI*, Malware-Schutz – Handlungsempfehlungen für Internet-Service-Provider (ISP), https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/netzwerk/BSI-CS-046.pdf?__blob=publicationFile.

unbefugten Zugriffen auf Daten und vor äußeren Störungen treffen. Zu diesen Störungen zählt auch die Infektion mit Malware als ein systemwidriger Eingriff[46].

Insbesondere § 109 Abs. 2 TKG definiert Sicherheitsanforderungen, denen Betreiber eines öffentlichen Telekommunikationsnetzes nachkommen müssen. Als Betrieb eines Telekommunikationsdienstes für die Öffentlichkeit gilt das gewerbliche Angebot von Übertragungswegen für beliebige natürliche und juristische Personen, also wenn nicht lediglich geschlossene Nutzergruppen den Telekommunikationsdienst nutzen können.[47] ISPs bieten ihre Dienste der Öffentlichkeit an und grds. steht es jedem offen, einen Vertrag mit dem ISP abzuschließen. Somit unterliegen die ISPs den Pflichten aus § 109 Abs. 2 TKG. Entscheidend ist, dass eine Einrichtung oder ein System betroffen ist, das zum Angebot des Telekommunikationsdienstes genutzt wird.[48] Eine Pflicht zur Unterbindung jedweder Bedrohung, die mit Hilfe des Telekommunikationsnetzwerks verbreitet wird, ergibt sich aus der Norm hingegen nicht. Da Botnetze allerdings die Telekommunikationsanlagen und den durch sie gewährleisteten Datenfluss durch eine gezielte Überlastung des Netzes hemmen können, muss eine Pflicht zur Bekämpfung von Botnetzen aus § 109 Abs. 2 TKG abgeleitet werden.

3.2.2 Vertragliche Verpflichtungen gegenüber den Kunden

Fraglich ist, inwiefern sich aus dem zwischen ISP und Kunden bestehenden Access-Provider-Vertrag, der nach herrschender Meinung (h. M.) in Rechtsprechung und Literatur als Dienstvertrag i. S. d. § 611 BGB einzuordnen ist[49], eine Pflicht zur Bekämpfung von Botnetzen ergibt. Als jeweilige Hauptleistungspflicht stehen die Zugangsgewährung zum Internet entsprechend den vertraglichen Bestimmungen durch den ISP und die (in der Regel monatliche) Zahlung des vereinbarten Entgelts durch den Kunden im Synallagma.[50] Eine Hauptleistungspflicht zur Botnetzbekämpfung besteht demnach nicht.

§ 241 Abs. 2 BGB statuiert im vertraglichen Bereich jedoch Neben- und Schutzpflichten für die Vertragsparteien. Anerkannt ist, dass den ISP die Schutzpflicht zur Gewährleistung einer ausreichenden Datensicherheit gegenüber

[46] Zum Begriff des systemwidrigen Eingriffs *Bock*, in: Geppert/Schütz, TKG, § 109 Rn. 33.
[47] *Bock*, in: Geppert/Schütz, TKG, § 109 Rn. 31.
[48] *Graulich*, in: Arndt/Fetzer/Scherer TKG, § 109 Rn. 9.
[49] Für die Praxis entschieden durch *BGH*, NJW 2005, 2076.
[50] *Hoeren*, in: Graf von Westphalen, Vertragsrecht und AGB-Klauselwerke, Kapitel: E-Commerce-Verträge Rn. 10 ff.

seinen Vertragskunden trifft.[51] Das bedeutet, dass der ISP dem Stand der Technik entsprechende Vorkehrungen gegenüber Gefahrenquellen durch die Zugangsgewährung zum Internet, auf die er Einfluss hat, treffen muss. Hierzu zählen insbesondere die Abwehr von Hacker-Angriffen und DDoS-Attacken sowie der Einsatz von Spamfiltern.[52] Entsprechend den Einsatzmöglichkeiten von Botnetzen und dem Streben nach präventiven Maßnahmen ergibt sich daraus, dass ebenfalls Maßnahmen gegen Botnetze zu treffen sind, da über Botnetze DDoS-Attacken und Spamkampagnen gesteuert werden können. In Ausnahmefällen kann der ISP im Rahmen von Sicherheitsmaßnahmen den Kunden vom Zugang zum Internet trennen, ohne sich schadensersatzpflichtig zu machen. Derartige Einschränkungen der Hauptleistungspflicht können über die in den Allgemeinen Geschäftsbedingungen (AGB) enthaltenen Verfügbarkeits- sowie Störungsbeseitigungsklauseln gerechtfertigt werden.[53]

Zu beachten ist, dass den Kunden im Gegenzug die Nebenpflicht trifft, rechtswidrige Nutzungen des ihm zur Verfügung gestellten Internetzugangs zu unterlassen und den Anbieter nicht zu schädigen.[54] Unter einer solchen Schädigung ist auch die Verbreitung von Malware zum Ausbau eines Botnetzes zu fassen. Um Maßnahmen gegen den aktiven Störer, der bewusst Malware verbreitet und/oder aktiver Teil eines Botnetzes ist, zu ermöglichen, sehen die AGB der Access-Provider häufig Sperr- und Verdachtsklauseln vor.[55]

3.2.3 Zwischenergebnis

Das TKG verpflichtet die ISPs dazu, bestimmte Sicherheitsvorkehrungen zu treffen, sofern ansonsten die Funktionsfähigkeit des Netzes gefährdet erscheint. Botnetze stellen eine solche Gefahr dar, sodass eine Verpflichtung zur Botnetzbekämpfung bejaht werden muss. Der Access-Provider-Vertrag umfasst die Pflicht, Datensicherheit zu gewährleisten. Ist das System eines Nutzers jedoch mit Malware befallen, besteht eine erhebliche Gefahr für die Daten des Nutzers. Insofern muss der ISP auch unter zivilrechtlichen Aspekten Schutzmaßnahmen treffen.

---

[51] *Schmitz/von Netzer*, in: Schuster, Vertragshandbuch Telemedia, Kapitel 12 Rn. 21.
[52] *Redeker*, in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil 12 Rn. 102; *Spindler*, Vertragsrecht der Internetprovider, Teil IV Rn. 81.
[53] *Hoeren*, in: Graf von Westphalen, Vertragsrecht und AGB-Klauselwerke, Kapitel: E-Commerce-Verträge, Rn. 11 ff. Diese müssen freilich den allgemeinen Anforderungen der §§ 305 ff. BGB genügen.
[54] *Schmitz/von Netzer*, in: Schuster, Vertragshandbuch Telemedia, Kapitel 12 Rn. 24.
[55] Ein Beispiel findet sich in den Allgemeinen Geschäftsbedingungen für Access-Verträge der Unitymedia NRW GmbH unter 3.2.

Wie diese Schutzmaßnahmen jeweils konkret auszusehen haben, geben weder das TKG noch das Vertragsrecht konkret vor. § 109 Abs. 2 Satz 4 TKG definiert allerdings einen Angemessenheitsvorbehalt. Technischer und wirtschaftlicher Aufwand müssen danach in einem angemessenen Verhältnis zur Bedeutung der zu schützenden Rechte und zur Bedeutung der zu schützenden Einrichtungen für die Allgemeinheit stehen.

Es ist damit festzuhalten, dass keine Pflicht der ISPs zu Desinfektionsmaßnahmen besteht. Sie sind jedoch eine Möglichkeit, wie dem Botnetz begegnet werden kann.

3.3 Haftungsrisiken

Zwar ist die (automatische) Desinfektion die wohl derzeit effektivste, bekannte Methode, um gegen Botnetze vorzugehen. Allerdings ergeben sich dabei zwei maßgebliche Problemfelder: Zunächst kann durch die Verbreitung des Botnetzes auf Systemen unterschiedlichster Beschaffenheit die genaue Wirkung des desinfizierenden Updates nicht mit absoluter Sicherheit vorhergesagt werden. Erschwerend tritt hinzu, dass auch kritische Infrastrukturen von dem Botnetz betroffen sein könnten.

3.3.1 Zivilrechtliche Haftung

In zivilrechtlicher Hinsicht sähe sich der ISP im Fall des Schadenseintritts Schadensersatzansprüchen ausgesetzt. Es ist danach zu unterscheiden, ob der ISP mit dem Geschädigten in einem vertraglichen Verhältnis steht oder nicht. Im Falle des Bestehens eines Access-Provider-Vertrages ergibt sich ein Anspruch aus §§ 280 Abs. 1, 241 Abs. 2 BGB. Gegenüber Geschädigten, zu denen der ISP kein vertragliches Verhältnis pflegt, erwachsen dem Betroffenen Ansprüche deliktsrechtlicher Natur, insbesondere also aus § 823 Abs. 1 BGB sowie aus § 823 Abs. 2 BGB i. V. m. einem (oftmals strafrechtlichen) Schutzgesetz.

3.3.1.1 Betroffene Rechtsgüter und Zurechnung

Welche Rechtsgüter durch eine Desinfektion tangiert sind, spielt eine wichtige Rolle für die Frage, ob der Schutzbereich des § 823 Abs. 1 BGB mit den umfassten absoluten und ihnen gleichzustellenden Rechten betroffen ist. Auch auf

Rechtsfolgenseite erscheint es maßgeblich, welche Rechtsgüter betroffen sein können, um eine effektive Risikoanalyse durchzuführen. Als problematischer Faktor stellt sich vor allem die Unvorhersehbarkeit der Folgen dar, die durch eine Desinfektionsmaßnahme ausgelöst werden können.

Denkbar sind insbesondere Hard- und Softwareschäden, aber auch die Beschädigung von Daten, die in dem betroffenen System gespeichert sind. Möglich sind auch Folgeschäden. Bei Betroffenheit einer Anlage, über die kritische Infrastrukturen kontrolliert werden, kann sogar die Tötung von Menschen nicht ausgeschlossen werden.

Das weite Spektrum an betroffenen Rechtsgütern bedingt, dass mehrere absolute Rechtsgüter berührt sein können. In erster Linie kann es zu Beeinträchtigungen des Rechtsguts Eigentum kommen, von dem sowohl Einwirkungen auf die Sachsubstanz als auch die bloße Beeinträchtigung der Nutzungsmöglichkeit erfasst sind.[56] Die Veränderung oder Löschung von Daten, die durch die Magnetisierung auf Speichermedien wie etwa einer Festplatte gespeichert sind, wird weit überwiegend als Eigentumsverletzung – und damit als von § 823 Abs. 1 BGB erfasst – angesehen.[57] Die Verletzung der Rechtsgüter Leben, Körper und Gesundheit in Folge einer (fehlerhaften) Desinfektion kann ebenfalls nicht ausgeschlossen werden. In Erwägung zu ziehen sind auch das als „sonstiges Recht“ anerkannte Recht am eingerichteten und ausgeübten Gewerbebetrieb und das Allgemeine Persönlichkeitsrecht. Ein Eingriff in das Recht am eingerichteten und ausgeübten Gewerbebetrieb wird allerdings an dem Erfordernis der Betriebsbezogenheit scheitern. Dazu müsste die Maßnahme nämlich die Zielrichtung inne haben, gerade in den Betrieb und seine Organisation einzugreifen. Der ISP – in der Regel auch ohne Kenntnis darüber, wer betroffen sein könnte – würde jedoch die Desinfektion vornehmen, um die Risiken durch ein bestehendes Botnetz einzudämmen, aber nicht um ein von Malware betroffenes Unternehmen zu beeinträchtigen. Das Allgemeine Persönlichkeitsrecht steht neben natürlichen auch juristischen Personen zu.[58] Daten und deren Offenlegung sind von dem Schutz erfasst: Entsteht also infolge der Desinfektion ein Datenleck, bei dem sensible persönliche Daten von Individuen oder kritische Unternehmensinterna an die

[56] *Schiemann*, in: Erman, BGB, § 823 Rn. 25.
[57] Zuletzt *OLG Oldenburg*, ZD 2012, 177. Ferner *OLG Karlsruhe*, NJW 1996, 200 (201); *LG Kaiserslautern*, DAR 2001, 225; *Bartsch*, CR 2000, 721 (723); *Koch*, NJW 2004, 801 (802); *Leible/Sosnitza*, K&R 2002, 51 (52); *Libertus*, MMR 2005, 507 (508); *Meier/Wehlau*, NJW 1998, 1585 (1588).
[58] *Sprau*, in: Palandt, BGB, § 823 Rn. 87 - 92.

Öffentlichkeit gelangen, liegt zumindest ein Eingriff vor. Ob dieser dann allerdings rechtswidrig ist, muss in einem weiteren Schritt auf der Ebene der Widerrechtlichkeit ermittelt werden. Diese Güter- und Interessenabwägung kann allerdings nur anhand des Einzelfalls vorgenommen werden, wobei dem Gefahrengrad, der durch das Botnetz ausgeht, und der Rechtssphäre der betroffenen Daten besondere Berücksichtigung zugemessen werden muss.

Fraglich ist, inwieweit eine Zurechnung im Fall des Schadenseintritts reicht. Die Rechtsprechung wendet dabei die Adäquanztheorie an, nach der die Ursache im Allgemeinen und nicht nur unter besonders eigenartigen, unwahrscheinlichen und nach dem gewöhnlichen Verlauf der Dinge außer Betracht zu lassenden Umständen geeignet sein muss, einen Erfolg dieser Art herbeizuführen.[59] Da bekannt ist, dass selbst kritische Infrastrukturen betroffen sein könnten, ist eine enorm hohe Anzahl an Szenarien und Schadensfolgen denkbar. Im Einzelfall kann sich der schädigende ISP u. U. auf eine hypothetische Kausalität berufen, also einwenden, dass der Schaden auch auf Grund des Botnetzes eingetreten wäre. Rechtssicherheit bietet dies aber nicht.

3.3.1.2 Verschulden des ISP

Der ISP muss die Nebenpflichtverletzung bzw. die Verletzung eines Rechtsguts zu vertreten haben. Dabei gilt nach § 276 Abs. 1 Satz 1 BGB, dass der Schuldner Vorsatz und Fahrlässigkeit zu vertreten hat. Im Rahmen von vertraglichen Schadensersatzansprüchen gilt § 280 Abs. 1 Satz 2 BGB, also die gesetzliche Vermutung, dass der Schuldner die Pflichtverletzung zu vertreten hat, sodass sich der ISP exkulpieren müsste.[60] Gleiches gilt für § 831 Abs. 1 Satz 1 BGB, aus dem sich ebenfalls eine Haftung ergeben kann, da regelmäßig ein Mitarbeiter des ISP die Desinfektion durchführen würde. Bei dem deliktischen Anspruch aus § 823 Abs. 1 BGB ist das Verschulden hingegen nachzuweisen. Da der ISP als juristische Person selber nicht handeln kann, findet jeweils eine Zurechnung statt, die sich für vertragliche Ansprüche aus § 278 BGB und § 31 BGB analog bzw. bei deliktischen Ansprüchen aus § 31 BGB analog oder durch § 831 Abs. 1 Satz 1 BGB ergibt.[61]

Nachgegangen werden muss der Frage, ob Fahrlässigkeit oder Vorsatz vorliegen. Vor allem im Verhältnis des ISP zu seinen Kunden spielt dies eine Rolle,

[59] Ständige Rechtsprechung: *BGH*, NJW 1953, 700; 1972, 36; 1995, 126 (127); 1998, 138; 2002, 2232 (2233).
[60] *Ernst*, in: MüKo BGB, § 280 Rn. 31.
[61] Auf eine genaue Abgrenzung und Beleuchtung der Unterschiede innerhalb der Hierarchie wird an dieser Stelle verzichtet.

da dem Vertrag AGB zugrunde liegen, die regelmäßig eine Haftungsbegrenzung auf Vorsatz und grobe Fahrlässigkeit in den Grenzen des § 309 Nr. 7 lit. b BGB im Fall eines etwaigen Schadenseintritts vorsehen.[62]

Ein vorsätzliches Handeln verlangt das Wissen und Wollen des Eintritts der objektiven Tatbestandsmerkmale.[63] Das Wissenselement gilt dabei dann als erfüllt, wenn der Handelnde den Eintritt des Erfolges auf Grund seines eigenen Verhaltens für möglich hält.[64] Ein Schadenseintritt wird dabei selbst dann als erkannt und gewollt qualifiziert, wenn der Kausalverlauf zwar vom intendierten abweicht, sich jedoch noch im Rahmen des Denkbaren hält und keine andere Bewertung der Tat angezeigt ist.[65] Sofern der Desinfizierende darum weiß, dass sein Handeln zu einem Schadenseintritt führen kann, ist das Wissenselement zu bejahen. Lediglich völlig unabsehbare Folgen würden das Wissenselement ausscheiden lassen. Da aber die Gefährdung kritischer Infrastrukturen nach derzeitigem Stand der Forschung ebenfalls nicht ausgeschlossen werden kann, dürfte selbst dieses Ausschlusskriterium nicht greifen. Das Willenselement verlangt, dass die handelnde Person mit dem für möglich gehaltenen Schadenseintritt einverstanden sein oder ihn wenigstens billigend in Kauf nehmen muss, wobei schon Gleichgültigkeit gegenüber dem nicht für unwahrscheinlich gehaltenen Erfolg genügt.[66] An diesem Punkt verläuft die Grenze zur bewussten Fahrlässigkeit, die gegeben ist, wenn auf den Nichteintritt des Schadens und die Möglichkeit der Abwendung berechtigterweise vertraut wurde. Damit ist festzuhalten, dass eine Maßnahme nur im Einzelfall unter Berücksichtigung der realistischen Erfolgschancen abschließend beurteilt werden kann. Kann allerdings überhaupt keine Risikoanalyse der Desinfektionsmaßnahme vorgenommen werden, kann auch kein Worst-Case-Szenario ausgeschlossen werden. Damit dürfte regelmäßig Vorsatz gegeben sein.

In technischer Hinsicht sollte also an Lösungen gearbeitet werden, mit deren Hilfe das Gefahrenpotenzial überschaubarer gemacht werden kann. Bei der Möglichkeit einer gewissenhaften Prüfung und ihrem positiven Ergebnis können Vorsatz und grobe Fahrlässigkeit dann u. U. entfallen.

---

[62] Siehe nur Allgemeine Geschäftsbedingungen der Telekom Deutschland GmbH „Call & Surf Basic, Comfort und Comfort Plus“ unter Ziffer 10.
[63] *BGH*, NJW 1965, 962 (963).
[64] *Grundmann*, in: MüKo BGB, § 276 Rn. 155 f.
[65] *BGH*, NJW 1951, 596 (597); 1963, 148 (150); 1971, 459 (461).
[66] *Grundmann*, in: MüKo BGB, § 276 Rn. 161 m. w .N. aus der Rechtsprechung des *BGH*.

3.3.1.3 Mitverschulden

Eine andere rechtliche Frage besteht darin, ob dem von der Desinfektion Betroffenen unter bestimmten Umständen im Fall des Schadenseintritts ein Mitverschulden nach § 254 Abs. 1 BGB angelastet werden muss. Verschulden i. S. d. § 254 Abs. 1 BGB bedeutet, dass ein vorwerfbarer Verstoß gegen Gebote des eigenen Interesses besteht, mithin ein „Verschulden gegen sich selbst“[67].[68]

Bei der Infektion mit einem Bot ist der Anknüpfungspunkt das Unterlassen der Einrichtung und Nutzung abwehrender Mittel wie etwa von Anti-Viren-Programmen, Firewalls oder sicheren Browsern. Festgestellt werden muss jedenfalls, dass jedem Nutzer bekannt sein sollte, dass das Internet kein gefahrenfreier Raum ist.[69] Konsequenterweise ist damit auch zu verlangen, dass mittlerweile jeder Nutzer ein Anti-Viren-Programm auf seinem Computer installiert hat, das er in angemessenen Abständen auf seine Aktualität hin überprüft. Ferner erwartet werden darf, dass sich der Nutzer in gewissem Maße informiert, also aktuelles Tagesgeschehen zumindest nicht ignoriert. Wird medienwirksam vor bestimmten Sicherheitslücken gewarnt, infiziert sich ein Nutzer über einen solchen Verbreitungsweg und findet in der Folge eine Desinfektion mit Schadensfolgen statt, die diese gefährliche Malware beseitigen will, kann ein Mitverschulden des Nutzers angenommen werden. Dennoch dürften Beweisschwierigkeiten bestehen, wann und wie sich der Nutzer mit der Malware infiziert hat.

Als relevante Entscheidungen des *BGH* sind die Dialer-Entscheidung[70] sowie seine Entscheidung zu den Pflichten eines WLAN-Inhabers[71] hervorzuheben. Im Rahmen der Dialer-Entscheidung kam er zu der nutzerfreundlichen These, dass auf ein Ausbleiben des Angriffs durch einen Dialer vertraut werden dürfe. Ob sich dies auf andere Gefahren bei der Nutzung des Internets und im Übrigen auch ein Jahrzehnt später noch vertreten lässt, erscheint fraglich und vom jeweiligen Einzelfall abhängig. Für WLAN-Router grenzt der *BGH* die Pflicht des Nutzers auf die marktübliche Sicherung im Zeitpunkt des Erwerbs des WLAN-Routers ein. Für die Nutzung des Internets kann diese Annahme wegen der hohen Schnelllebigkeit, die fortlaufend neue Risiken bedingt, nicht übertragen werden. Schon für die

[67] Zuletzt *BGH*, NJW 2009, 582 (585).
[68] *Grüneberg*, in: Palandt, BGB, § 254 Rn. 1.
[69] Man denke nur an die umfangreiche Berichterstattung über die Sicherheitslücke des Windows Internet Explorers im September 2012.
[70] *BGH*, MMR 2004, 308. Dialer sind Einwahlprogramme, die eine Wählverbindung mit dem Internet oder Rechnernetzen herstellen können und durch ihren vom Anschlussinhaber ungewollten und unbemerkten Einsatz in der Lage sind, Schädigungen herbeizuführen.
[71] *BGH*, GRUR 2010, 633 – Sommer unseres Lebens.

Entscheidung zu WLAN-Routern wird kritisiert, dass die vom *BGH* nicht erwähnte Pflicht zur Aktualisierung mitumfasst sein soll.[72] Dennoch wird deutlich, dass der *BGH* keine extensiven Anforderungen an den Nutzer stellen möchte.

Sollte es zu einem Datenverlust kommen, kann zudem ein Mitverschulden in der Tatsache gesehen werden, wenn über einen unverhältnismäßig langen Zeitraum keine Datensicherung erfolgte.[73]

Im Falle des Schadenseintritts kann es also unter bestimmten Umständen durch ein Mitverschulden des Nutzers zu einer Minderung der Anspruchshöhe kommen.

3.3.1.4 Zwischenergebnis

Es bestehen hohe zivilrechtliche Risiken, sollte ein ISP eine Desinfektion (durch einen Mitarbeiter) vornehmen. Die Haftung zu seinen Kunden ergibt sich dabei aus vertragsrechtlichen Ansprüchen und im Verhältnis zu Dritten aus deliktischen Ansprüchen. Der Umfang des Schadensersatzanspruchs kann ggf. infolge eines Mitverschuldens gemindert sein.

3.3.2 Strafrechtliche Haftung

Bei der Durchführung von Desinfektionsmaßnahmen stellt sich für die ISPs und deren Mitarbeiter neben der Frage einer zivilrechtlichen Haftung auch die Frage nach einer strafrechtlichen Haftung. Entscheidend für eine strafrechtliche Beurteilung ist der im Rahmen der Desinfektion entstandene Schaden und dessen Entstehung. Auch ist für eine strafrechtliche Bewertung bedeutend, bei wem Schäden oder Rechtsgutverletzungen auftreten. Als mögliche Opfer kommen zum einen die Inhaber der infizierten IT-Systeme in Betracht, bei denen die Desinfektionsmaßnahmen durchgeführt werden. Unter Umständen können aber auch unbeteiligte Dritte durch die Desinfektionsmaßnahmen betroffen sein. Sind etwa kritische Infrastrukturen von den Auswirkungen der Desinfektionsmaßnahme betroffen, können Schäden an IT-Systemen Dritter und deren Rechtsgütern entstehen. Nachfolgend werden nun mögliche Tatbestände erläutert, die bei der Durchführung von Desinfektionsmaßnahmen von Bedeutung sein könnten. Der Schwerpunkt der Untersuchung liegt hierbei auf computerstrafrechtlichen Tatbeständen.

---

[72] Vgl. *Borges*, NJW 2010, 2624 (2625 f.).

[73] Eingehend zu Datensicherungspflichten *Hoeren*, in: Graf von Westphalen, Vertragsrecht und AGB-Klauselwerke, Kapitel: IT-Verträge Rn. 84 ff. Ebenfalls beachtenswert *OLG Karlsruhe*, NJW 1996, 200 (201 f).

3.3.2.1 Relevante Straftatbestände

Zunächst ist an eine Strafbarkeit aus § 202a StGB (Ausspähen von Daten) zu denken. Im Strafrecht ist von einem weiten Datenbegriff auszugehen, der von § 202a Abs. 2 StGB eingeschränkt wird.[74] Daten im Sinne des § 202a Abs. 1 StGB sind danach nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

Nicht unmittelbar wahrnehmbar bedeutet, dass die Daten erst nach einer entsprechenden technischen Umformung sichtbar oder hörbar sein dürfen.[75] Die rechtliche Hürde, die für eine Strafbarkeit nach § 202a StGB besteht und vom Täter überwunden werden muss, ist recht niedrig: Bereits das Verschaffen des bloßen Zugangs zu den Daten reicht aus, um die Strafbarkeit zu begründen. Es genügt, dass der Täter bestehende Sicherheitseinrichtungen überwindet. Eine Kenntnisnahme der Daten durch den Täter ist nicht notwendig.[76] Dies bedeutet, dass auch das „reine Hacking" von § 202a StGB erfasst wird.[77] Hierzu zählt etwa der Einsatz von Trojanern, Sniffern oder Backdoorprogrammen, die der Aufzeichnung von Vorgängen auf dem Rechner, dem Ausspähen von Daten oder gar der gezielten Steuerungen des infizierten Rechners dienen.[78] Auf Grund dieser niedrigen Hürde liegt eine Erfüllung des objektiven Tatbestandes von § 202a StGB bei der Durchführung von Desinfektionsmaßnahmen nahe.

In bestimmten Fällen kann eine Desinfektion so durchgeführt werden, dass der Anwender der Desinfektionsmaßnahme selbst keine Zugangssicherung überwinden muss, um Zugriff auf fremde Rechnersysteme zu erhalten. Stattdessen wird der Zugang, den der Angreifer mit dem Bot geschaffen hat, genutzt, um den Bot zu beobachten und zu bekämpfen. Eine Strafbarkeit nach § 202a StGB dürfte daher in diesen Fällen ausscheiden, da die Zugangssicherung auf Grund des eingeschleusten Bots bereits überwunden ist und der Zugang zu fremden Daten durch den Anwender nicht unter Überwindung der Zugangssicherung erfolgt. Die Überwindung der Zugangssicherung muss für die Verschaffung des Zugangs jedoch ursächlich sein, um eine Strafbarkeit nach § 202a StGB begründen zu können.[79] Außerdem muss die

[74] *Fischer*, StGB, § 202a Rn. 3; *Lenckner/Eisele*, in: Schönke/Schröder, StGB, § 202a Rn. 3.
[75] *Lenckner/Eisele*, in: Schönke/Schröder, StGB, § 202a Rn. 4.
[76] *Lenckner/Eisele*, in: Schönke/Schröder, StGB, § 202a Rn. 10.
[77] *Ernst*, NJW 2007, 2661.
[78] *Fischer*, StGB, § 202a Rn. 10; *Lenckner/Eisele* in: Schönke/Schröder, StGB, § 202a Rn. 3.
[79] *Fischer*, StGB, § 202a Rn. 11b; *Lenckner/Eisele* in: Schönke/Schröder, StGB, § 202a Rn. 10a.

Zugangssicherung zum Zeitpunkt der Tathandlung wirksam sein.[80] An diesen Erfordernissen dürfte es in dem aufgegriffenen Szenario fehlen.

Bei der Durchführung von Desinfektionsmaßnahmen besteht zudem die Gefahr einer Verwirklichung von § 202b StGB (Abfangen von Daten). Entscheidend für eine Strafbarkeit nach § 202b StGB ist die konkrete Maßnahme und deren technische Vorgehensweise. Werden bei der Durchführung z. B. Dateien kopiert oder umgeleitet, so kann eine Strafbarkeit aus § 202b StGB bestehen. In den Anwendungsbereich von § 202b StGB fallen nur Daten, die sich zum Zeitpunkt der Tat in einem Übertragungsvorgang befinden.[81] Gespeicherte Daten, die früher übermittelt wurden, werden hingegen nicht von § 202b StGB erfasst.[82]

Ferner liegt bei der Durchführung von Desinfektionsmaßnahmen die Verwirklichung des Tatbestandes aus § 303a Abs. 1 StGB (Datenveränderung) nahe. Diese Gefahr besteht insbesondere dann, wenn durch die Maßnahme Daten gelöscht werden sollten. Eine besondere Zugangssicherung ist für die Erfüllung von § 303a StGB nicht notwendig. § 303a StGB erfasst die „virtuelle Sachbeschädigung“ und dient dem Schutz des Interesses des Verfügungsberechtigten am Zustand seiner Daten, deren unversehrte Verwendungsmöglichkeit und der in ihnen enthaltenen Informationen.[83]

Auch besteht die Möglichkeit einer Strafbarkeit nach § 303b Abs. 1 StGB (Computersabotage). Neben dem Qualifikationstatbestand aus § 303b Abs. 1 Nr. 1 StGB zu § 303a StGB kommt als Verletzungshandlung auch eine Tathandlung nach § 303b Abs. 1 Nr. 3 StGB in Betracht, wenn es im Rahmen der Desinfektionsmaßnahme zu Hardwareschäden kommen sollte. § 303b Abs. 1 Nr. 3 StGB erfasst Fälle, in denen eine erhebliche Störung der Datenverarbeitung durch das Zerstören, Beschädigen, Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers erfolgt. Als Datenträger kommen insbesondere Magnetbänder, Festplatten, CD-ROMs und Disketten in Betracht.[84] Eine Strafbarkeit aus § 303b Abs. 1 Nr. 2 StGB dürfte jedoch bei der Durchführung von Desinfektionsmaßnahmen zu verneinen sein, da der Täter in diesen Fällen nicht in Nachteilszufügungsabsicht handeln wird. Eine Strafbarkeit nach § 303b Abs. 1 StGB setzt eine erhebliche Störung der

[80] *Lenckner/Eisele*, in: Schönke/Schröder, StGB, § 202a Rn. 10a.
[81] *Eisele*, in: Schönke/Schröder, StGB, § 202b Rn. 3.
[82] *Eisele*, in: Schönke/Schröder, StGB, § 202b Rn. 3.
[83] *Ernst*, NJW 2007, 2661 (2664).
[84] *Fischer*, StGB, § 303b Rn. 13.

Datenverarbeitung voraus. Für eine erhebliche Störung ist bereits ausreichend, wenn ein einziger sonst möglicher Datenverarbeitungsvorgang nicht in bisheriger Form durchführbar ist.[85] Lässt sich hingegen eine Beeinträchtigung ohne großen Aufwand an Zeit, Mühe und Kosten beheben, so liegt lediglich eine unerhebliche Störung vor.[86] Durch die Beschränkung des § 303b Abs. 1 StGB auf Fälle „von wesentlicher Bedeutung" sollen Bagatellfälle von der Norm ausgeschlossen werden.[87]

Die Erfüllung weiterer Straftatbestände ist ebenfalls denkbar. So könnte es durch den Ausfall von IT-System zu Personenschäden kommen, sodass Straftatbestände, die den Schutz des Lebens bzw. der körperlichen Unversehrtheit bezwecken, einschlägig wären. Sollten durch die Desinfektionsmaßnahmen bspw. E-Mails gelöscht werden, ist auch eine Strafbarkeit wegen Verletzung des Post- oder Fernmeldegeheimnisses aus § 206 Abs. 2 Nr. 2 StGB möglich.

3.3.2.2 Kausalität und objektive Zurechnung

Neben der Erfüllung der Tatbestandsmerkmale erfordert eine Strafbarkeit auch, dass der Täter den tatbestandlichen Erfolg durch die Handlung verursacht hat und ihm der Erfolg zuzurechnen ist. Im Einzelfall kann eine objektive Zurechnung ausscheiden, wenn Desinfektionsmaßnahmen durchgeführt werden. So ist der Erfolg dann nicht zurechenbar, wenn der Täter diesen durch das Eingreifen in den Kausalablauf in seiner konkreten Gestalt zwar beeinflusst, jedoch dabei den drohenden (schwereren) Erfolg abmildert oder ein zeitliches Hinausschieben seines Eintritts bewirkt.[88] Wird durch die Desinfektionsmaßnahme ein größerer Schaden für den Betroffenen verhindert, so kann es an einer solchen Zurechnung mangeln. In diesem Falle können ggf. auch Rechtfertigungsgründe zugunsten des Täters eingreifen und eine Strafbarkeit ausschließen. Eine Zurechnung des tatbestandlichen Erfolges liegt aber dann vor, wenn der Täter zwar durch sein Handeln eine konkrete Gefahr abwendet, dabei jedoch eine neue eigenständige (rechtlich relevante) Gefahr begründet, die sich in dem von ihm verursachten Verletzungserfolg niederschlägt.[89]

3.3.2.3 Vorsatz

Eine weitere bedeutsame Frage im Zusammenhang mit einer strafrechtlichen Haftung ist die Frage nach dem Bestehen des Vorsatzes. Eine Strafbarkeit wegen

[85] *Stree/Hecker,* in: Schönke/Schröder, StGB, § 303b Rn. 9.
[86] *Stree/Hecker,* in: Schönke/Schröder, StGB, § 303b Rn. 9.
[87] *Kühl,* in: Lackner/Kühl, StGB, § 303b Rn. 2.
[88] *Lenckner/Eisele,* in: Schönke/Schröder, StGB, Vorb. § 13 Rn. 94.
[89] *Lenckner/Eisele,* in: Schönke/Schröder, StGB, Vorb. § 13 Rn. 94.

Fahrlässigkeit muss in der Strafnorm ausdrücklich festgelegt sein (vgl. § 15 StGB). So ist für bestimmte Straftatbestände – so auch für die erwähnten §§ 202a, 202b, 303a, 303b StGB – ein vorsätzliches Handeln für eine Strafbarkeit erforderlich. Bei der Durchführung von Desinfektionsmaßnahmen kann die Abgrenzung des bedingten Vorsatzes von der bewussten Fahrlässigkeit entscheidend für eine Strafbarkeit sein. Denn derjenige, der eine Desinfektion durchführt, wird nicht in Schädigungsabsicht handeln und auch keine Schäden an fremden Rechtsgütern verursachen wollen. Bzgl. der Anforderungen, die zur Annahme eines Vorsatzes erfüllt sein müssen, kann auf die Ausführungen zu den zivilrechtlichen Haftungsrisiken unter 3.3.1 verwiesen werden.

Kriterien zur Abgrenzung des bedingten Vorsatzes von der bewussten Fahrlässigkeit können die Offensichtlichkeit der Tatbestandsverwirklichung, die Gefährlichkeit oder auch die getroffenen Vorkehrungen zur Gefahrvermeidung sein.[90] Daher muss vor der Durchführung einer Desinfektionsmaßnahme geprüft werden, wie anfällig das Verfahren bei Probedurchläufen gewesen ist und welche Schäden hierbei aufgetreten sind. Insgesamt dürfte Vorsatz bei der Anwendung von Desinfektionsmaßnahmen naheliegen, wenn die Verletzung fremder Rechtsgüter nicht ausgeschlossen werden kann. Hält der Täter die Wahrscheinlichkeit eines strafbaren Erfolgseintritts für gering, weil er etwa Vorsichtsmaßnahmen getroffen hat und deshalb davon ausgeht, dass „schon alles gut gehen werde“, liegt in der Regel aber nur bewusste Fahrlässigkeit vor.[91]

3.3.2.4 Zwischenergebnis

Insgesamt ist festzuhalten, dass die Durchführung von Desinfektionsmaßnahmen die Gefahr einer strafrechtlichen Haftung in sich birgt. Die Frage nach einem möglichen Vorsatz spielt hierbei eine wichtige Rolle. Um die Gefahr einer strafrechtlichen Haftung zu minimieren, sollte daher im Vorfeld – bspw. durch Testläufe – geprüft werden, ob Schäden an Rechtsgütern eintreten könnten und wie hoch das entsprechende Risiko des Eintritts einer Rechtsgutverletzung ist. Eine Strafbarkeit kann zudem in Ausnahmefällen ausscheiden, falls Rechtfertigungsgründe eingreifen sollten.

[90] *Sieber*, in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil 19 Rn. 83.
[91] *Sieber*, in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil 19 Rn. 83.

3.3.3 Rechtfertigung im Falle des Schadenseintritts

Die hohen haftungsrechtlichen Risiken in zivil- und strafrechtlicher Sicht eröffnen die Frage, ob eine Desinfektionsmaßnahme einer Rechtfertigung zugänglich ist. So entfiele im Falle der Rechtfertigung im Rahmen der deliktischen Ansprüche die Rechtswidrigkeit ebenso wie die Rechtswidrigkeit etwaiger verwirklichter Straftatbestände. Die aus dem Strafrecht bekannten Rechtfertigungsgründe sind auch im Zivilrecht anerkannt[92] und umgekehrt. Betont werden muss allerdings, dass vertragliche Schadensersatzansprüche nicht gerechtfertigt werden können, sodass Kunden des ISP – im Falle des Schadenseintritts – stets der vertragliche Anspruch bliebe. Bei Dritten, denen keine vertraglichen Ansprüche zustehen, wäre dies dann anders.

3.3.3.1 Nothilfe

Zunächst ist an den Rechtfertigungsgrund der Notwehr bzw. Nothilfe zu denken. Eine Desinfektionsmaßnahme könnte eine Nothilfe darstellen, da sie dazu dient, dass der befallene Rechner von dem Botnetz befreit und somit nicht mehr rechtswidrig missbraucht wird sowie lokale Daten gesichert werden. Jedoch kann über § 32 StGB lediglich eine Handlung gerechtfertigt werden, die sich gegen den Angreifer richtet. Eingriffe in die Rechte Dritter sind nicht umfasst. Im Fall der Nutzung fremder Gegenstände, kann eine Beschädigung vielmehr über die §§ 228, 904 BGB gerechtfertigt werden.[93]

3.3.3.2 Regeln des rechtfertigenden Notstands

Eigentumsschäden, die bei der Desinfektion entstehen, könnten möglicherweise auch durch § 228 BGB oder § 904 BGB gerechtfertigt werden, die als Spezialvorschriften der allgemeinen Regelung des rechtfertigenden Notstands in § 34 StGB vorgehen.[94] Für Schäden, die nicht bloß fremde Sachen betreffen, bleibt § 34 StGB anwendbar. Richtigerweise muss unterschieden werden, ob die Gefahr von der Sache selbst im Sinne einer unmittelbaren Kausalität ausgeht (dann § 228 BGB) oder die Gefährdung nur mittelbar von der Sache ausgeht (dann § 904 BGB).[95] Die infizierten Computersysteme stellen selbst nicht den Ursprung der Gefahr dar, sondern vielmehr das Verhalten desjenigen, der das Botnetz

[92] *Wagner*, in: MüKo BGB, § 823 Rn. 314.
[93] *Fischer*, StGB, § 32 Rn. 24.
[94] Ganz h. M., s. *Erb*, in: MüKo StGB, § 34 Rn. 14; *Fischer*, StGB, § 34 Rn. 22; *Günther*, in: Wolter SK-StGB, § 34 Rn. 57; *Kühl*, in: Lackner/Kühl, StGB, § 34 Rn. 14; *Beulke*, in: *Wessels*/Beulke, Strafrecht Allgemeiner Teil, Rn. 287.
[95] *Ellenberger*, in: Palandt, BGB, § 228 Rn. 6; *Fahse*, in: Soergel, BGB, § 228 Rn. 13 f.; *Repgen*, in: Staudinger, BGB, § 228 Rn. 16.

unterhält und steuert. Er ist in der Lage, den infizierten Rechner als Teil des Botnetzes einzusetzen. Somit ist § 904 BGB anwendbar, der inhaltlich eine Duldungspflicht des Eigentümers begründet, obwohl von ihm selbst kein rechtswidriger Angriff ausgeht.[96]

§ 904 BGB verlangt zunächst, dass eine Notstandslage besteht, also eine gegenwärtige Gefahr vorliegt. Für eine Gefahr muss aus objektiver Sicht (ex ante) der Eintritt eines Schadens nicht nur als möglich, sondern als nahe liegend erscheinen.[97] Zu den Schäden, die durch Botnetze verursacht werden können, sind insbesondere Vermögensschäden durch mögliche DDoS-Attacken, Spam-Kampagnen oder die unbefugte Nutzung ausspionierter Daten und Eigentumsschäden durch die Löschung lokaler Daten[98] zu zählen. Ist der Rechner erst einmal mit Malware infiziert, lässt er sich bei bestehender Internetverbindung jederzeit zu missbräuchlichen Zwecken einsetzen oder lassen sich die in seinem System abgelegten sensiblen Daten ausspionieren. Damit ist sofortige Abhilfe notwendig und auch die Gegenwärtigkeit zu bejahen. Es liegt dann eine dauerhafte Gefahr vor. Auf ein Verschulden oder die Vorhersehbarkeit der Gefahr kommt es bei § 904 BGB nicht an.[99]

Die Notstandshandlung muss sodann auch geeignet und erforderlich sein. Zweifel bestehen an der Erforderlichkeit, wenn es technisch möglich sein sollte, den Betroffenen zu informieren und selber zu einer Desinfektionsmaßnahme aufzufordern. Dies ist bei einer Information per Brief mit hohem Aufwand verbunden und bei einer Information per Nachricht technisch ebenfalls nicht einfach zu bewerkstelligen. Hinzu tritt, dass Nutzer den Hinweis ignorieren könnten, sodass sich aus dem Risiko der Nichtbeachtung die Erforderlichkeit ergibt. Außerdem kann eine derart schnelle Desinfektion erforderlich sein, um akute Gefahren abzuwehren. Letztlich ist eine Interessenabwägung durchzuführen, bei der die gefährdeten Rechtsgüter miteinander abzuwägen sind: Überwiegt das geschützte das beeinträchtigte Interesse wesentlich, kann eine Rechtfertigung erfolgen. Zu wessen Seite die Interessenabwägung dabei ausschlägt, hängt von den Umständen des Einzelfalls und den entsprechend bedrohten Rechtsgütern ab: Sollte das Botnetz bspw. gezielt angelegt sein, um kritische Infrastrukturen und Menschenleben zu gefährden, wären mögliche Vermögensschäden zu rechtfertigen. Allerdings gilt

[96] *Schulte-Nölke*, in: Schulze et. al., BGB, § 904 Rn. 1.
[97] *BGH*, NJW 1963, 1069; 1964, 1911; 1969, 939.
[98] Daten können unter den Eigentumsbegriff gefasst werden: *Wiek-Noodt*, in: MüKo StGB, § 303 Rn. 33.
[99] *Seiler*, in: Staudinger, BGB, § 904 Rn. 13.

umgekehrt, dass eine Desinfektion nicht zu rechtfertigen wäre, wenn Desinfektionsmaßnahmen kritische Infrastrukturen gefährden und „nur“ Vermögensschäden durch das Botnetz möglich erscheinen. Drohen qualititativ gleichartige Verluste, kann es gerechtfertigt sein, den quantitativ größeren Verlust abzuwenden.[100]

Im Ergebnis ist also auf den Einzelfall und die konkret gefährdeten Rechtsgüter zu verweisen. Bei Vorliegen der Voraussetzungen des § 904 BGB erwächst dem Duldungspflichtigen jedoch aus § 904 Satz 2 BGB ein verschuldensunabhängiger Schadensersatzanspruch, sofern er die Notstandslage nicht schuldhaft verursacht hat. § 254 BGB kann bei diesem Anspruch ebenfalls herangezogen werden.

Die Erwägungen gelten auch für die Rechtfertigung anderer Rechtsgüter (abgesehen von Eigentum), die durch § 34 StGB möglich ist.

3.3.3.3 Mögliche weitere Rechtfertigungsgründe

Die Regeln der Geschäftsführung ohne Auftrag (§§ 677 ff. BGB) werden zumindest im Zivilrecht auch als Rechtfertigungsgrund für unerlaubte Handlungen angesehen. Allerdings liegen die Voraussetzungen einer Geschäftsführung ohne Auftrag des ISP im Verhältnis zu Kunden schon nicht vor, da der Vertrag zwischen ISP und Kunden eine Abwehr- und Schutzpflicht beinhaltet. Im Verhältnis zu Dritten besteht zwar kein Auftrag, aber im Ergebnis kann eine Beurteilung offen bleiben. Der ISP haftet regelmäßig – sollte ein deliktischer Anspruch ausscheiden – aus einem vertraglichen Anspruch (die Geschäftsführung ohne Auftrag als Schuldverhältnis und eine entsprechende Sorgfaltspflichtverletzung, die im Fall des – wenn auch nur bedingten – Vorsatzes nicht durch die Privilegierung des § 680 BGB legitimiert würde) oder dem Anspruch aus § 678 BGB, also einem Übernahmeverschulden, durch die dann nicht vorhandene verkehrserforderliche Sorgfalt.

Es kann ferner angedacht werden, § 109 Abs. 2 TKG, der die Erhaltung der Verfügbarkeit von Telekommunikationssystemen als zentraler Infrastruktur bezweckt,[101] als Rechtfertigungsgrund fruchtbar zu machen. Dieser schreibt den Betreibern öffentlicher Telekommunikationsnetze u. a. vor, Maßnahmen gegen Störungen durch äußere Eingriffe zu treffen. Allerdings wird weder aus dem Wortlaut noch aus dem Telos ersichtlich, dass eine Rechtfertigung schädigender

[100] Wenn auch zu § 34 StGB: *Fischer*, StGB, § 34 Rn. 13.
[101] *Klesczewski*, in: Säcker, TKG, § 109 Rn. 17.

Maßnahmen gewollt ist. Insbesondere vor dem Hintergrund des Rechtsstaatsprinzips und des ansonsten bestehenden Eingriffs in hochrangige Grundrechte wie u. a. Eigentum, ist eine andere Deutung nicht möglich.

3.3.3.4 Ergebnis

Die Desinfektion als effektivstes individuelles Mittel der Bekämpfung von Botnetzen birgt hohe rechtliche Risiken sowohl in zivil- als auch in strafrechtlicher Hinsicht. In gewissen Konstellationen ist eine Rechtfertigung zwar möglich, insgesamt muss den ISPs aber unter der aktuellen Rechtslage und den bestehenden Risiken abgeraten werden, Desinfektionen vorzunehmen. Dies gilt zumindest solange, wie kritische Infrastrukturen gefährdet sind. Um die Desinfektion nutzbar zu machen, müsste an Verfahren gearbeitet werden, die ein höheres Maß an Überschaubarkeit etwaiger Gegenmaßnahmen gewährleisten.

3.4 Fazit

Die Untersuchungen zeigen, dass präventive Lösungen erforderlich sind. Die reaktive Desinfektion als Mittel zur Bekämpfung von Botnetzstrukturen bringt unter den derzeitigen Gegebenheiten hohe rechtliche, nahezu unüberschaubare Risiken mit sich. Ein Ansatzpunkt ist zum einen die Sensibilisierung der Bevölkerung für die Thematik der IT-Sicherheit. Ein anderer Ansatzpunkt ist die Entwicklung von Verfahren, die im Vorfeld aktiv sind, um Angriffe und Gefahren zu vermindern. Auf dieser Basis arbeitet das MonIKA-Verfahren.

4 Vertrags- und haftungsrechtliche Rahmenbedingungen bei der Entwicklung, dem Vertrieb und dem Einsatz einer Software zur Informationsfusion und -klassifikation zur Erkennung von Anomalien im Unternehmensumfeld

Im Mittelpunkt des folgenden Kapitels steht das Szenario „Enterprise-Monitoring“.

4.1 Untersuchungsgegenstand

Innerhalb des MonIKA-Projekts wurden drei Anwendungsszenarien für den Einsatz des MonIKA-Verfahrens entwickelt. Auf Grund naheliegenden praktischen Einsatzes des MonIKA-Verfahrens im Unternehmensumfeld ist dabei dem Anwendungsszenario „Enterprise-Monitoring“ eine besonders hohe Relevanz beizumessen. Dies untersucht den Einsatz von MonIKA im Umfeld von wirtschaftlich miteinander verbundenen Unternehmen. Zu diesem Anwendungsszenario wurde auch der Proof-of-Concept (PoC) gebildet.

4.2 Sachverhalt (Proof-of-Concept)

Zunächst muss der Sachverhalt beschrieben werden, auf dessen Grundlage die Untersuchungen erfolgen.

erfolgen.

4.2.1 Ausgangsfall

Das MonIKA-Verfahren wird in dem vorliegenden Gutachten als Mittel zur Verwirklichung eines kooperativen Monitorings betrachtet. Durch MonIKA werden die Prozesse innerhalb der IT-Infrastruktur mehrerer wirtschaftlich miteinander verbundener Unternehmen aus dem produzierenden Gewerbe überwacht (sog. „Enterprise-Monitoring“)[102]. Das übergeordnete Ziel des Einsatzes von MonIKA liegt dabei in einer Minimierung von wirtschaftlichen Risiken der beteiligten Unternehmen, die sich insbesondere aus der Cyber-Spionage und Cyber-Sabotage ergeben.

Die fiktiven Unternehmen sind die McQueer AG, ein Automobilhersteller, und ihre Zulieferer für Bremsen (Stopper GmbH), Reifen (Fastrubbers GmbH) und Auspuffanlagen (NoisySys GmbH). Diese Unternehmen bilden zwar keinen Konzern im Sinne eines vertikalen Beherrschungsverhältnisses der McQueer AG über die Lieferanten, weisen aber auf Grund ihrer wirtschaftlichen Abhängigkeit voneinander das gemeinsame Interesse auf, gegenüber Angriffen auf die unternehmenseigene IT-Infrastruktur in höchstmöglichem Maße geschützt zu sein. Zu diesem Zweck unterhalten alle der beteiligten Unternehmen eine eigene IT-Sicherheitsabteilung. Während also üblicherweise jedes Unternehmen nur über eigene Strategien zur Erhöhung der Netz- und IT-Sicherheit verfügt, erweitert MonIKA dieses isolierte, dezentrale Vorgehen der lokalen IT-Sicherheit um einen kooperativen, zentralen Ansatz.

