GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

MonIKA

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

Ausarbeitung aus Perspektive des Datenschutzes und der Datensicherheit zur Zulässigkeit sowie zum Einsatz und zur Gestaltung von Anomalie erkennenden Verfahren in Internet-Infrastrukturen

Deliverable 5.2, V1.1

Editor: Malte Engeler
Institution: ULD
Erstellung: Februar 2014

Projektpartner

Fraunhofer FKIE
Friedrich-Ebert-Allee 144
53113 Bonn
Prof. Dr. Michael Meier
Telefon +49 228 73-54249
Fax +49 228 73-4571
mm@cs.uni-bonn.de

Cassidian Cybersecurity
Willy-Messerschmidt-Straße
85521 Ottobrunn
Dr. Tobias Kiesling
Telefon +49 89 3179 3807
Fax +49 89 3179 4031
tobias.kiesling@cassidian.com

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

Autorinnen und Autoren	Organisation
Malte Engeler	ULD
Meiko Jensen	ULD
Hannah Obersteller	ULD
Daniel Deibler	ULD
Marit Hansen	ULD

Über MonIKA

Die heutige Gesellschaft ist in hohem Maße auf sichere, insbesondere auf 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 deren 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 „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 aufgrund 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 oder 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 aufgrund der zunehmenden Komplexität und Verwundbarkeit der bereitgestellten Dienste, als auch der vielfältigen Möglichkeiten des Missbrauches, ist zukünftig ein gesamtheitlich hohes Sicherheitsrisiko zu erwarten. Dies gilt im Besonderen für das globale Umfeld des Cyber-Raums und der zugehörigen vernetzten Informationsinfrastrukturen. Von gezielt herbeigeführten Angriffen oder anderweitig verursachten Ausfällen dieser Infrastrukturen sind Staat, Wirtschaft und Gesellschaft gleichermaßen 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 Projekts MonIKA zu entwickeln, exemplarisch zu validieren und eine adäquate systematische Risikobehandlung vorzubereiten.

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

Inhaltsverzeichnis

1 Einleitung

Das vorliegende Dokument „D5.2 – Ausarbeitung aus Perspektive des Datenschutzes und der Datensicherheit zur Zulässigkeit sowie zum Einsatz und zur Gestaltung von Anomalie erkennenden Verfahren in Internet-Infrastrukturen“ ist das abschließende Ergebnis des Arbeitspakets „AP5.2 – Datenschutz“. Dieses Dokument enthält die Ausarbeitung des MonIKA-Projektteams des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein zu den Fragen des Datenschutzes und der Datensicherheit beim Einsatz von Anomalie erkennenden Verfahren in IT-Infrastrukturen.

Die Ausarbeitung stellt dabei zunächst den Sachverhalt, also die zu untersuchenden Umstände, dar. Dabei werden zunächst die relevanten Anwendungsszenarien des MonIKA-Systems beschrieben und rechtlich untersucht. Daran anschließend wird der Blickwinkel auf den Proof-of-Concept fokussiert. Gegenstand der Ausarbeitung sind relevante Rechtsfragen aus Sicht des Datenschutzes, die bei dem Einsatz eines MonIKA-Systems im Bereich der koordinierten Anomalieerkennung auftreten. Das MonIKA-System ist ein zentralisiertes Melde- und Auswertungsnetz. Sein Einsatzbereich reicht von nationalen und internationalen IT-Kooperationsnetzen bis zur Umsetzung in Unternehmensverbänden. In dieser Ausarbeitung werden exemplarisch die Bereiche Botnetz-Erkennung, BGP-Routing-Anomalien, IT-Sicherheitsforschung und – anhand eines konkreten Beispiels – das Enterprise-Monitoring untersucht. Das konkrete Beispiel, der Proof-of-Concept, betrachtet eine Unternehmensgruppe, bestehend aus dem zentralen Unternehmen McQueer AG, das PKW herstellt, und seinen Zulieferern für Bremsen (Stopper GmbH), für Reifen (Fastrubbers GmbH) und für Auspuffanlagen (NoisySys GmbH).