Dies geschieht durch die Teilnahme der Unternehmen an einem Netzwerk, in dessen Zentrum eine externe Stelle steht. Für den PoC nimmt die MonIKA GmbH die Rolle dieser externen Stelle ein. Diese GmbH ist ein eigenständiger IT-Sicherheitsdienstleister und juristisch sowohl von dem Automobilhersteller als auch von den beteiligten Lieferanten unabhängig. Die McQueer AG und ihre Lieferanten verpflichten sich über schuldrechtliche Verträge gegenüber der MonIKA GmbH, bestimmte Informationen an sie zu senden. Die zu übermittelnden Informationen werden durch seitens der MonIKA GmbH bereitgestellte MonIKA-Agenten gewonnen, die an die unternehmenseigene, datenliefernde Sensorik angebunden werden. Über diese Agenten erfolgt die Kommunikation mit der MonIKA GmbH. Die Organe der Unternehmen, die mit dem Einsatz von MonIKA betraut sind, sind die sog. „Security Operation Center“ (SOC). Diese beobachten an jedem Tag des Jahres rund um die Uhr den Netzwerkverkehr der unternehmenseigenen

[102] Vgl. Deliverable 4.1, S. 25 ff.; Deliverable 4.1.1, S. 22 ff.

Informationstechnik (Monitoring) und werden eingesetzt, um das aus dem Betrieb der Informationstechnik resultierende Sicherheitsrisiko zu minimieren. Die von den MonIKA-Agenten ermittelten Daten werden in aggregierter, pseudonymisierter oder anonymisierter Form an die MonIKA GmbH übermittelt. Denkbar ist es auch, dass die Monitoring-Daten nach vorheriger Sichtung durch das jeweilige Unternehmen an die externe Stelle gesendet werden. Im PoC besteht jedoch ein gewisses Maß an Vertrauen zwischen den Teilnehmern untereinander und gegenüber der MonIKA GmbH, sodass eine direkte Datenübermittlung zwecks Effektivierung des Verfahrens stattfindet.

Die MonIKA GmbH betreibt ein übergeordnetes SOC, das sog. „Common SOC“ (CSOC). Über das CSOC, als gemeinsames SOC, wird der zentrale Ansatz des MonIKA-Verfahrens organisiert und verwirklicht. Technisch erfolgt dies durch die Einrichtung und den Betrieb eines sog. „EvA-Service-Clusters“ (EvASC) bei der MonIKA GmbH. Durch den Betrieb des EvASC werden einerseits die gesammelten Sensordaten aus den einzelnen Unternehmen zusammengeführt und andererseits erfolgt die Kommunikation mit den Unternehmen als (regelmäßig identischen) Ergebniskonsumenten. Aufbau, Unterhaltung und Betrieb des CSOC obliegen der MonIKA GmbH, die sich dazu vertraglich gegenüber den Unternehmen gegen Entgelt verpflichtet. Die MonIKA GmbH wertet die auf diese Weise von dem Hersteller und allen Lieferanten übermittelten Informationen aus. Dadurch identifiziert das CSOC der MonIKA GmbH Bedrohungen für die gesamte Lieferkette, die bei isolierter Betrachtung in einem der Unternehmen nicht oder nur erschwert als solche erkannt worden wären. Ihre Analyseergebnisse stellt die MonIKA GmbH den Unternehmen in Form manuell verfasster Warnungen zur Verfügung, sodass es diesen möglich ist, sich überhaupt oder bereits in einem frühzeitigen Stadium vor Angriffen und Anomalien zu schützen.

Im zu begutachtenden Sachverhalt wird dieses System anhand einer Bedrohung der häufig eingesetzten SAP-Software durch einen externen Angreifer dargestellt und untersucht:

Ein externer Dritter plant die Automobilproduktion der McQueer AG durch Störungen der Lieferkette zu sabotieren. Sein Ziel ist es, die Verwaltung der Lieferkette gezielt lahm zu legen und damit die Produktion bei der McQueer AG zu stoppen. Obwohl der Dritte keine konkreten Kenntnisse über die in den einzelnen Unternehmen verwendete Software für die Ressourcenverwaltung hat, nimmt er an, dass in mindestens einem Unternehmen Softwareprodukte des Unternehmens SAP

genutzt werden, genauer: ein SAP-Netweaver System. Diese Software dient als Grundlage für viele Unternehmensanwendungen und beruht auf der Programmiersprache JAVA. Auf dieser SAP-Netweaver Grundlage betreiben die Lieferanten und die McQueer AG ihre Software für das Lieferkettenmanagement. Der Angreifer plant, den populären Verwundbarkeitstyp „Verb Tampering“[103] auszunutzen, bei dem eine systembedingte Schwachstelle des HTTP-Protokolls ausgenutzt wird.

Um derartige Schwachstellen in der Software der Unternehmen der McQueer-Lieferkette auszunutzen, muss der Angreifer zunächst herausfinden, welche Anwendungen genau von den jeweiligen Unternehmen eingesetzt werden, welche Version davon betrieben werden und auf welchen Ports diese mit der Außen(netz)welt kommunizieren. Dazu setzt er verschiedene Methoden und Werkzeuge ein. Zunächst nutzt der Angreifer allgemein zugängliche Internetsuchmaschinen, um sich anhand von öffentlichen Informationen einen Eindruck über das Unternehmensgeflecht rund um den Automobilhersteller McQueer zu verschaffen. So erfährt er etwa die Internetadressen der Lieferanten und damit auch den diesen Adressen entsprechenden IP-Adressbereich. Nachdem der Angreifer auf diesem Weg einen groben Überblick über die Unternehmensstruktur und die für diese Unternehmen vergebenen IP-Adressen erlangt hat, versucht er, herauszufinden, hinter welchen IP-Adressen und welchen Ports sich angreifbare SAP-Anwendungen befinden. Dazu setzt er Portscanner ein. Diese Software versucht, sich mit allen offenen Ports eines IP-Adressbereichs über das TCP Transportprotokoll zu verbinden und registriert die Antworten. Aus dem Inhalt der Antworten kann der Portscanner weitere Erkenntnisse ableiten, wie zum Beispiel die über den Port kommunizierende Software, die Version der Software oder die (Programmier-)Sprache. Mit diesem Wissen ausgestattet, plant der Angreifer sein weiteres Vorgehen.

Die Tätigkeiten des Angreifers werden von dem anvisierten Unternehmen registriert, sofern entsprechende Instrumente eingesetzt werden. Die Firewall registriert, welche Ports angesprochen wurden. Der Webserver, dessen Anwendung adressiert wurde, registriert die IP-Adresse und in gewissem Umfang auch den Inhalt der Anfrage. Zusätzlich genutzte Angriffserkennungssysteme wie ein Intrusion Detection System (IDS) registrieren weitere Daten. All diese Instrumente stellen Sensoren dar, mit deren Hilfe die Kommunikation mit dem Internet

[103] *Polyakov*, A crushing blow at the heart of SAP J2EE / ERPScan, Forschungsbericht 2011.

beobachtet wird. Die dabei anfallenden Daten werden jederzeit in den SOCs der McQueer AG und der Lieferanten gesammelt und nach bestimmten Kriterien bezüglich ihrer Gefährdung für die IT-Sicherheit analysiert. Diese Analyse erfolgt dabei grundsätzlich nur isoliert mit Blick auf die Bedrohungen für das jeweils durch das SOC überwachte Einzelunternehmen. Das SOC kann daraufhin mögliche Bedrohungen für das eigene Unternehmen feststellen. Durch die Einbindung der MonIKA-Agenten werden die Daten aus der Sensorik der MonIKA GmbH und dem von ihr betriebenen CSOC zur Verfügung gestellt. Im CSOC werden die Einzelerkenntnisse nun zusammengeführt (Fusion) und ihre Relevanz unter Berücksichtigung des größeren Pools an Daten bewertet (Klassifikation). Damit können Daten, die bei isolierter Betrachtung als unauffällig eingestuft worden wären, als planmäßiges Vorgehen gegen die Lieferkette der McQueer AG identifiziert werden. Als Beispiel dient hier der Portscan durch einen Angreifer: Ein betroffenes Unternehmen aus der Lieferkette würde diesem bei isolierter Betrachtung regelmäßig nur geringe Aufmerksamkeit schenken. Die fusionierte Auswertung ermöglicht aber die Erkenntnis, dass alle gescannten Ports zu der von den Unternehmen aus der Lieferantenkette genutzten Software für das Liefer- und Warenmanagement gehören. Es offenbart sich damit, dass es sich nicht um Zufälle, sondern um ein strategisches Abklopfen der Schwachstellen innerhalb der Lieferkette handelt.

4.2.2 Ergänzung

Für eine haftungs- und IT-rechtliche Betrachtung müssen auch die Vorgänge der Entwicklung und des Vertriebs einer MonIKA-Software zumindest berücksichtigt werden. Dabei wird davon ausgegangen, dass das Softwareunternehmen von den Entwicklern des Softwareframeworks alle notwendigen Rechte eingeräumt bekommen hat. Wesentliche Teile des Softwareframeworks sind der EvASC und die MonIKA-Agenten.

Das Softwareunternehmen will MonIKA jedoch nicht selber betreiben, sondern entwickelt MonIKA so, dass insbesondere IT-Sicherheitsdienstleister das Softwareframework nutzen können. Ein IT-Sicherheitsdienstleister – hier als MonIKA GmbH bezeichnet – sieht MonIKA als effektives Mittel zur Erhöhung der IT-Sicherheit seiner Kunden an und schließt daher mit dem Softwareunternehmen einen Vertrag über die Nutzung des MonIKA-Softwareframeworks. Um die Betrachtungen nicht ausufern zu lassen, wird vorliegend die Fehlerfreiheit des Softwareframeworks unterstellt und auf mögliche Gewährleistungsrechte nur

hingewiesen. Die MonIKA GmbH programmiert Plug-Ins, die sich in das Softwareframework integrieren.

4.3 Stakeholder

Im Folgenden sollen die einzelnen Beteiligten und ihre Rolle aufgezeigt werden.

4.3.1 MonIKA-Softwareunternehmen

Zunächst ist das MonIKA-Softwareunternehmen zu nennen. Dieses Softwareunternehmen beschäftigt Entwickler, die das MonIKA-Softwareframework entwickeln. Mit Hilfe dieses Softwareframeworks lässt sich MonIKA in verschiedenen Konstellationen betreiben. Das Softwareunternehmen verfügt über alle erforderlichen Rechte und ist damit in der Lage, das MonIKA-Softwareframework Dritten anzubieten, damit diese MonIKA betreiben.

An dem unmittelbaren Betrieb von MonIKA ist das Softwareunternehmen jedoch nicht beteiligt.

4.3.2 Unternehmen als MonIKA-Sender

Innerhalb von MonIKA treten zunächst die McQueer AG und deren Lieferanten als eigenständige juristische Personen auf. Jedes Unternehmen beschäftigt Angestellte und verfügt über eine eigene IT-Abteilung, in die auch das unternehmenseigene SOC eingegliedert ist. Die Angestellten verfügen über Zugang zum internen Firmennetz, zum Internet und haben einen Telefonanschluss sowie eine eigene E-Mail-Adresse. In der Betriebsvereinbarung ist festgelegt, dass Internet, Telefon und E-Mail nur dienstlich benutzt werden dürfen.

Die McQueer AG sowie die Unternehmen aus der Lieferkette treten dabei als Datenlieferanten für MonIKA auf. Sie sind also Sender im Sinne des Datenstroms. In dem SOC wird seitens der MonIKA GmbH entsprechend konfigurierte Software eingesetzt, die als Agent für MonIKA fungiert. Diese MonIKA-Agenten sind an die datenliefernde Sensorik angeschlossen und haben dadurch Zugriff auf die von den Sensoren (Webserver, Firewall, IDS) gewonnenen Rohdaten und auf die Daten des firmeninternen SOC. Der Agent wertet die Rohdaten selbstständig nach vorgegebenen Parametern auf auffällige Ereignisse hin aus und sendet so gewonnene Informationen und Daten an das CSOC der MonIKA

GmbH. Die Daten werden dabei kryptografisch aufbereitet und soweit wie möglich durch Pseudonymisierung und Anonymisierung verfremdet, um den Personenbezug zu verringern.

All diese Schritte werden von dem Datenschutzbeauftragten der einzelnen Unternehmen begleitet und organisatorisch von den zuständigen Personen des Managements beaufsichtigt.

4.3.3 IT-Sicherheitsdienstleister als MonIKA GmbH

Auf diesem Weg erhält das von der MonIKA GmbH betriebene EvASC die aufbereiteten Daten. Die MonIKA GmbH fungiert damit als CSOC. Durch die dortige Informationstechnik und die Mitarbeiter werden die Daten aller Teilnehmer (McQueer AG und Lieferanten) fusioniert, korreliert und klassifiziert. Diese Auswertung im CSOC findet rund um die Uhr an allen Tagen im Jahr statt. Die MonIKA GmbH ist bei alledem aber nicht auf die Tätigkeit für die hier betrachtete McQueer AG und ihre Lieferanten beschränkt, sondern bietet ihre Dienste grundsätzlich einer unbeschränkten Zahl von Interessierten an.

4.3.4 Unternehmen als MonIKA-Konsumenten

In doppelter Rolle treten die einzelnen am MonIKA-System beteiligten Unternehmen auf. Sie sind nicht lediglich Sender, sondern auch Empfänger von Daten in Form der Ergebnisse. Nach der Fusion, Klassifikation und Auswertung der Daten durch das CSOC bei der MonIKA GmbH erhalten die einzelnen Unternehmen diese Daten bei möglichen Bedrohungen mit einem zugehörigen Warnungshinweis zurück.

Konkret erhalten die firmeneigenen SOCs und das dortige Fachpersonal Kenntnis von Daten und dem Auswertungsergebnis durch das CSOC. Durch diese Warnhinweise erhalten die Beteiligten Erkenntnisse über Anomalien und konkrete Gefährdungen. Die Beteiligten sind dann in der Lage, das Bedrohungspotenzial nicht nur mit Blick auf das eigene Unternehmen, sondern auch mit Blick auf die gesamte Lieferkette einzuschätzen. Gleichzeitig können Angriffe gegen andere Teilnehmer im MonIKA-System auf ihre Bedeutung für das eigene Unternehmen hin analysiert werden. Die sich daran anschließende Reaktion, wie etwa die Installation bestimmter Softwareupdates im anvisierten SAP-System, die Verbesserung der HTTP-Blacklists oder die Sperrung der anvisierten Ports ist zwar nicht unmittelbarer Teil von MonIKA selber, aber für die haftungsrechtliche Beurteilung unerlässlich.

Zwar nicht Teil des PoC, aber denkbar und möglich ist es auch, dass Unternehmen – ohne MonIKA-Sender zu sein – als MonIKA-Konsumenten auftreten. Das könnten in dem Anwendungsfall „Enterprise-Monitoring“ etwa kleinere eigenständige Betriebe sein, die mangels der Unterhaltung von entsprechender Sensorik als MonIKA-Sender nicht in Betracht kommen, aber dennoch ein Interesse an Warnungen vor Angriffen auf die Lieferkette haben.

4.3.5 Externe

Als MonIKA-Externe lassen sich alle Beteiligten qualifizieren, die keinem der partizipierenden Unternehmen gesellschaftsrechtlich zuzurechnen sind und die in keinem vertraglichen Verhältnis mit der MonIKA GmbH (betreffend der Durchführung von MonIKA) stehen. Dabei handelt es sich zum einen um Kunden, Geschäftspartner und sonstige neutrale Dritte, die mit den MonIKA-Teilnehmern über das Internet kommunizieren, etwa durch den Aufruf der Webseite der MonIKA-Teilnehmer oder durch den Versand von E-Mails an sie.

Ein weiterer Externer ist der Angreifer. Er hat regelmäßig keine gesellschaftsrechtliche oder vertragliche Beziehung zu der McQueer AG, den Lieferanten oder der MonIKA GmbH.

Zumindest nicht direkt an der Durchführung von MonIKA beteiligt ist das Softwareunternehmen, das das MonIKA-Prozessframework entwickelt hat. Bei dem Softwareunternehmen handelt es sich jedoch auch nicht um einen Externen, da das Softwareframework die Basis für den Betrieb von MonIKA darstellt.

4.4 Entwicklung und Vertrieb der Software

Zunächst werden grundlegende Aspekte bei der Entwicklung und dem Vertrieb des MonIKA-Softwareframeworks beleuchtet. Dies betrifft zwar nicht das Verfahren als solches, erscheint aber dennoch für eine umfassende Betrachtung unerlässlich.

4.4.1 Schutz von Software

Bei der Frage nach dem rechtlichen Schutz des MonIKA-Prozessframeworks zur Informationsfusion und –klassifikation ist zu untersuchen, welchen Schutz das Gesetz für Software vorsieht. Dabei kommen insbesondere Bestimmungen des Urheberrechts, des Patentrechts, des Wettbewerbsrechts und des Markenrechts in

Betracht. Im Folgenden sollen die einschlägigen Vorschriften der verschiedenen Schutzregime genauer betrachtet werden.

4.4.1.1 Urheberrecht

Gem. § 2 Abs. 1 Nr. 1 UrhG[104] gehören Computerprogramme zu den geschützten Werken des Urheberrechts. Schutz besteht nach § 69a Abs. 1 UrhG für Programme in jeder Gestalt. Mit der Einfügung der auf der EU-Richtlinie zum Rechtschutz von Computerprogrammen[105] basierenden §§ 69a-g UrhG im Jahr 1993 hat der deutsche Gesetzgeber die Anforderungen an die urheberrechtliche Schutzfähigkeit merklich abgesenkt, sodass eine viel größere Zahl von Computerprogrammen urheberrechtlich geschützt wird.

Computerprogramme, also Programme in jeder Gestalt einschließlich des Entwurfmaterials (§ 69a Abs. 1 UrhG), sind demnach schutzwürdig, sobald sie das Ergebnis einer eigenen geistigen Schöpfung sind (§ 69a Abs. 3 UrhG). Hierbei sollen insbesondere qualitative oder ästhetische Kriterien keine Rolle spielen. Hatte der *BGH* in seiner diesbezüglichen Leitentscheidung von 1985[106] noch entschieden, nur solche Programme schützen zu wollen, die das handwerkliche Können eines Durchschnittsprogrammierers deutlich überragen, stellt § 69a UrhG nunmehr keine solch hohen Anforderungen an ein schutzwürdiges Computerprogramm. An die konkrete Form, d. h. die Gestalt der Software, werden ebenfalls keine gesonderten Anforderungen gestellt, sodass an einen Schutz z. B. von Source-Codes, Executables oder dem Programm in ausgedruckter Form zu denken ist.[107] Geschützt wird allerdings immer nur die konkrete Form, nie die hinter der Form stehende Idee (§ 69a Abs. 2 UrhG).

Sowohl Quell- als auch Objektcode des MonIKA-Softwareframeworks sind auf dieser Grundlage als urheberrechtlich schutzfähig zu beurteilen.

4.4.1.2 Patentrechtlicher Schutz

Allgemein betrachtet stellt das Patentrecht höhere Anforderungen an die Schutzfähigkeit von Software als das Urheberrecht. Ein wichtiger Unterschied zum urheberrechtlichen Schutz ist, dass nicht das konkrete Programm, sondern ein bestimmter Algorithmus oder eine bestimmte programmierte

[104] Gesetz über Urheberrecht und verwandte Schutzrechte (UrhG) in der Bekanntmachung vom 9. September 1965, BGBl. S. 1273.
[105] Richtlinie 91/250/EWG des Rates vom 14. Mai 1991 über den Rechtsschutz von Computerprogrammen.
[106] *BGH*, NJW 1986, 192.
[107] *Dreier*, in: Dreier/Schulze, UrhG, § 69a Rn. 12 f.

Datenverarbeitungsanlage vom Patentschutz erfasst ist. Auch erfolgt der Schutz nicht automatisch, sondern durch Anmeldung gem. § 34 PatG[108].

Ein patentrechtlicher Schutz für Computerprogramme wurde dabei mit Verweis auf § 1 Abs. 3 Nr. 3 PatG lange Zeit gänzlich abgelehnt. Demnach sind „Programme für Datenverarbeitungsanlagen" grundsätzlich nicht patentierbar. Dies schließt jedoch nicht aus, dass Programme als Teil einer Erfindung, die noch andere Bestandteile aufweist, patentiert werden.[109] Insgesamt wurden die Anforderungen an die Patentierfähigkeit von Software in der Rechtsprechung seit den 1990er-Jahren merklich gelockert. Früher beurteilte der *BGH* die Frage, ob patentrechtlicher Schutz angebracht ist, nach dem Maßstab, ob „eine Lehre für ein Computerprogramm durch eine Erkenntnis geprägt ist, die auf technischen Überlegungen beruht"[110]. In späteren Entscheidungen urteilte der *BGH*, dass der Ausschluss nach § 1 Abs. 3 Nr. 3 PatG dann nicht eingreife, wenn die Erfindung der Lösung eines technischen Problems mit technischen Mitteln diene und dabei nicht auf dem Fachmann bekannte Formen zurückgreife.[111] Nach heute wohl herrschender Auffassung ist ein Programm jedenfalls dann patentierbar, wenn es unmittelbar einen technischen Effekt auslöst.[112] Ein Beispiel ist das in Kraftfahrzeugen zur Anwendung kommende Antiblockiersystem.

Vor diesem Hintergrund ist eine Patentierbarkeit des Softwareframeworks eher kritisch zu sehen, da durch MonIKA lediglich Daten gesammelt werden und kein unmittelbar automatischer Effekt, z. B. ein Löschvorgang bei Erkennung einer Anomalie, ausgelöst wird. Auch wird kein bestimmtes technisches Problem mit technischen Mitteln gelöst.

4.4.1.3 Wettbewerbsrechtlicher Schutz

Wettbewerbsrechtlicher Schutz entsteht indirekt dadurch, dass die Entwicklungsleistung eines Softwareherstellers durch §§ 3 Abs. 1, 4 Nr. 9 UWG[113] vor unlauterer fremder Benutzung durch andere im Wettbewerb geschützt wird. Ein unlauteres Handeln ergibt sich grundsätzlich aus der Verschaffung eines Vorteils durch einfaches Vervielfältigen oder Kopieren des aufwendigen

[108] Patentgesetz (PatG) in der Bekanntmachung vom 25. Mai 1877, RGBl. S. 501.
[109] *Redeker*, IT-Recht, Rn. 126.
[110] *BGH*, NJW 2000, 1953.
[111] *BGH*, GRUR 2011, 610 – Webseitenanzeige; Vgl. auch *Liedke*, in: Kilian/Heussen, Computerrechts-Handbuch, Kapitel 73 Rn. 1.
[112] *Bacher*/*Melullis*, in: Benkard, PatG, § 1 Rn. 108; *Redeker*, IT-Recht, Rn. 134.
[113] Gesetz gegen den unlauteren Wettbewerb in der Fassung der Bekanntmachung vom 3. März 2010, BGBl. I S. 254.

Entwicklungsprozesses eines Mitbewerbers, ohne dabei ein eigenes wirtschaftliches Risiko zu tragen und der Mitbewerber dadurch in der Realisierung seiner Absatzchancen behindert wird.[114] Um wettbewerbsrechtlichen Schutz zu genießen, muss das Werk jedoch „wettbewerbliche Eigenart" aufweisen.[115] Diese wird bei Computer- und Softwareprogrammen, die in der Entwicklung hinsichtlich Struktur und Kreativität meistens ein hohes Maß an Individualität aufweisen, regelmäßig zu bejahen sein.[116] Dieses Kriterium trifft angesichts der Komplexität der Entwicklung auch auf das MonIKA-Softwareframework zu.

Der wettbewerbsrechtliche Schutz ist jedoch insofern enger, als dass er sich lediglich gegen die Benutzung der fremden Leistung im Wettbewerb richtet, nicht jedoch die Vervielfältigung oder das Erstellen einer Kopie für den privaten Gebrauch an sich verbietet.[117] Durch die erleichterte urheberrechtliche Schutzfähigkeit von Software durch Umsetzung der Softwarerichtlinie ist die Relevanz des wettbewerblichen Schutz gesunken. Zudem muss beachtet werden, dass durch die Anwendung des Wettbewerbsrechts nicht die durch das Urheberrecht geschaffenen Freiräume der Verwertung unterlaufen werden.

Unabhängig vom Bestehen urheberrechtlicher Ansprüche soll das Wettbewerbsrecht nunmehr jedoch anwendbar sein, wenn besondere Begleitumstände vorliegen, die außerhalb der Sonderschutztatbestände des Urheberrechts liegen, etwa wenn der Tatbestand des § 4 Nr. 9 UWG erfüllt ist.[118] So liegt es etwa in Fällen der Irreführung (§ 4 Nr. 9 lit. a UWG), der Rufausbeutung und -schädigung (§ 4 Nr. 9 lit. b UWG) oder beim Überwinden eines Kopierschutzes, was nach § 4 Nr. 9 lit. c UWG unzulässig sein kann. Darüber hinaus kommt ein Schutz der Software als Betriebsgeheimnis nach §§ 17, 18 UWG in Betracht.

Der wettbewerbsrechtliche Schutz gewinnt somit erst an Relevanz, sobald ein Dritter einen der Tatbestände mit seinem Handeln erfüllt.

---

[114] *Redeker*, IT-Recht, Rn. 180; *Loewenheim*, in: Schricker/Loewenheim, UrhG, Vor §§ 69a ff. Rn. 14. Zur dogmatischen Einordnung der Behinderung als unlauterkeitsbegründender Umstand s. *Köhler*, in: Köhler/Bornkamm, UWG, § 4 Rn. 9.63.
[115] *Redeker*, IT-Recht, Rn. 181.
[116] *Loewenheim*, in: Schricker/Loewenheim, UrhG, Vor §§ 69a ff. Rn. 14.
[117] *Loewenheim*, in: Schricker/Loewenheim, UrhG, Vor §§ 69a ff. Rn. 13.
[118] *BGH*, GRUR 2012, 58 (62 f.) – Seilzirkus; *Köhler*, in: Köhler/Bornkamm, UWG, § 4 Rn. 9.7.

4.4.1.4 Markenrechtlicher Schutz

In Betracht kommen weiterhin sowohl Marken- als auch Werktitelschutz. Geschützt wird jedoch in beiden Fällen nicht das Programm bzw. das MonIKA-Softwareunternehmen selbst, sondern nur der Titel oder die Bezeichnung, unter dem/der die Software vertrieben wird. Anderen ist es dadurch untersagt, die gleiche oder – bei Verwechlsungsgefahr – eine ähnliche Marke zu benutzen. Der Schutz entsteht durch Eintragung ins Markenregister oder durch das Erlangen von Verkehrsgeltung im geschäftlichen Verkehr (vgl. § 4 Nr. 1-2 MarkenG[119]). Zu beachten sind die absoluten Schutzhindernisse nach § 8 MarkenG, die eine Eintragung als Marke ausschließen.

Auch hinsichtlich des Werktitelschutzes nach § 5 Abs. 1 MarkenG bejaht der *BGH* nunmehr die Schutzfähigkeit von Software.[120] Dieser besteht regelmäßig jedoch nur dann, wenn konkrete Verwechslungsgefahr besteht.[121]

Über das Markenrecht kann demnach kein zusätzlicher Schutz für den Inhalt des Softwareframeworks erreicht werden, wohl aber ein Schutz in Bezug auf den Titel bzw. die Bezeichnung, unter der die Software vertrieben wird.

4.4.1.5 Fazit

Damit lässt sich festhalten, dass das Urheberrecht den primären rechtlichen Schutz für Software bereitstellt. Daneben kommt für das MonIKA-Softwareframework wettbewerbsrechtlicher und markenrechtlicher Schutz in Betracht. Die Erteilung eines Patents erscheint hingegen zweifelhaft. Neben den oben skizzierten Schutzrechten ist im Einzelfall noch an die Anwendung des Halbleiterschutzrechts sowie an die allgemeinen vertraglichen oder deliktische Ansprüche zu denken, ebenso wie an solche aus einer Geschäftsführung ohne Auftrag oder ungerechtfertigter Bereicherung.

4.4.2 Rechtsverhältnis Entwickler – Softwareunternehmen

Urheberrechtlichen Schutz genießt zunächst allein die Person des Entwicklers bzw. Programmierers, also diejenige Person, welche die persönlich geistige Schöpfung erbracht hat (vgl. § 7 UrhG). Urheber kann demnach nicht eine juristische Person (wie etwa das MonIKA-Softwareunternehmen oder die MonIKA GmbH) sein.

---

[119] Gesetz über den Schutz von Marken und sonstigen Kennzeichen (Markengesetz – MarkenG) in der Bekanntmachung vom 25. Oktober 1994, BGBl. I S. 3082.
[120] *BGH*, GRUR 2006, 594 m. w. N. – SmartKey; *Redeker*, IT-Recht, Rn. 173.
[121] *Redeker*, IT-Recht, Rn. 173; *Huppertz*/*Fritzsche*, ITRB 2011, 86 (87).

Das MonIKA-Softwareunternehmen wird jedoch entsprechend der Vorschrift des § 69b Abs. 1, 2 UrhG zur Ausübung der vermögensrechtlichen Befugnisse berechtigt sein, wenn der Urheber als Arbeitnehmer oder Dienstverpflichteter die Software in Wahrnehmung seiner Aufgaben oder nach Anweisungen des Arbeitgebers geschaffen hat. Unter die vermögensrechtlichen Befugnisse, die sich aus dem Urheberrecht ergeben, fallen sämtliche ausschließliche, zeitlich, räumlich und inhaltlich unbeschränkten Nutzungsrechte des § 69c UrhG.[122]

Über die gesetzliche Lizenz[123] des § 69b UrhG erwirbt der Arbeitgeber kraft Gesetzes ausschließliche Nutzungsrechte, die alle vermögensrechtlichen Nutzungsbefugnisse, also auch solche des Vertriebs, umfassen.

Zu beachten ist, dass die urheberpersönlichkeitsrechtlichen Befugnisse, die aber ohnehin nur höchst eingeschränkt an Computerprogrammen bestehen, nicht an das Softwareunternehmen übertragen werden würden.[124] Zu den bei Computerprogrammen relevanten Urheberpersönlichkeitsrechten zählen insbesondere das Namensnennungsrecht (§ 13 UrhG) sowie das Änderungsverbot (§ 39 UrhG). Dennoch ist anerkannt, dass der Urheber bis zu einem gewissen Grad auf sie verzichten und ihre Wahrnehmung dem Arbeitgeber überlassen kann: Es ist eine Interessenabwägung zwischen den Interessen des Urhebers und den Interessen des Arbeitgebers, dem es primär um eine ungestörte Verwertung gehen dürfte, durchzuführen.[125]

4.4.3 Rechtsverhältnis Softwareunternehmen – MonIKA GmbH

Als zentrale Instanz im MonIKA-Verfahren benötigt die MonIKA GmbH die entsprechende Software zur Informationsfusion und -klassifikation. Die Software besteht zum einen aus dem EvASC und zum anderen aus dem MonIKA-Agenten. Der EvASC wird bei der MonIKA GmbH eingesetzt. Der MonIKA-Agent wird von der MonIKA GmbH selber nicht genutzt, sondern von den teilnehmenden Unternehmen eingesetzt, um die Daten zu gewinnen und zu übermitteln. Allerdings stellt die MonIKA GmbH den Teilnehmern den MonIKA-Agenten zur Verfügung, sodass die MonIKA GmbH auch den MonIKA-Agenten und die entsprechenden Rechte vom Softwareunternehmen erwerben muss.

---

[122] *Dreier*, in: Dreier/Schulze, UrhG, § 69b Rn. 9.
[123] Die Rechtsnatur des § 69b UrhG ist streitg. Für die Einrodnung als gesetzliche Lizenz plädiert *Grützmacher*, in: Wandtke/Bullinger, UrhG, § 69b Rn. 1 m. w. N. Eine Legalzession nimmt hingegen *Schack*, Urheberrecht, Rn. 304.
[124] *Grützmacher*, in: Wandtke/Bullinger, UrhG, § 69b Rn. 26, 38.
[125] *Grützmacher*, in: Wandtke/Bullinger, UrhG, § 69b Rn. 38.

4.4.3.1 Erwerb des EvA-Service-Clusters und der Agenten

Es ist zu untersuchen, wie der Erwerb des EvA-Service-Clusters und der Agenten rechtlich bewertet werden kann.

4.4.3.1.1 Softwareüberlassung

Die vertragstypologische Einordnung des Softwareüberlassungsvertrages (Verpflichtungsgeschäft) ist seit jeher umstritten.[126] Maßgeblich ist dabei die Frage, ob es sich um die Überlassung von Standardsoftware oder die Erstellung von Individualsoftware handelt und ob eine Überlassung dauerhaft oder auf Zeit geschieht.[127]

Die Überlassung von Standardsoftware wird regelmäßig als Kaufvertrag eingeordnet, wenn die dauerhafte Überlassung gegen Zahlung eines einmaligen Entgelts geschuldet ist.[128] Erleichtert wird diese Einordnung auch dadurch, dass es auf Grund von § 453 Abs. 1 BGB nicht mehr auf die Sacheigenschaft von Software ankommt. Wird hingegen von der Einordnung als Individualsoftware ausgegangen, wäre möglicherweise Werkvertragsrecht anzuwenden.[129]

Fraglich ist daher, ob der EvASC als Standard- oder Individualsoftware anzusehen ist. Bei Standardsoftware handelt es sich um vorgefertigte Software, die auf ein breites Publikum zugeschnitten ist. Das Gegenstück dazu stellt die auf die individuellen Bedürfnisse des Anwenders zugeschnittene Individualsoftware dar.[130]

Die Software hat mit dem Ziel der Detektion und der Bewertung von Anomalien einen eng umrissenen Verwendungs- und Aufgabenzweck. Dies allein steht jedoch einer Einordnung als Standardsoftware noch nicht entgegen. Eine individuelle Anpassung an die Bedürfnisse des Anwenders und damit das Vorliegen von Individualsoftware wäre jedoch naheliegend, wenn die MonIKA GmbH an das Softwareunternehmen herantritt und dieses damit beauftragt, die passende Software für die Ermöglichung der Informationsfusion und -klassifikation zu entwickeln und diese auf Grund der individuellen Anpassung an die Bedürfnisse und die Systemstruktur der MonIKA GmbH lediglich bei selbiger genutzt werden kann. Ebenso stünde es, wenn neben der MonIKA GmbH weitere Abnehmer als

[126] *Hoeren*, IT-Vertragsrecht, S. 78; *Marly*, Praxishandbuch Softwarerecht, Rn. 641.
[127] Vgl. *Moritz*, in: Kilian/Heussen, Computerrecht, Kapitel 31 Rn. 75.
[128] *BGH*, NJW 1988, 406 (407 f.); *Hoeren*, IT-Vertragsrecht, S. 78; *Redeker*, IT-Recht, Rn. 523 ff. m. w. N.
[129] *Hoeren*, IT-Vertragsrecht, S. 80; Die Einordung ist jedoch nicht zuletzt wegen § 651 BGB höchst umstritten, vgl. dazu auch *von dem Bussche*/*Schelinski*, in: Münchener Anwaltshandbuch IT-Recht, Teil 1 Rn. 65 ff.
[130] Vgl. *Moritz*, in: Kilian/Heussen, Computerrecht, Kapitel 31 Rn. 91.

Anwender in Betracht kommen und diese jeweils an das MonIKA-Softwareunternehmen herantreten und eine Anpassung des EvASC sowie der Agenten an ihre individuellen Bedürfnisse einfordern. Nach der Rechtsprechung des *BGH* zur Lieferung von herzustellenden beweglichen Bauteilen soll es dabei darauf ankommen, ob trotz planerischer Elemente die Leistungserbringung im Vordergrund steht (dann Kaufvertragsrecht nach § 651 BGB) oder ob das planerische Element im Einzelfall überwiegt (dann Werkvertragsrecht).[131]

Vorliegend wird davon ausgegangen, dass der EvASC für den Betrieb des CSOC sowie die Agenten keiner derartig großen Anpassungen an individuelle Bedürfnisse bedürfen, auf Grund welcher die Software neben der MonIKA GmbH nicht auch durch andere Anwender genutzt werden könnte. Es ist davon auszugehen, dass das Softwareunternehmen auf der Grundlage der Einbindung in das MonIKA-Projekt nach eigener Konzeption ein Softwareprodukt (Softwareframework) entwirft, mit welchem es am Markt auftreten will und welches auch anderen Anwendern gegenüber angeboten werden soll.

Es wird daher vom Vorliegen von Standardsoftware ausgegangen.

Sind neben der Überlassung noch umfangreiche Einrichtungs- oder Installationsmaßnahmen als Hauptpflicht geschuldet, wird auch bei Standardsoftware eine Einordnung als Werkvertrag angenommen.[132] Entscheidend ist die konkret zu treffende Vereinbarung über die Hauptpflichten zwischen der MonIKA GmbH und dem Softwareunternehmen. Eine Einordnung in das Kaufrecht scheidet darüber hinaus auch dann aus, wenn die Software nicht auf Dauer überlassen wird. In diesem Fall soll es sich entweder um Mietverträge[133] oder um Pachtverträge[134] handeln. Die Relevanz dieser Unterscheidung ist dadurch geschmälert, dass die Regeln dieser Vertragsarten in vielen Fragen identisch sind oder analog anwendbar sein sollen.[135] Zudem wird eine Angleichung durch § 581 Abs. 2 BGB erzielt, nach dem auf die Pacht die Regelungen für die Miete entsprechend Anwendung finden, soweit sich aus den §§ 582 – 584 BGB nichts anders ergibt.

---

[131] *BGH*, NJW 2009, 2877 (2880).
[132] *Redeker*, IT-Recht, Rn. 527.
[133] *Köhler*/*Fritzsche*, in: Lehmann, Rechtsschutz und Verwertung von Computerprogrammen, Kap. XIII Rn. 27 f.
[134] *BGH*, NJW 2006, 915 (916), der von einem der Rechtspacht zuzuordnenden Lizenzvertrag ausgeht; *Heydn*, CR 2010, 765 (773).
[135] *Redeker*, IT-Recht, Rn. 596.

Vorliegend wird davon ausgegangen, dass es sich sowohl bei dem EvASC als auch bei dem MonIKA-Agenten um Standardsoftware handelt. Soll diese Software auch dauerhaft der MonIKA GmbH überlassen werden, so findet Kaufrecht Anwendung.

Hauptleistungspflicht des Verkäufers bei einem solchen Softwareüberlassungsvertrag ist es, dem Erwerber Eigentum an der Software zu verschaffen. Dies kann zum einen durch Übergabe und Übereignung eines Datenträgers erfolgen, auf dem die Software gespeichert ist.[136] Möglich ist aber auch, dass die Software dem Erwerber zum Download bereitsgestellt wird und dieser die Software auf einem Datenträger abspeichert.[137]

Zudem muss das verkaufende Softwareunternehmen der MonIKA GmbH auch die für die Verwendung der Software erforderlichen Nutzungsrechte einräumen. Gem. § 31 Abs. 1 Satz 1 UrhG kann das Softwareunternehmen als Rechtsinhaber[138] der MonIKA GmbH als Vertragspartner das Recht einräumen, das Werk auf einzelne oder alle Nutzungsarten zu nutzen. Das Nutzungsrecht kann gem. § 31 Abs. 1 Satz 2 UrhG als einfaches oder ausschließliches Recht sowie räumlich, zeitlich oder inhaltlich beschränkt eingeräumt werden. Allerdings ist bei Computerprogrammen auf die nicht abdingbaren Bestimmungen der § 69d und § 69e UrhG zu achten.

Mit dinglicher Wirkung – also gegenüber jedermann geltend – können Nutzungsbeschränkungen ferner nur für solche Vertriebsformen eingeräumt werden, die eigenständige Nutzungsarten darstellen.[139] Unter einer eigenständigen Nutzungsart wird jede nach der Verkehrsauffassung wirtschaftlich-technisch selbstständige und abgrenzbare Art und Weise der Verwendung des Werkes angesehen.[140] Kann keine Beschränkung mit dinglicher Wirkung erzielt werden, so hat die Beschränkung lediglich schuldrechtliche Wirkung und wirkt somit nur zwischen den Vertragsparteien.

Soweit keine ausdrückliche Aufzählung der Nutzungsrechte erfolgt, ist wiederum auf § 31 Abs. 5 UrhG abzustellen. Gemäß dieser Vorschrift richtet sich der Umfang der Rechteeinräumung nach dem zugrunde gelegten Vertragszweck. In

[136] *von dem Bussche*/*Schelinski*, in: Münchener Anwaltshandbuch IT-Recht, Teil 1 Rn. 157.
[137] *von dem Bussche*/*Schelinski*, in: Münchener Anwaltshandbuch IT-Recht, Teil 1 Rn. 157.
[138] S. dazu oben 4.4.2.
[139] *Wiebe*, in: Münchener Anwaltshandbuch IT-Recht, Teil 3 Rn. 62.
[140] *BGH*, WRP 2005, 1542 (1544); *Schulze* in: Dreier/Schulze, UrhG, § 31 Rn. 9; *Wandtke*/*Grunert*, in: Wandtke/Bullinger, UrhG, § 31 Rn. 2.

diesem Falle wäre – entsprechend einer zu formulierenden Präambel – auf die Nutzung im Rahmen des MonIKA-Verfahrens abzustellen.

In der vorliegenden Konstellation dürfte es sich um die Einräumung eines einfachen, nicht ausschließlichen Nutzungsrechts auf Dauer handeln.[141] Dies bedeutet, dass die MonIKA GmbH den EvASC und den MonIKA-Agenten auf die vertraglich erlaubte Art nutzen kann, ohne dass sie eine Nutzung durch Dritte ausschließen kann (vgl. § 31 Abs. 2 UrhG).

Die Hauptleistungspflicht der MonIKA GmbH als Käuferin besteht in der Zahlung des vereinbarten Kaufpreises.

4.4.3.1.2 Haftungsrechtliche Risiken

Sollten der EvASC oder die Agenten mangelhaft sein, so bestehen für die MonIKA GmbH verschiedene Gewährleistungsrechte, die sich – sofern Kaufrecht Anwendung findet – aus § 437 BGB ergeben. Diese Ansprüche setzen einen Sach- oder einen Rechtsmangel voraus.

Eine Sache weist Sachmängel auf, wenn die „Ist-Beschaffenheit“ negativ von der „Soll-Beschaffenheit“ abweicht. Dies ist gegeben, wenn der Wert oder die Tauglichkeit der Sache zum vertraglich vereinbarten (§ 434 Abs. 1 Satz 1 BGB), vertraglich vorausgesetzten (§ 434 Abs. 1 Satz 2 Nr. 1 BGB) oder gewöhnlichen (§ 434 Abs. 1 Satz 2 Nr. 2 BGB) Gebrauch aufgehoben oder gemindert ist.[142]

Weichen EvASC und Agenten von den vertraglich vereinbarten Anforderungen ab, so liegt ein Mangel vor. Daher sollten in einem Vertrag zwischen der MonIKA GmbH und dem Softwareunternehmen die Leistungsanforderungen festgelegt werden. Ohne eine vertragliche Vereinbarung ist auf die vertraglich vorausgetzte Verwendung abzustellen. Hierunter fallen z. B. konkludent vereinbarte Kriterien oder Leistungsbeschreibungen.[143] Der Nachweis einer gewöhnlichen Verwendung i. S. v. § 434 Abs. 1 Satz 2 Nr. 2 BGB ist schwierig. Hierbei ist darauf abzustellen, welche Beschaffenheit der Käufer erwarten kann, was nach dem Erwartungshorizont des Durchschnittskäufers zu bestimmen ist.[144]

Neben einem Sachmangel kann auch ein Rechtsmangel Gewährleistungsrechte begründen. Gem. § 435 BGB ist eine Sache frei von

[141] *von dem Bussche*/*Schelinski*, in: Münchener Anwaltshandbuch IT-Recht, Teil 1 Rn. 158.
[142] *Hoeren*, IT-Vertragsrecht, S. 101.
[143] *Hoeren*, IT-Vertragsrecht, S. 102.
[144] *Hoeren*, IT-Vertragsrecht, S. 102.

Rechtsmängeln, wenn Dritte in Bezug auf die Sache keine oder nur die im Kaufvertrag übernommenen Rechte gegen den Käufer geltend machen können. Urheberrechte, Patentrechte oder sonstige Immaterialgüterrechte können Rechte Dritter i. S. v. § 435 BGB darstellen. Von Bedeutung ist daher, ob das Softwareunternehmen zum Vertrieb des EvASC und des MonIKA-Agenten berechtigt ist.[145]

Liegt ein Mangel vor, so hat der Käufer zunächst einen Nacherfüllungsanspruch aus §§ 437 Nr. 1, 439 BGB. Kommt der Verkäufer dem Nacherfüllungsverlangen des Käufers nicht nach, so kann der Käufer nach Ablauf einer angemessenen Frist Rücktritt, Minderung und/oder Schadensersatz verlangen.

4.5 Einsatz der Software und Betrieb des MonIKA-Verfahrens

Nachfolgend werden die Beziehungen zwischen den Akteuren rechtlich bewertet.

4.5.1 Bewertung der rechtlichen Beziehungen zwischen den Akteuren

Um das MonIKA-Verfahren erfolgreich durchführen zu können, müssen die beteiligten Akteure verschiedene Leistungen erbringen. Von diesen Leistungen sind die einzelnen Teilnehmer abhängig. Daher sollten die jeweils zu erbringenden Leistungen vertraglich geregelt und festgelegt werden. Hierbei unterscheiden sich die Leistungen der MonIKA GmbH von den Leistungen der teilnehmenden Unternehmen. Jedenfalls handelt es sich bei den Verträgen im Rahmen der Durchführung des MonIKA-Verfahrens um schuldrechtliche Verträge i. S. d. § 311 Abs. 1 BGB. Darüber hinaus sind die unterschiedlichen Leistungspflichten der Beteiligten möglicherweise rechtlich unterschiedlich zu charakterisieren. Von Bedeutung ist hierbei, ob die von den Teilnehmern zu erbringenden Leistungen einem Vertragstyp des BGB zuzuordnen sind. Auf Grund der Vertragsfreiheit können die Parteien beliebige Leistungspflichten begründen und ausgestalten.[146] Auch sieht das BGB keine Bindung an bestimmte Vertragstypen vor. Diese Einteilung ist aber für die Auslegung bestehender Verträge und für das Eingreifen möglicher Gewährleistungsrechte von Bedeutung. Außerdem ist die vertragstypologische Einordnung auch für eine mögliche AGB-Kontrolle

[145] S. dazu oben 4.4.2.
[146] *Emmerich*, in: MüKo BGB, § 311 Rn. 24.

erforderlich. Um zu prüfen, ob AGB von Rechtsvorschriften abweichen, muss festgestellt werden, welche Rechtsvorschriften anwendbar sind, da sich die AGB-Kontrolle an den gesetzlich vorgegebenen Leitbildern orientiert.[147] Ist eine vertragstypologische Zuordnung nicht möglich, so handelt es sich um sog. atypische Verträge, auf die das allgemeine Schuldrecht anzuwenden ist.[148]

Die Vertragspartner haben die Möglichkeit, über jede einzelne Leistung einen separaten Vertrag abzuschließen, sodass mehrere Verträge vorliegen können. Diese Verträge sind dann rechtlich selbstständig. Solche getrennten Verträge können z. B. in einer einheitlichen Vertragsurkunde zusammengefasst werden. Jeder Vertrag kann dann für sich rechtlich bewertet und einem Vertragstyp zugeordnet werden.[149]

Daneben können von den Vertragspartnern mehrere Verträge bzw. Leistungspflichten auch in einem Gesamtvertrag zusammengefasst werden, sodass sie eine rechtliche Einheit i. S. v. § 139 BGB bilden (zusammengesetzter Vertrag).[150] Zusammengesetze Verträge liegen vor, wenn die vereinbarten Leistungspflichten einerseits getrennt werden können, diese aber andereseits durch den Parteiwillen in der Gestalt zu einer Einheit verbunden sind, dass die einzelnen Leistungspflichten miteinander „stehen und fallen“ sollen.[151]

Außerdem kann auch ein sog. typengemischter Vertrag oder gemischter Vertrag vorliegen. Hiervon ist auszugehen, wenn ein Vertrag sich aus einzelnen Leistungen zusammensetzt, die verschiedenen Vertragstypen zugeordnet werden können, die aber derart eng miteinander verbunden sind, dass sie nur in ihrer Gesamtheit ein sinnvolles Ganzes ergeben.[152] Die rechtliche Behandlung typengemischter Verträgen ist gesetzlich nicht geregelt und wird auch in der Literatur unterschiedlich behandelt. [153] Grundsätzlich ist für jede Leistung die für sie geltende Vorschrift heranzuziehen.[154] Sollte es zu einer Kollision von Vorschriften kommen, so ist das Recht anwendbar, das den Schwerpunkt des Vertrags bildet oder den Vertragszweck wiedergibt.[155]

---

[147] *Gennen/Völkel*, Recht der IT-Verträge, Rn. 457; *Feldmann/Löwisch*, in: Staudinger, BGB, § 311 Rn. 51.
[148] *von dem Bussche/Schelinski* in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 1 Rn. 35.
[149] *von dem Bussche/Schelinski* in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 1 Rn. 32.
[150] *Grüneberg*, in: Palandt, BGB, Überbl. v. § 311 Rn. 16.
[151] *BGH*, NJW 1980, 829 (830); *Gennen/Völkel*, Recht der IT-Verträge, Rn. 451.
[152] *Grüneberg*, in: Palandt, BGB, Überbl. v. § 311 Rn. 19.
[153] Siehe hierzu *Emmerich*, in: MüKo BGB, § 311 Rn. 28 ff.
[154] *Gennen/Völkel*, Recht der IT-Verträge, Rn. 457; *Emmerich*, in: MüKo BGB, § 311 Rn. 28 ff.
[155] *Gennen/Völkel*, Recht der IT-Verträge, Rn. 457; *Grüneberg*, in: Palandt, BGB, Überbl. v. § 311 Rn. 25.

4.5.1.1 Rechtliche Beziehung zwischen MonIKA GmbH und Teilnehmern

Im Folgenden werden die einzelnen Leistungen der beteiligten Akteure bestimmt und rechtlich eingeordnet, um dann die Rechtsnatur des Vertrages zu bewerten.

4.5.1.1.1 Bestimmung der zu erbringenden Leistungen

Es ist zu ermitteln, in welchen Handlungen rechtrelevante Leistungen zu erblicken sind.

4.5.1.1.1.1 Rechtsrelevante Leistungen der MonIKA GmbH

Die MonIKA GmbH versorgt zunächst die teilnehmenden Unternehmen mit der entsprechenden Software (MonIKA-Agenten). Im Mittelpunkt des MonIKA-Verfahrens steht allerdings die Datenverarbeitung bei der MonIKA GmbH. Dort laufen die Daten und Informationen der McQueer AG und deren Lieferanten zusammen. Diese Daten werden mit Hilfe des EvASC fusioniert, korreliert und ausgewertet. Auf Grundlage der Auswertungsergebnisse gibt die MonIKA GmbH von ihren Mitarbeitern manuell verfasste Warnungen oder Hinweise auf bestehende Gefahren an die Teilnehmer heraus.

4.5.1.1.1.2 Rechtsrelevante Leistungen der Teilnehmer

Die Zahlung eines – je nach Vereinbarung einmaligen oder periodischen (monatlich, quartalsweise, jährlich etc.) – Entgeltes der Teilnehmer an die MonIKA GmbH für die Durchführung des Analyseverfahrens stellt eine wesentliche Leistung dar. Die MonIKA GmbH ist für eine effektive Analyse auf die Daten und Informationen aus der Sensorik der teilnehmenden Unternehmen angewiesen. Das gesamte MonIKA-Verfahren ist von diesen Informationen abhängig. Bei der Bereitstellung der erforderlichen Daten handelt es sich daher um eine weitere wichtige Leistung der teilnehmenden Unternehmen. Zudem haben die Teilnehmer des MonIKA-Verfahrens für eine geeignete Systemumgebung zu sorgen, damit die Agenten auf ihren Systemen funktionieren können.

4.5.1.1.2 Vertragstypologische Einordnung der Leistungen

Fraglich ist nun, wie die verschiedenen Leistungen rechtlich zu bewerten sind und wie sie vertraglich ausgestaltet werden sollten.

4.5.1.1.2.1 Leistungen der MonIKA GmbH

In Bezug auf die Ausstattung der teilnehmenden Unternehmen mit der entsprechenden Software sind kaufrechtliche Regelungen anzuwenden. Hier kann auf die obigen Ausführungen zur Softwareüberlassung unter 4.4.3 verwiesen werden.

Die Analyse und Verarbeitung der Daten durch die MonIKA GmbH könnte als Dienstvertrag i. S. v. § 611 Abs. 1 BGB, aber auch als Werkvertrag nach § 631 Abs. 1 BGB eingeordnet werden. Gegenstand eines Werkvertrages ist die Erstellung eines vereinbarten Werkes. Der Werkvertrag unterscheidet sich vom Dienstvertrag darin, dass nicht lediglich eine Tätigkeit, sondern ein Erfolg geschuldet wird. Von der MonIKA GmbH wird die Durchführung des Analyseverfahrens geschuldet. Durch dieses Verfahren kann die MonIKA GmbH für die Teilnehmer Anomalien erkennen, aus denen sich möglicherweise Bedrohungen schließen lassen. Diese Erkenntnisse werden in einem weiteren Schritt von der MonIK-GmbH in Form von Warnungen an die teilnehmenden Unternehmen übermittelt. Diese Leistungen können beiden Vertragstypen zugeordnet werden. Zum einen könnte es sich bei der Durchführung des Analyseverfahrens um ein geschuldetes Werk i. S. v. § 631 Abs. 1 BGB handeln. Auch die ordnungsgemäße Durchführung von Untersuchungen und die Anfertigung von Berichten können einen Erfolg im werkvertraglichen Sinne darstellen.[156] Zum anderen könnte aber die Durchführung des Verfahrens auch als reine Dienstleistung zu werten sein, sodass dienstvertragliche Vorschriften zur Anwendung kämen.

Die Frage nach der Vertragsart hat Auswirkungen auf mögliche Gewährleistungsrechte. Für den Werkvertrag sieht das Gesetz in den §§ 633 ff. BGB spezielle Regelungen über die Gewährleistung vor. Hierbei steht die verschuldensunabhängige Nacherfüllung im Vordergrund.[157] Solche Gewährleistungsrechte bestehen für den Dienstvertrag nicht. Hier finden die allgemeinen Regelungen aus §§ 280 ff. BGB zum verschuldensabhängigen Schadensersatzanspruch Anwendung.

Im Vordergrund des Analyseverfahrens steht eine Tätigkeit und nicht ein Tätigkeitserfolg. Das Verfahren ist zudem auf einen längeren Zeitraum ausgerichtet und entspricht einem Dauerschuldverhältnis, was für eine Charakterisierung als Dienstvertrag spricht. Nach Ansicht des *BGH* liegt eine Einordnung als

[156] *Hoeren*, IT-Vertragsrecht, S. 200.
[157] *Peters/Jacoby*, in: Staudinger, BGB, Vorbem. zu § 631 Rn. 25.

Dienstvertrag nahe, wenn eine laufende Serviceleistung als solche geschuldet ist.[158] Auch weist die Leistung der MonIKA GmbH Ähnlichkeit zu einer Beratungstätigkeit auf, indem die MonIKA GmbH die Informationen auswertet und hierdurch eine Einschätzung im Hinblick auf mögliche Bedrohungssituationen in Gestalt von Warnungen abgibt. Zudem wäre es nicht interessengerecht, wenn die MonIKA GmbH einen auf Grund ihrer Tätigkeit herbeizuführenden Erfolg schulden würde. Dies beruht darauf, dass sie von einer korrekten, unverfälschten Übermittlung der Sensordaten mittels der/des Agenten abhängig ist.

Insgesamt ähnelt das Verfahren damit einem Dienstvertrag. Dementsprechend schuldet die MonIKA GmbH ein sorgfaltgerechtes Bemühen – d. h. eine korrekte Anwendung des Analyseverfahrens. Durch vertragliche Gestaltung und durch entsprechende Formulierungen kann versucht werden, die Zuordnung als Dienstvertrag i. S. v. § 611 Abs. 1 BGB zu verstärken. Auch wenn von einem Dienstvertrag ausgegangen wird, so sollte der Vertrag dennoch so ausgestaltet sein, dass er auch den weiteren Rechtsnormen entspricht, deren vertragstypologische Zuordnung in Betracht kommt. Dies gilt insbesondere für die Erstellung von AGB.

Da die MonIKA GmbH von den teilnehmenden Unternehmen Informationen und Daten zur Auswertung zugeleitet bekommt, hat sie darauf zu achten, dass diese Daten nicht nach außen gelangen. Hier stellt sich die Frage, ob es sich bei diesen Leistungen um Hauptleistungspflichten, Nebenleistungspflichten oder vertragliche Nebenpflichten bzw. Schutzpflichten handelt.

Hauptleistungspflichten geben einem Schuldverhältnis das charakteristische Gepräge und sind für die vertragstypologische Einordnung entscheidend.[159] Demgegenüber handelt es sich bei Nebenleistungspflichten um solche Pflichten, die nicht vertragstypusbestimmender, sondern dienender Natur sind.[160] Diese dienen der Vorbereitung, Durchführung und Sicherung der Hauptleistung.[161] Bei Neben- und Schutzpflichten handelt es sich um Pflichten, die nicht unmittelbar auf eine Leistung i. S. v. § 241 Abs. 1 BGB gerichtet sind, sondern ein sonstiges Interesse des Gläubigers befriedigen sollen.[162] Solche Pflichten werden von § 241 Abs. 2 BGB erfasst, wonach jeder Vertragspartner zur Rücksichtsnahme auf die Rechte, Rechtsgüter und Interessen des anderen Teils verpflichtet ist.

---

[158] *BGH*, NJW 2010, 1449 (1451).
[159] *Bachmann*, in: MüKo BGB, § 241 Rn. 29; *Grüneberg*, in: Palandt, BGB, § 241 Rn. 5.
[160] *Bachmann*, in: MüKo BGB, § 241 Rn. 29.
[161] *Grüneberg*, in: Palandt, BGB, § 241 Rn. 5.
[162] *Bachmann*, in: MüKo BGB, § 241 Rn. 33.

Denkbar ist, dass ein eigenständiger „Datenverwahrungsvertrag“ vorliegt, der sich nach den Vorschriften zum Verwahrungsvertrag (§§ 688 ff. BGB) richtet. Für Cloud-Computing wird teilweise die Annahme eines solchen Verrwahrungsvertrages angenommen. Möglich erscheint auch die Annahme eines Mietvertrages nach §§ 535 ff. BGB. Allerdings ist die Verwahrung der Daten durch die MonIKA GmbH nicht als eine eigenständige Hauptleistungspflicht zu werten. Im Mittelpunkt der Tätigkeit steht die Analyse der Daten. Bei den Maßnahmen zur Datensicherheit und zum Datenschutz handelt es sich vielmehr um allgemeine Rücksichtsnahmepflichten nach § 241 Abs. 2 BGB, wonach jeder Vertragspartner zur Rücksichtsnahme auf die Rechte, Rechtsgüter und Interessen des anderen Teils verpflichtet ist.

Insgesamt ist der Vertrag als ein typengemischter Vertrag einzuordnen, der bezüglich der Softwareüberlassung kaufrechtlichen Regeln unterliegt. Soweit das Analyseverfahren betroffen ist, sind die Regelungen über den Dienstvertrag anzuwenden.

4.5.1.1.2.2 Leistungen der Teilnehmer

Für die McQueer AG und deren Lieferanten stellt im Rahmen eines Dienstvertrages die Zahlung der vereinbarten Vergütung die Hauptleistungspflicht (vgl. § 611 Abs. 1 BGB) dar.

Zur Durchführung des MonIKA-Verfahrens und zur Erfüllung ihrer vertraglichen Pflichten benötigt die MonIKA GmbH die entsprechenden Daten und Informationen der teilnehmenden Unternehmen. Außerdem müssen diese für eine geeignete Systemumgebung sorgen, damit die MonIKA-Agenten wirksam eingesetzt werden können. Auch die Art dieser Pflicht ist fraglich. Zu Nebenpflichten i. S. v. § 241 Abs. 2 BGB zählen u. a. Mitwirkungs- und Aufklärungspflichten.[163] Hierunter ist auch die Pflicht der Teilnehmer, die erforderlichen Daten und Informationen an die MonIKA GmbH weiterzuleiten, zu fassen. Möglich ist es jedoch auch, dies als vertragliche Hauptpflicht zu vereinbaren. In AGB ist eine solche Ausgestaltung allerdings nur möglich, wenn der Vertragspartner nicht unangemessen benachteiligt wird.[164] Als Mitwirkungspflicht ist auch die Pflicht der Teilnehmer zur Schaffung einer geeigneten Systemumgebung einzuordnen.

[163] *Bachmann*, in: MüKo BGB, § 241 Rn. 33.
[164] *Gennen/Völkel*, Recht der IT-Verträge, Rn. 560.

Zur Verdeutlichung dieser Nebenpflichten und aus Rechtssicherheitsgründen erscheint es ratsam, diese Pflichten auch in einem schriftlichen Vertrag zu regeln. Dieser fixiert dann eine Verpflichtung der Teilnehmer zur Bereitstellung der für das Verfahren erforderlichen Informationen bzw. Daten. Diese Daten sollten durch die Teilnehmer derlei Natur übermittelt werden, dass die MonIKA GmbH sie für das Analyseverfahren nutzen kann. Auch sollten die erfoderlichen Systemanforderungen, für die jeder Teilnehmer selber verantwortlich ist, im Vertrag festgelegt werden.

4.5.1.2 Rechtliche Beziehung zwischen MonIKA GmbH und externen Unternehmen

Das MonIKA-Verfahren ermöglicht es grundsätzlich auch, dass Unternehmen lediglich als Konsumenten an dem Verfahren teilnehmen. Solche Konsumenten stellen selber keine Daten oder Informationen zur Auswertung durch die MonIKA GmbH zur Verfügung. Sie erhalten lediglich die Analyseergebnisse der ausgewerteten Daten von der MonIKA GmbH. In dieser Konstealltion sind die einzelnen Leistungen nicht anders zu bewerten als vorstehend beschrieben. Die Leistung des Konsumenten besteht dann in der Zahlung einer Vergütung, wenn dies vereinbart werden sollte. Der PoC sieht allerdings reine Konsumenten nicht vor.

4.5.1.3 Sonstige Rechtsverhältnisse

Außerhalb der aufgezeigten bestehen keine weiteren Rechtsverhältnisse der Teilnehmer von MonIKA untereinander. Zu beachten ist, dass im PoC zumindest zwischen der McQueer AG und den Lieferanten Verträge bestehen, die die Lieferung von Waren zum Gegenstand haben.

4.5.2 Mögliche Haftungsszenarien

Es kann nicht ausgeschlossen werden, dass es im Rahmen des MonIKA-Verfahrens zu Fehlern kommt. Dann stellt sich die Frage, wer für mögliche Schäden haftet bzw. ob überhaupt jemand für solche Fehler einzustehen hat. In der nachfolgenden Betrachtung werden mögliche Haftungsszenarien beleuchtet, die für den PoC, aber auch darüber hinaus relevant sein könnten.

4.5.2.1 Datenleck bei der MonIKA GmbH

Ein naheliegendes Haftungsszenario stellt ein Datenleck dar. Dabei gelangen die Daten, die an die MonIKA GmbH übermittelt wurden, an die Öffentlichkeit. Da es sich u. U. um sehr sensible Daten handeln kann, sind weitreichende negative Folgen

denkbar. Insbesondere in den Anwendungsfällen, die über den PoC hinausgehen, können personenbezogene Daten oder auch sensible Geschäftsdaten betroffen sein.

So werden innerhalb des Szenarios, von dem der PoC ausgeht, kaum Daten genutzt, die haftungsrechtlich relevant sind. Als personenbezogenes Datum kann jedoch die IP-Adresse des Angreifers bewertet werden.[165] Je nach Programmierung der Plug-Ins für die MonIKA-Agenten können auch andere personenbezogene Daten übermittelt werden und an die Öffentlichkeit gelangen. Darüber hinaus erscheint es auch möglich, dass Daten betroffen sind, die zwar keinen Personenbezug aufweisen, aber vertrauliche Geschäftsdaten darstellen. Diese könnten an das CSOC übermittelt werden, wenn der MonIKA-Agent ein Datenpaket fälschlicherweise als Malware-Sample einordnen würde, da es mit einem Exploit verbunden ist.

Es sind viele Ursachen für ein derartiges Datenleck denkbar. Die Ursache kann bspw. darin liegen, dass das CSOC die Daten nicht ordnungsgemäß verarbeitet oder der MonIKA-Agent und sein Plug-In fehlprogrammiert wurden. Aber auch der Teilnehmer kann für den Fehler und das Datenleck verantwortlich sein. Vorliegend soll davon ausgegangen werden, dass die Verantwortung bei dem CSOC liegt.

4.5.2.1.1 Vertragliche Ansprüche

Im Fall des Datenlecks ist zunächst an vertragliche Schadensersatzansprüche zu denken, die das betroffene Unternehmen gegenüber der MonIKA GmbH geltend machen könnte. Eine vertragliche Haftung der MonIKA GmbH hängt von der gegebenen Vertragsart ab. Bewertet man die Datenanalyse und die Ausgabe von Warnungen als Dienstvertrag, so kommen Ansprüche nach den allgemeinen Regeln der §§ 280 ff. BGB in Betracht. Das Dienstvertragsrecht sieht keine eigenen Mängelhaftungsrechte vor. Wie bereits oben erwähnt, gehört es zu den Pflichten der MonIKA GmbH aus § 241 Abs. 2 BGB auf die Rechte, Rechtsgüter und Interessen des Vertragspartners Rücksicht zu nehmen. Eine Verletzung solcher Neben- oder Schutzpflichten kann Schadensersatzansprüche nach § 280 Abs. 1, § 241 Abs. 2 BGB begründen. Die MonIKA GmbH muss sich die Handlungen ihrer Mitarbeiter über § 278 BGB zurechnen lassen, soweit es sich bei dem Mitarbeiter um einen Erfüllungsgehilfen handelt. Erfüllungsgehilfe ist derjenige, der nach den tatsächlichen Gegebenheiten bei der Erfüllung einer Verbindlichkeit des Schuldners mit dessen Willen als dessen Hilfsperson tätig wird.[166] Die MonIKA GmbH bzw.

[165] Ein Überblick über die Einordnung von IP-Adressen als personenbezogene Daten bei *Gola/Schomerus*, in: Gola/Schomerus, BDSG, § 3 Rn. 10a.
[166] *BGH*, NJW 1954, 1193; NJW 1996, 451.

das CSOC beschäftigt seine Mitarbeiter zur Erfüllung der Pflichten aus den mit den Teilnehmern abgeschlossenen Verträgen. Kommt es in Folge der Tätigkeit der Mitarbeiter zur Datenveröffentlichung, so muss sich die MonIKA GmbH das Verhalten ihrer Mitarbeiter über § 278 BGB zurechnen lassen.

Ein Schadensersatzanspruch nach § 280 Abs. 1 BGB setzt neben einem Schuldverhältnis und einer Pflichtverletzung voraus, dass die MonIKA GmbH die Pflichtverletzung zu vertreten hat. Zu beachten ist, dass das Verschulden gem. § 280 Abs. 1 Satz 2 BGB vermutet wird. Dies bedeutet, dass die MonIKA GmbH selbst darlegen muss, dass sie bzw. ihr Mitarbeiter nicht schuldhaft gehandelt hat. Gem. § 276 Abs. 1 Satz 1 BGB hat der Schuldner BGB Vorsatz und Fahrlässigkeit zu vertreten. Fahrlässig handelt nach § 276 Abs. 2 BGB, wer die im Verkehr erforderliche Sorgfalt außer Acht lässt. Dies setzt die Voraussehbarkeit und die Vermeidbarkeit des pflichtwidrigen Erfolges voraus.[167] Vorsatz wird definiert als Wissen und Wollen der objektiven Tatbestandsmerkmale.[168] Vorsatz besteht dementsprechend aus einem Wissenselement und einem Wollenselement. Regelmäßig wird es sich bei dem Handeln eines Mitarbeiters der MonIKA GmbH, das zu einem Datenleck führt, jedoch um Fahrlässigkeit handeln. In Anbetracht der haftungsrechtlichen Begrenzungsmöglichkeiten kann eine weitere Unterscheidung zwischen grober Fahrlässigkeit, also besonders unvernünftigem Handeln, und Vorsatz geboten sein.

Als letzte Voraussetzung für einen Schadensersatzanspruch muss ein ersatzfähiger Schaden vorliegen. Dieser Schaden muss ferner durch die Pflichtverletzung verursacht worden sein.[169] Art und Umfang des zu ersetzenden Schadens richtet sich nach den §§ 249 ff. BGB. Erfasst sind insbesondere auch reine Vermögensschäden.[170] Nach § 249 Abs. 1 BGB ist der Zustand herzustellen, der bestehen würde, wenn der zum Ersatz verpflichtende Zustand nicht eingetreten wäre. Nach überwiegender Auffassung ist dabei die Differenzhypothese zugrunde zu legen.[171] Danach ergibt sich der Schaden aus der Differenz zwischen dem hypothetischen Vermögensstand ohne das schädigende Ereignis und dem tatsächlich gegeben Zustand.[172] Während für Vermögensschäden neben der Naturalrestitution eine Entschädigung in Geld möglich ist, insbesondere wenn die Naturalrestitution

[167] *Grüneberg*, in: Palandt, BGB, § 276 Rn. 12.
[168] *Grundmann*, in: MüKo BGB, § 276 Rn. 154; *Grüneberg*, in: Palandt, BGB, § 276 Rn. 10.
[169] *Ernst*, in: MüKo BGB, § 280 Rn. 29.
[170] *Ernst*, in: MüKo BGB, § 280 Rn. 29.
[171] *Oetker*, in: MüKo BGB, § 249 Rn. 18f.
[172] *Oetker*, in: MüKo BGB, § 249 Rn. 18.

gem. § 251 Abs. 1 Alt. 1 BGB unmöglich ist, kann für Nichtvermögensschäden gem. § 253 Abs. 1 BGB nur dann eine Entschädigung in Geld verlangt werden, sofern das Gesetz dies anordnet.[173] Auch der Verlust einer Rechtsposition kann bereits einen Vermögensschaden darstellen. Zu verneinen ist ein Schaden nur dann, wenn kein Anspruch auf die Rechtsposition besteht.[174]

Denkbar ist, dass durch die Datenpanne geheime Geschäftsdaten oder geheimes betriebliches Know-How allgemein bekannt werden. Durch eine Veröffentlichung besteht die Gefahr, dass das Know-How bzw. geheime Geschäftsdaten ihre Eigenschaft als Betriebs- oder Geschäftsgeheimnis und damit den Schutz aus § 17 UWG verlieren.[175] § 17 UWG stellt den Verrat von Geschäfts- oder Betriebsgeheimnisse unter Strafe und gewährt somit dem betroffenen Unternehmen eine rechtliche Schutzposition hinsichtlich geheimer Geschäftsdaten. Deren Verlust kann ein ersatzfähiger Schaden darstellen. Ein Geschäfts- oder Betriebsgeheimnis nach § 17 UWG ist allgemein definiert als jede im Zusammenhang mit einem Geschäftsbetrieb stehende, nicht offenkundige, sondern nur einem begrenzten Personenkreis bekannte Tatsache, an deren Geheimhaltung der Unternehmensinhaber ein berechtigtes wirtschaftliches Interesse hat und die nach seinem bekundeten oder doch erkennbaren Willen auch geheim bleiben soll.[176] Darunter können prinzipiell auch Daten fallen.[177] Ihre Eigenschaft als Betriebs- oder Geschäftsgeheimnis behält eine Tatsache aber nur, solange sie nicht offenkundig ist. Offenkundig ist eine Tatsache erst dann, wenn sie allgemein bekannt oder leicht zugänglich ist.[178] Sollten Dritte ohne Zutun des Geheimnisinhabers von dem Geheimnis Kenntnis erlangen, so liegt nicht automatisch Offenkundigkeit i. S. v. § 17 UWG vor, solange ein überschaubarer Personenkreis gegeben ist.[179] Ob eine solche Konstellation vorliegt, ist nach den Umständen des Einzelfalls zu beurteilen. Für das vorliegende Haftungszenario ist Offenkundigkeit aber dann anzunehmen, wenn unbeteiligte Dritte Kenntnis von den Daten und Informationen erlangen sollten. Zu bejahen ist dann auch der Verlust des Schutzes aus § 17 UWG. Der

[173] *Oetker*, in: MüKo BGB, § 249 Rn. 24.
[174] *BGH*, NJW-RR 2006, 1682 (1683); *Oetker*, in: MüKo BGB, § 249 Rn. 28.
[175] *Duisberg/Picot*, CR 2009, 823 (828).
[176] *BGH* GRUR 1955, 424; GRUR 1961, 40 (43) – Wurftaubenpresse; GRUR 2006, 1044 (1046) – Kundendatenprogramm.
[177] *Köhler*, in Köhler/Bornkamm, UWG § 17 Rn. 4.
[178] *Harte-Bavendamm*, in: Harte-Bavendamm/Henning-Bodewig, UWG, § 17 Rn. 3.
[179] *BayObLG, GRUR 1991, 694, (696); Köhler*, in Köhler/Bornkamm, UWG, § 17 Rn. 7a.

Geschädigte hat in einem solchen Falle die Möglichkeit, eine fiktive Lizenz im Rahmen der Lizenzanalogie als Schadensersatz zu verlangen.[180]

Möglich ist auch, dass ein Mitbewerber das nunmehr bekannte Know-How für eigene Zwecke verwendet. Hierdurch können dem betroffenen Unternehmen Wettbewerbsnachteile entstehen und Gewinne entgehen. Auch dies könnte ein ersatzfähiger Schaden darstellen. Gem. § 252 BGB umfasst der zu ersetzende Schaden auch den entgangenen Gewinn. Unter entgangenem Gewinn sind legitime Vermögensvorteile aller Art zu verstehen, die dem Geschädigten im Zeitpunkt des schädigenden Ereignisses noch nicht zugeflossen sind, bei Nichteintreten des Ereignisses jedoch zugekommen wären.[181] Erleidet der MonIKA-Teilnehmer auf Grund der Veröffentlichung der Daten, die betriebliches Know-How darstellen, Gewinneinbußen, weil Wettbewerber dieses Wissen nutzen, so ist dies grundsätzlich als entgangener Gewinn einzustufen. Der Geschädigte muss aber darlegen, dass es nach dem gewöhnlichen Lauf der Dinge zu diesem Gewinn gekommen wäre.

Auch können Vertragsstrafen für den Fall, dass Daten und Informationen veröffentlicht werden sollten, vereinbart werden. Vereinbarungen von Vertragsstrafen haben für den Geschädigten den Vorteil, dass der Eintritt eines konkreten Schadens nicht nachgewiesen werden muss.

Werden Daten oder Informationen in Folge eines Datenlecks veröffentlicht, so kann ein vertraglicher Schadensersatzanspruch wegen Pflichtverletzung bestehen. Entscheidend sind hierbei die Daten und Informationen, die veröffentlicht werden. Hiervon hängt das Vorliegen eines ersatzfähigen Schadens ab.

4.5.2.1.2 Deliktsrechtliche Ansprüche

Neben einer vertraglichen Haftung ist auch an eine Haftung der MonIKA GmbH nach Deliktsrecht zu denken. Eine deliktische Haftung spielt insbesondere dann eine Rolle, wenn der Geschädigte in keiner vertraglichen Beziehung mit der MonIKA GmbH steht. Zu denken ist in diesem Zusammenhang z. B. an die Veröffentlichung sensibler Daten von Kunden der teilnehmenden Unternehmen. Fraglich ist, ob die MonIKA GmbH gegenüber diesen Kunden haftet.

Als mögliche Anspruchsgrundlage aus dem Deliktsrecht kommt § 823 Abs. 1 BGB in Betracht.

---

[180] Vgl. *BGH*, GRUR 1977, 539 (541) – Prozessrechner; *Harte-Bavendamm*, in: Harte-Bavendamm/Henning-Bodewig, UWG, § 17 Rn. 63.
[181] *Oetker*, in: MüKo BGB, § 252 Rn. 4.

Hiernach ist derjenige, der vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt, dem anderen zum Ersatz des daraus entstehenden Schadens verpflichtet. Zu beachten ist, dass § 823 Abs. 1 BGB keinen allgemeinen Schutz des Vermögens gewährt.[182]

Von den genannten Rechtsgütern könnten das Eigentum und das Recht am eingerichteten und ausgeübten Gewerbebetrieb als ein „sonstiges Recht" betroffen sein. Auch erscheint es nicht ausgeschlossen, dass im Einzelfall eine Verletzung des Allgemeinen Persönlichkeitsrechts als „sonstiges Recht" i. S. v. § 823 Abs. 1 BGB gegeben ist.

Um im Falle eines Datenlecks einen Schadensersatzanspruch nach § 823 Abs. 1 BGB auf die Verletzung des Eigentums stützen zu können, müssen Daten überhaupt unter den Eigentumsbegriff fallen. Gegenstand des Eigentums nach dem BGB können nur einzelne bewegliche und unbewegliche Sachen i. S. v. § 90 BGB sein.[183] Der *BGH* hat die Sacheigenschaft eines Computerprogramms bejaht, soweit es auf einem Datenträger verkörpert ist.[184] Daher wird man auch Daten als Sache i. S. v. § 90 BGB qualifizieren müssen, wenn sie auf einem Datenträger verkörpert sein sollten.[185] Aus diesem Grund wird auch das Löschen von Daten auf einer Festplatte von der Rechtsprechung und der Mehrheit in der Literatur als Eigentumsverletzung am Datenträger angesehen, da eine Beeinträchtigung der Funktionsfähigkeit als Eigentumsverletzung ausreicht.[186] Bejaht man die Sacheigenschaft betroffener Daten, so ist ferner fraglich, wer überhaupt Eigentümer dieser Daten ist. Denkbar ist, die MonIKA GmbH als Eigentümerin der Daten anzusehen, da die Daten von den Teilnehmern an sie übermittelt worden sind und sie diese auf ihren eigenen Servern abspeichert. Unabhängig von der Frage nach dem Eigentümer der Daten und der Qualifizierung von Daten als Sache i. S. v. § 90 BGB, scheidet eine Eigentumsverletzung aber aus, weil die Daten bei einem Datenleck nicht verloren gehen oder zerstört werden. Die Daten sind bei der MonIKA GmbH oder bei den Teilnehmern weiterhin vorhanden und können von diesen weiterhin verwendet werden.

---

[182] *Sprau*, in: Palandt, BGB, Einf. v. § 823 Rn. 1.
[183] *Bassenge*, in: Palandt, BGB, § 903 Rn. 2.
[184] *BGH*, NJW 1993, 2436 (2437 f.).
[185] *Koch*, NJW 2004, 801 (802).
[186] *OLG Karslruhe*, NJW 1996, 200 (201); *Koch*, NJW 2004, 801 (802); *Leible/Sosnitza*, K&R 2002, 51 (52); *Libertus*, MMR 2005, 507 (508).

Sollten Geschäfts- oder Betriebsgeheimnisse veröffentlicht werden, so stellt sich die Frage, ob dies auch zu Schadensersatzansprüchen über § 823 Abs. 1 BGB führt. Die überwiegende Auffassung geht davon aus, dass Betriebsgeheimnisse in den Anwendungsbereich des § 823 Abs. 1 BGB fallen.[187] Als Hauptargument dient der anderenfalls sehr lückenhafte Schutz des Betriebsgeheimnisses.[188] Unterschiedlich wird allerdings bewertet, ob das Betriebsgeheimnis lediglich als Teil des Rechts am eingerichteten und ausgeübten Gewerbebetrieb oder als eigenständiges sonstiges Recht i. S. d. § 823 Abs. 1 BGB zu qualifizieren ist.[189] Die Rechtsprechung ist dabei nicht einheitlich.[190]

Der Unterschied zwischen der Anerkennung als sonstigem Recht und als Teil des Rechts am eingerichteten und ausgeübten Gewerbebetrieb liegt in den besonderen und engen Voraussetzungen, unter denen ein Eingriff in das Recht am Gewerbebetrieb angenommen wird.

Es stellt sich also die Frage, ob das Betriebsgeheimnis vorliegend als Teil des Rechts am eingerichteten und ausgeübten Gewerbebetrieb geschützt ist. Der Schutzbereich umfasst das Unternehmen als Ganzes,[191] somit fällt auch das Betriebsgeheimnis prinzipiell darunter. Dies wird auch allgemein angenommen.[192] Einschränkend gilt jedoch als weitere Voraussetzung, dass der Eingriff betriebsbezogen sein muss, d. h. der konkrete Eingriff muss sich gegen den Betrieb als solchen richten.[193] Werden betriebsinterne Daten aufgrund eines Datenlecks fahrlässig veröffentlicht, so liegt darin keine gezielte Beeinträchtigung des Unternehmens. Vielmehr realisiert sich in solch einem Fall ein allgemeines Risiko im Bereich der IT-Systeme. Hinzu kommt, dass der Unternehmensbetrieb des MonIKA-Teilnehmers durch eine Datenveröffentlichung unmittelbar nicht beeinträchtigt wird. Diese ergeben sich erst im weiteren Verlauf der Ereignisse. Genau diese mittelbaren Schäden soll das Merkmal der Betriebsbezogenheit jedoch ausgrenzen.[194] Im vorliegenden Fall liegt also kein Eingriff in das Recht am ausgeübten und eingerichteten Gewerbebetrieb vor.

---

[187] *Harte-Bavendamm*, in: Harte-Bavendamm/Henning-Bodewig, UWG, § 17 Rn. 43; *Köhler*, in: Köhler/Bornkamm, UWG, § 17 Rn. 53; *Ohly*, in: Piper/Ohly/Sosnitza, UWG, § 17 Rn. 49; *Ann*, GRUR 2007, 39 (42); *Kiethe*/*Groeschke*, WRP 2005, 1358 (1362); *Mes*, GRUR 1979, 584 (590).
[188] *Mes*, GRUR 1979, 584 (590).
[189] *Köhler*, in: Köhler/Bornkamm, UWG, § 17 Rn. 53; *Ohly*, in: Piper/Ohly/Sosnitza, UWG, § 17 Rn. 49.
[190] *Wagner*, in: MüKo BGB, § 823 Rn. 228.
[191] *Spindler*, in: Bamberger/Roth, Beck'scher Onlinekommentar BGB, § 823 Rn. 105.
[192] *Ann*, GRUR 2007, 39 (42); *Staudinger*, in: Schulze et.al. BGB, § 823 Rn. 120.
[193] *Wagner*, in: MüKo BGB, § 823 Rn. 257.
[194] *Wagner*, in: MüKo BGB, § 823 Rn. 257.

Fraglich ist, ob das Betriebsgeheimnis über das Recht am eingerichteten und ausgeübten Gewerbebetrieb hinaus als sonstiges Recht i. S. d. § 823 Abs. 1 BGB zu qualifizieren ist. Dies ist umstritten.[195] Dagegen spricht die geringere Zuweisungs- und Ausschlussfunktion des Schutzes des Betriebsgeheimnisses im Vergleich zu anderen Immaterialgüterrechten.[196] Der Inhaber eines Betriebsgeheimnisses kann nicht mit vergleichbaren rechtlichen Möglichkeiten und rechtlicher Effektivität gegen eine Verletzung vorgehen wie etwa der Inhaber eines Marken-, Urheber- oder Patentrechts. Dem lässt sich jedoch entgegenhalten, dass der Gesetzgeber durch die strafrechtliche Sanktionierung des Geheimnisverrats diesem Rechtsgut durchaus eine herausragende Rolle zugesteht.[197] Zu beachten ist jedoch, dass eine Verortung des Betriebsgeheimnisses als sonstiges Recht nicht die Einschränkungen unterläuft, denen es als Teil des Rechts am eingerichteten und ausgeübten Gewerbebetrieb gerade unterliegt. Diese Gefahr erkennen die Befürworter an und fordern daher auch für einen Eingriff in das Betriebsgeheimnis als sonstiges Recht eine Interessenabwägung.[198] Dies verdeutlicht, dass eine Qualifikation des Betriebsgeheimnisses als sonstiges Recht dogmatische Schwierigkeiten bereitet. Daher erscheint es konsequenter, das Betriebsgeheimnis als Teil des Rechts am eingerichteten und ausgeübten Gewerbebetrieb zu betrachten und sich auf die dazu gefestigte Rechtsprechung zu stützen.

Weiterhin ist das Allgemeine Persönlichkeitsrecht zu beachten, das in verfassungskonformer Anwendung und Auslegung der Generalklauseln als „sonstiges Recht“ den Schutz der absoluten Rechte genießt.[199] Der Schutzbereich dieses Rahmenrechts umfasst das Recht des Einzelnen auf Achtung seiner persönlichen und sozialen Identität sowie Entfaltung und Entwicklung seiner individuellen Persönlichkeit gegenüber dem Staat und im privaten Rechtsverkehr.[200] Der Schutz steht natürlichen und in bestimmtem Umfang auch juristischen Personen und politischen Parteien zu (sog. Unternehmenspersönlichkeitsrecht).[201] Insbesondere Daten und ihre Offenlegung sind von dem Schutz erfasst. Entsteht infolge des MonIKA-Verfahrens ein Datenleck, bei dem sensible persönliche Daten von Individuen oder kritische Unternehmensinterna[202] an die Öffentlichkeit

[195] *Ann*, GRUR 2007, 39 (42); *Köhler*, in: Köhler/Bornkamm, UWG, § 17 Rn. 53.
[196] *Ann*, GRUR 2007, 39 (43).
[197] *Mes*, GRUR 1979, 584 (592).
[198] *Köhler*, in: Köhler/Bornkamm, UWG, § 17 Rn. 53.
[199] *BVerfG*, NJW 1958, 97.
[200] *BGH*, NJW 1957, 1146 (1147); NJW 1958, 1344.
[201] *Sprau*, in: Palandt, BGB, § 823 Rn. 87 ff.
[202] *BGH*, WM 2005, 1238.

gelangen, kann eine Verletzung des Allgemeinen Persönlichkeitsrechts bzw. des Unternehmenspersönlichkeitsrechts angenommen werden.

Erforderlich für eine Haftung nach § 823 Abs. 1 BGB ist, dass eines der dort genannten Rechtsgüter durch eine Handlung bzw. durch ein Unterlassen der MonIKA GmbH verletzt worden ist (haftungsbegründende Kausalität). Diese Handlung muss kausal für die Rechtsgutverletzung sein. Ausgangspunkt bildet hierbei die sog. Äquivalenztheorie, wonach jede Ursache kausal ist, über die nicht hinweggedacht werden kann, ohne dass der konkrete Erfolg entfiele.[203] Diese weite Formel wird im Zivilrecht durch die sog. Adäquanztheorie eingeschränkt, wonach ein Erfolg nicht zurechenbar ist, wenn er außerhalb aller Wahrscheinlichkeit liegt, sodass mit seinem Eintritt vernünftigerweise nicht zu rechnen war.[204] Eine weitere Einschränkung erfolgt durch den Schutzzweck der Norm.[205]

Als weitere Voraussetzung muss die Rechtsgutverletzung rechtswidrig sein. Dies wird nach der Rechtsprechung jedoch durch die Tatbestandsmäßigkeit indiziert.[206] Dies bedeutet, dass keine Rechtfertigungsgründe für die Verletzungshandlung eingreifen.[207] Zudem muss auch im Rahmen von § 823 Abs. 1 BGB ein Verschulden des Schädigers vorliegen.

Eine Einstandspflicht für unerlaubte Handlungen nach §§ 823 ff. BGB besteht allerdings nur für die Person, die die Rechtsgutverletzung begangen hat. Die MonIKA GmbH hat gem. §§ 30, 31, 89 BGB für das Handeln ihrer Geschäftsführer und ihrer Organe einzustehen. In solchen Fällen besteht die Gefahr einer Haftung der MonIKA GmbH nach § 823 Abs. 1 BGB. In Betracht kommt die Verletzung von Organisationpflichten durch ihre Organe. Es obliegt den Organen einer Gesellschaft, einen ordnungsgemäßen Arbeitsablauf zu organisieren.[208] Hierzu zählt auch die Pflicht, IT-Risiken vom Unternehmen abzuwenden.[209] Dementsprechend gehört es zur allgemeinen Unternehmensorganisation auch für den Einsatz sicherer Informationstechnik zu sorgen und organisatorische Maßnahmen mit dem Ziel der Erlangung von Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen innerhalb eines Unternehmens anzuordnen.[210]

---

[203] *Teichmann*, in: Jauernig, BGB, § 823 Rn. 22.
[204] *Grüneberg*, in: Palandt, BGB, Vorb. v. § 249 Rn 25 f.
[205] *Teichmann*, in: Jauernig, BGB, § 823 Rn. 26.
[206] *Sprau*, in: Palandt, BGB, § 823 Rn. 24.
[207] *Wagner*, in: MüKo BGB, § 823 Rn. 60.
[208] *Bäumer*, in: Reinhard/Pohl/Capellaro, IT-Sicherheit und Recht, Rn. 332.
[209] *Schmidl*, in: Hauschka, Corporate Compliance, § 29 Rn. 19. Dazu bereits oben unter 2.2.
[210] *Schmidl*, in: Hauschka, Corporate Compliance, § 29 Rn. 17; *Heckmann*, MMR 2006, 280 (281).

Erforderlich ist im Falle einer Haftung nach §§ 823 ff. BGB ein ersatzfähiger Schaden, was sich ebenfalls nach §§ 249 ff. BGB richtet. Die Rechtsgutverletzung muss zudem kausal für den eingetretenen Schaden sein (haftungsausfüllende Kausalität). Hier gelten die gleichen Anforderungen wie bei der haftungsbegründenden Kausalität.

Insbesondere bei einer Verletzung des Allgemeinen Persönlichkeitsrechts bereiten die Bewertung eines konkreten Schadens und die Bestimmung der Schadenshöhe Schwierigkeiten. Die Verletzung des Allgemeinen Persönlichkeitsrechts durch ein Datenleck dürfte in der Regel keinen Vermögensschaden bei dem Betroffenen hervorrufen. Bei einem immateriellen Schaden soll der Geschädigte aber nach § 253 Abs. 1 BGB grundsätzlich keinen Ausgleich in Geld erhalten. Dies ist nur möglich, wenn das Gesetz dies ausdrücklich vorsieht. So sieht § 253 Abs. 2 BGB einen Ausgleich für Nichtvermögensschäden im Falle einer Verletzung des Körpers, der Gesundheit, der Freiheit oder der sexuellen Selbstbestimmung vor. Verletzungen des Allgemeinen Persönlichkeitsrechts werden von § 253 Abs. 2 BGB nicht erfasst.[211] Allerdings soll nach Ansicht des *BGH* bei schwerwiegenden Verletzungen des Persönlichkeitsrechts eine Geldentschädigung möglich sein, wenn die entstandenen Nachteile anders nicht hinreichend ausgeglichen werden können. Abgeleitet wird diese Entschädigung aus dem Schutzauftrag von Art. 1 GG und Art. 2 Abs. 1 GG.[212] Einem Unternehmen als juristische Person steht kein Anspruch auf Ersatz des immateriellen Schadens zu, da nur natürliche Personen über ein Genugtuungsbedürfnis verfügen.[213] Als ersatzfähiger Schaden kommt aber auch hier ein entgangener Gewinn oder der Verlust der Rechtsposition aus § 17 UWG in Betracht (vgl. oben 4.5.2.1.1).

Eine weitere mögliche Anspruchsgrundlage stellt § 823 Abs. 2 BGB dar. Nach dieser Norm ist jeder, der gegen ein den Schutz eines anderen bezweckendes Gesetz verstößt, zum Schadensersatz verpflichtet. Zu den von § 823 Abs. 2 BGB erfassten Schutzgesetzen können u. a. Normen aus dem Datenschutzrecht sowie aus dem Strafrecht gezählt werden. Allerdings liegt im Falle eines Datenlecks, wie es oben beschrieben ist, die Verletzung einer Strafnorm nicht nahe. Zu denken ist zwar an eine Strafbarkeit aus § 206 Abs. 1 StGB (Verletzung des Post- oder Fernmeldegeheimnisses), jedoch ist die MonIKA GmbH im Szenario „Enterprise-

[211] *Oetker*, in: MüKo BGB, § 253 Rn. 27.
[212] *BGH*, NJW 1996, 984 (985); NJW 1996, 1131 (1134); *Rixecker*, in: MüKo BGB, Anhang zu § 12 Rn. 236.
[213] *BGH*, NJW 1980, 2807 (2810).

Monitoring“ nicht als ein Unternehmen i. S. v. § 206 Abs. 1 StGB einzuordnen, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt. Gegner eines Anspruchs aus § 823 Abs. 2 BGB ist zudem die handelnde Person, die das Schutzgesetz verletzt hat und nicht die MonIKA GmbH.

Eine Haftung der MonIKA GmbH kann sich ferner aus § 831 BGB ergeben. Bei dieser Norm handelt es sich um eine eigenständige Anspruchsgrundlage gegen den Geschäftsherrn für eine Handlung seines Verrichtungsgehilfen. § 831 Abs. 1 BGB verlangt, dass ein Verrichtungsgehilfe eine rechtswidrige Handlung vorgenommen hat. Beispiel für einen Verrichtungsgehilfen ist etwa ein Arbeitnehmer in der Ausführung ihm übertragener Arbeit. Bei den für die MonIKA GmbH handelnden Mitarbeiter handelt es sich um solche Verrichtungsgehilfen i. S. v. § 831 BGB. Eine Haftung nach § 831 Abs. 1 BGB tritt außerdem nur ein, wenn der Verrichtungsgehilfe „in Ausführung der Verrichtung“ gehandelt hat. Darunter ist zu verstehen, dass er nicht bloß bei Gelegenheit gehandelt hat, sondern ein innerer Zusammenhang zwischen übertragenem Aufgabenkreis und Schadenszufügung besteht.[214] Ist der handelnde Mitarbeiter für die technisch sichere Durchführung des Analyseverfahrens zuständig, so ist dieser innere Zusammenhang zu bejahen. Das Verhalten darf nicht aus dem Kreis oder allgemeinen Aufgaben der ihm anvertrauten Aufgaben herausfallen.[215]

Eine Besonderheit des Anspruchs aus § 831 Abs. 1 Satz 1 BGB liegt darin, dass das Verschulden des Geschäftsherrn bzw. seines verfassungsmäßigen Vertreters in Satz 2 vermutet wird. Es wird demnach vermutet, dass der Geschäftsherr den Verrichtungsgehilfen nicht ordnungsgemäß ausgewählt bzw. beaufsichtigt hat und die Verletzung dieser Pflicht für die Schädigung ursächlich geworden ist. Es obliegt dem Geschäftsherrn, nachzuweisen, dass er die Sorgfaltspflichten erfüllt hat (§ 831 Abs. 1 Satz 2 Alt. 1 BGB) bzw., dass die Verletzung der Pflichten für die Schädigung nicht ursächlich geworden ist (§ 831 Abs. 1 Satz 2 Alt. 2 BGB). Die Pflichten des Abs. 1 Satz 2 sind dabei übertragbar, wobei für eine interne Übertragung Besonderheiten gelten. Nach den Regeln des sog. dezentralen Entlastungsbeweises darf der Geschäftsherr die Auswahl und Überwachung zwar auf andere Personen übertragen, aber die Haftung wird nicht bereits dadurch ausgeschlossen, dass er diesen Beauftragten ordnungsgemäß überwacht. Vielmehr muss auch der Beauftragte seinerseits den Pflichten nachgekommen sein. Nur wenn

[214] *BGH*, NJW 1965, 391 (392); NJW 1971, 31 (32); NJW-RR 1989, 723.
[215] *BGH*, WM 1977, 1169.

beides gegeben ist, erscheint bei Großbetrieben eine Enthaftung möglich. Die Überwachungspflicht bedeutet eine fortgesetzte Prüfung, wobei Art und Ausmaß von individuellen Faktoren abhängig sind. Der Entlastungsbeweis im Hinblick auf die Ursächlichkeit (s. Abs. 1 Satz 2) wird dann nicht gelingen, wenn die MonIKA GmbH und ihre Organe die Mitarbeiter zu derartigen Maßnahmen veranlasst haben. Die Rechtsfolge ist der Ersatz des kausalen Schadens nach §§ 249 ff. BGB. Es kann daher auf obige Ausführungen verwiesen werden.

Ein deliktischer Schadensersatzanspruch kann im Falle des Datenlecks nicht ausgeschlossen werden. Allerdings ist auch hier das Vorliegen eines konkreten Schadens fraglich und hängt vom konkreten Einzelfall ab.

4.5.2.1.3 Weitere Anprüche gegen die MonIKA GmbH

Neben Schadensersatzansprüchen kann die MonIKA GmbH auch auf Beseitigung und Unterlassung in Anspruch genommen werden. Solche Ansprüche können sich aus § 1004 Abs. 1 BGB ergeben. Unmittelbar gelten die Ansprüche nach § 1004 BGB zwar nur für das Eigentum. Jedoch wendet die Rechtsprechung § 1004 BGB auch für weitere absolute Rechte an. Zu diesen Rechten zählen u. a. das Allgemeine Persönlichkeitsrecht[216] oder auch das Recht am eingerichteten und ausgeübten Gewerbebetrieb[217]. Insgesamt werden alle deliktisch geschützten Rechtsgüter, insbesondere auch die des § 823 Abs. 1 BGB und des § 823 Abs. 2 BGB i. V. m. einem Schutzgesetz, erfasst.[218] Der Beseitigungsanspruch aus § 1004 Abs. 1 Satz 1 BGB zielt auf die Beseitigung einer bestehenden Beeinträchtigung für die Zukunft ab. Der Unterlassungsanspruch aus § 1004 Abs. 1 Satz 2 BGB soll hingegen künftige Beeinträchtigungen verhindern. Beide Ansprüche erfordern kein Verschulden und setzen keinen Schaden voraus. Notwendig ist die Verletzung eines geschützten Rechtsgutes.

Weitere Ansprüche Dritter können sich aus § 44 Abs. 1 TKG ergeben. § 44 Abs. 1 TKG stellt einen lex-specialis-Anspruch zu § 823 Abs. 2 BGB dar, ohne diese Ansprüche jedoch zu verdrängen.[219] Nach § 44 TKG besteht bei Verstößen gegen die Vorschriften des TKG ein Anspruch des Betroffenen auf Beseitigung und bei Wiederholungsgefahr auf Unterlassung. Fällt dem Unternehmen Vorsatz oder Fahrlässigkeit zur Last, ist es außerdem einem Endverbraucher oder einem

[216] *BGH*, NJW 1996, 984; NJW 2006, 603 (604); NJW 2011, 744.
[217] *BGH*, NJW 1998, 2058 (2059 f.); NJW 2009, 2958 (2959).
[218] *BGH*, NJW 1998, 2058 (2059f.); *Berger*, in: Jauernig, BGB, § 1004 Rn. 3.
[219] *Ditscheid/Rudloff*, in: Spindler/Schuster, Recht der elektronischen Medien, § 44 TKG Rn. 4.