Es werden zunächst im Rahmen der Beschreibung des Untersuchungsgegenstands die handelnden natürlichen und juristischen Personen herausgearbeitet, welche – aktiv oder passiv – an dem System teilnehmen, sodann die jeweils dort auftretenden Datenverarbeitungsvorgängen dargestellt und schließlich ihre Vereinbarkeit mit dem Datenschutz untersucht. Im Rahmen dessen werden zunächst das geltende deutsche und europäische Recht betrachtet; im Anschluss wird auf zu erwartende Rechtsänderungen eingegangen. Die Netz- und Informationssicherheit wird gegenwärtig von einer Reihe anwendbarer deutscher und europarechtlicher Normen in Teilbereichen geregelt. Dabei sind Systeme im Entstehen begriffen, deren Konstruktion mit dem MonIKA-System durchaus Ähnlichkeiten aufweisen und eine Prognose über die zukünftigen rechtlichen Rahmenbedingungen für den Einsatz von kooperativen Monitoring-Systemen erlauben. Daneben ist im Schwerpunkt das derzeit geltende Datenschutzrecht – soweit möglich – zu prüfen und eine Einschätzung abzugeben, welche rechtlichen Herausforderungen oder Grenzen dem Einsatz eines solchen Systems derzeit gegenüberstehen. Insbesondere die Fragen nach dem Personenbezug, der Rechtsgrundlage für die Datenverarbeitung in einem solchen System und Aspekte der Datensparsamkeit nehmen dabei ebenso wie die Abwägung mit Datensicherheitsinteressen eine wichtige Rolle ein. Als Teilbereich des Datenschutzes werden im Anschluss zudem allgemeine Fragen und die Einordnung des MonIKA-Systems in diesen Rechtsrahmen untersucht.

Die Ausarbeitung zeigt auf, welche rechtlichen und technischen Folgefragen aus dem Projekt erwachsen sind, und schließt mit einer Zusammenfassung der größten datenschutzrechtlichen Herausforderungen.

2 Untersuchungsgegenstand

Die Thematik dieser Ausarbeitung ist mit der Erkennung von Anomalien in Internet-Infrastrukturen sehr weit gefasst. Dieser Untersuchungsgegenstand muss für konkrete Rechtsfragen auf bestimmte Anwendungsbeispiele reduziert werden. Ein Ziel des Projekts ist die Übertragbarkeit der entwickelten Konzepte auf andere Anwendungen. Aus diesem Grund sind die Anwendungsbeispiele so gewählt, dass sie möglichst unterschiedliche Anforderungen an die zu entwickelnde Lösung stellen.

Insgesamt werden drei Anwendungsfälle betrachtet: Überwachung des globalen Internet-Routings, kooperatives Monitoring von Botnetz-Aktivitäten und -Angriffen sowie Enterprise-Monitoring. Da innerhalb des Projektrahmens nicht alle möglichen Szenarien innerhalb dieser Anwendungsfälle betrachtet werden können, wird eine sinnvolle Auswahl möglichst unterschiedlicher Anwendungsszenarien getroffen. Diese werden im Laufe des Texts zunächst unabhängig voneinander betrachtet. Abschließend werden die relevanten Gemeinsamkeiten zusammengefasst.

2.1 Vorbemerkung

Der Kern jeglicher Anwendung der im Projekt MonIKA erarbeiteten Verfahren liegt in der Betrachtung verteilter, kooperativ zusammenarbeitender Akteure zur Erfüllung eines nur gemeinsam erreichbaren Zieles. Dementsprechend ist es ein Kernmerkmal von MonIKA, dass die erzielbaren Resultate nur aus dem vereinigten Datenbestand aller Akteure generiert werden können; eine äquivalente Erkenntnisgewinnung aus den Daten nur einzelner MonIKA-Akteure wäre schon informationstheoretisch nicht möglich.

Dieses Grundprinzip, das einen Basisaspekt der Cybersicherheit darstellt, erfordert von den beteiligten Akteuren die Bereitschaft zur uneingeschränkten Kooperation im Rahmen der definierten verteilten Verfahren. Dies steht jedoch oft im Konflikt mit den originären Interessen der einzelnen Akteure, ihre lokalen Datenbestände geheim zu halten. Um diesen Konflikt aufzulösen, ist es zwingend erforderlich, ein geeignetes Maß an Vertrauen der MonIKA-Teilnehmer untereinander zu etablieren. Dies kann durch geeignete technische Verfahren der Anonymisierung und Pseudonymisierung sehr gut unterstützt werden und verstärkt den Anreiz zur Teilnahme an einem MonIKA-typischen Szenario gegebenenfalls.