Wettbewerber zum Ersatz des Schadens verpflichtet, der ihm aus dem Verstoß entstanden ist. Voraussetzung der Norm ist also stets eine Verletzung des Fernmeldegeheimnisses. Den Schutz des Fernmeldegeheimnisses hat § 88 TKG zum Ziel, der auch als einfachgesetzliche Ausprägung des Fernmeldegeheimnisses nach Art. 10 GG bezeichnet werden kann.[220] Fraglich ist, ob die MonIKA GmbH als Diensteanbieterin i. S. d. TKG einzuordnen ist, also ob sie überhaupt den Ansprüchen aus § 44 TKG ausgesetzt sein kann. Der Begriff des Diensteanbieters ergibt sich aus § 3 Nr. 6 TKG. Diensteanbieter ist danach jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt (lit. a) oder an der Erbringung solcher Dienste mitwirkt (lit. b). Geschäftsmäßiges Erbringen von Telekommunikationsdiensten ist nach der Definition aus § 3 Nr. 10 TKG das nachhaltige Angebot von Telekommunikationsdiensten für Dritte mit oder ohne Gewinnerzielungsabsicht. Telekommunikationsdienste werden wiederum in § 3 Nr. 24 TKG definiert als in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen. Eine Übertragung von Signalen über Telekommunikationsnetze findet durch die MonIKA GmbH nicht statt. Die Leistungen der MonIKA GmbH im Anwendungsfall „Enterprise-Monitoring“ stellen damit keine Telekommunikationsdienste i. S. v. § 3 Nr. 6 a, Nr. 10 TKG dar. Ebenso erbringen die Teilnehmer keine solchen Telekommunikationsdienste, sodass die MonIKA GmbH auch nicht an der Erbringung solcher Dienste i. S. v. § 3 Nr. 6 b TKG mitwirkt. Daher ist die MonIKA GmbH im Rahmen des PoC keinen Ansprüchen aus § 44 TKG ausgesetzt.

Werden personenbezogene Daten als Folge des Datenlecks veröffentlicht, so sind auch Schadensersatzansprüche nach dem BDSG in Erwägung zu ziehen. § 7 BDSG und § 8 BDSG sehen solche Schadensersatzansprüche vor. Nach § 7 BDSG ist eine verantwortliche Stelle i. S. v. § 3 Abs. 7 BDSG bei einer datenschutzwidrigen Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten dem Betroffenen zum Schadensersatz verpflichtet, wenn diesem durch die Datenschutzverletzung ein Schaden entstanden sein sollte. Für einen Anspruch nach § 7 BDSG muss das MonIKA-Verfahren eine Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten im Sinne des Datenschutzrechts darstellen. Die MonIKA GmbH hat aber gem. § 7 Satz 2 BDSG die Möglichkeit sich zu exkulpieren. Hat die MonIKA GmbH die nach den Umständen des Falles gebotene

[220] *Bock*, in: Geppert/Schütz, TKG, § 88 Rn. 1.

Sorgfalt beachtet, besteht keine Haftung. Sie muss darlegen, dass sie alle erforderlichen Maßnahmen getroffen hat, um eine datenschutzkonforme Verarbeitung von personenbezogenen Daten zu ermöglichen. Auch bei einem Anspruch aus § 7 BDSG ist die Bewertung eines ersatzfähigen Schadens problematisch. Einen Ersatz immaterieller Schäden sieht § 7 BDSG nicht vor.[221] Wie bereits oben im Falle des § 823 Abs. 1 BGB angesprochen, ist bei schwerwiegenden Verletzungen des Persönlichkeitsrechts eine Geldentschädigung möglich.

4.5.2.1.4 Meldepflicht der MonIKA GmbH

Die MonIKA GmbH könnte ferner der Meldepflicht aus § 42a BDSG unterliegen, sofern es sich um Daten i. S. d. § 42a Satz 1 Nr. 1 – 4 BDSG handeln sollte. Nach § 42a Satz 1 BDSG besteht eine Meldepflicht gegenüber den Betroffenen und der zuständigen Datenschutzaufsichtsbehörde. Fraglich ist allerdings, ob „schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen“ drohen, wie es die Norm verlangt. Davon sind sowohl Beeinträchtigungen materieller als auch immaterieller Art umfasst, wobei es sich nicht bloß um Rechte, sondern auch um schutzwürdige Interessen handeln kann.[222] Der Normadressat des § 42a BDSG, also die MonIKA GmbH, muss eine Prognoseentscheidung treffen, die von der Eintrittswahrscheinlichkeit maßgeblich beeinträchtigt wird.[223]

4.5.2.2 Bloße Falschwarnung durch die MonIKA GmbH

Weiterhin ist es möglich, dass die MonIKA GmbH eine Falschwarnung an die Teilnehmer aussendet. Auf Basis dieser Falschwarnung können die Teilnehmer bestimmte Vorkehrungen treffen. Fraglich ist, ob bereits die bloße Falschwarnung zu einer Haftung der MonIKA GmbH führen kann.

Die Teilnehmer stehen mit der MonIKA GmbH in vertraglichen Beziehungen. Darin verpflichtet sich die MonIKA GmbH die zusammengeführten Daten auszuwerten und, falls erforderlich, Warnungen an die Unternehmen auszusprechen. Gibt die MonIKA GmbH eine fehlerhafte Warnung aus, verletzt sie ihre Pflicht aus diesem Dienstvertrag und es wird nach § 280 Abs. 1 Satz 2 BGB vermutet, dass sie die Pflichtverletzung zu vertreten hat. Jedoch entsteht den teilnehmenden Unternehmen durch die fehlerhafte Warnung als solche kein Schaden, sodass

[221] *Gola/Schomerus*, in: Gola/Schomerus, BDSG, § 7 Rn. 19.
[222] *Gola/Schomerus*, in: Gola/Schomerus, BDSG, § 42a Rn. 4.
[223] *Gabel*, in: Taeger/Gabel, BDSG, § 42a Rn. 20.

Schadensersatzansprüche im Falle von bloßen Falschwarnungen unwahrscheinlich sind. Allerdings könnten die Parteien auch an dieser Stelle Vertragsstrafen vereinbaren.

Deliktische Ansprüche dürften in dieser Konstellation nicht eingreifen. Haben die Warnungen keine Auswirkungen, so scheinen keine durch § 823 Abs. 1 BGB geschützten Rechtsgüter betroffen zu sein. Auch Ansprüche aus anderen Haftungsnormen sind nicht ersichtlich.

4.5.2.3 Falschwarnung durch MonIKA GmbH mit Auswirkungen

Es erscheint möglich, dass die Falschwarnung dazu führt, dass das SOC des Teilnehmers – ohne objektive Notwendigkeit – Vorkehrungen trifft, die zu einem Produktionsstillstand, einem Ausfall von Maschinen, einem Ausfall der gesamten IT oder ähnlich negativen Folgen für das Unternehmen führen. Dies liegt besonders im Anwendungsfall „Enterprise-Monitoring“ nahe, wenn die teilnehmenden Unternehmen dem produzierenden Gewerbe zuzuordnen sind.

4.5.2.3.1 Vertragliche Ansprüche

Wie unter 4.5.2.2 angesprochen, stellt die Erteilung einer Falschwarnung eine Pflichtverletzung der MonIKA GmbH dar. Folge ist, dass im Falle eines Schadens ein Schadensersatzanspruch nach § 280 Abs. 1 BGB besteht. Ob ein Schaden vorliegt, hängt von der Reaktion der Teilnehmer und deren Auswirkungen im Einzelfall ab. Ein entgangener Gewinn oder ein Verdienstausfall können hierbei einen ersatzfähigen Schaden darstellen.

Fraglich ist jedoch, wie der Umstand zu bewerten ist, dass das Unternehmen selbst die Entscheidung über die Reaktion trifft und dadurch die Schädigung hervorruft. Hierdurch könnte der erforderliche Zurechnungszusammenhang zwischen der durch die MonIKA GmbH begangenen Pflichtverletzung und dem entstandenen Schaden durchbrochen sein.

Problematisch für die Eigenverantwortlichkeit der Unternehmen ist das Informationsgefälle zwischen der MonIKA GmbH und den Unternehmen. Die Unternehmen haben sich mit dem Ziel zusammengeschlossen, ihre Daten fusionieren zu lassen, um sich auf Grundlage der gewonnenen Informationen besser schützen zu können, als ihnen dies auf Basis ihrer eigenen Informationen möglich ist. Die Bewertung der fusionierten Daten ist die Aufgabe der MonIKA GmbH. Die beteiligten Unternehmen müssen sich auf die Ergebnisse der Datenanalyse der

MonIKA GmbH verlassen. Je geringer die Möglichkeit der Unternehmen ist, die Gründe für die Warnung nachzuvollziehen und zu überprüfen, desto geringer ist ihr Entscheidungsspielraum und umso abhängiger sind sie von der Richtigkeit der Warnungen. Bei Warnungen, die auf einem großen Informationsgefälle zwischen den Unternehmen und der MonIKA GmbH beruhen, ist der entstehende Schaden daher tendenziell der MonIKA GmbH zuzurechnen. Können hingegen die Unternehmen mit den ihnen vorliegenden Informationen selbst zu einer validen Einschätzung der Situation kommen, ist ihnen der entstehende Schaden aufgrund ihrer eigenverantwortlichen Entscheidung zuzurechnen.

Als weiterer Aspekt der Zurechnung ist zu beachten, inwieweit sich die Unternehmen durch den Inhalt der Warnung zu ihrer Reaktion veranlasst sehen durften. Die Rechtsprechung hat für die sogenannten „Herausforderungsfälle“ eine Haftung unter der Voraussetzung bejaht, dass jemand den Geschädigten durch vorwerfbares Tun zu einem selbstgefährdenden Handeln herausgefordert haben muss.[224] Weist die Warnung auf schwerwiegende Schäden hin und erfahren die Unternehmen dadurch einen hohen Motivationsdruck, schützende Maßnahmen zu ergreifen, ist diese Reaktion im Eigeninteresse und zum Schutz Dritter nachvollziehbar. Je höher der Motivationsdruck der Unternehmen nach einer vorgenommenen Abwägung ist, umso eher kann der Schaden der MonIKA GmbH zugerechnet werden.

Um das Haftungsrisiko der MonIKA GmbH zu minimieren, kann in dem Vertrag auf die diesbezügliche Unverbindlichkeit der Warnung hingewiesen werden. Es kann klargestellt werden, dass die MonIKA GmbH keine Handlungsempfehlungen bezüglich der Warnungen abgibt und dass die Teilnehmer eigenverantwortlich entscheiden müssen, ob sie und wie sie auf mögliche Warnungen reagieren. Auch ein allumfassender Schutz vor Angriffen kann nicht garantiert werden. Möglich erscheint es ferner, dass die MonIKA GmbH die Warnung mit einer Prognosestufe bzgl. der Wahrscheinlichkeit (z. B. gering – mittel – hoch) verbindet oder eine prozentuale Wahrscheinlichkeit angibt.

4.5.2.3.2 Deliktische Ansprüche

Eine Schadensersatzpflicht kann sich zudem aus § 823 Abs. 1 BGB ergeben. Von den dort ausdrücklich genannten Rechtsgütern kommt zunächst eine Verletzung des Eigentums in Betracht. Voraussetzung hierfür ist eine Substanzverletzung, etwa in

[224] *BGH*, NJW 1996, 1533; *Schulze*, in: Staudinger, BGB, § 823 Rn. 55.

Gestalt einer Zerstörung, Beschädigung oder Entziehung einer Sache.[225] Es ist aber fernliegend, dass eine falsche Warnung unmittelbar zu einer solchen Eigentumsverletzung führt. Anders zu bewerten wäre der Fall jedoch, wenn die Produktion des Unternehmens Bestandteile beinhaltet, die nicht ohne weiteres in ihrem Zustand belassen werden können, bei denen also bereits der Stillstand der Produktion zu einer Beschädigung führt. Im PoC könnte dies für die Fertigung von Metallteilen eines Automobils gelten. So hat der *BGH* die Haftung auf Grund einer Eigentumsverletzung in einem Fall bejaht, bei dem ein Bauunternehmen fahrlässig Stromkabel durchtrennte und durch den Ausfall der Stromzufuhr Bruteier verdarben.[226] Der Stromausfall führte in dem vom *BGH* entschiedenen Fall nicht nur zu einem Produktionsstillstand. Dies wäre ein nicht ersatzfähiger Vermögensschaden gewesen.[227] Vielmehr verursachte der Stromausfall eine Beschädigung der Bruteier, weil diese eine bestimmte Temperatur benötigten. Ein Produktionsausfall als Folge der Fehlwarnung reicht daher alleine nicht aus, um eine Eigentumsverletzung annehmen zu können. Der Produktionsausfall muss zu einer Beschädigung des Eigentums führen. In dem hier untersuchten Haftungsszenario könnte zudem eine mittelbare Eigentumsverletzung vorliegen, wenn die Warnung zu einer Fehlkonfiguration der eigenen Hardware durch den MonIKA-Konsumenten führt.

Des Weiteren ist eine Eigentumsverletzung in Gestalt einer Nutzungsbeeinträchtigung möglich. Jedoch ist umstritten, inwieweit diese von einem nicht unter die Vorschrift fallenden Vermögensschaden abzugrenzen ist.[228] Nach Rechtsprechung und herrschender Meinung liegt ein nicht geschützter Vermögensschaden vor, wenn lediglich die Dispositionsfreiheit des Eigentümers beeinträchtigt wird.[229] Kann der Eigentümer also lediglich nicht mehr so mit seinem Eigentum verfahren, wie er möchte, dann ist dies nach der Vorschrift des § 823 Abs. 1 BGB ein nicht ersatzfähiger Schaden. Die Rechtsprechung erkennt jedoch an, dass eine nicht unerhebliche Beeinträchtigung der bestimmungsgemäßen Verwendung der Sache eine Eigentumsverletzung im Sinne der Vorschrift darstellt.[230] Für das vorliegende Szenario ist der Eintritt einer solchen Nutzungsbeeinträchtigung nicht wahrscheinlich. Dies ergibt sich aus dem Grund,

[225] *Spindler*, in: Bamberger/Roth, BGB, § 823 Rn. 40.
[226] *BGH*, NJW 1964, 720.
[227] *BGH*, NJW 1964, 720 (722).
[228] *Spindler*, in: Bamberger/Roth, BGB, § 823 Rn. 51; *Staudinger*, in: Schulze et. al., BGB, § 823 Rn. 24.
[229] *Spindler*, in: Bamberger/Roth, BGB, § 823 Rn. 51.
[230] *BGH*, NJW 1994, 517; *Spindler*, in: Bamberger/Roth, BGB, § 823 Rn. 50.

dass der betroffene Teilnehmer eine eigene autonome Entscheidung trifft, wie er auf eine Warnung reagiert und ob er Maßnahmen wie einen Produktionsstillstand vornimmt.

Daneben erscheint die Verletzung eines sonstigen Rechts in Form des durch die Rechtsprechung anerkannten Rechts am eingerichteten und ausgeübten Gewerbebetrieb möglich. Ein solcher Eingriff muss betriebsbezogen sein und darf nicht vom Gewerbebetrieb ohne weiteres ablösbare Rechte oder Rechtsgüter betreffen.[231] Unter der Betriebsbezogenheit wird die unmittelbare Beeinträchtigung des Gewerbebetriebs verstanden.[232] Die Verletzungshandlung muss über eine bloße Belästigung oder sozial übliche Behinderung hinausgehen.[233] Maßgeblich ist, dass gerade auf den Betrieb und seine Organisation abgezielt wurde. Dies kann jedoch bei Ausgabe von Warnungen im Rahmen des MonIKA-Verfahrens nicht bejaht werden. Die MonIKA GmbH zielt mit ihren Warnungen nicht darauf ab, den Betrieb der Teilnehmer zu beeinträchtigen. Vielmehr ist die Minimierung von möglichen Gefahren für das teilnehmende Unternehmen das Ziel. Zudem spricht auch hier gegen eine unmittelbare Beeinträchtigung und somit gegen die Annahme einer Betriebsbezogenheit, dass erst die Reaktion des Betroffenen zu den negativen Auswirkungen führt. Der Teilnehmer entscheidet eigenständig, wie er mit einer Warnung umzugehen hat und welche Maßnahmen auf Grundlage der Warnung eingeleitet werden.

Auch im Falle einer deliktischen Haftung muss der MonIKA GmbH ein etwaiger Schaden zurechenbar sein. Hierzu kann auf die obigen Ausführungen unter 4.5.2.3.1 verwiesen werden.

Festzuhalten ist, dass neben einer vertraglichen Haftung auch eine deliktische Haftung der MonIKA GmbH im Einzelfall möglich ist.

4.5.2.4 Falschwarnung mit Rückführbarkeit auf einen Teilnehmer

Nicht auszuschließen ist es, dass durch die ausgegebenen Warnungen Rückschlüsse auf andere Teilnehmer gezogen werden können. Sollte die Warnung falsch sein, könnte der betroffene Teilnehmer auf Grund seiner angeblich mangelhaften IT-Sicherheit in einem schlechten Licht stehen. Eine Rufschädigung des betroffenen Teilnehmers (zumindest innerhalb der an MonIKA teilnehmenden Unternehmen) ist

[231] *BGH*, NJW 1983, 2313 (2314).
[232] St. Rspr., vgl. *BGH*, NJW-RR 2005, 673 (675).
[233] *Spindler*, in: Bamberger/Roth, BGB, § 823 Rn. 108.

die Folge. Außerdem könnten die Teilnehmer ihre Kenntnisse über die (angeblich) mangelhafte IT-Sicherheit des betroffenen Teilnehmers weitergeben.

4.5.2.4.1 Vertragliche Ansprüche

In Betracht kommen zunächst wieder vertragliche Schadensersatzansprüche des betroffenen Unternehmens gegen die MonIKA GmbH, da beide Seiten in einer vertraglichen Beziehung zueinander stehen. Zu den Pflichten der MonIKA GmbH gehört es nicht nur, keine falschen Warnungen herauszugeben, sondern auch den Ruf der Vertragspartner nicht zu beschädigen. Daher kann das betroffene Unternehmen sich in diesem Haftungsszenario auf Schadensersatzansprüche aus § 280 Abs. 1 i. V. m. § 241 Abs. 2 BGB berufen.

4.5.2.4.2 Deliktische Ansprüche

Eine solche Falschwarnung, die Rückschlüsse auf ein bestimmtes Unternehmen zulässt, könnte unter deliktsrechtlichen Aspekten einen Eingriff in das Allgemeine Unternehmenspersönlichkeitsrecht oder in das Recht am eingerichteten und ausgeübten Gewerbebetrieb darstellen und Ansprüche aus § 823 Abs. 1 BGB begründen. Beide Rechtsinstitute sind nach Ansicht des *BGH* nebeneinander anwendbar und schließen sich nicht gegenseitig aus.[234] Geschäftsschädigende Kritik wie falsche Tatsachenbehauptungen können einen Eingriff in die genannten Rechtspositionen darstellen. Es erscheint im Einzelfall durchaus möglich, dass durch eine solch fehlerhafte Warnung unternehmensbezogene Interessen betroffen sein könnten. So kann das unternehmerische Ansehen durch eine solche Warnung beschädigt werden.

Ein Anspruch nach § 823 Abs. 1 BGB besteht, wenn die Warnung als Behauptung oder Verbreitung einer unwahren Tatsachenbehauptung einzuordnen ist. Eine Tatsachenbehauptung bezieht sich auf etwas Geschehenes oder einen gegenwärtigen Zustand und stellt eine Äußerung dar, deren Richtigkeit bewiesen werden kann.[235] Tatsachenbehauptungen sind von Meinungsäußerungen abzugrenzen. Diese sind durch Elemente der Stellungnahme, des Dafürhaltens oder Meinens geprägt.[236] Die Warnungen, die von der MonIKA GmbH abgegeben werden, beruhen auf den Ergebnissen des – möglicherweise fehlerhaft durchgeführten – MonIKA-Verfahrens. Diese Warnungen können als (unwahre)

[234] *BGH*, NJW 2008, 2110 (2111).
[235] *BVerfG*, NJW 1996, 1529; *BGH*, NJW 1992, 1314 (1316), NJW 2005, 279 (282); NJW 2010, 2110.
[236] *BVerfG*, NJW 1983, 1415 (1416).

Tatsachenbehauptungen eingestuft werden. Tathandlung stellt das Behaupten oder Verbreiten der unwahren Tatsache dar, wobei das Behaupten oder Verbreiten mindestens gegenüber einem Dritten erfolgen muss.[237] Diese Voraussetzung ist erfüllt, wenn die Warnung einem Teilnehmer übermittelt wird.

Ist die Warnung geeignet, den Kredit des Betroffenen zu gefährden oder ihm sonstige Nachteile für Erwerb und Fortkommen zuzufügen, so kann sich eine Haftung aus § 824 BGB ergeben. Eine Beeinträchtigung des Erwerbs wird hierbei angenommen, wenn die aktuelle Fähigkeit zur Einkommenserzielung geschmälert wird.[238] Soweit zukünftige Erwerbsaussichten gemindert werden, wird eine Benachteiligung des Fortkommens angenommen.[239] Jedoch werden von § 824 BGB nach Ansicht des *BGH* nur die wirtschaftlichen Beziehungen zu den Personen erfasst, „die dem Betroffenen als Kreditgeber, als Abnehmer und Lieferant, als Auftrag- und Arbeitgeber, d. h. im weiten Sinn als ‚Geschäftspartner', Existenz und Fortkommen im Wirtschaftsleben ermöglicht".[240] Eine Haftung nach § 824 BGB scheidet aus, wenn das Verhalten der Geschäftspartner nicht beeinflusst wird.[241]

Im Einzelfall können sich Schadensersatzansprüche auch aus § 823 Abs. 2 BGB und aus § 831 BGB ergeben.

Bei allen genannten Haftungsgrundlagen muss aber auf Grund der Warnung ein ersatzfähiger Schaden entstanden sein. Insbesondere bei einem Eingriff in das Unternehmenspersönlichkeitsrecht ist aber das Vorliegen eines ersatzfähigen Schadens problematisch, da juristischen Personen kein Anspruch auf Ersatz eines immateriellen Schadens zusteht.[242] Hier muss ein materieller Schaden eingetreten sein. Eine Haftung der MonIKA GmbH in diesem Szenario ist zudem durch die schwierige Beweisbarkeit unwahrscheinlich. Probleme ergeben sich bei der Frage nach der Kausalität zwischen der Falschwarnung und einem möglichen Schaden, der darin liegen könnte, dass das betroffene Unternehmen z. B. wegen seiner (angeblich) mangelhaften IT-Sicherheit keine Aufträge mehr erhält. Es ist weiterhin schon fraglich, ob überhaupt eine einzelne Falschwarnung, die auf einen bestimmten Teilnehmer rückführbar ist, Misstrauen auslösen würde.

[237] *OLG Düsseldorf*, NJW-RR 1997, 490 (491).
[238] *Wagner*, in: MüKo BGB, § 824 Rn. 36.
[239] *Wagner*, in: MüKo BGB, § 824 Rn. 36.
[240] *BGH*, NJW 1984, 1607 (1608).
[241] *Wagner*, in: MüKo BGB, § 824 Rn. 37.
[242] *Kannowski*, in: Staudinger, BGB, Vorbem. zu § 1 Rn. 30.

Liegen Eingriffe in das Unternehmenspersönlichkeitsrecht oder in das Recht am eingerichteten und ausgeübten Gewerbetrieb vor, so sind auch Beseitigungs- und Unterlassungsansprüche nach § 1004 Abs. 1 BGB analog möglich.

4.5.2.4.3 Vertragliche Vorbeugung

Allerdings sollten die MonIKA GmbH und die Teilnehmer diesen Fall zuvor in den Vertragsverhandlungen berücksichtigen und ihm durch entsprechende Regelungen vorbeugen. Sachgerecht erscheint es, dass Schadensersatzansprüche weitest möglich ausgeschlossen werden und eine Klarstellung seitens der MonIKA GmbH für ausreichend erachtet wird. I. Ü. sollten alle Teilnehmer zum Stillschweigen verpflichtet werden.

Ohnehin dürften derartige Rückschlüsse auf einen Teilnehmer praktisch nur schwerlich möglich sein, was zum einen an der Anonymisierung und Pseudonymisierung liegt. Zum anderen verfügen die Teilnehmer, deren Daten übermittelt werden, auch über ähnliche Sicherheitsvorkehrungen und Sensoren.

4.5.2.5 Mangelnde oder verfälschte Sendung von Daten durch Teilnehmer

In Betracht zu ziehen ist ferner der Fall, dass die teilnehmenden Unternehmen die Sendung von Daten an die MonIKA GmbH unterlassen. Die Motivation hierfür könnte etwa sein, dass sie lediglich an MonIKA teilnehmen wollen, um die Warnungen zu erhalten, aber selber trotz der Anonymisierungs- und Pseudonymisierungsverfahren keine Informationen über die IT-Sicherheit des eigenen Unternehmens preisgeben möchten.

4.5.2.5.1 Vertragliche Ansprüche

Die unverfälschte Sendung von Daten über den MonIKA-Agenten stellt eine Teilnahmevoraussetzung an MonIKA dar. Das gesamte Verfahren basiert darauf, dass relevante Informationen durch die MonIKA-Agenten an die MonIKA GmbH als Verarbeiter übermittelt werden, damit diese Anomalien entdecken kann. Insofern wird – wie bereits oben erarbeitet – die Übermittlung der Daten als eine Pflicht der teilnehmenden Unternehmen vereinbart. Die Übermittlung fehlerhafter Daten stellt dann eine Pflichtverletzung des Teilnehmers dar. Dies hat zur Folge, dass der MonIKA GmbH Schadensersatzansprüche gegen den Teilnehmer zustehen, die sich aus § 280 Abs. 1 BGB ergeben können. Ein solcher Anspruch ist abhängig von einem Schaden, der der MonIKA GmbH entstanden sein muss. Alleine durch die

fehlerhafte Datenübermittlung dürfte der MonIKA GmbH aber noch kein ersatzfähiger Schaden entstehen.

Innerhalb des beschriebenen Szenarios ist allerdings vorstellbar, dass sich die MonIKA GmbH Schadensersatzansprüchen der übrigen MonIKA-Teilnehmer ausgesetzt sieht. Diese Ansprüche könnten sich aus § 280 Abs. 1 BGB ergeben, weil die MonIKA GmbH möglicherweise ihre Pflicht zur fehlerfreien Analyse gegenüber den Teilnehmern auf Grund der fehlerhaften Datenübermittlung nicht erfüllen kann. Die MonIKA GmbH wird jedoch in einem solchen Falle nachweisen können, dass sie eine etwaige Pflichtverletzung nicht i. S. v. § 280 Abs. 1 BGB zu vertreten hat. Dann scheiden Schadensersatzansprüche der sonstigen Teilnehmer gegen die MonIKA GmbH aus. Gibt die MonIKA GmbH bspw. Fehlwarnungen aus und kommt es hierdurch zu Schäden bei den Teilnehmern, so ist im Rahmen des Vertretenmüssens zu prüfen, ob die MonIKA GmbH die Fehlerhaftigkeit der Daten erkennen konnte und diese Daten nicht zur Analyse verwenden durfte. Auch die Belastung mit einer Verbindlichkeit ist ein Schaden, der im Rahmen von § 249 Abs. 1 BGB ersatzfähig ist.[243]

Im Vertrag zwischen der MonIKA GmbH und den Teilnehmern sollte festgelegt werden, welche Daten für das MonIKA-Verfahren erforderlich sind und von dem jeweiligen Teilnehmer der MonIKA GmbH zur Erfüllung ihrer vertraglichen Pflichten übermittelt werden müssen. Auch kann eine Freistellungsverpflichtung vereinbart werden, wonach der Teilnehmer die MonIKA GmbH von Ansprüchen Dritter freizustellen hat, falls diese wegen Schäden auf Grund der fehlerhaften Datenübermittlung gegen die MonIKA GmbH vorgehen sollten.

Vertragliche Ansprüche der Teilnehmer untereinander sind abhängig von der vertraglichen Ausgestaltung des MonIKA-Verfahrens. Es ist möglich, dass die Teilnehmer sich untereinander vertraglich zur Bereitstellung der erforderlichen Informationen und Daten verpflichten. Für den Fall, dass ein Teilnehmer nicht die erforderlichen Daten oder Informationen bereitstellt, kann eine Vertragsstrafe fixiert werden.

[243] *Grüneberg*, in: Palandt, BGB, § 249 Rn. 4; *Oetker*, in: MüKo BGB, § 249 Rn. 29.

4.5.2.5.2 Deliktische Ansprüche

Ferner können auch deliktische Schadensersatzansprüche eines Teilnehmers bestehen. Bei einer gezielten Falschübermittlung sind Schadensersatzansprüche der Teilnehmer aus § 826 BGB möglich. Nach § 826 BGB ist derjenige zum Schadensersatz verpflichtet, der in einer gegen die guten Sitten verstoßenden Weise einem anderen vorsätzlich Schaden zufügt. Auch ein Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb und somit ein Anspruch aus § 823 Abs. 1 BGB dürfte dann zu bejahen sein. Ist die fehlerhafte Übermittlung jedoch nicht gezielt erfolgt, so wird man einen betriebsbezogenen Eingriff wohl verneinen müssen. Auch die Verletzung anderer von § 823 Abs. 1 BGB erfasster Rechtsgüter ist als unwahrscheinlich zu beurteilen, wenn auch nicht auszuschließen.

4.5.2.6 Nichtwarnung durch die MonIKA GmbH

Ein anderer Fall mit Haftungsrelevanz, der im Rahmen der Durchführung des MonIKA-Verfahrens auftreten könnte, ergibt sich daraus, dass die MonIKA GmbH trotz entsprechender Hinweise keine Warnung aussendet und ein (erkennbarer) Angriff von Externen nicht verhindert werden kann.

4.5.2.6.1 Vertragliche Ansprüche

Der Anspruch aus § 280 Abs. 1 BGB verlangt eine Pflichtverletzung. Die Nichtwarnung kann dabei sowohl als Unterlassung der Leistung als auch als qualitativ mangelhafte Leistung in Form der nicht korrekt erfolgten Analyse qualifiziert werden. Die konkrete Einordnung spielt jedoch für die Frage nach einer Pflichtverletzung keine Rolle, da beide Anknüpfungspunkte von § 280 Abs. 1 BGB erfasst sind.[244]

Eine höhere Hürde für das Bestehen eines Schadensersatzanspruchs stellt die Frage nach dem Verschulden dar. § 276 Abs. 2 BGB erfasst sowohl Vorsatz und Fahrlässigkeit. Dass die Mitarbeiter der MonIKA GmbH vorsätzlich nicht warnen, erscheint fernliegend. Jedoch wird sich – auch in Anbetracht einer möglichen Haftungsbegrenzung auf grobe Fahrlässigkeit – die Frage stellen, ob bzw. in welcher Form die Mitarbeiter fahrlässig gehandelt haben. Einen gerichtlichen Prozess unterstellt, müsste somit auf Basis der der MonIKA GmbH im unmittelbaren Zeitpunkt vor dem Angriff zur Verfügung stehenden Daten entschieden werden, ob überhaupt eine Erkennbarkeit bestand. Falls diese schon nicht bestand, muss das Merkmal des Vertretenmüssens verneint werden.

[244] S. *Schulze*, in: Schulze et. al., BGB, § 280 Rn. 9.

Ein Vertretenmüssen unterstellt, muss der betroffene Teilnehmer einen Schaden erlitten haben. Hier gelten die Ausführungen zu den anderen Haftungsszenarien.

4.5.2.6.2 Deliktische Ansprüche

Möglich erscheint zudem ein Schadensersatzanspruch nach § 823 Abs. 1 BGB, wenn es die MonIKA GmbH unterlassen sollte, eine berechtigte Warnung auszusprechen. Auch das Unterlassen einer gebotenen Handlung kann zu einer Haftung nach § 823 Abs. 1 BGB führen. Da allerdings keine allgemeine Rechtspflicht besteht, andere vor Schäden zu bewahren, ist ein Unterlassen nur dann haftungsrechtlich relevant, wenn den Schädiger eine Pflicht zur Handlung traf. [245] Solche Handlungspflichten können aus einer Garantenstellung folgen, die wiederum durch einen Vertrag begründet werden kann.[246] Alleine aus dem Bestehen einer vertraglichen Beziehung lässt sich eine Garantenstellung jedoch nicht ableiten.

Täter der unerlaubten Handlung i. S. v. § 823 Abs. 1 BGB ist der Mitarbeiter der MonIKA GmbH. Dieser müsste folglich auch die erforderliche Garantenstellung innehaben, was aber für die Mitarbeiter der MonIKA GmbH zu verneinen ist. Die MonIKA GmbH hat ihrerseits für die von ihren Organen begangenen Delikte über § 31 BGB einzustehen. Sollte eine Warnung unterbleiben, weil Organe der MonIKA GmbH ihre Aufsichts- oder Überwachungspflichten verletzt haben, so ist eine Haftung der MonIKA GmbH möglich. Dann stellt sich allerdings die Frage, ob eine allgemeine Pflicht i. S. v. § 823 Abs. 1 BGB für die MonIKA GmbH besteht, Teilnehmer vor Schäden Dritter durch Botnetze oder andere Cyber-Attacken zu bewahren. Dies ist nicht anzunehmen. Die MonIKA GmbH ist nicht dafür verantwortlich und hat nicht dafür einzustehen, dass Rechtsgüter der Teilnehmer durch sämtliche Arten von Attacken Dritter verletzt werden. Eine allgemeine Rechtspflicht, die Teilnehmer vor Gefahren zu warnen, besteht nicht.

Ansprüche aus § 823 Abs. 1 BGB oder aus anderen deliktischen Anspruchsgrundlagen sind in diesem Haftungsszenario daher zu verneinen.

4.5.2.7 Offenbarung von Daten Dritter durch fehlerhafte Sendung von Daten

Zu überprüfen ist ferner der Fall, dass die Übermittlung der Daten fehlerhaft erfolgt und die teilnehmenden Unternehmen Daten Dritter an die MonIKA GmbH senden. An dieser Stelle geht die Untersuchung ebenfalls über den konkreten PoC hinaus.

[245] *Spindler*, in: Bamberger/Roth, BGB, § 823 Rn. 6.
[246] *Hager*, in: Staudinger, BGB, § 823 Rn. H 11.

Relevant wird auch hier die bereits oben unter 4.5.2.1 angesprochene Unterscheidung zwischen solchen Daten, die im PoC verwendet werden und solchen Daten, die bei den weiteren Anwendungsfällen des MonIKA-Verfahrens betroffen sein könnten.

Das übermittelnde Unternehmen (bspw. die McQueer AG) könnte sich damit gegenüber den Dritten schadensersatzpflichtig machen, was insbesondere für den Fall gilt, dass sensible, wirtschaftlich relevante Daten Gegenstand der unerwünschten Übermittlung sind.

Der sichere Umgang mit Daten von Vertragspartnern lässt sich als von § 241 Abs. 2 BGB umfasste Obhutspflicht umfassen.[247] Das Unternehmen muss außerdem schon im eigenen Interesse Sicherheitsmaßnahmen bzgl. der Daten ergreifen, die sich bei solchen mit Personenbezug aus § 9 BDSG i. V. m. Anlage ergeben. Bei Daten ohne Personenbezug wird man § 9 BDSG i. V. m. Anlage zumindest als Maßstab heranziehen können.

Für das betroffene Unternehmen – sofern es sich rechtskonform verhält – greift u. U. zusätzlich die Meldepflicht aus § 42a BDSG.

Um den Problemen vorzubeugen, sollte zwischen der MonIKA GmbH und den teilnehmenden Unternehmen eine Verschwiegenheitspflicht in den Vertrag aufgenommen werden. Diese könnte derartige Fälle, in denen die Daten Dritter übermittelt werden, regeln und es könnte vereinbart werden, dass die MonIKA GmbH von den Teilnehmern erlangte Daten nicht veröffentlicht, nicht anderweitig verwertet/verwendet, diese Daten vernichtet und im Übrigen Stillschweigen gilt. So ließen sich Haftungsrisiken für die Teilnehmer erheblich verringern. Auch die Folgen für den Fall, dass die Voraussetzungen des § 42a Satz 1 BDSG vorliegen, könnten bereits geregelt werden.

Im Rahmen dieses Szenarios ist der Eintritt eines ersatzfähigen Schadens als unwahrscheinlich einzustufen. Möglich erscheint die Geltendmachung eines immateriellen Schadens im Falle eines Eingriffs in das Allgemeine Persönlichkeitsrecht. Falls geheime Geschäftsdaten übermittelt werden sollten, könnten diese, wie oben erwähnt, ihre Eigenschaft als Betriebs- oder Geschäftsgeheimnis und damit den Schutz aus § 17 UWG verlieren. Dieser Verlust der Rechtsposition kann im Einzelfall ebenfalls einen Schaden innerhalb dieses Szenarios darstellen.

[247] *Olzen*, in: Staudinger, BGB, § 241 Rn. 486.

Anspruchsgegner dieser gerade aufgezeigten Ansprüche ist aber der Teilnehmer, der die Daten übermittelt hat. Solange die MonIKA GmbH ihrerseits die fehlerhaft übersendeten Daten löscht und diese nicht verwendet, erscheint die Entstehung eines Schadensersatzanspruchs gegen sie nicht realistisch. Zudem ist bereits die Eintrittswahrscheinlichkeit dieses Szenarios als nicht besonders hoch zu bewerten. Dies ist darauf zurückzuführen, dass die MonIKA-Agenten lediglich an die Sensorik angeschlossen werden und zuvor ausreichend daraufhin getestet werden können, dass sie nur bestimmte Daten übermitteln. Durch die Pseudonymisierung oder Anonymisierung lassen sich die Risiken weiter verringern.

4.5.3 Vertragliche Gestaltungsmöglichkeiten

Es bestehen vertragliche Gestaltungsmöglichkeiten für die MonIKA GmbH, um ihr Haftungsrisiko zu verringern. So kann ein Haftungsausschluss mit den Teilnehmern vertraglich vereinbart werden. Im Umkehrschluss zu § 276 Abs. 3 BGB, der es untersagt, die Haftung für Vorsatz im Voraus auszuschließen, ist es prinzipiell möglich, eine Haftung für alle anderen Formen des Verschuldens bereits im Voraus auszuschließen.[248] Hierbei spielt eine entscheidene Rolle, ob AGB verwendet werden oder ob es sich um individualvertragliche Regelungen handelt. Entsprechend der Legaldefinition aus § 305 Abs. 1 BGB sind AGB alle für eine Vielzahl von Verträgen vorformulierten Vertragsbedingungen, die eine Vertragspartei der anderen Vertragspartei bei Abschluss eines Vertrags stellt. Ein Individualvertrag ist dagegen anzunehmen, wenn die Vertragsbestimmungen im Einzelnen ausgehandelt sind (vgl. § 305 Abs. 1 Satz 3 BGB). Die MonIKA GmbH wird mit den einzelnen Teilnehmern identische Verträge abschließen und die Verträge mehrfach verwenden wollen, sodass diese Verträge als AGB zu bewerten sind. Das AGB-Recht sieht engere Grenzen für einen Haftungsausschluss gegenüber individuellen Vereinbarungen vor.

Die inhaltlichen Anforderungen ergeben sich aus den §§ 307 – 309 BGB. Dabei kommt § 307 Abs. 1 und Abs. 2 BGB im Verhältnis zu den §§ 308, 309 BGB der Charakter von Generalklauseln und Auffangvorschriften zu.[249] § 307 Abs. 1 Satz 1 BGB stellt eine Grundsatznorm dar und zeigt die grundsätzliche Rechtsfolge, nämlich die Unwirksamkeit einer verstoßenden Klausel, auf. § 309 Nr. 7 lit. a BGB untersagt bereits den Haftungsausschluss für leichte bis

[248] *Grundmann*, in: MüKo BGB, § 276 Rn. 182; *Unberath*, in: Bamberger/Roth, BGB, § 276 Rn. 46.
[249] *Dammann*, in: Wolf/Lindacher/Pfeiffer, AGB-Recht, Vor §§ 308, 309 Rn. 10; *Fuchs*, in: Ulmer/Brandner/Hensen, AGB-Recht, Vor § 307 Rn. 7.

mittlere Fahrlässigkeit unter der Voraussetzung, dass Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit aufgetreten sind. In Bezug auf sonstige Schäden ist nach § 309 Nr. 7 lit. b BGB ein Ausschluss der Haftung für grobe Fahrlässigkeit und Vorsatz unzulässig. Mit anderen Worten ermöglicht § 309 Nr. 7 lit. b BGB eine Haftungsbegrenzung auf Vorsatz oder grobe Fahrlässigkeit, sodass leichte bis mittlere Fahrlässigkeit keine Haftung hervorrufen würde. Zu berücksichtigen ist, dass der Wortlaut des § 309 Nr. 7b BGB zwar an eine Pflichtverletzung anknüpft, jedoch nicht der Gegenschluss erlaubt ist, dass im Rahmen deliktischer Ansprüche eine totale Haftungsbegrenzung möglich sein soll.[250] Der Vertragspartner soll nicht schlechter gestellt werden als ein beliebiger Dritter, der in keinen vertraglichen Beziehungen zu dem Schädiger steht. Darüber hinaus ist es dem Verwender der AGB weiterhin möglich, seine Haftung auch deliktsrechtlich auf einfache Fahrlässigkeit zu begrenzen. Gegenüber Unternehmen findet § 309 BGB zwar nicht direkt Anwendung, aber die Wertungen des § 309 Nr. 7 BGB sind über § 307 BGB grundsätzlich auch im Unternehmensverkehr zu beachten.[251] Dies ist vorliegend von Bedeutung, da es sich bei den Teilnehmern des MonIKA-Verfahrens um Unternehmen handelt.

Allerdings ist nach Auffassung des *BGH* eine Freizeichnung von der nach § 280 Abs. 1 BGB bestehenden Haftung für einfache Fahrlässigkeit nicht möglich, wenn der Verwender wesentliche Rechte oder Pflichten, die sich aus der Natur der des Vertrags ergeben, so einschränkt, dass die Erreichung des Vertragszwecks i. S. d. § 307 Abs. 2 Nr. 2 BGB gefährdet wird.[252] Eine formularmäßige Freizeichnung von der Haftung für einfache Fahrlässigkeit darf nicht zur Aushöhlung von vertragswesentlichen Rechtspositionen des Vertragspartners führen, weil sie solche Rechte begrenzt, die der Vertrag nach seinem Inhalt und Zweck gerade gewährt.[253] Die Haftungsbeschränkung darf nicht dazu führen, dass der Verwender von Verpflichtungen befreit wird, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Vertragspartner regelmäßig vertrauen darf.[254] Verletzt die MonIKA GmbH wesentliche Vertragspflichten so haftet sie für den hierdurch entstehenden Schaden, unabhängig ob diese Pflichtverletzung

[250] Vgl. *Wurmnest*, in: MüKo BGB, § 309 Nr. 7 Rn. 9.
[251] *Basedow*, in: MüKo BGB, § 310 Rn. 7.
[252] *BGH*, NJW 1984, 1350 (1351).
[253] *BGH*, NJW 1988, 1785 (1786); NJW 1993, 335; NJW 2001, 292 (302); NJW 2002, 673 (674); NJW-RR 2005, 1496 (1505); NJW 2007, 3774 (3775).
[254] *Hoeren*, IT-Vertragsrecht, S. 149.

vorsätzlich oder fahrlässig verübt wird. Da die Ausgabe und Mitteilung von Warnungen zu den wesentlichen Leistungen im Rahmen des Analyseverfahrens darstellt, kann die Wirksamkeit eines Haftungsausschlusses mittels AGB für die Erteilung falscher Warnungen vor dem Hintergrund der eben skizzierten Grundsätze nicht bejaht werden.

In Betracht kommt jedoch eine Beschränkung des Haftungsumfangs auf Pflichtverletzungen, die nicht als grob fahrlässig oder vorsätzlich einzuordnen sind, also für leichte und mittlere Fahrlässigkeit. Eine dem Vertragstyp angemessene Haftungsbegrenzung ist in AGB möglich, wenn die leicht fahrlässig verursachte vertragliche Pflichtverletzung zu einem Vermögensschaden führt, der nicht auf einer Verletzung von Leib und Leben beruht.[255] Zulässig sind nach Ansicht der Rechtsprechung auch Regelungen über summenmäßige Haftungsbegrenzungen, soweit sie in einem angemessenen Verhältnis zum vertragstypischen Schadensrisiko stehen und der typischerweise vorhersehbare Schaden abgedeckt wird.[256]

Unwirksam ist ferner bei der Verwendung von AGB ein vollständiger Haftungsausschluss für mittelbare Schäden.[257] Beispiele für mittelbare Schäden sind Produktionsausfallschäden oder ein entgangener Gewinn.

An verschieden Stellen ist die Vereinbarung von Vertragsstrafen denkbar. Allerdings sind auch hierbei die §§ 305 ff. BGB zu berücksichtigen. Regelungen über Vertragsstrafen mit Unternehmen müssen § 307 BGB entsprechen und dürfen daher den Vertragspartner nicht unangemessen benachteiligen. Die Höhe der Vertragsstrafe hat in einem angemessenen Verhältnis zu dem möglichen Schaden zu stehen.[258] Zudem ist zu beachten, dass nach Ansicht des *BGH*, von dem Grundsatz der verschuldensabhängigen Haftung in AGB nur abgewichen werden kann, wenn ausnahmsweise Gründe vorliegen, die eine verschuldensunabhängige Haftung rechtfertigen.[259]

4.5.4 Ergebnis

Die Haftungsrisiken im Rahmen des PoC sind als gering zu beurteilen. Dies liegt in erster Linie daran, dass im PoC nur wenige sensible Daten verwendet werden und

[255] *Hoeren*, IT-Vertragsrecht, S. 150.
[256] *BGH*, NJW 1993, 335 (336); NJW 2013, 291 (295).
[257] *BGH*, NJW 2002, 2470 (2472); *OLG Hamm*, CR 2000, 289 (290).
[258] *Gennen/Völkel*, Recht der IT-Verträge, Rn. 547.
[259] *BGH*, NJW 1985, 57 (57 f.).

diese ohnehin anonymisiert werden. Die größte Gefahr dürfte die Veröffentlichung von IP-Adressen durch ein Datenleck darstellen, wodurch Schadensersatzansprüche entstehen können. Über den PoC hinaus könnte auch die Veröffentlichung sensibler Geschäftsdaten einen Haftungsfall auslösen. Auch durch die Ausgabe von falschen Warnungen können Haftungsansprüche bestehen. Entscheidend für eine Haftung sind hierbei die Reaktion auf die Warnung und deren Auswirkungen auf die Betroffenen.

Sollten AGB verwendet werden, so sind Haftungsausschlüssen enge Grenzen gesetzt. Haftungsausschlüsse, die wesentliche Vertragspflichten betreffen, sind nicht möglich. Zu diesen Pflichten ist auch die Erteilung von Warnungen zu zählen. Ein Haftungsausschluss für Schäden, die auf einer fehlerhaften Warnung beruhen, ist daher nicht möglich. Für nichtwesentliche Pflichtverstöße kann die Haftung für einfache bis mittlere Fahrlässigkeit ausgeschlossen werden.

Im Gegensatz zu AGB sind individualvertraglich weitergehende Haftungsbegrenzungen und Haftungsausschlüsse möglich. Gem. § 276 Abs. 3 BGB kann eine Haftung für vorsätzlich verursachte Schäden nicht ausgeschlossen werden.

4.6 Verein als alternativer MonIKA-Verarbeiter

Als Alternative zu einem externen IT-Sicherheitsdienstleister (MonIKA GmbH), der für den PoC als MonIKA-Verarbeiter gewählt wurde, ist in Betracht zu ziehen, dass die Unternehmen, die MonIKA betreiben wollen, selbstständig die Rechte an dem Softwareframework erwerben und eine eigene Instanz gründen.

Als Rechtsform könnte hierfür ein Verein gewählt werden, da das Vereinsrecht im Gegensatz zum Kapitalgesellschaftsrecht keine besonderen Schutzbestimmungen für die Gläubiger und den Rechtsverkehr vorsieht. Die Gründung eines MonIKA-Vereins erscheint somit attraktiver für Unternehmen, die sich zu dem Betrieb eines MonIKA-Netzes entscheiden sollten. Fraglich ist jedoch, ob die Gründung eines Vereins möglich ist oder ob zwingend eine andere Gesellschaftsform gewählt werden müsste.

4.6.1 Grundzüge des Vereinsrechts

Ein eingetragener Verein kann in Form eines Idealvereins oder eines wirtschaftlichen Vereins bestehen.

4.6.1.1 Idealverein

Die §§ 21 ff. BGB gehen von dem Gedanken aus, dass der Rechtsverkehr bei Vereinen, die eine nichtwirtschaftliche Zielsetzung verfolgen, keines besonderen Schutzes bedarf.[260] Dies beruht darauf, dass keine nach außen gerichtete wirtschaftliche Betätigung stattfindet und somit keine Gläubigerinteressen berührt werden. Im Unterschied zum Kapitalgesellschafts- und Genossenschaftsrecht sind keine besonderen Schutzbestimmungen für die Gläubiger und den Rechtsverkehr wie eine Mindestkapitalausstattung oder Bilanzierungs-, Publizitäts- und Prüfungspflichten vorgesehen. Die Vorschriften beschränken sich auf die Normen über die Liquidation des Vereins nach §§ 47 ff. BGB und die Pflicht des Vorstandes, den Insolvenzantrag nach § 42 Abs. 2 BGB zu stellen.

Die Mitglieder des Vereins bestimmen einen gemeinsamen Zweck, den sie durch die allseitige Leistung von Beiträgen fördern. Zulässig ist jeder erlaubte nichtwirtschaftliche und somit ideelle Zweck.[261] Altruistische Merkmale muss der Zweck hingegen nicht aufweisen. Er wird vom Registergericht geprüft. Der Gründer trägt dabei die objektive Beweislast für die Eintragungsvoraussetzungen. Die Tätigkeit darf bei einem Idealverein grundsätzlich nicht auf einen wirtschaftlichen Geschäftszweck gerichtet sein. Ein wirtschaftlicher Geschäftszweck kann unabhängig von einer Gewinnerzielungsabsicht vorliegen. Maßgebliches Abgrenzungskriterium ist somit, ob der Vereinszweck auf eine wirtschaftliche Betätigung gerichtet ist. Die Abgrenzung erfolgt nach dem Schutzgedanken der §§ 21, 22 BGB anhand der Frage, ob sich der Verein unternehmerisch am Markt betätigt und das damit verbundene Risiko trägt. Liegt eine solche unternehmerische Betätigung vor, kann es sich nicht um einen nichtwirtschaftlichen Verein handeln.[262]

Eine unternehmerische Tätigkeit setzt nicht zwingend eine Leistung an Dritte voraus. Auch wenn der Verein die Leistung nur an seine Mitglieder erbringt und dies entgeltlich erfolgt, kann eine unternehmerische Tätigkeit in einem Binnenmarkt vorliegen. Um einen Idealverein handelt es sich jedoch, wenn der Verein seinen Mitgliedern die Leistung zur Verwirklichung seiner ideellen Zwecke

[260] *BGH*, NJW 1966, 2007; *Schöpflin*, in: Bamberger/Roth, BGB, § 21 Rn. 81.
[261] *Schöpflin*, in: Bamberger/Roth, BGB, § 21 Rn. 84.
[262] *Schöpflin*, in: Bamberger/Roth, BGB, § 21 Rn. 93.

anbietet und die Leistung nur von Vereinsmitgliedern erworben werden kann (mitgliedschaftlicher Charakter der Leistung).[263] In diesem Fall kann die Leistung auch entgeltlich erfolgen.[264] Die Mitglieder stehen dem Verein nicht als Kunden gegenüber und der Verein ist keinem Wettbewerb ausgesetzt, sodass nicht fortwährend risikobehaftete Entscheidungen getroffen werden müssen. Daher bedarf es keiner Vorkehrungen zum Schutz der Gläubigerinteressen.

Beispiele für einen nichtwirtschaftlichen Verein sind kassenärztliche Vereinigungen und Vereine zum Betrieb von Werkskantinen oder einem Betriebsarztzentrum, da sie den Arbeitnehmer nicht als Kunden sehen, sondern eine betriebliche Fürsorgepflicht erfüllen.

4.6.1.2 Wirtschaftlicher Verein

Der wirtschaftliche Verein erwirbt seine Rechtsfähigkeit durch Verleihung gem. § 22 BGB. Das Land, in dessen Gebiet der Verein seinen Sitz hat, genehmigt den wirtschaftlichen Verein und verleiht die Konzession.[265]

Ob es sich um einen wirtschaftlichen Verein handelt, bestimmt sich nach seinem Hauptzweck. Es handelt sich um einen wirtschaftlichen Verein, wenn es sein Hauptzweck ist, mit Hilfe eines wirtschaftlichen Geschäftsbetriebs Gewinne zu erzielen, die dem Verein selbst oder seinen Mitgliedern zufließen sollen.[266] Dies setzt eine nach außen gerichtete, planmäßige und dauernde Tätigkeit als Anbieter von Wirtschaftsgütern im weitesten Sinne voraus.[267]

Hierbei muss der wirtschaftliche Verein von der Kapitalgesellschaft abgegrenzt werden. Der Verein als Grundform der juristischen Person des Privatrechts weist Gemeinsamkeiten mit den Kapitalgesellschaften als Handelsvereinen auf. Der entscheidende Unterschied liegt in dem gesetzlichen Haftkapital der Kapitalgesellschaften zum Schutz der Gläubiger und Anteilseigner. Vergleichbare Vorschriften zur Kapitalaufbringung und -sicherung liegen für den wirtschaftlichen Verein nicht vor. Deshalb muss als Rechtsform eine Form der Kapitalgesellschaft (Aktiengesellschaft, Gesellschaft mit beschränkter Haftung, Genossenschaft) gewählt werden, wenn die erstrebte Zielsetzung auch in einer dieser Rechtsformen erreicht werden kann (Grundsatz der Subsidiarität).[268] Nur in Form

[263] *BVerwG*, NJW 1998, 1166 (1167).
[264] *BVerwG*, NJW 1998, 1166 (1167).
[265] *Reuter*, in: Säcker/Rixecker, BGB, § 22 Rn. 72.
[266] *Eisenhardt*, Gesellschaftsrecht, Rn. 111.
[267] *Eisenhardt*, Gesellschaftsrecht, Rn. 111.
[268] *Eisenhardt*, Gesellschaftsrecht, Rn. 115 f.

der AG, GmbH oder eG soll es möglich sein, die persönliche Haftung der Mitglieder auszuschließen. Eine Verleihung der Rechtsfähigkeit nach § 22 BGB kommt nur ausnahmsweise in Betracht, wenn es dem Verein wegen atypischer Umstände unzumutbar ist, sich einer der Rechtsformen des Gesellschaftsrechts zu bedienen.[269]

Es haben sich drei Fallgruppen von wirtschaftlichen Vereinen herausgebildet, nach denen eine Einordnung und Abgrenzung auch von der Rechtsprechung vorgenommen wird. Danach stellen unternehmerisch tätige Vereine, Vereine zum Zwecke der genossenschaftlichen Kooperation sowie Vereine mit unternehmerischer Tätigkeit in einem Binnenmarkt wirtschaftliche Vereine dar.[270]

Ein unternehmerisch tätiger Verein bietet Waren oder Dienstleistungen entgeltlich und planmäßig, d. h. am Marktgeschehen ausgerichtet, an einen äußeren Markt an.

Bei einem genossenschaftlichen Verein gliedern die Mitglieder einen Teil ihrer unternehmerischen Tätigkeit aus und übertragen sie auf den Verein. Erbringt der Verein seine Leistungen auch gegenüber Dritten, ist eine Entgeltlichkeit unerheblich.

Ein Verein mit unternehmerischer Tätigkeit in einem Binnenmarkt bietet die Leistungen nur an einen Binnenmarkt an. Es besteht ein vereinsinterner Markt gegenüber den Mitgliedern. Dabei muss keine Gewinnerzielungsabsicht gegeben sein, erforderlich ist nur die Entgeltlichkeit. Die Entgeltlichkeit kann in Form von Vereinsbeiträgen, Umlagen, Aufnahmegebühren oder Mitgliedsbeiträgen gegeben sein oder gesondert erhoben werden.[271] Beiträge oder Umlagen sind als Entgelt anzusehen, wenn sie im direkten Eintausch mit der angebotenen Ware erbracht werden. Das Mitglied tritt dem Verein als Kunde gegenüber, sodass das Mitgliedsverhältnis nur auf den Austausch einer Ware oder Dienstleistung gegen Entgelt gerichtet ist.[272] Bei den angebotenen Leistungen muss es sich um solche handeln, die entgeltlich auf einem äußeren Markt erworben werden. Sie können somit unabhängig von der mitgliedschaftlichen Beziehung erworben werden, die angebotene Leistung hat daher keinen mitgliedschaftlichen Charakter.[273] Ein

[269] *BVerwG*, NJW 2979, 2261; *Schöpflin,* in: Bamberger/Roth, BGB, § 21 Rn. 79.
[270] *Schöpflin*, in: Bamberger/Roth, BGB, § 21 Rn. 94.
[271] *OLG Schleswig*, NJWE-MietR 1997, 40; *LG Karlsruhe*, Rpfleger 1984, 22.
[272] *Ellenberger*, in: Palandt, BGB, § 22 Rn. 5.
[273] *Hadding*, in: Soergel, BGB, § 21 Rn. 28.

Beispiel hierfür sind Buchclubs oder ein Verein zum Erwerb und zur Vermietung von Eigentumswohnungen.[274]

4.6.2 Betrieb von MonIKA durch einen Verein

Fraglich ist nun, ob die Gründung eines solchen MonIKA-Vereins rechtlich möglich ist oder ob eine andere Gesellschaftsform gewählt werden müsste.

4.6.2.1 Leistungserbringung ausschließlich an Mitglieder

Dabei ist von der Konstellation auszugehen, dass sich mehrere Unternehmen – etwa die im PoC gewählte McQueer AG und ihre Zulieferer – dazu entschließen, MonIKA zu betreiben und hierzu ein eigenes CSOC gründen möchten, das die Leistungen ausschließlich gegenüber den partizipierenden Unternehmen erbringt. Mitglieder des Vereins können also nur die McQueer AG sowie Zulieferer aus der McQueer-Lieferantenkette werden.[275] Der so gegründete Verein erhebt von den Mitgliedern Mitgliedsbeiträge, um das CSOC zu unterhalten.

Die Gründung als Idealverein setzt voraus, dass es sich nicht um einen wirtschaftlichen Verein handelt, also dass ein ideeller Zweck verfolgt wird. Damit ist eine Negativabgrenzung zu den bereits angesprochenen Formen des wirtschaftlichen Vereins in Form eines genossenschaftlichen oder unternehmerischen Vereins erforderlich.

Da der Verein von seinen Mitgliedern gegründet und unterhalten würde, wären keine Mitgliedsbeiträge von den Unternehmen zu leisten. Es bestünde somit auch keine Gewinnerzielungsabsicht. Da zudem keine Dritten von der Datenauswertung und der entsprechenden Analyse profitieren können sollen bzw. die Ergebnisse nicht in Anspruch nehmen können sollen, handelt es sich nicht um einen unternehmerisch tätigen Verein.

Fraglich ist jedoch, ob es sich um einen genossenschaftlichen Verein handeln würde, bei dem die Unternehmer einen Teil ihrer Unternehmenstätigkeit ausgliedern und auf einen Verein verlagern.[276] Zunächst erscheint es nicht abwegig, dass es sich bei einem MonIKA-Verein um einen nichtwirtschaftlichen Verein handelt. Dies beruht darauf, dass der Verein nicht direkt gegenüber Dritten auftritt und damit der Rechtsverkehr – entsprechend dem Schutzzweck der §§ 21, 22 BGB – keines

[274] *OLG Schleswig*, Rpfleger 2012, 693.
[275] Ein weiteres Beispiel bietet der Fall, dass sich mehrere ISP zusammenschließen, um ein MonIKA-Netz in Form eines eigens gegründeten Vereins zu betreiben.
[276] *BGH*, NJW 1966, 2007.

besonderen Schutzes bedarf. Allerdings sprechen die besseren Gründe für das Vorliegen eines genossenschaftlichen Vereins. Dies steht damit im Zusammenhang, dass die Gewährleistung von IT-Sicherheit – wie oben erarbeitet[277] – einen Teil der Compliance im Unternehmen darstellt. Die Verletzung der IT-Sicherheit durch unzureichende Maßnahmen kann sowohl für das Unternehmen als auch die Unternehmensführung zu einer Haftung führen. Überträgt das Unternehmen einen Teil dieser Verantwortung auf den Verein, gliedert er einen wesentlichen Teilbereich aus. Aus den beschriebenen Haftungsszenarien ergibt sich, dass infolge eines Fehlers des CSOC (hier also des Vereins) auch Daten Dritter offenbart werden könnten und für diese hieraus ein Schaden entstehen könnte. Da es nach dem *BGH* auch unerheblich ist, ob der Verein entgeltlich tätig ist oder nicht und ob er selbstständig gegenüber Dritten geschäftlich handelt, liegt die Einordnung als genossenschaftlicher Verein näher.[278] So entschied der *BGH* in dem Fall „Taxizentrale“ mit o. g. Argumenten, dass die Gründung einer Anruferzentrale durch Inhaber oder Pächter von Taxikonzessionen nicht in der Form eines Idealvereins möglich sei. Der Fall ist insofern vergleichbar, als dass in beiden Fällen ein Teil der Geschäftstätigkeit auf den Verein ausgegliedert wird.

Somit wäre ein MonIKA-Verein wohl nur in der Form eines wirtschaftlichen Vereins möglich, wobei dann der Subsidiaritätsgrundsatz zu berücksichtigen wäre.
Zu betonen ist allerdings, dass die Leitentscheidung des *BGH* bereits knapp 50 Jahre zurückliegt. Mit vertretbaren Argumenten erscheint auch eine Einordnung als nichtwirtschaftlicher Verein mit ideellem Zweck möglich – insbesondere, wenn der Verein neben der Verbesserung der unternehmenseigenen IT-Sicherheit auch die Verbesserung der IT-Sicherheit insgesamt zum Ziel hat.[279]

4.6.2.2 Leistungserbringung auch an Nichtmitglieder

Eine andere Konstellation ergibt sich, wenn der Verein seine Leistungen auch an Nichtmitglieder anböte. Für den dem PoC zugrunde liegenden Anwendungsfall „Enterprise-Monitoring“ ist dies weniger naheliegend. Für den Anwendungsfall „Botnetz-Monitoring“ am Beispiel des Spam-Szenarios könnten jedoch ISPs einen MonIKA-Verein gründen, der Leistungen theoretisch an Dritte erbringen könnte – so etwa an andere ISPs oder Unternehmen. Hierfür könnten die Analyseergebnisse den SOCs dritter Unternehmen gegen Entgelt zur Verfügung gestellt werden.

[277] S. bereits Abschnitt 2.2.
[278] *BGH*, NJW 1966, 2007.
[279] Vergleichbar der Allianz für Cybersicherheit e. V.

Indem Leistungen entgeltlich an Dritte angeboten werden, scheitert die Gründung als Idealverein allerdings an der unternehmerischen Betätigung und der damit verbundenen Risikotragung. Allenfalls ein wirtschaftlicher Verein in Form des unternehmerisch tätigen Vereins kommt in Betracht, wobei dieser zu den Formen der Kapitalgesellschaften lediglich subsidiär ist. Die Subsidiarität erstreckt sich nicht auf Personengesellschaften. Es ist nicht ersichtlich, weshalb die Gründung in Form einer Kapitalgesellschaft unzumutbar sein sollte, sodass eine Verleihung der Rechtsfähigkeit als wirtschaftlicher Verein nach § 22 BGB nicht in Betracht kommt.

4.6.3 Haftungsrecht

Angenommen, die Einordnung als nichtwirtschaftlicher Verein wäre möglich, würde sich auch für einen derartigen MonIKA-Verein, der von mehreren Unternehmen gegründet wurde, die Frage stellen, wie er haftet. Für mögliche Haftungsszenarien kann auf den Abschnitt 4.5.2 verwiesen werden.

Für den eingetragenen Verein gilt der Grundsatz, dass er gegenüber Dritten nur auf das Vereinsvermögen haftet.[280] Im Innenverhältnis haften die Vereinsorgane und die Vereinsmitglieder gegenüber dem Verein und anderen Vereinsmitgliedern für einen von ihnen verursachten Schaden.

4.6.3.1 Haftung gegenüber dem Verein

Verursachen Organe oder Vereinsmitglieder Dritten gegenüber einen Schaden, für den der Verein haftet, sind sie dem Verein zum Ersatz verpflichtet. Wenn sie unentgeltlich tätig sind oder eine Vergütung erhalten, die 720,00 € jährlich nicht übersteigt, beschränkt sich ihre Haftung gesetzlich auf Vorsatz und grobe Fahrlässigkeit (§§ 31a Abs. 1, 31 b Abs. 1 BGB).

4.6.3.2 Haftung gegenüber Vereinsmitgliedern oder Dritten

Schädigen Organe oder Vereinsmitglieder andere Vereinsmitglieder, haften sie diesen für die entstandenen Schäden nach §§ 31 a Abs. 2 Satz 1, 31 b Abs. 2 Satz 2 BGB. Die Geschädigten haben insbesondere einen Schadensersatzanspruch aus § 823 Abs. 1 BGB.[281] Sind die Organe oder Vereinsmitglieder unentgeltlich tätig oder erhalten sie eine Vergütung, die 720 € nicht übersteigt, steht ihnen ein Freistellungsanspruch von der Haftung gegenüber dem Verein zu (§ 31a Abs. 2 BGB). Dieser entfällt jedoch, wenn die schädigende Handlung vorsätzlich oder grob fahrlässig begangen wurde.

[280] *Eisenhardt*, Gesellschaftsrecht, Rn. 161.
[281] *Schöpflin*, in: Bamberger/Roth, BGB, § 31b Rn. 4.

4.6.3.3 Haftung der MonIKA-Unternehmen

Die MonIKA-Unternehmen als Vereinsmitglieder haften einem eigens gegründeten Verein und den anderen Vereinsmitgliedern für von ihnen verursachte Schäden nach den soeben genannten Maßgaben.

Würden die Unternehmen, die den MonIKA-Verein gegründet haben, bei ihnen angestellte Arbeitnehmer für die Aufgaben des CSOC freistellen, könnten sie gegenüber den anderen Vereinsmitgliedern nach den Grundsätzen der Haftung der Vereinsmitglieder untereinander für verursachte Schäden haftbar sein. Für Schäden, die aus der spezifischen Tätigkeit des CSOC herrühren, kann die Haftung der Unternehmen jedoch verhindert werden, wenn die Aufgaben des CSOC nicht direkt von den Unternehmen wahrgenommen werden. Daher ist es für die Haftung der Unternehmen günstiger, wenn der Verein als Arbeitgeber tätig wird und Personen als Arbeitnehmer beschäftigt, die die im CSOC anfallenden Aufgaben erledigen. Ein etwaiges Verschulden der Arbeitnehmer wird in dieser Konstellation nicht den Unternehmen zugerechnet.

Beschäftigt der Verein Personen, die die Aufgaben des CSOC übernehmen und fügen diese einem der beteiligten Unternehmen einen Schaden zu, kann es zu einer direkten Haftung des Vereins gegenüber den Unternehmen kommen. Den Verein trifft als juristische Person eine besondere Organisationspflicht. Dies bedeutet, dass der Verein für Tätigkeiten, die ein besonderes Maß an Verantwortung erfordern, ein Mitglied des Vorstandes oder einen besonderen Vertreter bestellen muss.[282] Dies beträfe wohl nur Warnungen, die besonders risikobelastete Reaktionen der Unternehmen hervorrufen könnten. Alltägliche Warnungen hingegen wären davon ausgenommen. Der besondere Vertreter hat nach § 30 BGB Vertretungsmacht für die seinem Aufgabenbereich zugewiesenen Geschäfte. Kommt der Verein seiner Organisationspflicht nicht nach und beauftragt lediglich eine Person ohne leitende Stellung, kann er sich bei einem Verschulden dieser Person, nicht dadurch entlasten, dass er i. S. v. § 831 BGB bei der Auswahl der betreffenden Person die im Verkehr erforderliche Sorgfalt beachtet hat. Erfüllt der Verein jedoch seine Organisationspflichten, haftet er nur nach den allgemeinen Vorschriften der §§ 278, 831 BGB. Für den Fall der Erfüllung seiner Organisationspflichten haftet der Verein nur für unerlaubte Handlungen eines Angestellten, wenn die Pflichtverletzung von einem seiner Vertreter hinzukommt. Die Pflichtverletzung des Vertreters kann darin bestehen, dass er nach § 831 BGB bei der Auswahl des Angestellten oder der

[282] *Waldner/Wörle-Himmel*, in: Sauter/Schweyer/Waldner, Der eingetragene Verein, Rn. 291.

Anleitung der Tätigkeit die im Verkehr erforderliche Sorgfalt nicht beachtet hat. In der Satzung kann die Bestellung und Abberufung eines besonderen Vertreters geregelt werden.[283] Es kann auch festgelegt werden, dass der besondere Vertreter durch den Vorstand zu bestimmen ist. Trifft die Satzung hierzu keine Regelung, ist die Mitgliederversammlung zuständig.

Eine Haftung des Angestellten ist aus § 823 Abs. 1 BGB möglich. Im Rahmen des innerbetrieblichen Schadensausgleichs kann der Angestellte vom Verein als seinem Arbeitgeber den Ausgleich des von ihm verursachten Schadens verlangen.[284] Der Umfang dieses Anspruchs richtet sich nach dem Verschuldensgrad des Arbeitnehmers (leichte, mittlere oder grobe Fahrlässigkeit). Der Ausgleichsanspruch ist unabhängig von der Haftung des Arbeitnehmers gegenüber dem geschädigten Dritten.

Sind die mit den Aufgaben des CSOC betrauten Personen direkt bei dem Verein angestellt, haften demnach nur der Verein und die Angestellten selbst, aber nicht die Unternehmen als Mitglieder des Vereins.

4.6.3.4 Haftungsbeschränkung des Vereins

Der Verein kann in der Satzung seine Haftung gegenüber Dritten aus § 31 BGB nicht ausschließen.[285] Die Haftung des Vereins gegenüber Vereinsmitgliedern für leichte Fahrlässigkeit kann allerdings ausgeschlossen werden. Für vorsätzliches oder grob fahrlässiges Verhalten kann die Haftung hingegen auch gegenüber den Vereinsmitgliedern nicht ausgeschlossen werden.

Sollten die Unternehmen durch Handlungen des MonIKA-Vereins geschädigt werden, würden sie bei der Geltendmachung von Schadensersatzansprüchen im Ergebnis gegen sich selber vorgehen. Damit kommt diesem Szenario keine erhöhte Bedeutung zu und Haftungsrisiken als solche bestehen nicht.

4.6.4 Ergebnis

Die Gründung eines MonIKA-Idealvereins böte den Unternehmen Vorteile bei einer möglichen Haftung. Allerdings handelt es sich wohl eher nicht um einen ideellen Verein, wie obige Ausführungen aufzeigen. Dies beruht darauf, dass IT-Sicherheit einen Teil der Geschäftstätigkeit jedes Unternehmens darstellt. Bei einer – wenn auch nur teilweisen oder nur zu Zwecken der Verbesserung – Ausgliederung dieses

[283] *Waldner/Wörle-Himmel*, in: Sauter/Schweyer/Waldner, Der eingetragene Verein, Rn. 313.
[284] *Belling*, in: Staudinger, BGB, § 831 Rn. 15.
[285] *Waldner/Wörle-Himmel*, in: Sauter/Schweyer/Waldner, Der eingetragene Verein, Rn. 292 d.

Aufgabenbereichs, dürfte es sich der Rechtsprechung des *BGH* folgend um eine wirtschaftliche Tätigkeit des Vereins handeln.

4.7 Öffentlich-rechtliche Stelle als alternativer MonIKA-Verarbeiter

Zumindest möglich ist es auch, dass eine öffentlich-rechtliche Stelle als MonIKA-Verarbeiter und CSOC fungiert. Die derzeitigen Pläne für eine umfassende staatliche Regulierung der IT-Sicherheit deuten allerdings nicht darauf hin, dass der Staat ein übergreifendes Monitoring samt Klassifikation plant.[286] Dennoch kann nicht vollends ausgeschlossen werden, dass mittel- oder langfristig die IT-Infrastruktur von Unternehmen einzelner Branchen, von denen die Gesellschaft in besonderer Weise abhängig ist (bspw. Energieversorger), durch eine staatliche Instanz zentral und direkt überwacht wird, indem die Unternehmen zur Teilnahme an einem staatlichen kooperativen Monitoring verpflichtet werden.[287]

Sollte eine staatliche Stelle damit betraut werden, ein Monitoring durchzuführen, bedürfte es entsprechend dem Vorbehalt des Gesetzes aus Art. 20 Abs. 3 GG wegen entsprechender Grundrechtseingriffe[288] einer Ermächtigungsgrundlage, die die Unternehmen zum Einsatz der MonIKA-Agenten und der Übermittlung der Daten an ein staatliches CSOC verpflichtet.

Angenommen, der Staat würde als CSOC handeln, stellt sich auch hier die Frage, wie er haften würde, sofern er eine Falschwarnung über ein (nicht) bestehendes Sicherheitsrisiko ausgegeben hat oder er – entgegen den Hinweisen, die er durch die Daten erhalten hat, und ihm dadurch möglichen Rückschlüssen – nicht vor einem tatsächlich bestehenden Risiko warnt. In diesen Fällen könnten die zur Übermittlung der Daten verpflichteten Unternehmen, denen in einer der in 4.5.2 beschriebenen Konstellationen ein Schaden entstanden ist, Amtshaftungsansprüchen nach § 839 BGB i. V. m. Art. 34 GG geltend machen wollen.

[286] Ausführlich zu den Plänen unter Abschnitt 7.
[287] Zu bisherigen Initiativen des Bundes s. *Roos*, K&R 2013, 769 (769 f.).
[288] Zu denken ist insbesondere an die Berufsfreiheit aus Art. 12 Abs. 1 GG und das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG.

4.7.1 Rechtliche Einordnung von Warnungen

Bei Warnungen durch eine staatliche Instanz – als Unterfall von staatlicher Informationstätigkeit – handelt es sich um einen Realakt und schlicht-hoheitliches Verwaltungshandeln.[289] Damit scheidet im Unterschied zu staatlichen Ge- und Verboten auch eine zwangsweise Durchsetzung aus.[290] Typischerweise entsteht die rechtliche Brisanz von Warnungen immer dadurch, dass ein Unternehmen oder die ganze Branche, vor dessen/deren Produkten gewarnt wird, erhebliche Image- und Umsatzeinbußen zu verzeichnen hat.[291] Zwar entfällt diese Brisanz bei staatlichen Warnungen vor solchen Sicherheitsrisiken aus dem Cyber-Raum, die nicht produktbezogen erfolgen, aber dennoch sind Schäden, die in einem kausalen Zusammenhang mit der Warnung stehen, denkbar (ähnlich den oben gebildeten Szenarien).

Fraglich ist, ob für die Warntätigkeit eine gesetzliche Ermächtigungsgrundlage erforderlich ist. Das *Bundesverfassungsgericht* (BVerfG) ist in den Entscheidungen „Glykol“ und „Osho“ davon ausgegangen, dass sich die Bundesregierung für die Informationstätigkeit auf ihre verfassungsrechtliche Aufgabe der Staatsleitung berufen kann, ohne dass eine weitere gesetzliche Ermächtigungsgrundlage erforderlich ist.[292] Das Gericht begründet dies mit der Bedeutung der Selbstverantwortung und der eigentverantwortlichen Mitwirkung der Bürger bei der Lösung gesellschaftlicher Probleme in der politischen Ordnung.[293] Die Aufgabe der Staatsleitung umfasse dabei auch, durch Informationsweitergabe neuen, oft kurzfristig auftretenden Herausforderungen entgegenzutreten und auf Krisen und Besorgnisse der Bürger schnell und sachgerecht reagieren und zu einer Orientierung verhelfen zu können.

Die Argumentation des *BVerfG* kann auf den Bereich der IT-Sicherheit übertragen werden. Dabei ist auf die erhöhte Bedeutung der Informationstechnik in wirtschaftlicher Hinsicht, aber ebenso für die Persönlichkeitsentfaltung des Einzelnen[294] hinzuweisen. Vorhandene Sicherheitslücken in der Informationstechnik

---

[289] *Detterbeck*, Allgemeines Verwaltungsrecht, Rn. 297, 885. Nur Bezug nehmend auf die Warnung *Maurer*, Allgemeines Verwaltungsrecht, § 15 Rn. 8.
[290] *Detterbeck*, Allgemeines Verwaltungsrecht, Rn. 297.
[291] Ein Beispiel ist die vom Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz geäußerte Verzehrempfehlung gegen Gurken, Tomaten und Blattsalat im Frühjahr 2011 auf Grund einer vermuteten Verunreinigung mit EHEC-Erregern. Vgl. dazu *Bayerisches Landesamt für Steuern* vom 7.6.2001, 1 S 1915.1.1 – 7/2 St 32 und *Oberste Finanzbehörden der Länder*, DStR 2011, 1523.
[292] *BVerfG*, NJW 2002, 2621 (2624); NJW 2002, 2626 (2629).
[293] *BVerfG*, NJW 2002, 2621 (2623); NJW 2002, 2626 (2629).
[294] Vgl. dazu etwa *BVerfG*, NJW 2008, 822 (824).

und deren Ausnutzung weisen oftmals ein erhebliches Gefährdungspotenzial auf und erfordern regelmäßig ein schnelles Handeln.

4.7.2 § 7 BSIG als taugliche Ermächtigungsgrundlage

Unabhängig davon, dass das *BVerfG* im Einzelfall mitunter keine besondere gesetzliche Ermächtigung verlangt, existiert im BSIG in Form von § 7 BSIG[295] bereits eine Ermächtigungsgrundlage speziell für Warnungen. Fraglich ist, ob Warnungen, wie sie ein (staatliches) Common SOC bei Betrieb eines Monitoring-Programms wie MonIKA ausgeben würde, von § 7 BSIG umfasst wären.

§ 7 BSIG bezweckt die Förderung der IT-Sicherheit durch die Beratung und Warnung der Stellen des Bundes, der Länder sowie der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen (s. § 3 Abs. 1 Nr. 14 BSIG). Dies stimmt insoweit mit MonIKA überein.

Behandlungsgegenstand des § 7 BSIG sind – wie sich schon aus seiner amtlichen Überschrift ergibt – Warnungen. Dies betrifft Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten und vor Schadprogrammen. Ebenfalls sind Empfehlungen für den Einsatz bestimmter Sicherheitsprodukte erfasst. Sowohl für Sicherheitslücken als auch für Schadprogramme enthält das BSIG Legaldefinitionen. Nach § 2 Abs. 6 BSIG sind Sicherheitslücken als Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen zu verstehen, durch deren Ausnutzung sich Dritte unberechtigt Zugang zu informationstechnischen Systemen verschaffen oder die Funktion der Systeme beeinflussen können. Schadprogramme definiert § 2 Abs. 5 BSIG als Programme und sonstige informationstechnische Routinen und Verfahren, die dem Zweck dienen, unbefugt Daten zu nutzen oder zu löschen oder die das Ziel verfolgen, unbefugt auf sonstige informationstechnische Abläufe einzuwirken.

Die Absätze 1 und 2 – auf den ersten Blick nahezu inhaltsgleich – unterscheiden sich dadurch, dass es nach § 7 Abs. 2 BSIG auch möglich ist, die Warnung unter Nennung der Produktbezeichnung und des Herstellers des betroffenen Produktes auszugeben, während § 7 Abs. 1 BSIG lediglich Warnungen

[295] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) in der Bekanntmachung vom 14. August 2009, BGBl. I S. 3154.

vor Sicherheitslücken in Produkt- und Dienstgruppen ohne Herstellerbezeichnung erfasst. § 7 Abs. 2 BSIG verlangt daher, dass hinreichende Anhaltspunkte für Gefahren der IT-Sicherheit vorliegen müssen. § 7 Abs. 1 BSIG enthält diese Anforderung nicht. Adressaten der Warnungen und Empfehlungen nach Abs. 1 sind dabei neben den Herstellern und Vertreibern auch stets die Anwender von Informationstechnik (in der Norm zusammengefasst als „betroffene Kreise“). Die Warnungen und Empfehlungen gemäß § 7 Abs. 2 BSIG richten sich lediglich an die Öffentlichkeit.

MonIKA ermöglicht ein kooperatives Monitoring, über das sich Anomalien feststellen lassen. Sollte der Staat ein kooperatives Monitoring betreiben, das (wie im Anwendungsfall „Enterprise-Monitoring“) über ein CSOC organisiert wird, würde die staatliche Stelle dann Frühwarnungen über generelle Risiken, aber auch über Software-Schwachstellen, die sich Angreifer zunutze machen wollen, ausgeben. Damit in Zusammenhang stünde auch die Warnung vor im Umlauf befindlicher Malware. Vor all diesen Risiken kann nach § 7 Abs. 1 BSIG gewarnt werden und nach § 7 Abs. 2 BSIG sogar unter Nennung des betroffenen Produkts und seines Herstellers, sofern hinreichende Anhaltspunkte für eine Gefahrenlage für die IT-Sicherheit vorliegen. Das Merkmal grenzt die Absätze 1 und 2 voneinander ab und ist daher i. S. einer erhöhten Anforderung zu verstehen. Die Hinweise müssen sich also verdichtet haben und es muss eine erhöhte Wahrscheinlichkeit für die Gefährdung der IT-Sicherheit bestehen. Sofern ein staatliches CSOC auf Basis der ausgewerteten Monitoring-Daten zu dem Ergebnis kommt, dass eine Gefahrenlage gegeben ist, wird die Voraussetzung der „hinreichenden Anhaltspunkte“ erfüllt sein.

Eine Besonderheit ist darin zu sehen, dass § 7 Abs. 1 BSIG in Satz 4 den Fall berücksichtigt, dass das BSI den Kreis der Warnenden beschränken kann, wenn ansonsten eine rechtswidrige Ausnutzung der festgestellten Sicherheitslücken oder Schadprogramme zu befürchten ist. Damit stellt bereits das Gesetz klar, dass die Informationen rechtlich zulässig an einen begrenzten Kreis ausgegeben werden können, wie es bei einem staatlichen Monitoring innerhalb einer bestimmten Branche der Fall sein würde.

Festhalten lässt sich damit, dass für staatliche Warnungen durch Gefährdungen aus dem Cyber-Raum bereits eine Ermächtigungsgrundlage besteht. Die Unternehmen müssten jedoch dazu verpflichtet werden, überhaupt an einem

kooperativen, staatlichen Monitoring teilzunehmen und entsprechende Daten an die staatliche Stelle zu übermitteln.

4.7.3 Staatliche Haftung

Die staatliche Haftung bestimmt sich maßgeblich danach, ob die Behörde ihre Amtspflichten beachtet hat. Damit kommt den Aspekten der inhaltlichen Richtigkeit der Information, der Offenlegung etwaiger Unsicherheit und dem genauen Inhalt der Informationsmaßnahme die entscheidende Bedeutung zu.[296]

In erster Linie erscheint es möglich, dass die staatliche Instanz entweder eine Falschwarnung ausgibt, also die ausgegeben Informationen nicht den tatsächlichen Gegebenheiten entsprechen, oder keine Warnung ausgibt, obwohl das Risiko auf Basis der übermittelten Daten erkennbar gewesen wäre.

4.7.3.1 Amtspflichten

Eine erste Amtspflicht ergibt sich aus der Verpflichtung zur Einhaltung der Zuständigkeits- und Formvorschriften. Das BSI ist gem. §§ 3 Abs. 1 Satz 2 Nr. 14 i. V. m. § 7 BSIG sachlich für Warnungen zuständig. Eine Anhörung nach § 28 Abs. 1 VwVfG[297] ist mangels des Charakters eines Verwaltungsakts i. S. d. § 35 VwVfG nicht erforderlich. Allerdings verlangt § 7 Abs. 1 Satz 2 BSIG, dass die Hersteller der betroffenen Produkte rechtzeitig vor Veröffentlichung der Warnung zu informieren sind, sofern der mit der Maßnahme verfolgte Zweck hierdurch nicht gefährdet wird. Diese Information dürfte allerdings vielmehr den Zweck verfolgen, dass die Hersteller mögliche Risiken für die Anwender durch entsprechende Updates schließen, bevor die Lücken in Folge ihrer allgemeinen Bekanntheit von einem noch größeren Kreis ausgenutzt werden. Somit unterscheidet sich die Intention dieser Informationspflicht grundlegend von der Pflicht zur Anhörung.

Ein Aspekt, der im Rahmen von § 7 BSIG relevant werden kann, ist die Amtspflicht zur sachgemäßen Sachverhaltsermittlung. Das BSI hat zu ermitteln, ob konkrete Anhaltspunkte für Gefahren i. S. v. § 7 BSIG vorliegen. Dabei ist nicht zwingend erforderlich, dass lediglich eigens gewonnene Informationen verwendet werden. Vielmehr muss ggf. weiterer sachverständiger Rat eingeholt oder der Hersteller kontaktiert werden, um Ungewissheiten zu beheben.[298] Bei § 7 Abs. 2 BSIG sind überdies hinreichende Anhaltspunkte dafür erforderlich, dass

[296] *Schoch*, NJW 2012, 2844 (2849).
[297] Verwaltungsverfahrensgesetz in der Fassung der Bekanntmachung vom 23. Januar 2003, BGBl. I S. 102.
[298] Für die vergleichbare Regelung des § 26 Abs. 2 Nr. 9 ProdSG *Tremml*/*Luber*, NJW 2013, 262 (264).

die Gefahren für die Sicherheit in der Informationstechnik von dem Produkt oder dem Dienst bzw. dem Schadprogramm ausgehen. Die reine Vermutung einer Gefährdungslage ohne eine konkret überprüfbare Tatsachengrundlage reicht dafür nicht aus. Fehler in der sachgemäßen Sachverhaltsermittlung können gegen den Untersuchungsgrundsatz (vgl. § 24 VwVfG) verstoßen.

Weiterhin muss sich das Handeln als verhältnismäßig herausstellen (Amtpflicht zu verhältnismäßigem Handeln). Die Warnung muss daher geeignet sein, der Gefahr für die Sicherheit der Informationstechnik effektiv entgegenzutreten. Sowohl Form als auch Inhalt der Warnung müssen im Zeitpunkt der Aussprache erforderlich sein und die Warnung darf nicht außer Verhältnis zum (möglichen) Sicherheitsgewinn stehen.[299] Bei § 7 Abs. 2 BSIG gelten gesteigerte Anforderungen, da die Öffentlichkeit hierbei einen betroffenen Hersteller klar identifizieren kann. Darüber hinausgehende nachteilige Wirkungen sowohl für den Hersteller als auch für unbeteiligte Dritte sind zu vermeiden.[300] Die Behörde hat sich stets am Gebot des geringstmöglichen Eingriffs zu orientieren, ohne dass dabei die Eignung zur Gefahrenabwehr leiden darf. So kann das BSI aus Gründen der Zweckmäßigkeit und Verhältnismäßigkeit auch eine Einschränkung des zu warnenden Personenkreises nach § 7 Abs. 1 Satz 3 BSIG vornehmen.

Sowohl § 7 Abs. 1 BSIG als auch § 7 Abs. 2 BSIG gehen von einem Entschließungsermessen des BSI aus („kann“). Es besteht daher auch die Amtspflicht zur fehlerfreien Ermessensausübung. Den Zweck und die Grenzen des behördlichen Ermessens regelt § 40 VwVfG. Zwar bezieht sich § 40 VwVfG unmittelbar nur auf den Erlass von Verwaltungsakten[301], jedoch kommt in der Regelung der allgemeine Rechtsgedanke zum Ausdruck, dass Ermessen auch außerhalb des Verwaltungsverfahrens i. S. d. § 9 VwVfG anzuwenden ist.[302] Damit gelten die Grundsätze zur Ermessensfehlerlehre auch bei staatlicher Informationstätigkeit, sodass die Behörde eine Amtspflicht zur fehlerfreien Ermessensausübung trifft. Zudem lassen sich die Anforderungen an die fehlerfreie Ermessensausübung auch auf Verhältnismäßigkeitsgesichtspunkte zurückführen. In die Erwägungen zu § 7 BSIG sind die Schwere des durch die Sicherheitslücke drohenden Schadens sowie die schutzwürdigen Interessen des betroffenen Unternehmens einzubeziehen. Ferner müssen das Maß an Zuverlässigkeit der

[299] Vgl. *Tremml/Luber*, NJW 2013, 262 (265) m. w. N.
[300] Vgl. *Tremml/Luber*, NJW 2013, 262 (265) m. w. N.
[301] *Aschke*, in: Bader/Ronellenfitsch, VwVfG, § 40 Rn. 1.
[302] *Aschke*, in: Bader/Ronellenfitsch, VwVfG, § 40 Rn. 1; *Foerster/Jäde*, Praxis der Kommunalverwaltung, A 15 Bund, S. 95 f.

eigenen Analyseergebnisse sowie eine mögliche Selbstbindung und Verwaltungspraxis in die Entscheidung einbezogen werden.

4.7.3.2 Falschwarnung

Entspricht die Information nicht den tatsächlichen Gegebenheiten und stellt sich damit als Falschmeldung dar, bedeutet dies nicht zwingend auch eine Amtspflichtverletzung. So verlangt § 7 BSIG für die Information der Öffentlichkeit zumindest hinreichende Anhaltspunkte dafür, dass eine Gefährdung durch ein Produkt oder einen Dienst besteht, jedoch keine absolute Sicherheit. Auch eine tatsächlich falsche Information kann dem BSI daher nicht in jedem Fall zur Last gelegt werden. Spricht die Behörde die Warnung jedoch auf Grund einer reinen Vermutung aus oder ist sie sich einer Unsicherheit bewusst, lässt dies aber nicht erkennen, so verletzt sie damit die Amtspflicht zur sachgemäßen Sachverhaltsermittlung bzw. zum verhältnismäßigen Handeln.

In Bezug auf die Programmhersteller muss der Gleichbehandlungsgrundsatz beachtet werden. Die Programmhersteller sind von den Warnungen eines CSOC an die Teilnehmer mittelbar betroffen, wenn Sicherheitslücken von ihren Produkten festgestellt werden. Der Gleichbehandlungsgrundsatz kann dann verletzt sein, wenn das Programm eines Herstellers ohne nachvollziehbare Gründe wie eine weitreichende Marktbeherrschung besonders im Fokus der Beobachtung steht, aber ein vergleichbares Programm mit vergleichbaren Sicherheitsrisiken kaum beobachtet bzw. vor seinen Risiken gewarnt wird und die Teilnehmer den Eindruck gewinnen könnten, dass zweiteres Programm wesentlich sicherer ist.

Liegt jedoch eine Amtspflichtverletzung vor, ist weiterhin zu fragen, ob der Schaden bei dem Teilnehmer auch adäquat kausal auf der Pflichtverletzung beruht. Hier gelten die bereits unter 4.5.2.1.2 erfolgten Ausführungen.

4.7.3.3 Nichtwarnung

Fraglich ist, ob Amtshaftungsansprüche auch dann in Betracht kommen, wenn das BSI als CSOC eine Warnung nicht oder nicht rechtzeitig ausspräche und Teilnehmern dadurch Schäden entstünden.

Sowohl § 839 Abs. 1 Satz 1 als auch Art. 34 Satz 1 GG verlangen die vorsätzliche oder fahrlässige Verletzung einer drittgerichteten Amtspflicht. Ersatzansprüche erfordern neben dem Verschulden des Amtsträgers daher, dass die Amtspflicht auch dem Geschädigten gegenüber besteht und dessen Schutz vor dem erlittenen Schaden bezweckt. Der *BGH* stellt bei der Amtshaftung im

Zusammenhang mit staatlicher Informationstätigkeit ebenso auf die Drittbezogenheit der Amtspflichtverletzung ab. So verneinte das Gericht bspw. in einem Streit um eine unterlassene bzw. verspätete Hagelwarnung des Deutschen Wetterdienstes Ansprüche von Flugzeug-Versicherern mit der Begründung, die Warnpflicht diene lediglich dem Allgemeininteresse, nicht aber den individuellen Interessen Dritter.[303]

Um als Dritter i. S. d. § 839 Abs. 1 Satz 1 BGB zu gelten, muss die Amtspflicht nach der Rspr. des *BGH* zumindest auch den Zweck haben, das Interesse des Geschädigten wahrzunehmen.[304] Die Schadensersatzpflicht soll nur bestehen, wenn der Geschädigte zu dem Personenkreis zählt, dessen Belange nach dem Zweck und der rechtlichen Bestimmung des Amtsgeschäfts geschützt und gefördert werden sollen.

Ein subjektives öffentliches Recht auf den Schutz vor Bedrohungen aus dem Cyber-Raum in Form von Warnungen und Hinweisen besteht nicht, sodass nach dem Zweck der Amtspflicht zu fragen ist. Die die Amtspflicht begründenden und inhaltlich prägenden Normen dienen dafür als Indikator.[305] Insbesondere der normativ gewollte Schutzzweck gibt Auskunft darüber, wo die sachlichen Grenzen liegen.[306]

Entschlösse man sich also dazu, ein staatliches kooperatives Monitoring zu betreiben, wäre in der Gesetzesbegründung genau zu bestimmen, wer zu dem durch das Monitoring geschützten Kreis gehören soll. Die Motivation des Staates würde wohl nicht primär darin liegen, dass die beteiligten Unternehmen um ihrer selbst willen geschützt werden. Vielmehr würde der Staat das Monitoring betreiben, um gesellschaftliche Interessen von übergeordneter Relevanz wahrzunehmen. Das äußert sich bereits darin, dass (wenn überhaupt) kritische Infrastrukturen zur Teilnahme verpflichtet würden, deren Funktionsfähigkeit eine übergeordnete gesellschaftliche Relevanz besitzt. Zudem wird man sich an den Motiven orientieren können, die für die Schaffung des IT-SiG bereits genannt wurden. Dazu zählen der Schutz der IT-Systeme, die Vereinheitlichung des Schutzstandards, aber auch der Erhalt der Attraktivität und Wettbewerbsfähigkeit der Bundesrepublik Deutschland als Wirtschaftsstandort.[307]

[303] *BGH*, NJW 1995, 1830.
[304] *BGH*, NJW 1994, 3012; NJW 1994, 2413 (2416).
[305] Vgl. *Papier*, in: Maunz/Dürig, GG, Art. 34 Rn. 183 m. w. N.
[306] *Papier*, in: Maunz/Dürig, GG, Art. 34 Rn. 185.
[307] Entwurf IT-SiG, S. 1; *Friedrich*, MMR 2013, 273 (273 f.).

Es ist daher zu empfehlen, dass die Schutzzwecke eines solchen Monitorings in der Gesetzesbegründung genau beschrieben würden und gegenüber den Betreibern der teilnehmenden Unternehmen verdeutlicht wird, dass aus staatlicher Sicht nicht der Schutz des Unternehmens im Vordergrund steht, sondern die Interessen der Allgemeinheit. Die Unverbindlichkeit von Handlungsempfehlungen sollte unter diesen Voraussetzungen ebenfalls herausgestellt werden.

Insofern kann bei Einhaltung dieser Voraussetzungen davon ausgegangen werden, dass nur ein minimales Haftungsrisiko bei einer nicht erfolgten Warnung bestünde. Dieses Ergebnis stimmt auch mit der Rechtsprechung des *BGH* in einem zumindest ähnlich gelagerten Fall überein, indem der Betreiber einer Seilbahn gegen das Land Bayern auf Ersatz der Schäden klagte, die ihm infolge eines Seilbahnunglücks entstanden waren.[308] Dabei berief sich der Kläger darauf, dass die staatliche Aufsicht über den Bau und Betrieb der Seilbahn auch der Minimierung seines eigenen unternehmerischen Risikos liege. Dies hatte jedoch keinen Erfolg: Der *BGH* entschied, die Überwachung diene vielmehr Allgemeininteressen und begründe kein besonderes Fürsorgeverhältnis zwischen Staat und Unternehmer. Das Seilbahnunglück liege ausschließlich im Risikobereich des Unternehmers. Dieser Gedankengang lässt sich auch auf die vorliegende Konstellation übertragen, in der der Staat das Monitoring zum Schutz der Allgemeinheit und deren Interessen durchführen würde.

4.7.4 Ergebnis

Ein kooperatives staatliches Monitoring würde für den Staat – sofern einerseits in der Norm ein gewisser Spielraum enthalten ist, wann der Staat warnen darf, und andererseits die Schutzzwecke eines staatlichen Monitorings genau beschrieben würde – nur zu geringen Haftungsrisiken führen. Das gilt sowohl für das Szenario einer Falsch- als auch einer Nichtwarnung. Während für Warnungen vor Sicherheitslücken und vor Schadprogrammen mit § 7 BSIG bereits eine Ermächtigungsgrundlage besteht, müsste eine Ermächtigungsgrundlage, die die Unternehmen zur Übermittlung der Daten für die Nutzung eines kooperativen Monitorings verpflichtet, erst geschaffen werden. Ob es in absehbarer Zeit jedoch zu einer derart intensiven Kooperation zwischen Staat und Wirtschaft kommen wird, bleibt abzuwarten.

[308] *BGH*, NJW 1965, 200.

5 Haftungsrechtliche Rahmenbedingungen bei dem Einsatz einer Software zur Informationsfusion und -klassifikation zur Erkennung von Botnetzen

In diesem Kapitel wird der Einsatz von MonIKA zur Detektion von Botnetzen rechtlich untersucht.

5.1 Untersuchungsgegenstand

Das MonIKA-Verfahren beschränkt sich jedoch nicht nur darauf, miteinander verbundenen Unternehmen die Möglichkeit zu bieten, durch eine Informationsfusion und –klassifikation ihre IT-Sicherheit zu verbessern. Vielmehr können mit Hilfe von MonIKA auch Botnetze identifiziert werden. Rechtliche Aspekte bei dem Einsatz von MonIKA zur Erkennung von Botnetzen werden im Folgenden am Anwendungsszenario „Spam-Kampagnen-Erkennung zur Klassifikation von Bots“ erörtert.

5.2 Sachverhalt

Im Anwendungsszenario „Spam-Kampagnen-Erkennung zur Klassifikation von Bots“ geht es darum, dass durch die Zusammenführung einer möglichst hohen Anzahl von E-Mails, die entweder durch den jeweiligen E-Mail-Provider oder den Empfänger selbst als Spam klassifiziert wurden, Rückschlüsse auf Spam-Kampagnen gewonnen werden. Spam-Kampagnen erfolgen mittels der mit einem Bot infizierten Rechner. Anhand der Untersuchung, ob Übereinstimmungen zwischen Spam-E-Mails bestehen, kann festgestellt werden, ob es sich um eine gezielte Spam-Kampagne handelt, die über ein Botnetz ferngesteuert wurde. Das

Clustering erscheint bei einer höheren Anzahl potentieller Spam-E-Mails wesentlich erfolgsversprechender. So deutet die Sendung einer Spam-E-Mail, die sich einer Kampagne zuordnen lässt, in hohem Maße darauf hin, dass der Sender mit einem Bot infiziert ist.

Für die E-Mail-Provider, die als Anwender auftreten, besteht der Vorteil, dass sie durch den Einsatz von MonIKA ihre eigenen Sender-Blacklists erweitern – also verbessern – können. Die frühzeitige Erkennung unerwünschter Nachrichten ermöglicht es ihnen, diese ressourcenschonend auszufiltern.[309] So wird Spam seit jeher als eines der wesentlichen Probleme bei der Nutzung des Internets angesehen und richtet erheblichen wirtschaftlichen Schaden an, den insbesondere die E-Mail-Provider tragen müssen.[310] Ihre Infrastruktur ist durch Spam-E-Mails einer Belastung in finanzieller, zeitlicher, und personeller Sicht ausgesetzt, sodass sie angehalten sind, Gegenmaßnahmen zu treffen.[311] Die E-Mail-Provider sind somit darauf angewiesen, effektive Filter einzusetzen, die die Flut unerwünschter E-Mails eindämmen können. Ihre Motivation liegt daher insbesondere darin, durch MonIKA die Abwehrmechanismen zu effektivieren.

Die Arbeit mit den Blacklists gilt immer noch als gängig und effektiv zur Abwehr von Spam-E-Mails. MonIKA fokussiert sich jedoch nicht auf den Betrieb der Blacklist selber, sondern bietet die Möglichkeit der Effektivierung. Damit ist MonIKA im Anwendungsfall „Spam-Kampagnen-Erkennung zur Klassifikation von Bots“ nicht den rechtlichen Risiken der E-Mail-Provider bei der Filterung von E-Mails ausgesetzt. Diese rechtlichen Risiken – insbesondere handelt es sich um strafrechtliche Risiken – wurden in der Literatur bereits ausführlich diskutiert.[312] Vor allem wird stets auf eine Strafbarkeit aus § 206 Abs. 2 Nr. 2 StGB (Verletzung des Post- und Fernmeldegeheimnisses) durch die Unterdrückung einer Nachricht sowie aus § 303a StGB (Datenveränderung) hingewiesen. MonIKA unterstützt lediglich die vorhandenen Strukturen und Instrumentarien, von deren Rechtskonformität vorliegend ausgegangen werden muss. Ihre rechtskonforme Ausgestaltung obliegt im Übrigen dem E-Mail-Provider selbst.