In jedem einzelnen der drei nachfolgend dargestellten und analysierten Anwendungsfälle lassen sich dieses Grundprinzip und die daraus ableitbaren notwendigen Bedingungen wiederfinden. Für die rechtliche Bewertung der einzelnen Verfahren spielt dieses Grundprinzip zwar nur eine untergeordnete Rolle, es wird aber maßgeblichen Einfluss auf die Realitätsnähe der elaborierten Szenarien nehmen. Ein juristisch korrekter Anwendungsfall, der den originären Interessen der einzelnen Akteure zuwiderläuft (beispielsweise wenn aus der Teilnahme an einem Verfahren kein hinreichender eigener Vorteil erzielt wird), wird folglich nicht zu einer Implementierung unter realen Bedingungen führen.

2.2 Botnetz-Monitoring

Der Anwendungsfall Botnetz-Monitoring befasst sich mit der Nutzung der durch das MonIKA-System bereitgestellten Monitoring-Infrastruktur und der im Rahmen dieser Infrastruktur verfügbaren Informationsfusions-Einrichtungen zur Erkennung und Beobachtung von Botnetzen. Die Infrastruktur des MonIKA-Systems soll hier dazu dienen, weithin verfügbare Sicherheitssensorik ohne Detektionslogik für Botnetze mithilfe des MonIKA-Ansatzes zur Erkennung von Botnetz-Aktivitäten und zur Identifikation von durch Botnetze infizierten Computersystemen zu nutzen.

Auf Basis der entwickelten MonIKA-Infrastrukturen werden die von diesen Sensoren gesammelten Daten zusammengeführt und deren Informationen fusioniert. Erkenntnisse sowohl über die allgemeine

Natur von Botnetzen als auch speziell über die Funktionsweise bestimmter Botnetze werden in entsprechenden Algorithmen implementiert, welche zur Fusion der Informationen genutzt werden und anschließend die Gewinnung Botnetz-relevanter Informationen ermöglichen. Die so gewonnenen Botnetz-Informationen werden zu einem Lagebild der Gefährdung durch Botnetze vereint. Aus der Informationsfusion gewonnene Detailinformationen können an die teilnehmenden Stellen zurückgeführt werden und dazu genutzt werden, die Erkennungsleistung der dort genutzten Sensoren zu verbessern.

Zur Veranschaulichung der Funktionsweise des MonIKA-Systems für den Anwendungsfall Botnetz-Erkennung dient das Beispielszenario der Spam-Erkennung zur Identifikation von Bots. Dieses beschreibt den Einsatz von Spam-Filtern bei E-Mail-Providern als Sensoren zur Botnetz-Erkennung im MonIKA-System. Als Spam klassifizierte E-Mails werden dabei an zentraler Stelle ausgewertet und zu von Botnetzen verbreiteten Kampagnen zusammengefasst (geclustert), also anhand von Ähnlichkeit ausdrückenden Merkmalen gruppiert. Das Senden einer Spam-Mail, die sich einer Kampagne zuordnen lässt, weist stark auf eine Infektion des Senders durch einen Bot hin. Ziel des Szenarios ist es, eine Liste der an einem Botnetz beteiligten Rechner, identifiziert durch ihre IP-Adresse, zu generieren.

2.2.1 Szenario und technischer Ansatz

Ein Großteil der heutzutage über das Internet versandten E-Mails dient der Verbreitung von (vom Empfänger oft unerwünschter) Werbung. Dieser sogenannte Spam wird dabei gezielt an eine möglichst breite Masse von Adressaten versandt, um selbst bei geringer Reaktionsquote dennoch einen hinreichend großen Werbeerfolg zu erzielen. Auf Empfängerseite erzeugt es jedoch großen Aufwand, eingehende E-Mails einzeln auf ihren Spam-Charakter zu prüfen und gegebenenfalls zu löschen. Daher wird die automatische Vorfilterung und Prüfung eingehender E-Mails auf ihren Spam-Charakter oft als zusätzlicher Dienst vom E-Mail-Provider oder vom lokalen E-Mail-Programm angeboten. Auch der massenhafte Versand der Spam-Nachrichten an eine große Menge an Empfängern innerhalb kürzester Zeit wird von E-Mail-Dienstanbietern inzwischen technisch unterbunden, was die Versender solcher Spam-Nachrichten zur Nutzung anderer Technologien treibt. Hier ist insbesondere der Versand von Spam-Nachrichten aus Botnetzen zu beobachten, bei der die einzelnen infizierten Rechner eines Botnetzes (Bots) angewiesen werden, eine bestimmte E-Mail (in identischer oder leicht variierender Form) an eine bestimme Liste von Empfängern zu versenden.