Die Zusammenführung und das darauf basierende Clustering werfen datenschutzrechtliche Fragen auf, die im Folgenden außen vor bleiben. Vielmehr ist

[309] *Heidrich*, CR 2009, 168 (168).
[310] Dazu *Tschoepe*, Heise Online-Recht, Abschnitt III. Rn. 100.
[311] *Hoeren*, NJW 2004, 3513 (3513).
[312] U. a. *Heidrich*, CR 2009, 168; *Heidrich/Tschoepe*, MMR 2004, 75; *Hoeren*, NJW 2004, 3513; *Spindler*/*Ernst*, CR 2004, 437.

unter haftungsrechtlichen Aspekten zu untersuchen, ob und wie der IT-Sicherheitsdienstleister, der den EvASC betreibt und den teilnehmenden E-Mail-Providern den MonIKA-Agenten zur Verfügung stellt, gegenüber Dritten und gegenüber dem E-Mail-Provider haften könnte, sofern es zu haftungsrelevanten Fällen kommt. Auch sind die strafrechtlichen Risiken für die Mitarbeiter der MonIKA GmbH und des E-Mail-Providers zu erörtern.

5.3 Stakeholder

Im Folgenden sollen die Stakeholder und ihre Rolle aufgezeigt werden.

5.3.1 E-Mail-Provider als MonIKA-Sender

Bei dem MonIKA-Sender handelt es sich um den E-Mail-Provider. Dieser bindet die MonIKA-Agenten, die ihm von dem IT-Sicherheitsdienstleister zur Verfügung gestellt werden, an seine Sensorik an. Dabei ist erforderlich, dass die Agenten auf die als Spam klassifizierten E-Mails Zugriff haben. Über die MonIKA-Agenten werden die Spam-E-Mails in verschlüsselter Form weitergeleitet. Es handelt sich dabei sowohl um von dem E-Mail-Provider als Spam klassifizierte E-Mails als auch von den Nutzern manuell als Spam eingeordnete E-Mails.

5.3.2 IT-Sicherheitsdienstleister als MonIKA GmbH

In dem vorliegenden Anwendungsfall wird – wie bereits im Anwendungsfall „Enterprise-Monitoring“ – davon ausgegangen, dass ein externer IT-Sicherheitsdienstleister MonIKA betreibt, indem bei ihm das EvASC angesiedelt ist. Bei dem IT-Sicherheitsdienstleister werden die E-Mails fusioniert und auf inhaltliche sowie strukturelle Übereinstimmungen überprüft. Ziel des IT-Sicherheitsdienstleisters ist dabei das Clustering der Spam-E-Mails, um damit die Zugehörigkeit der E-Mails zu einer Spam-Kampagne festzustellen. Dies lässt dann Rückschlüsse auf bestehende Botnetze zu. Der IT-Sicherheitsdienstleister stellt den E-Mail-Providern seine gewonnenen Erkenntnisse zur Verfügung, damit diese ihre Schutzvorkehrungen betreffend Spam erhöhen können.

5.3.3 E-Mail-Provider als MonIKA-Konsument

Der E-Mail-Provider stellt wieder zugleich MonIKA-Sender und MonIKA-Konsument dar. Durch die Zur-Verfügung-Stellung der Ergebnisse seitens der

MonIKA GmbH können die E-Mail-Provider Maßnahmen zum Schutz vor Spam-E-Mails treffen und insbesondere ihre bestehenden Blacklists erweitern.

5.3.4 Kunden des E-Mail-Providers

Weiterhin handelt es sich bei den Kunden des E-Mail-Providers um Stakeholder. Zum einen ist vorgesehen, dass die MonIKA GmbH auch auf Basis der von den Kunden als Spam markierten E-Mails arbeitet. Zum anderen hat der Kunde des E-Mail-Providers jeweils ein Interesse daran, dass an ihn adressierte E-Mails bei ihm ankommen und dass E-Mails, die er versendet, bei anderen ankommen, sich seine Adresse also auf keiner Blacklist befindet.

5.3.5 Externe

Als Externe sind Personenen zu nennen, die mit den Kunden der teilnehmenden E-Mail-Provider in Kontakt stehen und an diese E-Mails versenden. So besteht das Risiko, dass ihre E-Mails nicht bei dem Adressaten ankommen, wenn es zu fehlerhaften Analysen durch die MonIKA GmbH kommen sollte.

Weiterhin sind die Botmaster als Externe einzuordnen. Die Botmaster steuern das Botnetz und somit auch die mit Malware infizierten Computersysteme von Nutzern. Sie können das Botnetz u. a. dazu nutzen, um Spam-Kampagnen in Gang zu bringen.

5.4 Haftung

Die Frage nach der Haftung spielt auch in dem vorliegenden Szenario eine wichtige Rolle.

5.4.1 Haftungsrelevante Szenarien

Zunächst sind (nicht abschließend) haftungsrelevante Szenarien zu skizzieren.

Ein erstes haftungsrelevantes Szenario besteht darin, dass es durch die Übermittlung der E-Mails zu einem Datenleck kommt und es möglich ist, den Inhalt der E-Mails unverschlüsselt einzusehen. Dies kann sowohl auf einer Fehlkonfiguration durch die MonIKA GmbH als auch auf einer Fehlkonfiguration durch den E-Mail-Provider beruhen. Als Anspruchsteller kommen der Empfänger (Kunde des E-Mail-Providers) und der Absender in Betracht. Sofern sich in den E-

Mails vertrauliche Informationen befinden, von denen Dritte betroffen sind, können auch sie einen Schaden aufweisen und als Anspruchsteller auftreten. Ferner kann der E-Mail-Provider in Fällen, bei denen ein Fehler der MonIKA GmbH für das Datenleck ursächlich ist, selber als Anspruchsteller auftreten.

Ein zweites haftungsrelevantes Szenario besteht darin, dass E-Mails von Dritten auf Grund des Einsatzes von MonIKA nicht an die legitimen Adressaten (Kunden des E-Mail-Providers) zugestellt werden. Dies kann entweder damit im Zusammenhang stehen, dass die Dritten unberechtigt auf eine Blacklist geraten sind, die E-Mail anderweitig in Folge des Betriebs von MonIKA als Spam klassifiziert wird oder ein anderer Fehler auftritt, der mit MonIKA in Zusammenhang steht und es dem Kunden unmöglich macht, auf sein E-Mail-Konto zuzugreifen.

Denkbar erscheint es auch, dass die Kunden des E-Mail-Providers fälschlicherweise auf eine Blacklist geraten und in Folge dessen ihre E-Mails nicht mehr zugestellt werden können.

Anspruchsteller können stets der E-Mail-Provider selber, aber auch die Kunden des E-Mail-Providers sein. Diese sind aus Sicht der MonIKA GmbH ebenfalls Dritte. Zwar kann bei dem Vertrag, der zwischen E-Mail-Provider und IT-Sicherheitsdienstleister besteht, an einen Vertrag mit Schutzwirkung zugunsten Dritter gedacht werden. Dies scheitert allerdings an der Voraussetzung, dass der Kreis der geschützten Personen für den Schuldner vorhersehbar sein muss. Zwar kann auch ein großer Personenkreis im Umfang einer Massenveranstaltung einbezogen sein.[313] Die Anzahl der Kunden von E-Mail-Providern kann jedoch ohne Weiteres ein Vielfaches von 100.000 Nutzern übersteigen[314], sodass die Vorhersehbarkeit zu verneinen ist.

Als weitere mögliche Anspruchsteller kommen Dritte in Betracht, die von einem Datenleck betroffen sind oder deren E-Mails nicht zugestellt werden.

5.4.2 Zivilrechtliche Haftung

Bei der Beurteilung der zivilrechtlichen Haftung muss zwischen Ansprüchen unterschieden werden, die Kunden des E-Mail-Providers und Externe gegen die MonIKA GmbH geltend machen können, sowie solchen Ansprüchen, die der E-Mail-Provider in seiner Rolle als MonIKA-Sender und –Empfänger gegen die MonIKA GmbH geltend machen könnte.

[313] S. *BGH*, NJW 1965, 1757.
[314] Man denke an marktbeherrschende Anbieter wie GMX oder WEB.DE.

5.4.2.1 Mögliche Ansprüche Externer gegen die MonIKA GmbH

Externe weisen kein vertragliches Verhältnis zu der MonIKA GmbH auf, sodass ihnen keine vertraglichen, sondern nur gesetzliche Ansprüche zustehen können, also insbesondere solche aus dem Deliktsrecht. Ferner müssen die Regelungen aus dem TKG und dem BDSG berücksichtigt werden.

5.4.2.1.1 Deliktische Ansprüche

Für den Fall eines Datenlecks können den Betroffenen gegenüber der MonIKA GmbH Ansprüche aus § 823 Abs. 1 BGB zustehen. Die erforderliche Rechtsgutverletzung kann in diesem Fall in einer Verletzung des Allgemeinen Persönlichkeitsrechts liegen, sofern über diesen Weg persönliche Daten an die Öffentlichkeit gelangt sind.

Überdies muss sowohl bei einem Datenleck als auch bei einer verhinderten Zustellung und dem verhinderten Absenden von E-Mails mit geschäftlichem Bezug an die Verletzung des Rechts auf den eingerichteten und ausgeübten Gewerbebetrieb gedacht werden. Allerdings wird es regelmäßig an der Betriebsbezogenheit fehlen, da sich diese potenziellen Fehler bei dem Einsatz von MonIKA nicht gegen den Geschäftsbetrieb als solchen richten.

Problematisch aus Sicht der Geschädigten erscheint, dass über § 823 Abs. 1 BGB nicht das Vermögen als solches geschützt ist, sondern stets nur die Verletzung von einem der dort genannten Rechtsgüter. Reine Vermögensschäden können aber über § 823 Abs. 2 BGB i. V. m. der Verletzung eines Schutzgesetzes bestehen. Um Schutzgesetze, die durch das MonIKA-Verfahren verletzt sein könnten, handelt es sich bspw. bei § 202a StGB, § 202b StGB, § 206 Abs. 1 StGB, § 303a StGB und § 303b StGB. Sofern das Fernmeldegeheimnis verletzt ist, sind in § 1004 Abs. 1 BGB, § 823 Abs. 2 BGB i. V. m. § 206 Abs. 1 StGB und § 823 Abs. 1 BGB i. V. m. Art. 10 GG potenzielle Anspruchsgrundlagen zu sehen.

5.4.2.1.2 Ansprüche aus dem TKG

Weitere Ansprüche von Externenen (Dritte und Kunden des E-Mail-Providers) können sich aus § 44 Abs. 1 TKG ergeben. Bei § 44 Abs. 1 TKG handelt es sich um einen lex-specialis-Anspruch zu § 823 Abs. 2 BGB bzw. § 1004 BGB, ohne dass diese Ansprüche verdrängt werden.[315] Voraussetzung ist stets eine Verletzung des Fernmeldegeheimnisses. Bei E-Mail-Providern, die – sofern es um die

[315] *Ditscheid/Rudloff*, in: Spindler/Schuster, Recht der elektronischen Medien, § 44 TKG Rn. 4.

Nachrichtenübermittlung geht – als unter das TKG fallende Diensteanbieter i. S. d. § 3 Nr. 24 TKG anzusehen sind[316], ist § 88 Abs. 1 TKG zu beachten. Danach unterliegen dem Fernmeldegeheimnis der Inhalt der Telekommunikation und die näheren Umstände.

Fraglich ist, ob die MonIKA GmbH für den Fall der Durchführung eines Monitorings- und Klassifikationsverfahrens zur Erkennung von Botnetzen durch die Untersuchung von Spam-E-Mails auch als Diensteanbieter i. S. d. TKG einzuordnen ist. Der Begriff des Diensteanbieters ergibt sich aus § 3 Nr. 6 TKG. Diensteanbieter ist danach jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt (lit. a) oder an der Erbringung solcher Dienste mitwirkt (lit. b). Aus der Regelung, die ihrerseits auf § 3 Nr. 10 TKG verweist, wird geschlossen, dass eine Gewinnerzielungsabsicht nicht erforderlich ist[317], die aber bei einem Unternehmen, das IT-Sicherheitsdienstleistungen erbringt, ohnehin gegeben sein wird. Für die MonIKA GmbH ist vielmehr von Relevanz, dass auch solche Unternehmen, die Infrastrukturleistungen erbringen, unter den Diensteanbieterbegriff des TKG fallen.[318] Eine rechtliche Einordnung des IT-Sicherheitsdienstleisters als unternehmenseigener Erfüllungsgehilfe scheint nicht ausgeschlossen, doch auch diese können als Diensteanbieter qualifiziert werden.[319] Somit muss auch seitens der MonIKA GmbH das TKG beachtet werden.

Nach § 44 TKG besteht bei Verstößen gegen die Vorschriften des TKG ein Anspruch des Betroffenen auf Beseitigung und bei Wiederholungsgefahr auf Unterlassung. § 88 TKG hat – wie Art. 10 GG – den Schutz des Fernmeldegeheimnisses zum Ziel und kann auch als einfachgesetzliche Ausprägung des Fernmeldegeheimnisses nach Art. 10 GG bezeichnet werden.[320]

Nach § 88 Abs. 3 Satz 1 TKG ist es Anbietern von Telekommunikationsdiensten untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste (einschließlich des Schutzes ihrer technischen Systeme) erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. § 88 Abs. 3 Satz 3 TKG untersagt die Weitergabe von Kenntnissen, die dem Fernmeldegeheimnis unterliegen, an Dritte.

---

[316] *Redeker*, in: Hoeren/Sieber/Holznagel, Teil 12 Rn. 217 f.
[317] *Holznagel/Ricke*, in: Spindler/Schuster, Recht der elektronischen Medien, § 3 TKG Rn. 8.
[318] *Fetzer*, in: Arndt/Fetzer/Scherer, § 3 Rn. 22.
[319] *Holznagel/Ricke*, in: Spindler/Schuster, Recht der elektronischen Medien, § 3 TKG Rn. 8.
[320] *Bock*, in: Geppert/Schütz, TKG, § 88 Rn. 1.

§ 88 Abs. 2 TKG verpflichtet ausschließlich den Diensteanbieter als Anspruchsgegner für einen Anspruch aus § 44 Abs. 1 TKG i. V. m. § 88 Abs. 1 TKG. Daher können sowohl der E-Mail-Provider als auch die MonIKA GmbH Ansprüchen ausgesetzt sein.

Es stellt sich die Frage, ob auf Seiten der MonIKA GmbH Rechtfertigungsgründe eingreifen könnten. Eine Durchbrechung des Fernmeldegeheimnisses ist gem. § 88 Abs. 3 Satz 3 TKG jedoch nur dann erlaubt, wenn eine gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Dem Wortlaut der Norm folgend ist also davon auszugehen, dass allgemeine Rechtfertigungsgründe etwaige Verstöße nicht rechtfertigen können und nur Sondertatbestände anwendbar bleiben.

5.4.2.1.3 Ansprüche aus dem BDSG

Weiterhin kann sich aus § 7 BDSG ein Schadensersatzanspruch ergeben, sofern personenbezogene Daten betroffen sind. Es handelt sich bei § 7 BDSG um eine eigenständige Haftungsnorm, deren Haftungsmodalitäten sich aus dem allgemeinen Schuldrecht ergeben.[321] Das bedeutet auch, dass der Schuldner für Vorsatz und Fahrlässigkeit entsprechend § 276 BGB haftet. Dabei gilt die Verschuldensvermutung aus § 280 Abs. 1 Satz 2 BGB zugunsten des Gläubigers.[322]

5.4.2.1.4 Zwischenergebnis

Es ist zu bilanzieren, dass in sämtlichen Haftungsszenarien auch tatsächlich das Risiko einer Haftung liegt. Daher sollte ihr Eintritt vermieden werden. Im besonderen Maße ist auch das Fernmeldegeheimnis zu berücksichtigen, da die im TKG vorgesehenen Ansprüche für etwaige Betroffene weitere Ansprüche darstellen, die sie gegenüber der MonIKA GmbH geltend machen könnten.

5.4.2.2 Eigene Ansprüche des E-Mail-Providers gegen die MonIKA GmbH

Zwischen dem E-Mail-Provider und der MonIKA GmbH besteht ein Vertrag darüber, dass die MonIKA GmbH gegen Entgelt bestimmte Dienste verrichtet. Parallel zu dem Ergebnis im Anwendungsfall „Enterprise-Monitoring“ sprechen die besseren Gründe für die Einordnung des Vertrags als Dienst- und nicht als Werkvertrag.[323] Im Mittelpunkt steht, dass die MonIKA GmbH die ihr seitens des E-Mail-Providers zur Verfügung gestellten Spam-E-Mails untersucht und sie mit den

[321] *Gola/Schomerus*, in: Gola/Schomerus, BDSG, § 7 Rn. 1.
[322] *Gola/Schomerus*, in: Gola/Schomerus, BDSG, § 7 Rn. 8 f.
[323] S. oben unter 4.5.1.

von anderen Teilnehmern zur Verfügung gestellten Spam-E-Mails vergleicht, clustert und Rückschlüsse auf Spam-Kampagnen durch bestehende Botnetze gewinnt. Ihre Erkenntnisse stellt sie den teilnehmenden E-Mail-Providern zur Verfügung, damit diese ihre Blacklists verbessern und weitere Schutzmaßnahmen treffen können.

Für den Fall eines Datenlecks können nicht nur Ansprüche Externer bestehen, sondern auch der betroffene E-Mail-Provider kann Schadensersatzansprüche geltend machen, sollte er einen Schaden haben. So handelt es sich auch gegenüber dem E-Mail-Provider um eine Pflichtverletzung, wenn Daten an die Öffentlichkeit gelangen sollten. Der sorgsame Umgang mit den übermittelten Daten kann, wenn nicht schon als Hauptleistungspflicht zumindest als Nebenpflicht i. S. d. § 241 Abs. 2 BGB gesehen werden, wenn es sich um einen Vertrag zur Erbringung von IT-Sicherheitsdienstleistungen handelt.

Ebenfalls kann eine Pflichtenverletzung darin zu sehen sein, wenn Kunden des E-Mail-Providers unberechtigt auf die Blacklists geraten oder an sie adressierte E-Mails in Folge der Hinweise der MonIKA GmbH nicht zugestellt werden können. Jedoch ist auch zu beachten, dass der MonIKA GmbH ein gewisser Spielraum für falsche Annahmen verbleiben muss, da ansonsten ihr Haftungsrisiko ungemein hoch wäre. Daher sollte in dem Vertrag zwischen den Beteiligten u. a. festgelegt werden, welche Leistungen mit welcher Qualität und ggf. welchem Fehlerspielraum erwartet werden. Dies kann in einem Service-Level-Agreement genauer bestimmt werden und obliegt den Verhandlungen der Parteien.

Sofern die so festgelegten Pflichten mit den entsprechenden Qualitätsanforderungen nicht eingehalten werden, stehen dem E-Mail-Provider vertragliche Schadensersatzansprüche aus § 280 Abs. 1 BGB zu. Wenn es in Folge von Fehlern, die auf dem Betrieb von MonIKA beruhen, zu einer Datenlöschung kommt, ist neben vertraglichen Ansprüchen auch an den deliktischen Anspruch aus § 823 Abs. 1 BGB zu denken, sofern die Daten auf einem magnetischen Datenträger verkörpert sind und daher als Eigentum qualifiziert werden können.[324] Allerdings würde dem E-Mail-Provider ein Mitverschulden anzulasten sein, sofern er vor umfangreicheren Installationen oder sonstigen Maßnahmen keine Sicherungsvorkehrungen träfe. Der rechtliche Umgang mit entsprechend vorhersehbaren Fällen kann ebenfalls in einer im Vorfeld getroffenen Vereinbarung geklärt werden.

[324] So zuletzt *OLG Oldenburg*, ZD 2012, 177.

5.4.2.3 Ausgleichsansprüche des E-Mail-Providers gegen die MonIKA GmbH

Beachtet werden muss, dass dem E-Mail-Provider Ausgleichsansprüche gegen die MonIKA GmbH zustehen könnten.

5.4.2.3.1 Verantwortlichkeit des E-Mail-Providers gegenüber dem Kunden

Der Kunde des E-Mail-Providers wird in o. g. Haftungsszenarien vornehmlich Schadensersatzansprüche gegen den E-Mail-Provider und nicht gegen die MonIKA GmbH geltend machen. Dies erscheint aus dem Grund naheliegend, dass zwischen dem E-Mail-Provider und dem Kunden ein Vertrag besteht und der Kunde von der MonIKA GmbH in den überwiegenden Fällen überhaupt keine Kenntnis haben wird.

5.4.2.3.1.1 Rechtsverhältnis zwischen E-Mail-Provider und Kunde

Zunächst ist ein genauerer Blick auf das rechtliche Verhältnis zwischen E-Mail-Provider und Kunden zu werfen. Zwischen diesen besteht ein sog. E-Mail-Providervertrag. Es findet sich zum E-Mail-Providervertrag keine Regelung im BGB, weshalb Rückgriff auf die allgemeinen Vertragsarten des BGB zu nehmen ist. Ähnlich wie beim Access-Provider-Vertrag sind sich Rechtsprechung und Literatur uneins über die genaue Einordnung, wobei Dienst-, Werk- und Mietvertrag in Rede stehen. Der E-Mail-Provider schuldet jedenfalls die Übermittlung der Nachrichten von seinem Vertragspartner an Dritte bzw. von Dritten an seinen Vertragspartner. Diese Leistung steht im Mittelpunkt. Für alle in Betracht kommenden Vertragstypen lassen sich Argumente finden. Interessant ist auch, dass vielmals nach verschiedenen Kriterien unterschieden wird: So etwa zwischen der Lagerung von Nachrichten in der Mailbox oder etwa dem Versand innerhalb eines Netzes bzw. in ein fremdes Netz.

Das Postfach, in dem die Nachrichten gespeichert werden, lässt sich dabei nach den Regeln des Mietvertrages behandeln,[325] wobei die Einordnung dieses Teils als Werkvertrag ebenfalls nicht ausgeschlossen erscheint[326]. Als werkvertragliches Element kann die Verpflichtung zur korrekten Übergabe von Nachrichten zwischen dem eigenen Netzwerk des Betreibers und dem Internet angesehen werden.[327] Auch die komplette Übermittlung eigener Nachrichten bzw. die jederzeitige Möglichkeit, eingehende E-Mails zu empfangen, kann als Werkvertrag eingeordnet werden.[328]

[325] Etwa *Härting*, CR 2001, 37 (41).
[326] Vertreten von *Spindler*, Vertragsrecht der Internet-Provider, Teil IV Rn. 140 ff.
[327] *Redeker*, IT-Recht, Rn. 1091.
[328] So *Redeker*, IT-Recht, Rn. 1091.

Überlegenswert erscheint es ferner, die *BGH*-Rechtsprechung zu Access-Provider-Verträgen[329] – diese werden vom *BGH* als Dienstverträge i. S. d. §§ 611 ff. BGB eingestuft – heranzuziehen und den E-Mail-Provider-Vertrag unter Hinweis auf die fehlende Einflussmöglichkeit des E-Mail-Providers auf einen Empfang versendeter Nachrichten (insbesondere in fremde Netze[330]) und beschränkter Leistungskapazitäten ebenfalls als Dienstvertrag zu qualifizieren.[331]

Unabhängig von der konkreten Qualifikation der Vertragsnatur ist es maßgeblich, dass jedenfalls ein Vertrag zwischen dem E-Mail-Provider und dem Kunden besteht. Einigkeit besteht nämlich darüber, dass der E-Mail-Provider die Speicherung der E-Mails in dem digitalen Postfach des Nutzers schuldet.

5.4.2.3.1.2 Vertragliche Nebenpflicht zur Spam-Filterung

Fraglich erscheint, ob sich aus dem E-Mail-Providervertrag eine (Neben-)Pflicht zur Filterung von Spam ergibt. Wurde noch Anfang bis Mitte der 2000er-Jahre keine Pflicht des E-Mail-Providers zur Spam-Filterung unter Hinweis auf die berechtigten Erwartungen des Nutzers sowie eine fehlende Selbstverständlichkeit von Filterungsmaßnahmen angenommen[332], ist mittlerweile von einer Pflicht zur Filterung auszugehen.

Das Bestehen einer Nebenpflicht hängt vom jeweiligen Schuldverhältnis, der Verkehrssitte und den Anforderungen des redlichen Geschäftsverkehrs ab.[333] Dabei gewinnen die Nebenpflichten umso mehr an Gewicht, je mehr die Fachkunde einer Partei gefragt ist und je größer die Gefahren sind, denen die Parteien ausgesetzt sind.[334] Die Kategorisierung von Nebenpflichten erfolgt in Schutzpflichten im engeren Sinne, Aufklärungspflichten, Loyalitätspflichten und leistungssichernden Nebenpflichten. Schutzpflichten werden auch als Fürsorge- und Obhutspflichten bezeichnet. Entscheidend für die Annahme solcher Pflichten ist, dass nicht das Erhaltungsinteresse, sondern das Leistungsinteresse betroffen ist.[335] Die Spam-Filterung könnte somit als Schutz- bzw. Obhutspflicht klassifiziert werden, da der eigentliche Vertragsgegenstand in der Übermittlung von E-Mails sowie deren Speicherung gesehen werden kann. Die Filterung von Spam-E-Mails dient nicht

[329] *BGH*, MMR 2005, 373.
[330] *Spindler*, Vertragsrecht der Internet-Provider, Teil IV Rn. 140 ff.
[331] Ohne nähere Erläuterung *OLG Naumburg*, K&R 2014, 41; *Müller*/*Bohne*, Providerverträge, A. I. 5. § 1.
[332] *Ernst*, Vertragsgestaltung im Internet, Rn. 590; *Spindler*/*Ernst*, CR 2006, 437 (442).
[333] *BGH*, NJW 2010, 1135; *Grüneberg*, in: Palandt, BGB, § 241 Rn. 7.
[334] *Schulze*, in: Schulze et al., BGB, § 241 Rn. 5.
[335] *Bachmann*/*Roth*, in: MüKo BGB, § 241 Rn. 54 f.

diesem Vertragsgegenstand, sondern soll die übrigen Interessen und Rechte des Kunden schützen.

Um eine Schutzpflicht zu bejahen, müssen folgende Kriterien vorliegen: Erstens muss ein Wissens- bzw. Machtgefälle zwischen den Parteien bestehen und zweitens müssen die gefährdeten Rechtsgüter schwerer wiegen als der zu betreibende Aufwand, um diese Gefährdung zu beseitigen.[336]

Ein Machtgefälle zwischen E-Mail-Provider und Kunde ist unschwer zu bejahen. Die technischen Möglichkeiten eines E-Mail-Providers übersteigen diejenigen des Kunden.[337] Die prinzipielle Schutzwürdigkeit der betroffenen Partei ergibt sich bereits aus den sonderverbindungsspezifischen Einwirkungsmöglichkeiten des anderen.[338] Es ist somit zwischen der Gefährdung der Rechtsgüter und dem Risikobeseitigungsaufwand abzuwägen.

Auf Seiten des Kunden droht eine massive Beeinträchtigung seiner E-Mail-Kommunikation, da diese erschwert und im Extremfall gar unmöglich sein kann. Jedenfalls drohen massive Zeitverluste und infolge dessen u. U. auch wirtschaftliche Einbußen. Teilweise sind die Spam-E-Mails auch mit Viren verseucht. Durch das Öffnen einer im Anhang befindlichen Datei können Schäden an der Hardware des Rechners entstehen und/oder Daten vernichtet werden. Der Aufwand seitens des E-Mail-Providers, durch ein automatisiertes Filterungsprogramm Spam zu identifizieren und dadurch dieser Gefährdung zu begegnen, hält sich hingegen in Grenzen, wenn es sich um „offensichtlichen Spam“ handelt. Dies ist ihm somit zumutbar. Zwar lässt sich darüber diskutieren, in welchen Fällen „offensichtlicher Spam“ anzunehmen ist, jedenfalls liegt dieser aber vor, wenn der E-Mail-Provider über deutliche Hinweise auf eine Spam-Aktivität verfügt. Entsprechende Maßnahmen wird er nämlich schon aus dem eigenen Interesse an einer möglichst ressourcenschonenden Arbeit vornehmen. Spam hat zudem eine derart hohe wirtschaftliche und gesellschaftliche Bedeutung erlangt, dass durchaus die berechtigte Erwartung des Nutzerkreises besteht, dass der E-Mail-Provider gewisse Vorkehrungen trifft, um den Nutzer möglichst „spamfrei“ zu halten. Der Einsatz von Spam-Filtern gilt heutzutage also als verkehrsüblich, was ein weiteres Argument für die Annahme einer Schutzpflicht darstellt.[339] Somit ist eine Schutzpflicht zur Filterung von solchen Nachrichten, die auf Grund von Hinweisen, auf die der E-

[336] *Olzen*, in: Staudinger, BGB, § 241 Rn. 486, 487.
[337] *Spindler*/*Ernst*, CR 2004, 442.
[338] *Olzen*, in: Staudinger, BGB, § 241 Rn. 487.
[339] *Redeker*, in: Hoeren/Sieber/Holznagel, Teil 12 Rn. 102; *Spindler/Ernst*, CR 2004, 441.

Mail-Provider Zugriff hat oder denen er sich bei normaler Aufmerksamkeit nicht verwehren kann, eindeutig als Spam identifiziert werden können, zu bejahen. Entscheidend ist, dass die Spam-Filter rechtskonform ausgestaltet sind, da ansonsten zivil-, aber vor allem strafrechtliche Risiken bestehen.

Den E-Mail-Provider trifft damit eine vertragliche Nebenpflicht zur (gesetzeskonformen) Spam-Filterung.

5.4.2.3.2 Haftung des E-Mail-Providers gegenüber dem Kunden

Bei den in 5.4.1 geschilderten Szenarien liegt ein Verstoß gegen Aufbewahrungspflichten (durch Löschung und Verlust), gegen die Pflicht zur Übermittlung von Nachrichten (bei Fehlgeraten auf eine Blacklist) und gegen die Bereitstellungspflicht (kein Zugriff auf E-Mail-Konto[340]) vor.

Allerdings würde – eine kausale Handlung der MonIKA GmbH vorausgesetzt für die Pflichtverletzung – gar nicht der E-Mail-Provider selber, sondern die MonIKA GmbH gegen diese vertraglichen Pflichten verstoßen. Bei der MonIKA GmbH handelt es sich jedoch um einen Erfüllungsgehilfen i. S. d. § 278 BGB, da sie eingesetzt wird, um den Pflichten zur Bereitstellung eines möglichst spamfreien E-Mail-Postfachs und zur Spam-Filterung generell nachzukommen. Fehler, die im Rahmen des Betriebs von MonIKA entstehen, stehen in einem inneren Zusammenhang mit der Pflichterfüllung. Somit muss sich der E-Mail-Provider die zur Pflichtverletzung führende Handlung der MonIKA GmbH zurechnen lassen.

In Betracht kommt ferner ein Anspruch des Kunden gegen den E-Mail-Provider aus § 831 Abs. 1 Satz 1 BGB, sofern die MonIKA GmbH als Verrichtungsgehilfe und der E-Mail-Provider als Geschäftsherr einzuordnen sind. Dies ist jedoch abzulehnen, da die MonIKA GmbH nicht weisungsabhängig von dem E-Mail-Provider tätig ist. Bei ihr handelt es sich um ein selbstständiges Unternehmen, das aus dem Anwendungsbereich des § 831 BGB herausfällt[341].

Zu beachten ist, dass der E-Mail-Provider seine Haftung gegenüber dem Kunden – auch für Erfüllungsgehilfen – auf grobe Fahrlässigkeit und Vorsatz begrenzen kann, sofern dem Vertrag rechtswirksame AGB zugrunde liegen. Für die in § 309 Nr. 7 lit. a BGB genannten Rechtsgüter Leben, Körper und Gesundheit gilt diese Einschränkung nicht, wobei eine Gefährdung dieser Rechtsgüter in denkbaren

[340] Dazu *OLG Naumburg*, K&R 2014, 41.
[341] *Wagner*, in: MüKo BGB, § 831 Rn. 16.

Haftungskonstellationen eher fernliegend erscheint. Auch eine Begrenzung auf Mangelschäden wird von der Rechtsprechung bei hinreichend klarer Formulierung für zulässig erachtet.[342]

5.4.2.3.3 Möglichkeit der Schadloshaltung für den E-Mail-Provider durch Ausgleichsansprüche

Sofern der E-Mail-Provider auch gegenüber dem Kunden haften würde, kann er über Ausgleichsansprüche aus einer Gesamtschuldnerschaft, in der er mit der MonIKA GmbH stünde, gegen diese vorgehen. Sämtliche Merkmale des § 421 BGB sind erfüllt. Insbesondere ist es unschädlich, dass der E-Mail-Provider aus Vertrag und die MonIKA GmbH aus Delikt haftet, da die Leistungsidentität ausreicht und die Befriedigung desselben Leistungsinteresses maßgeblich ist.[343]

Im Innenverhältnis steht dem E-Mail-Provider, sollte er von dem Kunden herangezogen worden sein, ein Ausgleichsanspruch aus § 426 Abs. 1 BGB zu. Mangels anderer Regelung besteht dieser in der Höhe des Verschuldensanteils durch die MonIKA GmbH. § 426 Abs. 1 BGB schließt dabei nicht aus, dass ggf. ein Ausgleichsanspruch in voller Höhe besteht.[344]

Vertraglich bietet es sich an, bereits im Vorfeld Regelungen für den Umgang mit Schadensfällen von Kunden des E-Mail-Providers zu treffen. Es geht dabei um die Frage, wer im Innenverhältnis unter welchen Umständen für entstehende Schäden aufkommt. Denkbar ist etwa eine Regelung, nach der die Haftung der MonIKA GmbH, die ja nur unterstützend tätig wird, auf Vorsatz und grobe Fahrlässigkeit begrenzt wird. Eine andere Möglichkeit besteht darin, dass sie nur in bestimmten Fallkonstellationen, die technisch möglichst genau umschrieben werden müssten, haftet. Es besteht Vertragsfreiheit und derartige Fragen sind Verhandlungssache der Parteien.

5.4.2.3.4 Ergebnis

Für oben geschilderte Fälle besteht eine Haftung der MonIKA GmbH gegenüber den Kunden des E-Mail-Providers. Betont werden muss, dass der Kunde vielmals zunächst gegen seinen Vertragspartner, also den E-Mail-Provider, vorgehen wird, sofern ihm ein Schaden entstanden ist, der nicht zugunsten des E-Mail-Providers durch AGB ausgeschlossen ist. Dem E-Mail-Provider wird regelmäßig ein, wenn

[342] *BGH*, NJW-RR 1989, 953 (956).
[343] *Bydlinski*, in: MüKo BGB, § 421 Rn. 5.
[344] *Bydlinski*, in: MüKo BGB, § 426 Rn. 14.

auch nur geringes, Mitverschulden anzulasten sein. MonIKA GmbH und E-Mail-Provider sind dann Gesamtschuldner. In einem Vertrag zwischen ihnen sollte bereits der Umgang mit vorhersehbaren Szenarien geregelt sein.

5.4.3 Strafrechtliche Risiken für die Mitarbeiter des E-Mail-Providers

Es erscheint fraglich, ob die Übermittlung der als Spam klassifizierten E-Mails (durch Spam-Filter oder nach manueller Sortierung durch den Kunden) an die MonIKA GmbH unter strafrechtlichen Gesichtspunkten rechtskonform ist. Die Problematik liegt darin, dass die Daten dann an einen – aus der Perspektive von E-Mail-Provider und Kunden – Dritten übermittelt werden. Die MonIKA GmbH ist als rechtlich selbstständig einzuordnen bzw. kann nicht mehr zu dem E-Mail-Provider gezählt werden.

Die Übermittlung wird von MonIKA vorausgesetzt und von dem E-Mail-Provider durchgeführt. Als Täter kommen die Mitarbeiter des E-Mail-Providers in Betracht. Die Problematik, dass E-Mails zum Zwecke der Verbesserung der IT-Sicherheit an einen Dritten übermittelt werden, ist – soweit ersichtlich – bis dato noch nicht Gegenstand juristischer Untersuchungen gewesen. Der Fall stellt sich auch anders dar, als die Frage, ob Spam- oder Viren-E-Mails gefiltert und gelöscht werden dürfen.

5.4.3.1 Strafbarkeit nach § 202a Abs. 1 StGB

Zunächst ist an eine Strafbarkeit aus § 202a Abs. 1 StGB zu denken.

Der E-Mail-Provider könnte durch die Übermittlung der als Spam klassifizierten E-Mails der MonIKA GmbH Daten i. S. v. § 202a StGB verschaffen. Nach § 202a Abs. 1 StGB macht sich strafbar, wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft.

Eine Strafbarkeit nach § 202a StGB erfordert, dass die Daten nicht für den Täter bestimmt sind. Entscheidend ist daher, ob die als Spam klassifizierten E-Mails für den E-Mail-Provider und seine Mitarbeiter bestimmt sind. Daten sind für eine Person bestimmt, wenn sie nach dem Willen des Berechtigten im Zeitpunkt der Tathandlung in den Herrschaftsbereich dieser Person gelangen sollen.[345] Es spielt keine Rolle, ob der Täter möglicherweise Eigentümer des Datenträgers ist, auf dem

[345] *Kühl*, in: Lackner/Kühl, StGB, § 202a Rn. 3.

sich die Daten befinden, oder ob sie sich inhaltlich auf den Täter beziehen[346], sodass die Mitarbeiter des E-Mail-Providers nicht aus diesem Grund als Berechtigte anzusehen sind. Strafbar macht sich auch derjenige, der auf ihn selber bezogene Daten abruft, die aber von einem anderen abgespeichert worden sind.[347] Es kommt auf die Rechtsmacht zur Verfügung über die Daten an.[348] Dies ist bei gespeicherten Daten derjenige, der die Daten abgespeichert hat.[349] Berechtigter bei übermittelten Daten ist die übermittelnde Stelle und nach Erhalt der Datenempfänger.[350] Das Bestimmungsrecht ist übertragbar.[351] Daher ist der E-Mail-Provider als Berechtigter in diesem Sinne anzusehen und die E-Mails sind für ihn i. S. v. § 202a StGB bestimmt, solange der Empfänger die jeweilige E-Mail noch nicht erhalten haben sollte.

Allerdings wurde – soweit ersichtlich – weder in der Rechtsprechung noch in der Literatur bisher thematisiert, wer als Berechtigter i. S. v. § 202a StGB anzusehen ist, wenn ein Nutzer die E-Mails zwar abgerufen und ggf. abgespeichert haben sollte, aber die E-Mails auch weiterhin auf dem Server des E-Mail-Providers bereitgehalten werden (z. B. bei der Nutzung des IMAP-Verfahrens). Der Empfänger von Daten, die für ihn zum Abruf bereitgehalten werden, wird erst dann zum Berechtigten, wenn er von seinem Abrufsrecht Gebrauch macht.[352] Daraus kann geschlossen werden, dass der Empfänger im Rahmen des IMAP-Verfahrens dann Berechtigter wird, sobald er das erste Mal die betreffende E-Mail abgerufen hat, unabhängig davon, ob er die E-Mail auf dem Server des E-Mail-Providers belässt. Jedenfalls bis zu diesem Zeitpunkt dürfte der E-Mail-Provider als Berechtigter anzusehen sein und eine Strafbarkeit dürfte an dem Tatbestandsmerkmal „nicht für ihn bestimmt“ scheitern. Für noch nicht abgerufene E-Mails besteht also schon auf Grund des Scheiterns an diesem Tatbestandsmerkmal kein Strafbarkeitsrisiko.

Bei bereits abgerufenen E-Mails scheitert eine Strafbarkeit aus § 202a StGB an dem Erfordernis einer besonderen Zugangssicherung, die für den E-Mail-Provider nicht besteht.[353] § 202a StGB erfordert jedoch gerade die Überwindung von Zugangssicherungen.

---

[346] *Lenckner/Eisele*, in: Schönke/Schröder, StGB, § 202a Rn. 6.
[347] *Kargl*, in: Kindhäuser/Neumann/Paeffgen, StGB, § 202a Rn. 7.
[348] *Fischer*, StGB, § 202a Rn. 7.
[349] *Lenckner/Eisele*, in: Schönke/Schröder StGB § 202a Rn.6.
[350] BayObLG JR 1994, 477; *Graf*, in: MüKo StGB, § 202a Rn. 19; *Kargl*, in: Kindhäuser/Neumann/Paeffgen, StGB, § 202a Rn. 7.
[351] *Graf*, in: MüKo StGB, § 202a Rn. 20.
[352] *Lenckner/Eisele*, in: Schönke/Schröder, StGB, § 202a Rn. 6.
[353] *Spindler/Ernst*, CR 2004, 437 (439).

Das Risiko einer Strafbarkeit nach § 202a Abs. 1 StGB durch die Übermittlung an einen Dritten in Form der MonIKA GmbH ist daher als gering einzustufen. Hinzu kommt, dass das Bestimmungsrecht i. S. v. § 202a StGB übertragbar ist, sodass sich der E-Mail-Provider dies auch zusätzlich von seinen Kunden einräumen lassen sollte, um das Risiko einer Strafbarkeit nach § 202a Abs. 1 StGB weiter zu verringern. Mit der Übertragung des Bestimmungsrechts ist gesichert, dass auch bereits abgerufene und manuell als Spam qualifizierte E-Mails übermittelt werden können, ohne dass eine Strafbarkeit aus § 202a StGB droht. Ob es der Kunde gestattet, dass die manuell als Spam qualifizierte E-Mail im Rahmen von MonIKA genutzt wird, könnte für jede einzelne E-Mail durch einen Disclaimer abgefragt werden. Vorstellbar ist auch, dass sich der E-Mail-Provider das Recht zur Übertragung durch (eine Erweiterung der) Nutzungsbedingungen und/oder der Datenschutzerklärung einräumen lässt. Dabei handelt es sich dann um AGB.[354]

5.4.3.2 Strafbarkeit nach § 206 Abs. 2 Nr. 1 StGB

Eine Strafbarkeit nach § 206 Abs. 2 Nr. 1 StGB scheitert daran, dass sich die Norm auf körperliche Gegenstände bezieht – E-Mails sind daher nicht erfasst.[355]

5.4.3.3 Strafbarkeit nach § 206 Abs. 1 StGB

Ferner muss untersucht werden, ob die Übermittlung der Nachricht an die MonIKA GmbH den Tatbestand des § 206 Abs. 1 StGB erfüllen könnte. § 206 Abs. 1 StGB stellt es unter Strafe, Mitteilungen über Tatsachen zu machen, die dem Post- oder Fernmeldegeheimnis unterliegen und die dem Täter als Inhaber oder Beschäftigter eines Unternehmens bekannt geworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt.

5.4.3.3.1 Strafrechtliches Subjekt

Für eine Strafbarkeit nach § 206 Abs. 1 StGB müssen die Mitarbeiter des E-Mail-Providers zunächst taugliche Täter sein. Dazu muss es sich bei dem E-Mail-Provider um ein Unternehmen handeln, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt. Sowohl nach dem funktionalen Unternehmensbegriff als auch nach dem institutionellen Unternehmensbegriff[356] ist ein E-Mail-Provider, der an MonIKA teilnähme, als Unternehmen im Sinne von

[354] So *LG Berlin*, U. v. 19.11.2013 – Az. 15 O 402/12 (nicht veröffentlicht).
[355] *Lenckner/Eisele*, in: Schönke/Schröder, StGB, § 206 Rn. 17.
[356] Zum funktionalen und institutionellen Unternehmensbegriff *Altenhain*, in: MüKo StGB, § 206 Rn. 13 f.

§ 206 Abs. 1 StGB erfasst. Unter der geschäftsmäßigen Erbringung von Post- oder Telekommunikationsdiensten ist das nachhaltige Betreiben der Beförderung von Postsendungen oder Anbieten von Telekommunikation gegenüber Dritten mit oder ohne Gewinnerzielungsabsicht zu verstehen.[357] Auch hieran bestehen bei einem E-Mail-Provider keine Zweifel. Dadurch, dass keine Gewinnerzielungsabsicht bestehen muss, sind insbesondere auch solche E-Mail-Provider erfasst, die ihre Dienste kostenfrei anbieten.[358] Bei dem E-Mail-Provider werden i. d. R. Beschäftigte und nicht die ebenfalls von § 206 Abs. 1 StGB erfassten Inhaber operativ tätig sein. Unter Beschäftigten sind jedenfalls sämtliche Mitarbeiter des Unternehmens zu verstehen,[359] sodass es sich bei den für einen E-Mail-Provider tätigen Personen um Täter des § 206 Abs. 1 StGB handeln kann.

5.4.3.3.2 Tatsachen

Erforderlich ist, dass der Gegenstand der Mitteilung an die andere Person eine oder mehrere Tatsache(n) ist/sind, die dem Post- und Fernmeldegeheimnis unterliegen. Jede Handlung, die zur Kenntniserlangung durch eine andere Person führt, ist eine Mitteilung.[360] Hierzu ist es ausreichend, wenn dem Dritten die Gelegenheit zur Kenntnisnahme verschafft wird.[361]

Ob die Tatsache dem Post- und Fernmeldegeheimnis unterliegt, beurteilt sich nach § 206 Abs. 5 StGB. In der vorliegenden Konstellation sind dabei lediglich die das Fernmeldegeheimnis betreffenden Sätze 2 und 3 des § 206 Abs. 5 StGB relevant, die § 88 Abs. 1 TKG nachgebildet sind. Schutz durch das Fernmeldegeheimnis genießen alle tatsächlichen Teilnehmer am Fernmeldeverkehr, wobei auch die Nutzung des Fernmeldewesens zu strafbaren oder sonst rechtswidrigen Zwecken erfasst ist[362], wie es bei Spam-Kampagnen durch Botnetze der Fall ist. Der Schutz richtet sich auch auf den Inhalt der Telekommunikation i. S. v. § 3 Nr. 22 TKG und ihre näheren Umstände. Folglich sind auch E-Mails als Art individueller Nachrichtenübermittlung dem Fernmeldegeheimnis zu unterstellen.

Das Fernmeldegeheimnis erfasst Kommunikationsvorgänge, die noch nicht beendet sind. Werden zu diesem Zeitpunkt E-Mails abgefangen und kopiert, so ist

[357] *Altenhain*, in: MüKo StGB, § 206 Rn. 16 ff.
[358] Wobei die Kostenfreiheit auch hier fraglich ist: Die „Währung", mit der gezahlt wird, sind die Daten des Nutzers, die dem E-Mail-Provider die Möglichkeit zur gezielten Werbung eröffnen (s. AGB WEB.DE Ziffer 3.3). Ferner können auch kostenpflichtige Premium-Dienste in Anspruch genommen werden.
[359] *Kühl*, in: Lackner/Kühl, StGB, § 206 Rn. 3.
[360] *Altenhain*, in: MüKo StGB, § 206 Rn. 40.
[361] *Altenhain*, in: MüKo StGB, § 206 Rn. 40.
[362] *BVerfG*, NJW 1992, 1875 (1876); *Lenckner*/*Eisele*, in: Schönke/Schröder, StGB, § 206 Rn. 6a.

das Fernmeldegeheimnis betroffen, wenn die E-Mails nachträglich ausgewertet und weitergeleitet werden.[363] Daher ist es für eine Strafbarkeit nicht entscheidend, wenn die für eine Strafbarkeit erforderliche Mitteilung an eine andere Person erst nach Abschluss des Übertragungsvorgangs erfolgen sollte.[364] Ist die E-Mail beim Empfänger angekommen, so endet in diesem Moment der Schutz des Fernmeldegeheimnisses.[365] Werden die E-Mails beim Abruf auf dem Server des E-Mail-Providers gelöscht und sind sie anschließend nur auf dem Rechner des Nutzers gespeichert, so ist das Fernmeldegeheimnis nicht mehr betroffen.

Allerdings sind E-Mails in einem E-Mail-Postfach, auf das der Nutzer nur über eine Internetverbindung zugreifen kann, weiterhin durch das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG geschützt.[366] Auch E-Mails, die der Nutzer zwar abgerufen hat, die aber nach dem Abrufen auf dem Server des E-Mail-Providers gespeichert bleiben (z. B. im Rahmen des IMAP-Verfahrens), sind vom Fernmeldegeheimnis erfasst. Für den E-Mail-Provider hat dies zur Folge, dass der Übermittlungsvorgang nicht beendet ist und der Schutzbereich des Fernmeldegeheimnisses eröffnet bleibt, solange der Nutzer die E-Mail nicht von dem Server des E-Mail-Providers gelöscht hat.[367]

Inhalt der Telekommunikation ist nach der Legaldefinition aus § 3 Nr. 22 TKG der Inhalt des technischen Vorgangs des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen. Selbst wenn es sich bei den Nachrichten, die an MonIKA übermittelt werden, um Spam handelt, ist dieser Spam immer noch durch das Fernmeldegeheimnis geschützt. Eine Unterscheidung zwischen rechtswidrigen und rechtmäßigen Nachrichten findet insofern nicht statt.

Unter die näheren Umständen der Kommunikation ist schon nach der wörtlichen Hervorhebung in § 206 Abs. 5 Satz 2 StGB zu zählen, ob jemand an dem Telekommunikationsvorgang beteiligt ist oder war. Davon sind die Verbindungsdaten von Telekommunikationsvorgängen erfasst, also wer, wann, von wo, auf welche Weise, wie lange und wie oft mit wem und wohin kommuniziert hat.[368] Diese Verbindungsdaten müssen also durch eine entsprechende

[363] *Schuster*, ZIS 2010, 68 (72).
[364] *Schuster*, ZIS 2010, 68 (72).
[365] *BVerfG*, MMR 2009, 673 (674).
[366] *BVerfG*, MMR 2009, 673 (674).
[367] *Sassenberg/Mantz*, BB 2013, 889 (890).
[368] *Lenckner/Eisele*, in: Schönke/Schröder, StGB, § 206 Rn. 6a mit Verweis auf *BVerfG*; NJW 1985, 121 ff.; NJW 1992, 1875 ff.; NJW 2006, 2757 ff.

Pseudonymisierung bei Übermittlung an die MonIKA GmbH verschlüsselt oder generell aus den zu übermittelnden Informationen entfernt werden.

Problematisch erscheint, dass die Mitarbeiter der MonIKA GmbH von dem Inhalt der übermittelten E-Mails Kenntnis erlangen könnten, wenn sie Zugriff auf die Verschlüsselung haben, um die Pseudonymisierung aufzulösen. Es muss also dafür gesorgt sein, dass die Nachrichten verschlüsselt bleiben und dieser Schlüssel nicht ohne Weiteres zugänglich ist. So wäre auch sichergestellt werden, dass an die MonIKA GmbH fehlgeleitete Nachrichten nicht erkannt werden. Wenn diese Anforderung erfüllt ist, handelt es sich um Tatsachen, die nicht dem Fernmeldegeheimnis unterfallen. Auch dürfte in diesem Falle ein Mitteilen i. S. v. § 206 Abs. 1 StGB ausscheiden. Ansonsten wäre das Merkmal „Mitteilen einer Tatsache“ i. S. v. § 206 Abs. 1 StGB erfüllt, was die Durchführung von MonIKA in diesem Anwendungsfall ungemein erschweren würde.

Nur für den Fall, dass dies bei einer Durchführung von MonIKA wider Erwarten nicht gelänge, müssen die folgenden Ausführungen beachtet werden. Es ist dann weiter zu prüfen, ob eine Strafbarkeit aus § 206 Abs. 1 StGB bestehen könnte. Die Handlungen, an die für die Prüfung anzuknüpfen sind, sind dann die inhaltliche Kenntnisnahme der E-Mails sowie die manuelle Weiterleitung durch den Mitarbeiter eines E-Mail-Providers an die MonIKA GmbH ohne Wissen des Kunden.

5.4.3.3.3 Bekanntwerden

So verlangt § 206 Abs. 1 StGB ferner, dass die Tatsachen dem Täter zudem in seiner Funktion als Inhaber oder Beschäftigter eines Unternehmens, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, bekannt geworden sein.

Die Vorschrift sagt jedoch nichts darüber aus, wann ein solches „Bekanntwerden“ i. S. v. § 206 Abs. 1 StGB vorliegt, sodass der Begriff einer Auslegung bedarf. Eine Tatsache ist dem Täter nur dann bekannt geworden, wenn er sie zuvor noch nicht gekannt hat.[369] Stützt man sich auf den Normzweck von § 206 Abs. 1 StGB, könnte es für eine Strafbarkeit ausreichen, dass der Täter die Tatsachen anderen mitteilt, ohne sich selbst Kenntnis zu verschaffen. § 206 Abs. 1 StGB soll nicht die Geheimhaltung der relevanten Tatsachen vor dem Täter bezwecken, sondern, dass der Täter die Tatsachen nicht einem Dritten mitteilt.[370]

[369] *Altenhain*, in: MüKo StGB, § 206 Rn. 36; *Kühl*, in: Lackner/Kühl, StGB, § 206 Rn 7.
[370] *Altenhain*, in: MüKo StGB, § 206 Rn. 36.

Daher ist es nach einer Auffassung im Schrifttum nicht notwendig, dass der Täter selbst Kenntnis von der Tatsache hat.[371] Vielmehr soll es genügen, dass er einem Dritten Kenntnis von der Tatsache verschafft und sich darüber bewusst ist, dass es sich um eine Tatsache handelt, die durch das Fernmeldegeheimnis geschützt ist.[372]

Gegen diese Auslegung und für eine Kenntnisnahme der Tatsachen durch den Täter als „Bekanntwerden" spricht hingegen der eindeutige Wortlaut von § 206 Abs. 1 StGB, wonach die Tatsachen *dem Täter* bekannt geworden sein müssen. Aus diesem Grund wird in der ersten Auffassung auch teilweise ein Verstoß gegen Art. 103 Abs. 2 GG und das sog. Bestimmtheitsgebot gesehen.[373] Das Bestimmtheitsgebot verpflichtet den Gesetzgeber, die Voraussetzungen der Strafbarkeit so konkret zu umschreiben, dass der Normadressat erkennen kann, welches Verhalten der Gesetzgeber sanktioniert.[374] Der Anwendungsbereich und die Tragweite der Straftatbestände müssen sich aus dem Wortlaut ergeben oder müssen sich durch Auslegung ermitteln lassen.[375] Nach allgemeinem Sprachgebrauch und Wortverständnis erfordert ein „Bekanntwerden" die Kenntnisnahme der jeweiligen Tatsache durch den Täter.[376] Auch der Vergleich zu anderen Normen im StGB wie § 203 Abs. 1 StGB und § 355 Abs. 1 StGB macht deutlich, dass eine Kenntnisnahme seitens des Täters notwendig ist.[377] Es ist daher vorzugswürdig, für eine Strafbarkeit nach § 206 Abs. 1 StGB auf die Kenntnisnahme durch den Täter abzustellen.

Damit würde sich der Angestellte des E-Mail-Providers strafbar machen, wenn er Kenntnis vom Inhalt einer E-Mail erlangen und die E-Mail weiterleiten sollte. Jedenfalls in dieser Konstellation läge ein „Bekanntwerden" vor. Daher ist darauf zu achten, dass der Mitarbeiter den konkreten Inhalt zu keiner Phase wahrnehmen kann. Sollte dies gewährleistet sein, würde die Strafbarkeit nach § 206 Abs. 1 StGB zusätzlich an dieser Hürde scheitern.

5.4.3.3.4 Unbefugt

Damit eine Strafbarkeit besteht, muss der Täter zudem unbefugt handeln.

---

[371] *Kühl*, in: Lackner/Kühl, StGB, § 206 Rn. 7; *Lenckner*/*Eisele*, in: Schönke/Schröder, StGB, § 206 Rn. 10.
[372] *Kühl*, in: Lackner/Kühl, StGB, § 206 Rn. 7; *Lenckner*/*Eisele*, in: Schönke/Schröder, StGB, § 206 Rn. 10.
[373] *Altenhain*, in: MüKo StGB, § 206 Rn. 40.
[374] *BVerfG*, NJW 2010, 754 (755).
[375] *BVerfG*, NJW 1995, 1141.
[376] *Schmitz*, in: MüKo StGB, § 355 Rn 20.
[377] *Cierniak*, in: MüKo StGB, § 203 Rn. 46; *Schmitz*, in: MüKo StGB, § 355 Rn. 20.

Nach allgemeiner Auffassung kommt dem Tatbestandsmerkmal „unbefugt“ im Rahmen von § 206 StGB eine Doppelfunktion zu.[378] Liegt ein Einverständnis des Betroffenen vor, so ist das Merkmal „unbefugt“ nicht erfüllt und das Einverständnis lässt bereits die Tatbestandsmäßigkeit entfallen. Im Übrigen handelt es sich bei dem Merkmal um ein allgemeines Rechtswidrigkeitsmerkmal.[379] Der Täter handelt daher unbefugt, wenn der in seinen Rechten Betroffene nicht einverstanden ist oder kein Rechtfertigungsgrund einschlägig ist.

Fraglich ist allerdings, ob allein das Einverständnis des Kunden des E-Mail-Providers (als Empfänger der E-Mail) ausreicht, um eine Strafbarkeit nach § 206 Abs. 1 StGB ausschließen zu können[380], oder ob zudem auch das Einverständnis des Absenders der E-Mail notwendig ist[381]. Das *OLG Karlsruhe* hat in einer Entscheidung zu § 206 Abs. 2 Nr. 2 StGB entschieden, dass ein Einverständnis nur dann von Bedeutung sein könne, wenn es von allen an dem konkreten Fernmeldeverkehr Beteiligten erteilt werde.[382] Auch das *BVerfG* hat im Jahr 1992 entschieden, dass ein Eingriff in das Fernmeldegeheimnis aus Art. 10 GG das Einverständnis beider Kommunikationspartner erfordere.[383]

Selbst wenn man im Falle des § 206 Abs. 2 Nr. 2 StGB ein doppeltes Einverständnis entgegen der Rechtsprechung für nicht erforderlich erachten sollte und damit das Einverständnis des Empfängers genügen lassen würde, so lässt sich diese Ansicht nicht ohne Weiteres auf § 206 Abs. 1 StGB übertragen. Dies ergibt sich aus den unterschiedlichen Schutzrichtungen beider Normen. Die Strafbarkeit des § 206 Abs. 2 Nr. 2 StGB liegt in der unbefugten Unterdrückung einer Nachricht durch den Täter in seiner Funktion als Beschäftiger oder Inhaber eines Unternehmens, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt und dem die Sendung anvertraut war. Ein solches Unterdrücken liegt bspw. darin, dass eine E-Mail durch den E-Mail-Provider nicht zugestellt wird. § 206 Abs. 2 Nr. 2 StGB schützt neben den Interessen des Betroffenen an dem ordnungsgemäßen Umgang mit der Sendung auch das öffentliche Vertrauen in die

[378] Vgl. *OLG Karlsruhe*, ZUM-RD 2005, 143 (147 f.); *Lenckner/Eisele*, in: Schönke/Schröder StGB, § 206 Rn. 11; a. A. wohl *Kargl*, in: Kindhäuser/Neumann/Paeffgen, StGB, § 206 Rn. 44.
[379] *OLG Karlsruhe*, ZUM-RD 2005, 143 (147 f.); *Lenckner/Eisele*, in: Schönke/Schröder, StGB, § 206 Rn. 11.
[380] Für den Tatbestand von § 206 Abs. 2 Nr. 2 StGB vertreten von: *Härting*, CR 2007, 311 (316), *Kitz*, CR 2005, 450 (453), *Spindler/Ernst*, CR 2004, 437 (439).
[381] So *Kargl*, in: Kindhäuser/Neumann/Paeffgen, StGB, § 206 Rn. 44; *Lenckner/Eisele*, in: Schönke/Schröder, StGB, § 206 Rn. 12.
[382] *OLG Karslruhe*, ZUM-RD 2005, 143 (147 f.).
[383] *BVerfG*, NJW 1992, 1875 (1876).

Sicherheit und Zuverlässigkeit des Post- und Telekommunikationssektors.[384] Zwar kann der Einzelne, auch wenn eine Norm zugleich seine Individualrechtsgüter schützt, nicht auf ein Universalgut der Allgemeinheit verzichten.[385] Das Vertrauen der Öffentlichkeit in die Zuverlässigkeit des Telekommunikationsverkehrs wird allerdings nicht verletzt, wenn eine Zustellung mit dem Einverständnis des Empfängers unterbleibt. Die Funktionsfähigkeit des Telekommunikationssystems wird nicht erschüttert, wenn der Übermittler (also der E-Mail-Provider) nicht eigenmächtig Sendungen unterdrückt und nur auf Aufforderung des Empfängers dessen Rechte wahrnimmt.[386]

§ 206 Abs. 1 StGB dient darüber hinausgehend auch dem Schutz des Post- und Fernmeldegeheimnisses und hat das Mitteilen von Tatsachen zum Gegenstand, die diesem unterliegen.[387] Eine Mitteilung i. S. v. § 206 Abs. 1 StGB umfasst nicht nur Daten des Empfängers, sondern auch solche des Absenders. Daher ist es berechtigt, es nicht alleine der Entscheidung des Empfängers zu überlassen, ob Tatsachen über einen Kommunikationsvorgang einem Dritten mitgeteilt werden.[388]

Dies bedeutet, dass für eine Mitteilung i. S. v. § 206 Abs. 1 StGB auch das Einverständnis des Absenders erforderlich ist. Für MonIKA ist daraus zu folgern, dass Rechtssicherheit immer nur dann besteht, wenn beide Kommunikationspartner ein Einverständnis zur Nutzung der E-Mail für die Verbesserung der IT-Sicherheit abgegeben haben. Bei Spam-Kampagnen wird das Einverständnis des tatsächlichen Absenders der E-Mail jedoch nicht vorhanden sein. Bei Missbrauch eines fremden E-Mail-Accounts allerdings könnte das Einverständnis dessen Inhabers bestehen, sofern in den Nutzungsbedingungen ein entsprechender Passus enthalten ist. Der E-Mail-Provider des missbrauchten Accounts müsste dafür auch Teilnehmer an MonIKA sein.

5.4.3.3.5 Vorsatz

Eine vorsätzliche Begehung ist auch gegeben, solange sich der Mitarbeiter darüber im Klaren ist, was er tut.

5.4.3.3.6 Rechtswidrigkeit

Es ist zu fragen, ob Rechtfertigungsgründe eingreifen können.

---

[384] *Kitz*, CR 2005, 450 (453); *Köcher*, DuD 2005, 163 (164).
[385] *Lenckner/Sternberg-Lieben*, in: Schönke/Schröder, StGB, Vorb. §§ 32 ff. Rn. 36.
[386] *Kitz*, CR 2005, 450 (453).
[387] *Lenckner/Eisele*, in: Schönke/Schröder, StGB, § 206 Rn. 2; *Kitz*, CR 2005, 450 (453).
[388] *Köcher*, DuD 2005, 163 (164).

5.4.3.3.6.1 Spezielle Rechtfertigungsgründe

So könnte sich aus den Bestimmungen des TKG ein spezieller Rechtfertigungsgrund ergeben.

Nach § 88 Abs. 3 Satz 1 TKG ist es Anbietern von Telekommunikationsdiensten untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Gem. § 88 Abs. 3 Satz 3 TKG ist eine Verwendung der Kenntnisse für andere als die in § 88 Abs. 3 Satz 1 TKG genannten Zwecke – insbesondere die Weitergabe an andere – nur zulässig, soweit das TKG oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Im Rückschluss bedeutet dies, dass die Kenntnisverschaffung zum Schutz der technischen Systeme in einem erforderlichen Maß zulässig ist, wenn es das TKG so vorsieht. Telekommunikationsdienste i. S. v. § 88 Abs. 3 Satz 1 TKG stellen auch die Dienste eines E-Mail-Providers dar.[389]

Die Verhinderung von Spam ist als Schutzmaßnahme zugunsten der technischen Systeme zu verstehen. Folglich muss auch die Verwendung eines Spam-Filters als Schutzmaßnahme verstanden werden, da von einem Diensteanbieter nicht verlangt werden kann, dass er Inhalte verbreitet, die seinen Kunden oder seinen eigenen Systeme Schaden zufügen.[390] Hierfür spricht zum einen die Auslegung des Störungsbegriffs aus § 100 Abs. 1 TKG durch den *BGH*. Der *BGH* stellte in einem Urteil zu § 100 TKG fest, dass eine Störung von Telekommunikationsanlagen auch bei einem erheblichen Spam-Aufkommen vorliegen kann.[391] Durch Spam finde eine direkte Bedrohung der Infrastruktur statt, weil der Spam diese in erheblichem Ausmaß in Anspruch nehme und die Kapazitäten der regulären Nutzung nicht mehr zur Verfügung stünden.[392] Zum anderen spricht auch der Störungsbegriff aus § 109 Abs. 2 Nr. 1 TKG hierfür. Der Begriff der Störung wird hier sogar weiter gefasst als der des § 100 TKG, der nur Störungen an den Anlagen selbst umfasst. Eine Störung nach § 109 Abs. 2 Nr. 1 TKG liegt vor, wenn die Dienste nicht oder nicht hinnehmbar beschränkt funktionieren.[393] Ein hohes Spam-Aufkommen kann

[389] *Bock*, in: Geppert/Schütz, TKG, § 88 Rn. 22.
[390] *Bock*, in: Geppert/Schütz, TKG, § 88 Rn. 26.
[391] *BGH*, MMR 2011, 341 (341 ff.).
[392] *BGH*, MMR 2011, 341 (344).
[393] *Bock*, in: Geppert/Schütz, TKG, § 109 Rn. 34.

daher eine solche Störung i. S. v. § 109 Abs. 2 Nr. 1 TKG darstellen. Maßnahmen gegen Spam-E-Mails können auch als Schutz der technischen Systeme i. S. v. § 88 Abs. 3 Satz 1 TKG angesehen werden.

Allerdings muss die Maßnahme erforderlich sein, um über § 88 Abs. 3 Satz 1 TKG gerechtfertigt werden zu können. Es darf also kein milderes Mittel gleicher Eignung zur Verfügung stehen.

Hier ist zweifelhaft, ob eine inhaltliche Kenntnisnahme und die mögliche Weiterleitung von der E-Mail zum Schutz der Systeme erforderlich sind, wenn auch durch ein automatisiertes Verfahren eine Einordnung als Spam erfolgen kann. Denn bereits durch die technische Einordnung als Spam dürften die Systeme der E-Mail-Provider in hohem Maße geschützt sein. Allerdings kann durch die Übermittlung für die Nutzung im Rahmen eines Fusions- und Klassifikationsverfahrens ein noch höherer Systemschutz vor Spam-E-Mails erreicht werden, sodass hierin ein effektiveres Mittel zur Spam-Bekämpfung gesehen werden kann.

Es muss weiterhin der Verhältnismäßigkeitsgrundsatz beachtet werden, durch den die Befugnisse des Diensteanbieters begrenzt werden. Hierfür müssen die Interessen des einzelnen Nutzers auf Wahrung seiner Rechte (Wahrung des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG, § 88 TKG und Wahrung des Grundrechts auf informationelle Selbstbestimmung aus Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG) mit den berechtigten Belangen des Diensteanbieters an der Funktions- und Leistungsfähigkeit seiner Systeme (Art. 12 Abs. 1 GG, Art. 14 Absatz 1 GG) abgewogen werden. Zu berücksichtigen ist hierbei auch das hohe öffentliche Interesse an der Funktionsfähigkeit des Telekommunikationssektors und damit einhergehend das Interesse der anderen Nutzer an dieser Funktionsfähigkeit. Im Rahmen der Verhältnismäßigkeitsprüfung ist aber ebenfalls darauf zu achten, dass das *BVerfG* den in Art. 10 Abs. 1 GG garantierten Grundrechten des Brief-, Post- und Fernmeldegeheimnisses einen hohen Rang zuweist. Art. 10 GG dient der freien Entfaltung der Persönlichkeit, weil hierdurch ein privater Austausch von Nachrichten, Gedanken und Meinungen gewährleistet wird.[394] Die Grundrechte aus Art. 10 GG wahren damit die Würde des denkenden und freiheitlich handelnden Menschen.[395] Auf Grund dieser hohen Bedeutung, die das *BVerfG* Art. 10 GG und dem Fernmeldegeheimnis beimisst, dürfte die Kenntnisnahme von E-Mail-Inhalten zu präventiven Zwecken bei der

[394] *BVerfG*, NJW 2004, 2213 (2215).
[395] *BVerfG*, NJW 2004, 2213 (2215).

Botnetz- und Spambekämpfung nur bei einer konkreten Gefahrenlage angemessen sein. Ansonsten erscheint dieses Vorgehen als zu weitreichend und das Recht auf informationelle Selbstbestimmung zu stark eingeschränkt. Es überwiegen damit das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung des Kunden.

Eine Befugnis zur inhaltlichen Kenntnisnahme und der anschließenden Übermittlung der E-Mails, die unter Spam-Verdacht stehen, durch einen Mitarbeiter könnte sich aber aus § 109 Abs. 2 Nr. 1 TKG ergeben. Nach dieser Norm ist derjenige, der ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, verpflichtet, angemessene technische Vorkehrungen und Maßnahmen zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen, zu treffen. Ein erhebliches Spam-Aufkommen ist als Störung i. S. v. § 109 Abs. 2 Nr. 1 TKG anzusehen. Auch kann sich eine Rechtfertigung aus § 109 Abs. 2 Nr. 2 TKG ergeben, wonach Vorkehrungen zur Beherrschung der Risiken für die Sicherheit von Telekommunikationsnetzen und -diensten zu leisten sind.

Im Rahmen des § 109 TKG ist der Verhältnismäßigkeitsgrundsatz jedoch ebenso zu beachten.[396] Dies wird durch § 109 Abs. 2 Satz 4 TKG verdeutlicht, wonach technische Vorkehrungen und sonstige Schutzmaßnahmen angemessen sind, wenn der dafür erforderliche technische und wirtschaftliche Aufwand nicht außer Verhältnis zur Bedeutung der zu schützenden Telekommunikationsnetze oder -dienste steht. Bei der Abwägung sind neben den Interessen der Netzbetreiber auch die Belange der Nutzer und Anwender zu berücksichtigen. Eine Befugnis zur Kenntnisnahme und Weiterleitung der E-Mail-Inhalte ergibt sich daher nach § 109 Abs. 2 Nr. 1, Nr. 2 TKG nur im Ausnahmefall.

Das TKG erlaubt die inhaltliche Kenntnisnahme mit entsprechender Weiterleitung damit nicht und somit ergeben sich aus ihm keine Rechtfertigungsgründe.

5.4.3.3.6.2 Allgemeine Rechtfertigungsgründe

Eine weitere Frage ist, ob neben den gerade aufgezeigten besonderen Rechtfertigungsgründen auch allgemeine Rechtfertigungsgründe herangezogen werden können. Nach überwiegender Meinung greifen die allgemeinen

[396] Vgl. *Schommertz*, in: Scheurle/Mayen, TKG, § 109 Rn. 7.

Rechtfertigungsgründe im Falle von § 206 StGB grundsätzlich nicht ein.[397] Der Grund hierfür liegt in § 88 Abs. 3 Satz 3 TKG, da den allgemeinen Rechtfertigungsgründen der erforderliche ausdrückliche Bezug auf Telekommunikationsvorgänge fehlt.

Teile der Literatur nehmen jedoch eine Einschränkung vor und lassen zumindest die mutmaßliche Einwilligung bei § 206 Abs. 1 StGB eingreifen.[398] Eine weitere Ansicht will die allgemeinen Rechtsfertigungsgründe dann anwenden, wenn besondere Fallgestaltungen vorliegen, die außerhalb des Rahmens von § 88 Abs. 3 Satz 3 TKG liegen.[399] Ob das Übermitteln an die MonIKA GmbH eine solch besondere Fallgestaltung darstellt, ist bereits zweifelhaft, da die Übermittlung gerade dem in § 88 Abs. 3 Satz 1 TKG erwähnten Zweck – der Schutz der technischen Systeme – dienen soll.

Die Vertreter, die ein Eingreifen der allgemeinen Rechtfertigungsgründe bei § 206 StGB ermöglichen wollen, wenden die allgemeinen Rechtfertigungsgründe zudem auch nur in den Fällen an, in denen es nicht um die Verschaffung und Verwendung der Kenntnisse vom Inhalt und den näheren Umständen der Telekommunikation geht.[400] In diesen Konstellationen sei der Anwendungsbereich von § 88 Abs. 3 TKG Satz 3 nicht eröffnet und ein Rückgriff auf die allgemeinen Rechtfertigungsgründe möglich.[401] Die vorliegende Untersuchung hat aber gerade die Übermittlung von Tatsachen, die dem Fernmeldegeheimnis unterliegen, zum Gegenstand. Daher scheidet auch nach dieser Ansicht eine Rechtfertigung über die allgemeinen Rechtfertigungsgründe aus. Außerdem lässt der eindeutige Wortlaut von § 88 Abs. 3 TKG keinen Raum für die Anwendung allgemeiner Rechtfertigungsgründe. Eine gegenteilige Auslegung widerspräche der Gesetzesbegründung. Der Gesetzgeber wollte sich die Entscheidung darüber vorbehalten, wann ein Eingriff in das als besonders schützenswert angesehene Post- oder Fernmeldegeheimnis erlaubt ist.[402]

Daher können die allgemeinen Rechtfertigungsgründe nicht herangezogen werden.

---

[397] Siehe hierzu *Fischer*, StGB, § 206 Rn. 9; *Kühl*, in: Lackner/Kühl, StGB, § 206 Rn. 15.
[398] *Lenckner/Eisele*, in: Schönke/Schröder, StGB, § 206 Rn. 14.
[399] *OLG Karlsruhe*, ZUM-RD 2005, 143 (147); *Cornelius/Tschoepe*, K&R 2005, 269 (270).
[400] *Cornelius/Tschoepe*, K&R 2005, 269 (271).
[401] *Cornelius/Tschoepe*, K&R 2005, 269 (271).
[402] *Altenhain*, in: MüKo StGB, § 206 Rn. 68; *Fischer*, StGB, § 206 Rn. 9; *Kargl*, in: Kindhäuser/Neumann/Paeffgen, StGB, § 206 Rn. 47.

5.4.3.3.7 Zwischenergebnis

Eine Strafbarkeit nach § 206 Abs. 1 StGB für die Mitarbeiter des E-Mail-Providers durch die Anwendung von MonIKA ist solange ausgeschlossen, wie eine inhaltiche Kenntnisnahme der E-Mails – unabhängig davon, ob Spam oder nicht – für sie nicht möglich und nicht erforderlich ist. Dies muss sichergestellt werden. Das konkrete MonIKA-Verfahren im untersuchten Szenario arbeitet jedoch mit einer Pseudonymisierung in Form der Vorverarbeitung zu Meta-Daten, die der MonIKA-Agent vor Weiterleitung an den EvASC leistet. Diese stellt sicher, dass eine inhaltliche Kenntnisnahme für Mitarbeiter nicht oder nur unter besonders schwierigen Umständen möglich ist. Zudem sollte es nur in äußerst seltenen Fällen dazu kommen, dass eine E-Mail fehlgeleitet wird, da durch die Vielzahl der Parameter mit hoher Genauigkeit gearbeitet werden kann.

Um ein möglichst hohes Maß an Rechtssicherheit für die Übermittlung der Meta-Daten von manuell durch den Kunden als Spam markierten E-Mails zu erreichen, sollte ein entsprechender Disclaimer den Kunden darüber informieren, dass der E-Mail-Provider die Nachrichten in Form von Meta-Daten an einen Dritten zur Verbesserung des Spam-Schutzes übermitteln möchte. Sodann sollte der Kunde dazu aufgefordert werden, in diese Handlung einzuwilligen.

5.4.3.4 Strafbarkeit nach § 44 Abs. 1 BDSG i. V. m. § 43 Abs. 2 BDSG

Schließlich kommt noch eine Strafbarkeit aus dem BDSG in Betracht. Dies verlangt jedoch einen datenschutzrechtlichen Verstoß i. S. d. § 43 Abs. 2 BDSG. Die Beurteilung der datenschutzrechtlichen Problematik von MonIKA findet in Deliverable 5.2 Behandlung.

5.4.4 Strafrechtliche Risiken für die Mitarbeiter der MonIKA GmbH

Fraglich ist, ob im vorliegenden Szenario auch strafrechtliche Risiken für die Mitarbeiter der MonIKA GmbH bestehen.

5.4.4.1 Strafbarkeit nach § 206 Abs. 1 StGB

Zu denken ist an § 206 Abs. 1 StGB, wenn im Rahmen von MonIKA einzelne Mitarbeiter auf die Inhalte der E-Mails zugreifen und diese zur Kenntnis nehmen sollten. Bei einer Pseudonymisierung der Inhalte ergeben sich für die Mitarbeiter der MonIKA GmbH jedoch – wie bereits für die Mitarbeiter des E-Mail-Providers erarbeitet – keine strafrechtlichen Risiken bzgl. einer Strafbarkeit nach § 206 Abs. 1 StGB.

5.4.4.2 Strafbarkeit nach § 206 Abs. 2 Nr. 1 StGB

Das Risiko einer Strafbarkeit nach § 206 Abs. 2 Nr. 1 besteht ebenfalls nicht, da sich die Norm nicht auf E-Mails, sondern nur auf körperliche Gegenstände bezieht.[403]

5.4.4.3 Strafbarkeit nach § 202a Abs. 1 StGB

Ferner kommt eine Strafbarkeit nach § 202a Abs. 1 StGB in Betracht. Es stellt sich die Frage, ob die E-Mails, die die E-Mail-Provider an die MonIKA GmbH weiterleitet, auch für die MonIKA GmbH i. S. v. § 202a StGB bestimmt sind. Wie oben bereits erwähnt, ist der Berechtigte bei übermittelten Daten die übermittelnde Stelle und nach Erhalt der Datenempfänger.[404] Wurden die Daten von dem Berechtigten einem anderen zugänglich gemacht, so sind sie für diesen bestimmt.[405]

E-Mails sind daher für die MonIKA GmbH i. S. v. § 202a Abs. 1 StGB bestimmt, wenn sie von dem E-Mail-Provider weitergeleitet werden und dieser als Übermittler verfügungsberechtigt ist. Diese Verfügungsberechtigung des E-Mail-Providers dürfte solange bestehen, wie der Empfänger die betreffende E-Mail nicht abgerufen hat. Sollte der Kunde die betroffene E-Mail vor der Weiterleitung abgerufen haben, besteht jedoch keine Verfügungsberechtigung des E-Mail-Providers und die E-Mail wäre nicht für die MonIKA GmbH bestimmt. Überträgt der Kunde des E-Mail-Providers aber auch sein Bestimmungsrecht hinsichtlich einer Übermittlung durch den E-Mail-Provider an die MonIKA GmbH als externer IT-Sicherheitsdienstleister, dürften die auf Grund dieser Übertragung übermittelten Daten wiederum für die Nutzung im Rahmen von MonIKA bestimmt sein.

Wird eine E-Mail verschlüsselt, so ist eine Strafbarkeit nach § 202a Abs. 1 StGB möglich, wenn die E-Mail von einer nicht berechtigten Person gelesen werden sollte. Ist eine E-Mail nicht verschlüsselt, so fällt diese schon nicht in den Schutzbereich des § 202a StGB.

Eine Strafbarkeit nach § 202a StGB dürfte jedoch auch deshalb ausscheiden, da durch MonIKA keine Zugangssicherung i. S. v. § 202a Abs. 2 StGB überwunden wird. Die entsprechenden E-Mails und Informationen werden vom E-Mail-Provider übermittelt, damit MonIKA diese verwenden kann.

Schließlich müsste der Täter gem. § 202a StGB unbefugt handeln. Mit „unbefugt“ ist im Rahmen von § 202a StGB das allgemeine Deliktsmerkmal der

[403] *Lenckner/Eisele*, in: Schönke/Schröder, StGB, § 206 Rn. 17.
[404] BayObLG JR 1994, 477; *Graf*, in: MüKo StGB, § 202a Rn. 19; *Kargl*, in: Kindhäuser/Neumann/Paeffgen, StGB, § 202a Rn. 7.
[405] *Lenckner/Eisele*, in: Schönke/Schröder, StGB, § 202a Rn. 6.

Rechtswidrigkeit gemeint.[406] Liegt ein Rechtfertigungsgrund vor, so entfällt eine Strafbarkeit nach § 202a StGB.

5.4.4.4 Bestehen von Rechtfertigungsgründen

Handlungen der Mitarbeiter der MonIKA GmbH, die – entgegen der vorliegenden rechtlichen Beurteilung – den Tatbestand von §§ 202a, 202b, 303a oder 303b StGB erfüllen, könnten jedoch gerechtfertigt sein, sofern eine Einwilligung des Betroffenen gegeben ist.

Für eine wirksame Einwilligung muss der Betroffene über das verletzte Rechtsgut verfügen können. Zudem muss er einwilligungsfähig sein, die Einwilligung vor der Tat nach außen hin zum Ausdruck gebracht haben und sie freiwillig äußern.[407] Jedoch muss sie nicht an den Täter gerichtet sein.[408] Dies bedeutet, dass auch gegenüber dem E-Mail-Provider in Handlungen von der MonIKA GmbH eingewilligt werden kann. Allerdings muss die handelnde Person auf Grund der Einwilligung handeln[409], sodass die MonIKA GmbH von der Einwilligung informiert werden muss. Problematisch ist, dass der E-Mail-Provider gegenüber den einzelnen Kunden vorformulierte Einwilligungen einsetzen wird. Diese Formulareinwilligungen könnten als AGB eingestuft werden und dürften dann als Folge nicht gegen die AGB-Vorschriften der §§ 305 ff. BGB verstoßen. Die Frage, ob es sich bei Formulareinwilligungen um AGB handelt und sie somit einer AGB-Kontrolle nach §§ 305 ff. BGB standhalten müssen, ist umstritten.[410] Eine formularmäßige Einwilligung sollte konkret gefasst sein. Das bedeutet, dass die strafrechtlich-relevanten Handlungen konkret bezeichnet werden. Außerdem sollte die Einwilligung auf einem eigenen Formular erfolgen, in das der Kunde extra einwilligen muss. Zu beachten ist außerdem, dass eine Einwilligung jederzeit widerrufen werden kann.

Im Falle von § 206 Abs. 1 StGB ist, wie oben bereits erörtert, neben dem Einverständnis des Empfängers auch das Einverständnis des Absenders erforderlich.

Eine Rechtfertigung kann sich ferner aus § 88 Abs. 3 TKG ergeben. Fraglich ist aber auch hier, ob es sich bei der MonIKA GmbH um einen Diensteanbieter i. S. v. § 3 Nr. 6 TKG handelt. Nur in diesem Falle ist eine Handlung nach

[406] *Lenckner/Eisele*, in: Schönke/Schröder, StGB, § 202a Rn. 11.
[407] *Lenckner/Sternberg-Lieben, in:* Schönke/Schröder, StGB, Vorb. §§ 32 ff. Rn. 35.
[408] *Lenckner/Sternberg-Lieben, in:* Schönke/Schröder, StGB, Vorb. §§ 32 ff. Rn. 43.
[409] *Fischer*, StGB, Vor § 32 Rn. 3c.
[410] *Lenckner/Sternberg-Lieben*, in: Schönke/Schröder, StGB, Vorb. §§ 32 ff. Rn. 43.

§ 88 Abs. 3 TKG zulässig. Dies dürfte allerdings zu bejahen sein, da nach § 3 Nr. 6 lit. b TKG unter Diensteanbieter auch derjenige fällt, der ganz oder teilweise geschäftsmäßig an der Erbringung von Telekommunikationsdiensten mitwirkt. Hierzu zählen insbesondere auch externe Erfüllungsgehilfen, Subunternehmer und Dienstleister, die bei der technischen Erbringung der Dienstleistung mitwirken.[411] Unter Telekommunikationsdienste i. S. v. § 3 Nr. 24 TKG fallen auch die Bereitstellung eines Internet-Zugangs und die E-Mail-Übertragung.[412]

Im Rahmen einer möglichen Rechtfertigung durch § 109 Abs. 2 Nr. 1, Nr. 2 TKG stellt sich die Frage, ob die MonIKA GmbH ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt. Unter Berücksichtigung von § 3 Nr. 6 lit. b TKG dürfte jedenfalls die zweite Möglichkeit gegeben sein, sodass eine Rechtfertigung über § 109 Abs. 2 Nr. 1, Nr. 2 TKG auch möglich ist.

5.4.4.5 Strafbarkeit nach § 44 Abs. 1 BDSG i. V. m. § 43 Abs. 2 BDSG

Für den Fall eines datenschutzrechtlich relevanten Verstoßes (s. § 43 Abs. 2 BDSG) besteht die Gefahr einer strafrechtlichen Haftung aus § 44 Abs. 1 BDSG.

5.4.4.6 Zwischenergebnis

Auch für die Mitarbeiter der MonIKA GmbH ergeben sich unter Berücksichtigung der o. g. Hinweise keine strafrechtlichen Risiken.

5.5 Ergebnis

Im Anwendungsfall „Spam-Kampagnen-Erkennung zur Klassifikation von Bots“ tritt das Problem auf, dass durch die E-Mails Daten Dritter, die dem Fernmeldegeheimnis unterfallen, unmittelbar berührt sind. Daher gilt in besonderem Maße, dass zumindest pseudonymisiert werden muss. Die technische Ausgestaltung von MonIKA für diesen Anwendungsfall – ihr Funktionieren unterstellt – ist jedoch rechtlich zulässig und ein Verstoß gegen das Fernmeldegeheimnis scheint nicht gegeben.

[411] *Heun*, in: Lehmann/Meents, Informationstechnologierecht, Kapitel 23 Rn. 37.
[412] *Heun*, in: Lehmann/Meents, Informationstechnologierecht, Kapitel 23 Rn. 26.

Haftungsrisiken treten auch in diesem Szenario auf. Diese sollten bereits bei den Vertragsverhandlungen angesprochen und besprochen werden. Die tatsächlichen Risiken dürften allerdings überschaubarer Natur bleiben, da der Agent die E-Mails auf eine Vielzahl übereinstimmender Merkmale hin untersucht, sodass selten fehlgeleitete E-Mails auftreten dürften.

6 Haftungsrechtliche Rahmenbedingungen bei dem Einsatz einer Software zur Informationsfusion und –klassifikation zur Überwachung des Internetroutings

Die Überwachung des Internetroutings stellt einen weiteren Anwendungsfall innerhalb des MonIKA-Projekts dar.

6.1 Untersuchungsgegenstand

Untersuchungsgegenstand in diesem Anwendungsfall ist der Einsatz von MonIKA als Verfahren zur Informationsfusion und –klassifikation zur Überwachung des Internetroutings. Ziel des Einsatzes von MonIKA ist es hierbei, Bedrohungen für das Routing zwischen Autonomen System (AS) wie Fehlkonfigurationen und Pfadmanipulationen schneller aufzudecken und beseitigen zu können.

6.2 Sachverhalt

Der Sachverhalt für den Anwendungsfall ist dabei offen gestaltet, da an diesem Anwendungsfall vielmehr in technischer Hinsicht demonstriert werden soll, dass MonIKA auch für derartige Zwecke nutzbar gemacht werden kann.

Um Fehlkonfigurationen und Pfadmanipulationen frühzeitig entgegen zu treten, wird eine Stelle gewählt, die den EvASC betreibt und die Analyse der eingehenden Daten vornimmt (MonIKA-Betreiber). Dies können sowohl ein privatrechtlicher IT-Sicherheitsdienstleister als auch eine öffentlich-rechtliche Einrichtung oder ein CERT sein.

Die entsprechenden Agenten werden bei den MonIKA-Teilnehmern installiert. Teilnehmer sind zum einen die Betreiber Autonomer Systeme (AS-Betreiber), die ihre Routingdaten an den MonIKA-Betreiber mittels der Agenten zur Verfügung stellen. Zusätzlich können sie Informationen über Peeringpartner oder Routing-Filter liefern. Zum anderen können auch herkömmliche Internetteilnehmer, die keine AS-Betreiber sind, durch Übermittlung ihrer Routing-Informationen an MonIKA teilnehmen.

Der MonIKA-Betreiber sendet nach Fusion und Klassifikation der von den Teilnehmern zur Verfügung gestellten Daten und solchen Daten, die er aus frei zugänglichen Datensammlungen von Border Gateway Protokoll-Nachrichten erlangt, seine Informationen über möglicherweise festgestellte illegitime Routen-Announcements an die Teilnehmer. Diese können mit Handlungsempfehlungen versehen sein.

Ansonsten zu nennen sind die Internetteilnehmer als von Routinganomalien Betroffene. Sie können davon betroffen sein, wenn sie eine bestimmte Website aufrufen wollen, aber fehlgeleitet werden.

6.3 Rechtliche Erwägungen

Ob und wie der Betreiber von MonIKA haftet, hängt von der näheren Ausführung in der Praxis ab.

Betreibt ein externer IT-Sicherheitsdienstleister MonIKA zu Zwecken der Überwachung des Internetroutings, ist die Ausgestaltung der Verträge entscheidend. Haftungsrechtliche Relevanz erlangen die bereits im Anwendungsfall „Enterprise-Monitoring“ behandelten Fälle, dass der IT-Sicherheitsdienstleister fehlerhafte Analyseergebnisse – also Falschwarnungen – ausgibt und die Teilnehmer manipulierte Daten übermitteln. Es ergeben sich jedoch vorliegend keine Unterschiede.

Sollte eine als öffentlich-rechtlich einzuordnende Stelle MonIKA anwenden, um das globale Internetrouting zu überwachen, müssten die Teilnehmer gesetzlich verpflichtet werden, nicht frei zugängliche Daten zur Verfügung zu stellen. Als Alternative kommt die freiwillige Übermittlung in Betracht. Gibt die öffentlich-rechtliche Stelle Analyseergebnisse aus, kann sie diese mit einem

Unverbindlichkeitsvorbehalt versehen, um einer Haftung zu entgehen. Es müsste sich zur Begründung einer Haftung bei der Fehlanalyse zudem um eine Amtspflichtverletzung handeln. Wird eine Gefährdungslage für eine Anomalie des Internetroutings vorausgesetzt, verpflichtet dies die staatlichen Organe nicht stets zu korrekten Analyseergebnissen, solange hinreichende Anhaltspunkte für die Gefährdungslage bestanden.

Auch Forschungsinstitutionen, die als Verein o. ä. organisiert sind, können einer Haftung vorbeugen, indem sie deutlich sichtbar machen, dass ihre Analyseergebnisse und Handlungsempfehlungen rechtlich unverbindlich sind.

6.4 Ergebnis

Der Anwendungsfall „Überwachung des Internetroutings“ dient vielmehr als technisches Beispiel für den Einsatz von MonIKA, denn als Exempel, das weitere rechtliche Problematiken enthält. Sollte ein externer IT-Sicherheitsdienstleister MonIKA betreiben, gilt für Haftungsrisiken die im PoC zum Anwendungsfall „Enterprise-Monitoring“ erarbeitete Analyse. Auch bezüglich der staatlichen Haftung können die dort erfolgten Ausführungen sinngemäß herangezogen werden.

7 Kooperatives Monitoring im Lichte der Pläne zur staatlichen Regulierung der IT-Sicherheit[413]

Das MonIKA-Projekt befasst sich mit dem übergeordneten Ziel der IT-Sicherheit. Sowohl die Europäische Kommission als auch das Bundesministerium des Innern planen eine staatliche Regulierung der IT-Sicherheit, mit der u. a. branchenübergreifende Meldepflichten und Mindestanforderungen eingeführt werden sollen.

7.1 Pläne auf dem Gebiet der IT-Sicherheit

Im Folgenden werden die wesentlichen Inhalte der Pläne aufgezeigt.

7.1.1 Pläne der Europäischen Kommission

Die Kommission hat am 7. Februar 2013 eine umfassende Cybersicherheitsstrategie[414] sowie – als deren Kernelement – einen Vorschlag für eine Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit veröffentlicht.[415] Als weitere Maßnahmen sind die Sensibilisierung der Öffentlichkeit, der Aufbau eines Binnenmarktes für Cybersicherheitsprodukte und –dienste sowie die Förderung von Investitionen in die Forschung geplant.

Die Cybersicherheitsstrategie und die angestrebte Verabschiedung einer NIS-RL ordnen sich in eine Reihe verschiedener Maßnahmen ein, welche die EU innerhalb der letzten zehn Jahre getroffen hat. Herauszustellen ist dabei die 2004 erfolgte Einrichtung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA). Hinzu kommen europaweit geltende Verpflichtungen für Telekommunikationsunternehmen und Datenverarbeiter.

---

[413] Die Ausführungen in diesem Kapitel werden voraussichtlich in ähnlicher Form in der juristischen Fachzeitschrift Computer und Recht publiziert: *Roos*, CR 2014, n. n. Ergänzend wird auf die Publikation *Roos*, K&R 2013, 769 hingewiesen.

[414] JOIN(2013) 1 final, Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum.

[415] COM(2013) 48 final. Im Folgenden NIS-RL-E.

Sämtliche der im Februar 2013 publik gewordenen Pläne und Maßnahmen stehen im Kontext mit dem übergeordneten Ziel des NIS-RL-E nach einer Erhöhung der Sicherheit des Internets und privater Netze, die eine herausgehobene gesellschaftliche und volkswirtschaftliche Relevanz aufweisen. Sicherheit versteht der NIS-RL-E als die Fähigkeit von Netzen und Informationssystemen zur Abwehr von Störungen und böswilligen Angriffen, um dadurch die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten und die Funktionsfähigkeit von Diensten aufrecht zu erhalten.[416] Die Kommission verdeutlicht in der Begründung[417], dass sie der Netzsicherheit in Zukunft einen hohen Stellenwert einräumen wird. Als Hintergrund dieser Offensive benennt sie die Bedrohungslage für Informationssysteme, die sich zukünftig kaum verringern werde. Der europäische Binnenmarkt sei durch die bestehenden Verflechtungen auf robuste Netze angewiesen. Ein rein freiwilliges, isoliertes Vorgehen der Mitgliedstaaten und der dort ansässigen Unternehmen biete in Anbetracht der Bedrohungen keinen ausreichenden Schutz. Insofern sollen die Mitgliedstaaten zur Umsetzung verschiedener Maßnahmen angehalten werden. Dadurch soll jeder Mitgliedstaat ein Mindestniveau an IT-Sicherheit gewährleisten und ein europäisches Netz aufgebaut werden, mittels dessen sich die Mitgliedstaaten gegenseitig informieren können. Weiterhin verfolgt die Kommission das Ziel, die Zusammenarbeit von Staat und Wirtschaft für Belange der Netzsicherheit generell auszubauen. Statt der Beibehaltung des derzeitigen, auf freiwilligem Vorgehen basierenden Ansatzes oder eines gemischten Ansatzes von freiwilligen, jedoch zu gewissen Teilen regulierten Maßnahmen, entscheidet sich die Kommission für einen regulatorischen Ansatz.[418] Dieser ist mit rechtlichen Pflichten und Anforderungen an die öffentliche Verwaltung und Privatwirtschaft als Marktteilnehmer verknüpft.

7.1.1.1 Sicherheitsanforderungen und Meldepflichten

Art. 14 Abs. 1 NIS-RL-E verpflichtet die Mitgliedstaaten zur Sicherstellung, dass „geeignete technische und organisatorische Maßnahmen“ von der öffentlichen Verwaltung und den Marktteilnehmern getroffen werden, um Sicherheitsrisiken für deren Netze und Informationssysteme einzuschränken. Das Ziel ist ein fortlaufender Betrieb der Kerndienste, auch wenn es zu Sicherheitsvorfällen gekommen sein sollte. Die Maßnahmen müssen angemessen sein und dem Stand der Technik entsprechen. Ferner bestimmt Art. 14 Abs. 2 NIS-RL-E, dass Sicherheitsvorfälle an

[416] Art. 3 Abs. 2 NIS-RL-E.
[417] S. 2 ff. NIS-RL-E.
[418] S. 7 f. NIS-RL-E.

eine bestimmte Behörde gemeldet werden müssen. Zu den Sicherheitsvorfällen zählt der Entwurf solche, die erhebliche Auswirkungen auf die Sicherheit der Kerndienste haben.

Die Pflichten zur Einrichtung von Sicherheitsmaßnahmen und zur Meldung von Sicherheitsvorfällen treffen im Ergebnis die öffentliche Verwaltung und Marktteilnehmer, von denen der Entwurf spricht. Um wen es sich bei den Marktteilnehmern handeln soll, ergibt sich aus Art. 3 Abs. 8 i. V. m. Anhang II NIS-RL-E: Dies sind zum einen typische Dienste der Informationsgesellschaft (bspw. Online-Shops, soziale Netzwerke und Suchmaschinen) und zum anderen kritische Infrastrukturen, von deren Betrieb Wirtschaft und Gesellschaft in höchstem Maße abhängig sind (Energie, Verkehr, Bankwesen, Finanzmarktinfrastruktur und Gesundheitswesen). Deren Betreiber müssen damit rechnen, zukünftig sicherheitsgemäße Strukturen nachweisen und bei eingetretenen Sicherheitsbeeinträchtigungen Meldepflichten nachkommen zu müssen. Ausdrücklich ausgenommen von dem NIS-RL-E sind Telekommunikationsunternehmen und Vertrauensdiensteanbieter[419], also privatwirtschaftliche Unternehmen, an die bereits ähnliche Verpflichtungen gestellt werden.[420]

7.1.1.2 Verpflichtungen der Mitgliedstaaten

Die Kommission nimmt in besonderem Maße die Mitgliedstaaten in die Pflicht, um die mit dem NIS-RL-E verbundenen Ziele zu erreichen. Dies äußert sich zunächst darin, dass nach Art. 5 NIS-RL-E jedem Mitgliedstaat die Aufgabe zukommt, eine eigenständige Strategie zur Herstellung und Aufrechterhaltung einer hohen Netz- und Informationssicherheit zu entwickeln. Die Strategie dient u. a. der Festlegung von Zielen, Beteiligten, sichernden Maßnahmen und Forschungsperspektiven. Ein wesentlicher Baustein liegt auch in der Errichtung eines Kooperationsplans, durch den Aufgabenfelder und die Zusammenarbeit der Beteiligten – dies können neben staatlichen auch privatwirtschaftliche Einrichtungen sein – näher bestimmt werden.

Zudem obliegt es jedem Mitgliedstaat, eine Behörde als für die Netz- und Informationssicherheit zuständig zu erklären und diese so auszustatten, dass sie ihre

[419] Unter Vertrauensdiensteanbietern versteht der NIS-RL-E natürliche oder juristische Personen, die elektronische Dienste bereitstellen, die der Gewährleistung von Sicherheit elektronischer Signaturen, elektronischer Siegel, elektronischer Dokumente etc. dienen, s. Art. 3 Nr. 11 NIS-RL-E.
[420] Vgl. die auf Art. 13a Abs. 3 der RL 2009/140/EG zurückgehende Meldepflicht für TK-Unternehmen in § 109 Abs. 5 TKG.

Aufgaben wirksam und effizient wahrnehmen kann.[421] Ihre Aufgaben liegen maßgeblich in der Sicherstellung, dass die Betroffenen die Sicherheitsanforderungen einhalten und ihren Meldepflichten nachkommen. Ferner kommuniziert und kooperiert die NIS-Behörde mit anderen nationalen Behörden wie Strafverfolgungs- und Datenschutzbehörden.

Eine weitere Verpflichtung der Mitgliedstaaten besteht in dem Aufbau eines nationalen CERTs, das im Regelfall an die NIS-Behörde angeschlossen oder in ihr integriert sein wird.[422] Die Aufsicht über das CERT führt ebenfalls die NIS-Behörde. Das CERT ist das Organ, das sich für die praktische Durchführung der Maßnahmen verantwortlich zeigt (s. Anhang I NIS-RL-E). So überwacht es die nationalen Sicherheitsvorfälle und reagiert ggf. auf diese, gibt Frühwarnungen aus und analysiert stetig die Gefährdungslage. Über das CERT soll auch die Kooperation mit der Privatwirtschaft erfolgen.

7.1.1.3 Schaffung eines Kooperationsnetzes

Die Kommission erwägt, ein sog. Kooperationsnetz zu schaffen.

7.1.1.3.1 Plan für ein Kooperationsnetz

Sämtliche Maßnahmen, die von den Mitgliedstaaten getroffen werden sollen, stehen in Verbindung mit der Grundidee der Kommission, über eine Kooperation der Mitgliedstaaten ein höchstmögliches Maß an Netz- und Informationssicherheit zu erzielen. Der kooperative Ansatz soll durch ein sog. Kooperationsnetz verwirklicht werden, über das die NIS-Behörden untereinander und mit der Kommission kommunizieren können. Über das Kooperationsnetz sollen die nationalen NIS-Behörden bestimmte ihnen bekannte Sicherheitsrisiken und Sicherheitsvorfälle melden und sich gegenseitig die erforderlichen Informationen zur Verfügung stellen.[423] Der nächste Schritt besteht dann in einer Abstimmung der Beteiligten, wie dem Risiko oder Vorfall möglichst effektiv begegnet werden kann.[424] Die Kooperation soll sich auch auf gemeinsame Sicherheitsübungen und die gegenseitige Unterstützung mit Expertise erstrecken.

Die Kommission erarbeitet einen Plan, der detailliertere Vorgaben für die Umsetzung kooperativer Verfahren macht, und kann vorschreiben, in welcher Form

[421] Art. 6 Abs. 1, Abs. 3 NIS-RL-E.
[422] Art. 7 Abs. 1 NIS-RL-E.
[423] Art. 10 NIS-RL-E.
[424] Art. 11 NIS-RL-E.

der Meldepflicht an die nationalen NIS-Behörden nachzukommen ist.[425] Weiterhin kann sie festlegen, ob ein Mitgliedstaat überhaupt an dem Kooperationsnetz teilnehmen darf, was einer qualitativen Kontrolle entspricht.[426] Wesentliche Voraussetzungen für eine Teilnahme liegen in der ausreichenden Ausstattung der nationalen NIS-Behörden und der CERTs sowie in der Bereitstellung von sicheren Informations- und Kommunikationskanälen.

7.1.1.3.2 Gestaltung des Kooperationsnetzes

Der Entwurf zeigt auf, welche Vorstellungen die Kommission von den zukünftigen Rahmenbedingungen hat, die zur Gewährleistung von EU-weiter Netz- und Informationssicherheit erforderlich sind. Fraglich bleibt jedoch, wie das Kooperationsnetz konkret ausgestaltet sein wird. In Betracht kommen dabei eine zentrale und eine dezentrale Organisationsform.

Bei einer zentralen Organisation stünde in der Hierarchie über den nationalen NIS-Behörden und ihren CERTs noch eine EU-NIS-Behörde, die an die ENISA angegliedert sein könnte. Ein Vorteil dieses Ansatzes bestünde darin, dass damit eine Stelle existieren würde, die koordinative Aufgaben wahrnehmen kann. Ferner könnte eine solche zentrale Behörde die Meldungen der einzelnen NIS-Behörden vorsortieren und zusammenfassen. Dadurch kann sich das Verfahren insgesamt übersichtlicher gestalten. Auch dem Ziel von Vertraulichkeit der übermittelten Daten kann besser nachgekommen werden, etwa indem die Behörde vertrauliche Daten nochmals überprüft.

Der Entwurf scheint jedoch eher von einer dezentralen Organisation auszugehen, bei der keine mit besonderen eigenständigen Befugnissen ausgestattete, übergeordnete Behörde besteht. So spricht Erwägungsgrund 13 lediglich davon, dass die ENISA ganz allgemein Unterstützung bei dem Aufbau des Kooperationsnetzes leistet. Es ist jedoch keine Rede davon, dass der Informationsaustausch über sie koordiniert wird. Auch die Schaffung einer anderen, neuen EU-Behörde erwähnt der Entwurf nicht. Insofern hätte der Entwurf von einer übergeordneten NIS-Behörde sprechen können. Stattdessen ist lediglich die Rede von dem Kooperationsnetz. Dieses soll allerdings auch nicht ohne Aufgabe bleiben, sondern den Austausch von Verfahren fördern sowie die Organisation bei Sicherheitsprüfungen leiten.[427] Dies kann ein bloßer Kommunikationskanal allerdings kaum leisten, sodass zumindest

[425] Art. 12 NIS-RL-E und Art. 14 Abs. 6 NIS-RL-E.
[426] Vgl. Art. 9 Abs. 3 NIS-RL-E sowie Erwägungsgrund 14.
[427] S. Erwägungsgrund 13.

der (wohl) auf EU-Ebene angesiedelte Netzbetreiber in geringem Umfang auch außerhalb der bloßen Bereitstellung des Netzes tätig sein würde.

Hintergrund dürfte sein, dass ein möglichst zeitnaher und reger Austausch zwischen den NIS-Behörden der Mitgliedstaaten das Ziel ist. Eine weitere Zwischenstelle mit eigenständigen, weitreichenden Befugnissen und Pflichten scheint hierfür aus Sicht der Kommission hinderlich und verzögernd zu wirken, zumindest jedoch nicht erforderlich zu sein. Vorausgesetzt wird damit ein hohes Maß an Vertrauen, das zwischen den teilnehmenden Mitgliedstaaten besteht. Die entscheidende Bedeutung kommt der Sicherheit des Netzes selber zu, da über das Netz hochvertrauliche Informationen übermittelt werden würden, wenn alle Teilnehmer ihre Verpflichtungen ernst nähmen. Damit müssen wiederum die Netze der Teilnehmer selbst Sicherheit und Robustheit aufweisen, was von der Kommission zu Recht als Teilnahmevoraussetzung definiert wird.

Somit lässt sich festhalten, dass die dezentrale Organisationsform die von der Kommission bevorzugte Variante zu sein scheint. Das Kooperationsnetz braucht jedoch auch einen Betreiber. Dieser soll allerdings – die derzeitige Informationslage zugrunde legend – keine oder nur sehr eingeschränkte eigene Befugnisse haben und keine zentrale Anlaufstelle bilden. Die Kommunikation erfolgt nach Kommissionsplanungen vielmehr direkt zwischen den NIS-Behörden der Mitgliedstaaten unter Beteiligung der Kommission.

7.1.2 Pläne des Bundesministerium des Innern

Das Bundesministerium des Innern unter der Ägide *Hans-Peter Friedrich*s legte am 5. März 2013 einen Entwurf für ein Gesetz vor, das sich mit der Sicherheit der Netze und Informationstechnik auseinandersetzt. Der Entwurf für ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme[428] weist zahlreiche Übereinstimmungen mit den Plänen der Kommission auf.[429] Er sollte ursprünglich noch vor der Bundestagswahl 2013 verabschiedet werden, was jedoch auf Grund des kurzen Zeitraums zwischen März und September und dem von der Wirtschaft

[428] Referentenentwurf des BMI vom 5. 3. 2013, Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme. Im Folgenden IT-SiG-E.
[429] Eine ausführliche Erarbeitung der Regelungsinhalte des IT-SiG-E sowie ein Vergleich mit dem NIS-RL-E erfolgt in *Roos*, K&R 2013, 769. Zu Auswirkungen auf Compliance und Haftung bei *Beucher/Utzerath*, MMR 2013, 362.

geäußerten Widerstand nicht gelang. Nach dem Koalitionsvertrag von CDU, CSU und SPD wird jedoch an dem Vorhaben zur Schaffung eines IT-SiG festgehalten.[430]

Der IT-SiG-E aus dem März 2013 sieht ebenfalls die Verpflichtung der Betreiber kritischer Infrastrukturen vor, „schwerwiegende Beeinträchtigungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, das heißt Beeinträchtigungen, die Auswirkungen auf die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastruktur haben können, unverzüglich an das Bundesamt [für Sicherheit in der Informationstechnik] […] melden" zu müssen.[431] Damit würde ein mögliches IT-SiG bereits die von dem NIS-RL-E verlangte Meldepflicht einführen. Überdies sollen die Betreiber kritischer Infrastrukturen zur Schaffung angemessener organisatorischer und technischer Vorkehrungen zum Schutz ihrer Informationstechnik verpflichtet werden, was ebenfalls auf der Linie des Richtlinienvorschlags liegt.

Ein Unterschied zum Richtlinienvorschlag der Kommission besteht jedoch darin, dass sich der IT-SiG-E auch an Telekommunikationsunternehmen wendet und u. a. deren bereits bestehende Meldepflicht aus § 109 Abs. 5 TKG erweitern will, indem die Anforderungen, wann eine Meldung zu erfolgen hat, abgesenkt werden.[432] Es bleibt nach den Plänen jedoch dabei, dass die BNetzA als Meldestelle fungiert. Diese wiederum unterrichtet das BSI über die ihr bekannten Vorfälle. Die Sicherheitsanforderungen an Telekommunikationsunternehmen würden ebenfalls angehoben werden und der „Stand der Technik" als Maßstab gelten.

Mit der Anhebung der allgemeinen Sicherheitsanforderungen und der Einführung von Meldepflichten verbunden wäre die Erweiterung des Aufgabenspektrums des BSI. Über seine Funktion als zentrale Meldestelle für die Betreiber kritischer Infrastrukturen hinaus würde ihm auch die Aufgabe der Überprüfung zukommen, ob die Sicherheitsstandards eingehalten werden. Weiterhin ist vorgesehen, dass das BSI beratend und unterstützend fungiert. Zudem soll es mit Hilfe der ihm übermittelten Daten einen Lagebericht erstellen, der mindestens einmal jährlich veröffentlicht wird, und somit auch für eine Sensibilisierung des Bewusstseins für IT-Sicherheit in der Bevölkerung sorgen soll.

[430] Koalitionsvertrag zwischen CDU, CSU und SPD (18. Legislaturperiode), S. 147. Abrufbar unter https://www.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf.
[431] § 8b Abs. 4 BSIG IT-SiG-E.
[432] § 109a Abs. 4 TKG IT-SiG-E.

7.2 Einordnung in die legislativen Vorhaben

Das wesentliche Merkmal von MonIKA besteht in dem kooperativen Ansatz, der sich in Form des kooperativen Monitorings durch das CSOC äußert.

7.2.1 Vergleich zwischen MonIKA-Verfahren und Plänen für ein Kooperationsnetz

Fraglich ist zunächst, ob sich die Mechanismen von MonIKA und des geplanten EU-weiten Kooperationsnetzes gleichen oder voneinander unterscheiden.

7.2.1.1 Grundlegende Mechanismen des Kooperationsnetzes

Das EU-Kooperationsnetz ist – soweit der NIS-RL-E Rückschlüsse zulässt – dreigliedrig aufgebaut, wenn es um die Schritte von der Erkennung des Sicherheitsvorfalls oder Sicherheitsrisikos durch einen Betroffenen bis zu der Warnung durch die nationale NIS-Behörde an andere geht.

Der erste Schritt besteht darin, dass die zur Einhaltung von Mindestanforderungen und der Meldung Verpflichteten ein Sicherheitsrisiko oder einen Sicherheitsvorfall erkennen müssen. Dies bedeutet, dass diese Verpflichteten einen Umstand oder ein Ereignis, das potenziell oder tatsächlich negative Auswirkungen auf die Netz- und Informationssicherheit haben könnte bzw. sogar schon hatte, erfasst haben. Auf welche Weise dies zu geschehen hat, schreibt der NIS-RL-E nicht konkret vor. Vielmehr wird die Sicherstellung, dass ein derartiger Angriff oder eine derartige Störung auch von dem Verpflichteten registriert werden kann, Teil der Mindestanforderungen sein, die die Verpflichteten einzuhalten haben und die sie gegenüber der nationalen NIS-Behörde nachweisen müssen.

In einem zweiten Schritt müssen die Verpflichteten diesen registrierten Vorfall ihrer nationalen NIS-Behörde melden. Der NIS-RL-E verlangt, dass lediglich Sicherheitsvorfälle gemeldet werden müssen, die eine erhebliche Auswirkung auf die Sicherheit von Kerndiensten haben: Die Meldung von Sicherheitsrisiken der Verpflichteten an die nationale NIS-Behörde verlangt die Kommission damit nicht. Der NIS-RLE verlangt (nach derzeitigem Stand) nur die Einhaltung von Mindestanforderungen – die Mitgliedstaaten könnten auch eine Verpflichtung zur Meldung von Sicherheitsrisiken vorschreiben. Das ergibt sich aus Art. 2 NIS-RL-E, der deutlich macht, dass die Vorgaben aus dem NIS-RL-E nur i. S. einer Mindestharmonisierung zu deuten sind.

Nachdem die nationale NIS-Behörde durch die Meldung Kenntnis von dem Sicherheitsvorfall (oder ggf. dem Sicherheitsrisiko) erlangt hat, liegt das Heft des Handelns in ihrer Hand und sie muss tätig werden. Dazu zählt zum einen, dass sie sich an die ihr vorliegenden nationalen Warn- und Alarmierungskontakte wendet. Zum anderen ist sie dazu verpflichtet, unter bestimmten Umständen eine Frühwarnung i. S. d. Art. 10 NIS-RL-E über das Kooperationsnetz zu entsenden. Eine Frühwarnung muss ausgegeben werden, wenn mindestens das Potenzial für eine rasche Ausweitung oder die Übersteigung der nationalen Kapazitäten besteht. Auch für den Fall, dass das Sicherheitsrisiko oder der Sicherheitsvorfall einen anderen Mitgliedstaat betreffen könnte, muss die Frühwarnung über das Kooperationsnetz ausgegeben werden.

Über diese Mechanismen erhalten die anderen NIS-Behörden Kenntnis und können ihre Informationen an die national ansässigen Unternehmen sowie an die Verwaltungsträger weiterreichen.

7.2.1.2 Grundlegende Mechanismen bei MonIKA

Für die Erklärung der Funktionsweise von MonIKA kann beispielhaft auf den Sachverhalt des PoC (4.2) verwiesen werden. Zu betonen ist, dass MonIKA darauf aufbaut, dass die Teilnehmer die MonIKA-Agenten an die Sensorik ihres eigenen Unternehmens anschließen und MonIKA somit in ihr Sicherheitskonzept integrieren. Über die angeschlossenen MonIKA-Agenten werden bestimmte Daten an das CSOC übermittelt, das auf Basis der gesammelten Daten aller Teilnehmer eine fortlaufende Auswertung vornehmen kann. Die Ergebnisse dieser Analyse werden den Teilnehmern dann als Frühwarnungen zur Verfügung gestellt.

7.2.1.3 Übereinstimmungen und Unterschiede

Übereinstimmend dienen sowohl das Kooperationsnetz als auch MonIKA dem Zweck, dass potenzielle Opfer von Cyber-Attacken rechtzeitig gewarnt werden und sich auf die möglichen Angriffe vorbereiten können. Der Schwerpunkt liegt damit jeweils auf der Prävention. Dies soll durch die Einbeziehung einer Vielzahl von Teilnehmern, also einer Kooperation, gelingen.

Aus einem detaillierteren Vergleich der Abläufe ergeben sich jedoch auch Unterschiede.

Als entscheidender Unterschied kristallisiert sich dabei heraus, dass MonIKA vornehmlich darauf ausgerichtet ist, dass Sicherheitsrisiken (und möglicherweise auch Sicherheitsvorfälle) entdeckt werden, während das

Kooperationsnetz von den Verpflichteten entdeckte Risiken und Vorfälle als Voraussetzung betrachtet. MonIKA setzt damit im Schema der Mechanismen des Kooperationsnetzes noch auf bzw. vor der ersten Stufe an. Die Anwendung von MonIKA unterstützt zum einen die an dem Verfahren partizipierenden Unternehmen. Zum anderen wirkt sich die durch MonIKA erzielte Verbesserung der Möglichkeiten eines Unternehmens, Anomalien zu entdecken, auch positiv auf die Funktionsfähigkeit und Effektivität des Kooperationsnetzes aus, wenn in frühzeitigerem Stadium meldepflichtige Fälle entdeckt werden können und der Meldepflicht nachgekommen wird.

Unterschiedlich ist weiterhin, dass bei MonIKA die Warnungen das Ergebnis einer Datenanalyse sind, während eine Datenanalyse – zumindest betreffend ungefiltert, automatisiert übersendeter Daten – in dem Aufbau des Kooperationsnetzes an keiner Stelle vorgesehen ist: Weder den nationalen NIS-Behörden noch einer Instanz auf EU-Ebene sollen automatisiert Daten übermittelt werden, die diese dann analysieren. Abgesehen von dem unschwer vorherzusagenden massiven Widerstand durch die Wirtschaft, würde es die derzeitigen Kapazitäten der nationalen NIS-Behörden wohl auch erheblich überfordern, wenn sämtliche der Verpflichteten bestimmte Daten ungefiltert an sie überspielen müssten. Vielmehr sollen der nationalen NIS-Behörde nur die entscheidenden Informationen zur Verfügung gestellt werden. Die Intensität der Kooperation, die das Netz und MonIKA verlangen, ist somit ebenfalls eine andere.

7.2.1.4 Zwischenergebnis

Es lässt sich damit festhalten, dass sich die Ansätze von Kooperationsnetz und MonIKA in ihren Details durchaus unterscheiden. Der signifikanteste Unterschied liegt darin, dass MonIKA die Entdeckung von Risiken und Vorfällen zum Ziel hat, während das Kooperationsnetz bereits entdeckte (und auch gemeldete) Vorfälle und Risiken voraussetzt. Das sagt jedoch nichts darüber aus, dass die MonIKA-Agenten bei entsprechender Konfiguration nicht auch für das Kooperationsnetz oder den Meldemechanismus gegenüber der nationalen NIS-Behörde nutzbar gemacht werden könnten.

7.2.2 Kooperatives Monitoring als gesetzliche Pflicht?

Fraglich ist, ob ein kooperatives Monitoring, wie es Grundidee von MonIKA ist, zu einer gesetzlichen Pflicht für die Unternehmen und die Verwaltung erhoben werden könnte.

Anhaltspunkte für die Beantwortung dieser Frage enthält Erwägungsgrund 15 des NIS-RL-E. Dort heißt es:

„*Da die meisten Netze und Informationssysteme privat betrieben werden, ist die Zusammenarbeit zwischen dem privaten und dem öffentlichen Sektor von zentraler Bedeutung. Die Marktteilnehmer sollten angehalten werden, sich eines eigenen informellen Kooperationsmechanismus zur Gewährleistung der NIS (Anm.: NIS steht für Netz- und Informationssicherheit) zu bedienen. Sie sollten ferner mit dem öffentlichen Sektor zusammenarbeiten und Informationen und bewährte Verfahren austauschen und im Gegenzug operative Unterstützung im Falle von Sicherheitsvorfällen erhalten.*“

Entscheidend ist dessen zweiter Satz, in dem die Kommission verdeutlicht, dass die Etablierung eines eigenen Kooperationsmechanismus durch die Marktteilnehmer ein Ziel der Sicherheitsstrategie sein sollte. Unter einem Kooperationsmechanismus versteht der NIS-RL-E einen Informationsaustausch sowie eine koordinierte Erkennungs- und Reaktionsfähigkeit.[433] Adressaten von Erwägungsgrund 15 Satz 2 sind dabei die Mitgliedstaaten, die Anreize für derartige Kooperationen setzen sollen. Es liegt also ganz auf der Linie des NIS-RL-E, sollten sich Private – unabhängig von ihren Pflichten gegenüber dem Staat und frei von staatlicher Kontrolle („informell“) – dazu entschließen, sich gegenseitig über Vorfälle und Risiken zu informieren und zu warnen. Es sollen also privat betriebene Netzwerke eingerichtet werden.

Der Kooperationsansatz ist MonIKA jedenfalls immanent. Das kooperative Monitoring geht sogar über die bloße Meldung und Warnung hinaus und es besteht eine nähere Zusammenarbeit. Durch diese Zusammenarbeit entsteht auch das Potenzial, dass ein höheres Maß an Sicherheit gewährleistet werden kann. Grundvoraussetzung hierfür ist ein Mindestmaß an gegenseitigem Vertrauen der Partner.

Der Koalitionsvertrag greift den Aspekt der Kooperation ebenfalls auf und es ist die Rede davon, die Betreiber kritischer Infrastrukturen neben den gesetzlichen Vorgaben auch zu Kooperationen anhalten zu wollen, durch die der Schutz verbessert werden kann.[434] Der IT-SiG-E geht auf diesen Aspekt des Erwägungsgrundes 15 (noch) nicht explizit ein, aber strebt jedenfalls – entsprechend Erwägungsgrund 15 Satz 3 – auch eine Zusammenarbeit von Staat und Wirtschaft

[433] Vgl. Erwägungsgrund 4 NIS-RL-E.
[434] Koalitionsvertrag zwischen CDU, CSU und SPD (18. Legislaturperiode), S. 150.

an.[435] Dass gerade Kooperationen innerhalb der Wirtschaft aus Sicht des Bundesministerium des Innern ein erstrebenswertes Ziel darstellen, verdeutlicht § 8a Abs. 3 BSIG IT-SiG-E. Die Norm betrifft die nach § 8a Abs. 1 BSIG IT-SiG-E verlangte Einhaltung der Mindeststandards und eröffnet den Betreibern kritischer Infrastrukturen bzw. deren Branchenverbänden die Möglichkeit der gemeinsamen – innerhalb der Branche geltenden – Mindeststandards, die vom BSI als angemessene Sicherheitsmaßnahmen anerkannt werden können. In diesem Kontext erscheint es möglich, dass für die Betreiber kritischer Infrastrukturen innerhalb einer Branche ein kooperatives Monitoring-Verfahren wie MonIKA einen – möglicherweise sogar wesentlichen – Baustein darstellt, um den Sicherheitsanforderungen nachzukommen.

Zu betonen ist aber auch, dass der Betrieb kooperativer Monitoring-Verfahren durch privatwirtschaftliche Unternehmen oder Verwaltungsträger kurzfristig wohl nicht als gesetzliche Pflicht eingeführt werden wird. Allerdings weisen sowohl das Bundesministerium des Innern als auch die Kommission ein Interesse daran auf, dass Unternehmen in Sachen IT-Sicherheit zusammenarbeiten. Dies rührt schon aus dem Umstand her, dass die Bundesrepublik Deutschland und die Europäische Union ein attraktiver Wirtschaftsstandort sein und bleiben wollen, wobei die Netzsicherheit als wesentlicher Faktor hierfür qualifiziert werden kann.

7.2.3 Ergebnis

Es zeigt sich, dass MonIKA und die Schritte im Kooperationsnetz von ihrer Konzeption her nicht miteinander gleichzusetzen sind, auch wenn beide Ansätze insbesondere das Ziel einer Prävention vor Sicherheitsvorfällen in den Mittelpunkt stellen. Die Kommission rät allerdings den Mitgliedstaaten dazu, auf die Unternehmen und Verwaltungsträger einzuwirken, damit diese unabhängig vom Staat zusammenarbeiten.

Es erscheint damit auch möglich, dass der Staat die Unternehmen bei dem Aufbau kooperativer Monitoring-Verfahren unterstützt. Die Möglichkeiten hierfür sind vielfältig: Sie reichen von einer finanziellen Unterstützung bis zu einer Unterstützung durch die kostenfreie Bereitstellung entsprechender Verfahren, die betrieben werden können. Dabei ist jedoch wichtig, dass es zu keiner staatlichen Kontrolle kommt, denn ansonsten würden mögliche Angebote wohl nur mit Zurückhaltung angenommen werden.

[435] IT-SiG-E, S. 2.

7.3 Einsatz von MonIKA zur Unterstützung bei der Einhaltung von Sicherheitsstandards und der Erfüllung von Meldepflichten

Im Folgenden soll erarbeitet werden, wie MonIKA in Anbetracht dieser – zu unterstellenden – neuen rechtlichen Rahmenbedingungen eingesetzt werden könnte.

7.3.1 Integration in das IT-Sicherheitskonzept der Unternehmen

Die im PoC untersuchte Möglichkeit für einen Einsatz von MonIKA durch privatrechtlich organisierte Unternehmen lässt sich als wahrscheinlichste Variante benennen. Die Unternehmen versprechen sich von dem Einsatz des Verfahrens – schon im eigenen Interesse – ein höheres Maß an IT-Sicherheit. Es müssen jedoch nicht nur (wie im PoC) wirtschaftlich voneinander abhängige Unternehmen die Teilnehmer an einem MonIKA-Netzwerk sein. Auch Unternehmen, die übereinstimmende oder zumindest ähnliche Angriffsfelder bieten, könnten ein MonIKA-Netzwerk betreiben (lassen). Zu denken ist hier an Betreiber kritischer Infrastrukturen einer bestimmten Branche wie ISPs oder Energieversorger.

MonIKA kann für die Unternehmen zum einen ein Mittel sein, um den vom BSI bzw. den Auditoren überprüften Sicherheitsmindeststandards nachzukommen. Das kooperative Monitoring sorgt für eine Verbesserung der Überwachung des Netzwerkverkehrs hinsichtlich Bedrohungen und Vorfällen. Insofern ist die Integration von MonIKA in das Sicherheitskonzept schon unter diesem Aspekt lohnenswert.

Zum anderen könnte der Einsatz von MonIKA dazu führen, dass die Unternehmen den mit der Meldepflicht verbundenen Verwaltungsaufwand reduzieren können, indem sie dies den IT-Sicherheitsdienstleister, der MonIKA betreibt und übergeordnete Instanz ist (CSOC), erledigen lassen. Dies bietet sich an, da diesem sämtliche sicherheitsrelevanten Daten durch die Agenten übermittelt und ihm Risiken und etwaige Vorfälle ohnehin bekannt werden.

7.3.2 Zulässigkeit der Übernahme von Meldepflichten durch Dritte

Fraglich ist allerdings, ob es rechtlich zulässig wäre, dass ein Dritter für den Verpflichteten der Meldung eines Sicherheitsvorfalls nachkommt.

An einer ausdrücklichen Regelung zu dieser Fragestellung mangelt es sowohl dem NIS-RL-E als auch dem IT-SiG-E. Während der NIS-RL-E die Mitgliedstaaten lediglich allgemein dazu verpflichtet, zu gewährleisten, dass

Sicherheitsvorfälle an die NIS-Behörde gemeldet werden[436], wird der IT-SiG-E an dieser Stelle schon konkreter, indem Vorgaben existieren, wie die Unternehmen ihrer Meldepflicht nachkommen können. Die Betreiber kritischer Infrastrukturen müssen dem BSI – als nationaler NIS-Behörde – Warn- und Alarmierungskontakte benennen, deren jederzeitige Erreichbarkeit vorausgesetzt wird. Über diese soll das Unternehmen dem BSI Sicherheitsvorfälle melden, aber auch Informationen bzw. Warnungen empfangen können.[437] Orientiert man sich an dem Wortlaut der Norm, so kann man davon ausgehen, dass es nicht ausgeschlossen ist, dass ein Dritter der Warn- und Alarmierungskontakt sein kann. Auch trifft der IT-SiG-E keine klare Aussage darüber, ob mehrere Warn- und Alarmierungskontakte bestehen können. Einzig die Verwendung des Plurals gibt einen Hinweis darauf, dass es zulässig sein dürfte, dass mehrere Ansprechpartner innerhalb des Unternehmens existieren. Jedenfalls muss sichergestellt sein, dass eine jederzeitige Erreichbarkeit gegeben ist.

Orientiert man sich an den Zielen des NIS-RL-E, ist es entscheidend, dass ein möglichst direkter Kontakt zu den Unternehmen besteht und Verzögerungen weitgehend ausgeschlossen sind. Dies beruht darauf, dass sich ein effektiver Schutz ansonsten kaum gewährleisten lassen dürfte. Daher könnte man folgern, dass ein Dritter – bspw. der externe IT-Sicherheitsdienstleister, der MonIKA betreibt – unmittelbar auf die Komponenten der unternehmenseigenen IT zugreifen können muss. Das wird jedoch wohl nur in seltenen Fällen praktiziert und geht im Übrigen über MonIKA hinaus.

Allerdings bietet es sich durchaus an, zwischen der Meldung durch das Unternehmen und dem Empfang von Informationen durch die NIS-Behörde zu unterscheiden. Ein Dritter, der über eine Vielzahl sicherheitsrelevanter Daten verfügt und somit über Risiken und Vorfälle bei der Unternehmens-IT jederzeit informiert ist, kann auf demselben (oder zumindest ähnlich hohem) Kenntnisstand wie das Unternehmen selbst sein. Schon aus diesem Grund liegt es nahe, dass es rechtlich zulässig ist, dass ein Dritter der Meldepflicht ebenfalls nachkommen kann, insbesondere wenn meldepflichtige Vorgänge durch ihn für den Verpflichteten aufgedeckt wurden.

Sollte sich das Unternehmen dazu entschließen, dass das CSOC für ihn der Meldepflicht nachkommen soll, dann liegt es im beiderseitigen Interesse, dass eine Policy erarbeitet wird oder der Vertrag bereits Bezug darauf nimmt, welche Daten in

[436] S. Art. 14 Abs. 2 NIS-RL-E.
[437] § 8b Abs. 3 und Abs. 4 BSIG IT-SiG-E.

welcher Form an das BSI übermittelt werden, soweit überhaupt Spielraum besteht. Auch für Haftungsfragen sollten Regelungen enthalten sein. Das Unternehmen muss ferner sicherstellen, dass das CSOC seiner Aufgabe tatsächlich nachkommt, da die Letztverantwortlichkeit bei dem verpflichteten Unternehmen liegt.

7.3.3 Ergebnis

MonIKA bietet auch unter Berücksichtigung der legislativen Vorhaben Vorteile für die partizipierenden Unternehmen. Es kann ein wichtiger Baustein des IT-Sicherheitskonzepts sein, dessen Resilienz in den Audits durch das BSI geprüft werden wird. Weiterhin kann das CSOC als die Sicherheitsvorfälle meldende Stelle eingesetzt werden, sofern das partizipierende Unternehmen dies wünscht. NIS-RL-E und IT-SiG-E schließen nicht aus, dass Dritte für das Unternehmen der Meldepflicht nachkommen, soweit sie über dieselben Informationen verfügen.

7.4 Einsatz von MonIKA durch eine staatliche Stelle

Zumindest denkbar erscheint es auch, dass MonIKA durch eine staatliche Stelle wie das BSI genutzt würde und das BSI das Monitoring sämtlicher oder bestimmter einzelner kritischer Infrastrukturen übernimmt.[438] Dies dürfte jedoch einerseits in praktischer Hinsicht weit über die derzeitigen und mittelbar absehbaren Kapazitäten des BSI hinausreichen. Andererseits werden dies nach derzeitigem Stand auch die Unternehmen mit Vehemenz ablehnen, sofern man sich schon ihren Widerstand gegen eine Meldepflicht vor Augen führt. Zumindest für die nächsten Jahre kann dieses Szenario also ausgeschlossen werden, da die Zusammenarbeit von Staat und Wirtschaft in Fragen der IT-Sicherheit noch am Anfang steht. Erste Schritte wie die Gründung der Allianz für Cybersicherheit e. V. als co-regulierte Initiative durch das BSI in Zusammenarbeit mit dem Branchenverband BITKOM können aber Grundlagen für eine nachhaltigere und intensivere Zusammenarbeit schaffen.

Zu überlegen wäre jedoch, ob das BSI ein Verfahren wie MonIKA für die übergreifende Überwachung der IT-Sicherheit von Bundes- und Landesbehörden nutzt. Auch hier könnte ein kooperatives Monitoring, sollte es nicht bereits betrieben werden, einen Sicherheitsfortschritt bedeuten. Angesichts der möglichen Brisanz

[438] S. bereits oben unter 4.7.

einer ungewollten Veröffentlichung vertraulicher staatlicher Dokumente sollten keine Möglichkeiten zur Steigerung der IT-Sicherheit außer Acht gelassen werden.

7.5 Fazit

Festhalten lässt sich, dass die Ziele der Anwendung von MonIKA mit den Zielen und Bestrebungen der Kommission und des BMI nach einer Kooperation der Beteiligten, die zu besseren Präventionsmöglichkeiten führt, übereinstimmen.

MonIKA kann in Anbetracht der legislativen Bestrebungen zudem eine sinnvolle Anwendung und ggf. Ergänzung innerhalb jedes IT-Sicherheitskonzepts darstellen. Geht man von einer Umsetzung der derzeitigen Pläne aus, wird es auch rechtlich zulässig sein, dass der IT-Sicherheitsdienstleister als Dritter Meldepflichten für das/die Unternehmen übernimmt, was die Anwendung von MonIKA zusätzlich lohnenswert erscheinen lässt.

8 Zusammenfassung der Thesen

Für Unternehmen bestehen sowohl öffentlich-rechtliche als auch zivilrechtliche Verpflichtungen zur Schaffung von IT-Sicherheit. Sollten diese Verpflichtungen nicht eingehalten werden, so kann dies eine Haftung sowohl für das Unternehmen als auch für die Unternehmensleitung begründen.

Die ISPs haben ihre Netze und ihre Kunden vor Gefährdungen zu schützen. Allerdings folgt hieraus keine Pflicht für die ISPs, Desinfektionsmaßnahmen durchzuführen. Die Durchführung von Desinfektionsmaßnahmen bedeutet hohe zivilrechtliche Risiken für die ISPs oder andere Handelnde. Auch besteht die Gefahr einer strafrechtlichen Haftung für die ausführenden Personen.

Das MonIKA-Softwareframework ist als Software urheberrechtlich geschützt. Auch ist wettbewerbsrechtlicher und markenrechtlicher Schutz möglich. Das MonIKA-Softwareframework (EvASC, MonIKA-Agent) kann nach derzeitiger Informationslage als Standardsoftware eingeordnet werden. Die Überlassung des MonIKA-Softwareframeworks richtet sich nach kaufrechtlichen Regelungen.

Der Vertrag, der zwischen der MonIKA GmbH und den einzelnen Teilnehmern geschlossen wird, ist als typengemischter Vertrag zu bewerten. In Bezug auf die Überlassung der MonIKA-Agenten an die Teilnehmer sind kaufrechtliche Regeln anzuwenden. Das Analyseverfahren unterfällt dienstvertraglichen Regelungen. Die Teilnehmer haben die Pflicht, die erforderlichen Daten und Informationen an die MonIKA GmbH weiterzuleiten. Dies sollte vertraglich festgelegt werden. Hier sollten die erforderlichen Daten und Informationen definiert und einzeln aufgezählt werden. Es sollte festgelegt werden, welche Daten für das MonIKA-Verfahren erforderlich sind.

Innerhalb der im Rahmen des PoC untersuchten Haftungsszenarien kann eine Haftung nicht ausgeschlossen werden, wenn die Risiken auch überwiegend gering sein dürften. Der Grund liegt in der Verwendung von kaum haftungsrelevanten Daten im PoC. Das Eingreifen eines Schadensersatzanspruchs hängt entscheidend von den Auswirkungen im Einzelfall ab. Insbesondere die Frage nach dem Vorliegen eines ersatzfähigen Schadens beurteilt sich nach den konkreten Auswirkungen in der jeweiligen Situation. Das geringste Haftungsrisiko besteht bei einer bloßen Falschwarnung, da dort der Eintritt eines Schadens nicht realistisch erscheint.

Vertraglich können Haftungsbegrenzungen und Haftungsausschlüsse vereinbart werden. Insbesondere individualvertraglich sind weitgehende Haftungsbegrenzungen und Haftungsausschlüsse möglich. Eine Haftung für vorsätzlich verursachte Schäden kann jedoch nicht ausgeschlossen werden. Im Rahmen von AGB sind derart weitgehende Haftungsbegrenzungen nicht möglich. Für wesentliche Vertragspflichten kann in AGB eine Haftung nicht ausgeschlossen oder begrenzt werden. Wesentliche Vertragspflicht innerhalb des MonIKA-Verfahrens stellt die Durchführung des Analyseverfahrens mit der Ausgabe von Warnungen an die Vertragspartner dar. Die Haftung für einfache bis mittlere Fahrlässigkeit kann für nichtwesentliche Vertragspflichten ausgeschlossen werden.

Die Verträge sollten einen ausdrücklichen Hinweis auf die Unverbindlichkeit der Warnungen enthalten. Auch sollte festgehalten werden, dass die Teilnehmer eigenverantwortlich entscheiden, wie sie auf mögliche Warnungen reagieren wollen. Ferner kann für den Fall, dass ein Teilnehmer nicht die erforderlichen Daten oder Informationen bereitstellt, eine Vertragsstrafe fixiert werden.

Ein Idealverein kann als alternative Rechtsform für die MonIKA GmbH nicht gewählt werden. Dies gilt jedenfalls für die Konstellation im PoC, da die Tätigkeit der MonIKA GmbH als wirtschaftliche Tätigkeit einzustufen ist.

Ein durch den Staat durchgeführtes kooperatives Monitoring beinhaltet ein geringes Haftungsrisiko. Für die Abgabe einer staatlichen Warnung kann § 7 BSIG als Ermächtigungsgrundlage herangezogen werden. Allerdings müsste noch eine Ermächtigungsgrundlage geschaffen werden, die die Unternehmen zur Datenübermittlung verpflichtet.

Im Anwendungsverfahren „Spam-Kampagnen-Erkennung zur Klassifikation von Bots“ bestehen geringe zivilrechtliche Haftungsrisiken für den Anwender des MonIKA-Verfahrens. Auch unter strafrechtlichen Gesichtspunkten besteht keine Haftung, soweit die Pseudonymisierung funktionsfähig ist.

Für den Anwendungsfall „Überwachung des Internetroutings“ sind haftungsrechtlich keine Unterschiede zum PoC und zum Anwendungsfall „Enterprise-Monitoring“ feststellbar.

Es ist davon auszugehen, dass kurz- oder mittelfristig ein IT-Sicherheitsgesetz verabschiedet wird, das verschiedene Akteure dazu verpflichtet, Mindeststandards an IT-Sicherheit zu etablieren. Überdies kann davon ausgegangen werden, dass Meldepflichten bei IT-Sicherheitsvorfällen eingeführt werden. MonIKA gewinnt

durch diese legislativen Vorhaben an Relevanz. Dass der Staat selber kurz- oder mittelfristig ein kooperatives Monitoring – vergleichbar mit MonIKA – durchführen wird, ist jedoch nicht abzusehen. Das MonIKA-Verfahren kann für die Unternehmen ein wichtiger Baustein sein, um den (neuen) Sicherheitsanforderungen nachzukommen. Auch dürfte es zulässig sein, dass – ausgehend vom PoC – der IT-Sicherheitsdienstleister (als Dritter) den Meldepflichten für das Unternehmen nachkommt.

9 Literaturverzeichnis

Ahlberg/Götting, Beck'scher Online-Kommentar Urheberrecht, Edition 3, Stand: 1.9.2013, München 2013.

Ann, Know-how – Stiefkind des Geistigen Eigentums?, GRUR 2007, S. 39 – 43.

Arndt/Fetzer/Scherer, TKG: Telekommunikationsgesetz Kommentar, Berlin 2008.

Bader/Ronellenfitsch, Beck'scher Online - Kommentar Verwaltungsverfahrensgesetz, Edition 21, Stand: 1.10.2013, München 2013.

Bamberger/Roth, Beck'scher Online-Kommentar BGB, Edition 29, Stand: 1.11.2013, München 2013.

Bartsch, Computerviren und Produkthaftung, CR 2000, S. 721 – 725.

Benkard, Patentgesetz, 10. Auflage, München 2006.

Beucher/Utzerath, Cybersicherheit – Nationale und internationale Regulierungsinitiativen – Folgen für die IT-Compliance und die Haftungsmaßstäbe, MMR 2013, S. 362 – 367.

Borges, Pflichten und Haftung beim Betrieb privater WLAN, NJW 2010, S. 2624 – 2627.

Bundeskriminalamt, Bundeslagebild Cybercrime 2012, abrufbar unter http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true.

Cornelius/Tschoepe, Strafrechtliche Grenzen der zentralen E-Mail-Filterung und -Blockade, K&R 2005, S. 269 – 271.

Detterbeck, Allgemeines Verwaltungsrecht, 11. Auflage, München 2013.

Dreier/Schulze, Urheberrechtsgesetz, 4. Auflage, München 2013.

Duisberg/Picot, Rechtsfolgen von Pannen in der Datensicherheit, CR 2009, S. 823 – 828.

Eisenhardt, Gesellschaftsrecht, 14. Auflage, München 2009.

Erman, Kommentar zum BGB, 13. Auflage, Köln 2011.

Ernst, Das neue Computerstrafrecht, NJW 2007, S. 2661 – 2666.

Ernst, Vertragsgestaltung im Internet, München 2003.

Fischer, Strafgesetzbuch und Nebengesetze, 60. Auflage, München 2013.

Foerster/Jäde, Praxis der Kommunalverwaltung , A 15 Bund, Wiesbaden 2013.

Friedrich, IT-Sicherheitsgesetz: Maßvolle Regulierung als Standortvorteil, MMR 2013, S. 273 – 274.

Gennen/Völkel, Recht der IT-Verträge, Heidelberg 2009.

Geppert/Piepenbrock/Schütz/Schuster, Beck'scher TKG-Kommentar,
4. Auflage,
München 2013.

Gola/Schomerus, Bundesdatenschutzgesetz,
11. Auflage,
München 2012.

Graf, Beck'scher Online-Kommentar
Strafprozessordnung,
Edition 17, Stand: 30.9.2013,
München 2013.

Graf von Westphalen, Vertragsrecht und ABG-Klauselwerke,
31. Auflage,
München 2012.

Härting, Die Gewährleistungspflichten von Internet-Dienstleistern,
CR 2001, S. 37 – 43.

Härting, E-Mail und Telekommunikationsgeheimnis,
CR 2007, S. 311 – 317.

Harte-Bavendamm/Henning-Bodewig, Gesetz gegen den unlauteren Wettbewerb,
3. Auflage,
München 2013.

Hauschka, Corporate Compliance,
2. Auflage,
München 2010.

Heckmann, Rechtspflichten zur Gewährleistung von IT-Sicherheit im Unternehmen - Maßstäbe für ein IT-Sicherheitsrecht,
MMR 2006, S. 280 – 285.

Heidrich, Rechtliche Fragen bei der Verwendung von DNS-Blacklisting zur Spam-Filterung,
CR 2009, S. 168 – 173.

Heidrich/Forgó/Feldmann, Heise Online-Recht,
3. Ergänzungslieferung,
Hannover 2011.

Heidrich/Tschoepe, Rechtsprobleme der Email-Filterung,
MMR 2004, S. 75 – 80.

Heydn, Identitätskrise eines Wirtschaftsguts: Software im Spannungsfeld zwischen Schuldrecht und Urheberrecht, CR 2010, S. 765 – 776.

Hoeren, IT-Vertragsrecht, 2. Auflage, Köln 2012.

Hoeren, Virenscanning und Spamfilter - Rechtliche Möglichkeiten im Kampf gegen Viren, Spams & Co., NJW 2004, S. 3513 – 3517.

Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 36. Ergänzungslieferung, München 2013.

Huppertz/Fritzsche, Titelschutz für Software, ITRB 2011, S. 86 – 89.

Jauernig, Bürgerliches Gesetzbuch, 15. Auflage, München 2014.

Joecks/Miebach, Münchener Kommentar zum StGB, 2. Auflage, München 2011.

Jüngel/Schwan/Neumann, Das Abfangen von E-Mails nach § 303a StGB, MMR 2005, S. 820 – 824.

Kiethe/Groeschke, Die Durchsetzung von Schadensersatzansprüchen in Fällen der Betriebs- und Wirtschaftsspionage, WRP 2005, S. 1358 – 1370.

Kilian/Heussen, Computerrechts-Handbuch, 31. Ergänzungslieferung, München 2012.

Kindhäuser/Neumann/Paeffgen, Strafgesetzbuch, 5. Auflage, Baden-Baden 2013.

Kitz, Meine Emails les‘ ich nicht!, CR 2005, S. 450 – 454.

Koch, Haftung für die Weiterverbreitung von Viren durch E-Mails, NJW 2004, S. 801 – 807.

Köcher, Strafbarkeit der Ausfilterung von E-Mails, DuD 2005, S. 163 - 165.

Köhler/Bornkamm, Gesetz gegen den unlauteren Wettbewerb, 31. Auflage, München 2013.

Lackner/Kühl, Strafgesetzbuch, 27. Auflage, München 2011.

Lehmann, Rechtsschutz und Verwertung von Computerprogrammen, 2. Auflage, Köln 1993.

Lehmann/Meents, Handbuch des Fachanwalts Informationstechnologierecht, Köln 2008.

Lensdorf, IT-Compliance - Maßnahmen zur Reduzierung von Haftungsrisiken von IT-Verantwortlichen, CR 2007, S. 413 – 418.

Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, 2. Auflage, München 2011.

Libertus, Zivilrechtliche Haftung und strafrechtliche Verantwortlichkeit bei unbeabsichtigter Verbreitung von Computerviren, MMR 2005, S. 507 – 512.

Loewenheim, Handbuch des Urheberrechts, 2. Auflage, München 2010.

Marly, Praxishandbuch Softwarerecht, 5. Auflage, München 2009.

Martinek/Semler/Habermeier/Flohr, Handbuch des Vertriebsrechts, 3. Auflage, München 2010.

Maunz/Dürig, Grundgesetz-Kommentar, 69. Ergänzungslieferung, München 2013.

Maurer, Allgemeines Verwaltungsrecht, 18. Auflage, München 2011.

Meier/Wehlau, Die zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung, NJW 1998, S. 1585 – 1591.

Mes, Arbeitsplatzwechsel und Geheimnisschutz, GRUR 1979, S. 584 – 593.

Müller/Bohne, Providerverträge, München 2005.

Müller-Broich, Telemediengesetz, Baden-Baden 2012.

Nolte/Becker, IT-Compliance, BB Beilage 2008, S. 23 – 27.

Oberste Finanzbehörden der Länder, Steuerliche Maßnahmen zur Berücksichtigung der Schäden aufgrund der EHEC-Epidemie, DStR 2011, S. 1523.

Palandt, Bürgerliches Gesetzbuch, 73. Auflage, München 2014.

Piper/Ohly/Sosnitza, Gesetz gegen den unlauteren Wettbewerb, 5. Auflage, München 2010.

Redeker, IT-Recht,
5. Auflage,
München 2012.

Redeker, Handbuch der IT-Verträge,
Band 2,
25. Ergänzungslieferung,
Köln 2013.

Reinhard/Pohl/Capellaro, IT-Sicherheit und Recht,
Berlin 2007.

Roos, CR 2014, n. n.

Roos, Der Entwurf eines IT-Sicherheitsgesetzes: Regelungsinhalte und ihre Übereinstimmung mit dem Richtlinienvorschlag der EU-Kommission,
K&R 2013, S. 769 – 775.

Roos/Schumacher/Elsner/ Meier/Wübbeling, Rechtliche Betrachtung von Desinfektionsmaßnahmen zur Botnetzbekämpfung durch Internet-Service-Provider, in: Hange, Michael, Informationssicherheit stärken - Vertrauen in die Zukunft schaffen (Tagungsband zum 13. Deutschen IT-Sicherheitskongress), S. 37 – 53.

Säcker, Berliner Kommentar zum Telekommunikationsgesetz,
3. Auflage,
Frankfurt a. M. 2013.

Säcker/Rixecker, Münchener Kommentar zum Bürgerlichen Gesetzbuch,
6. Auflage,
München 2012.

Sassenberg/Mantz, Die (private) E-Mail-Nutzung im Unternehmen,
BB 2013, S. 889-894.

Sauter/Schweyer/Waldner, Der eingetragene Verein,
19. Auflage,
München 2010.

Schack, Urheber- und Urhebervertragsrecht,
6. Auflage,
Tübingen 2013.

Scheurle/Mayen, Telekommunikationsgesetz,
2. Auflage,
München 2008.

Schneider, Handbuch des EDV-Rechts,
4. Auflage,
Köln 2009.

Schoch, Amtliche Publikumsinformation zwischen staatlichem Schutzauftrag und Staatshaftung,
NJW 2012, S. 2844 - 2850.

Schönke/Schröder, Strafgesetzbuch,
29. Auflage,
München 2014.

Schricker/Loewenheim, Urheberrecht,
4. Auflage,
München 2010.

Schulze u.a., BGB Handkommentar,
7. Auflage,
Baden-Baden 2011.

Schuster, IT-gestützte interne Ermittlungen in Unternehmen – Strafbarkeitsrisiken nach den §§ 202a, 206 StGB,
ZIS 2010, S. 68 – 75.

Schuster, Vertragshandbuch Telemedia,
München 2001.

Schwartmann, Praxis Handbuch Medien-, IT- und Urheberrecht,
2. Auflage,
Heidelberg 2011.

Soergel, Bürgerliches Gesetzbuch,
13. Auflage,
Stuttgart 2000.

Spindler, IT-Sicherheit – Rechtliche Defizite und rechtspolitische Alternativen, MMR 2008, S. 7 – 13.

Spindler, Vertragsrecht der Internetprovider, 2. Auflage Köln 2004.

Spindler/Ernst, Vertragsgestaltung für den Einsatz von E-Mail-Filtern, CR 2004, S. 437 – 445.

Spindler/Schuster, Recht der elektronischen Medien, 2. Auflage, München 2011.

Staudinger, Bürgerliches Gesetzbuch, 15. Auflage, Berlin 2014.

Taeger/Gabel, BDSG, 2. Auflage, Frankfurt a. M. 2014.

Tremml/Luber, Amtshaftungsansprüche wegen rechtswidriger Produktwarnungen, NJW 2013, S. 262 – 267.

Ulmer/Brandner/Hensen, AGB-Recht, 11. Auflage, Köln 2011.

Wandtke/Bullinger, Praxiskommentar zum Urheberrecht, 3. Auflage, München 2009.

Wessels/Beulke, Strafrecht Allgemeiner Teil, 43. Auflage, Heidelberg 2013.

Westermann/Grunewald/ Maier-Reimer, Erman Bürgerliches Gesetzbuch, 13. Auflage, Köln 2011.

Wolf/Lindacher/Pfeiffer, AGB-Recht,
6. Auflage,
München 2013.

Wolter, Systematischer Kommentar zum Strafgesetzbuch,
138. Ergänzungslieferung,
Köln 2013.