Auf technischer Ebene muss sich dafür jeder einzelne Bot an einem E-Mail-Server anmelden und die zu versendende Nachricht übertragen. Das hierfür zugrundeliegende technische Protokoll heißt SMTP. Dabei wird zwangsläufig die IP-Adresse des Bots an den empfangenden E-Mail-Server übertragen. Dieser E-Mail-Server kann die derart entgegengenommene (Spam-)E-Mail dann nach Bedarf an die E-Mail-Server der jeweiligen Empfänger weiterleiten, wobei wiederum das Protokoll SMTP eingesetzt wird. Die Weiterleitung muss dabei nicht zwangsweise direkt geschehen, d. h. eine Spam-Mail kann von einer größeren Anzahl von SMTP-Servern weitergeleitet werden, bis sie ihren eigentlichen Empfänger erreicht.

Für die Betrachtung im Kontext der Botnetz-Identifikation im Projekt MonIKA ist hierbei relevant, dass die IP-Adressen der originären Absender solcher Spam-Nachrichten folglich identisch sind mit denen der infizierten Rechner des Botnetzes, den Bots. Eine Klassifikation einer E-Mail als Spam kann also als Hinweis darauf verstanden werden, dass die E-Mail möglicherweise zu einer umfassenden Spam-Welle gehört und dass der originäre Absender Teil eines Botnetzes ist.

Der im Projekt MonIKA verfolgte Ansatz besteht nun darin, diese IP-Adressen für eine möglichst große Anzahl von Spam-E-Mails zu sammeln, um so eine Enumerierung der Bots eines Botnetzes zu erhalten. Dabei sind allerdings einige technische Aspekte zu beachten, die im Folgenden genauer analysiert werden.

Zunächst ist die IP-Adresse des originären Senders nicht explizit in einer E-Mail-Nachricht enthalten. Vielmehr fügt jeder SMTP-Server der E-Mail eine weitere Header-Zeile hinzu, aus der hervorgeht, vom welcher IP-Adresse die E-Mail entgegengenommen wurde. Die Ableitung, dass folglich die IP-Adresse aus dem ersten derartigen `Received`-Header gleich der IP-Adresse des originären Senders zu setzen wäre, ist aber nicht immer zutreffend. So kann zum einen ein SMTP-Server selbst entscheiden, ob und in welchem Umfang er einen weiteren `Received` -Header zu einer E-Mail hinzufügt, zum anderen kann ein Spam-Versender auch selbst beliebige `Received` -Header in die von ihm versandten E-Mails einbauen, um so die Absender-Identifikation zu behindern.

Die Zugehörigkeit einer einzelnen E-Mail zu einer Spam-Welle kann darüber hinaus statistisch nur anhand ihrer Ähnlichkeit zu den anderen E-Mails derselben Spam-Welle erkannt werden. Da oftmals identische oder nur leicht modifizierte Nachrichteninhalte an viele Adressaten versandt werden, kann folglich aus der Häufung von ähnlichen E-Mail-Inhalten ein Rückschluss auf eine Spam-Welle gezogen werden. Die Ähnlichkeit allein reicht aber nicht zur Klassifikation als Spam aus, da auch erwünschte E-Mails (wie etwa Newsletter oder automatische Benachrichtigungen) durchaus ähnliche Inhalte an eine große Menge an Adressaten versenden. Ob eine E-Mail also unerwünscht und damit Spam ist oder nicht, ist somit auch eine subjektive Frage des Empfängers. Entsprechend gibt es bei allen derzeit im Einsatz befindlichen Spam-Erkennungssystemen eine gewisse Wahrscheinlichkeit für fehlerhaft als Spam klassifizierte erwünschte E-Mails (sog. *false positives*) und für fehlerhaft nicht als Spam klassifizierte unerwünschte E-Mails (sog. *false negatives*). Beide Werte dienen als Richtwert zur Beurteilung der Effizienz eines Spam-Klassifikationssystems.

2.2.2 Stakeholder

Ein typisches MonIKA-Szenario umfasst stets eine Menge von dedizierten Teilnehmern sowie eine zentrale MonIKA-Stelle. Die Teilnehmer im Anwendungsszenario „Spam-Kampagnen-Erkennung zur Identifikation von Bots“ sind in jedem Fall die E-Mail-Provider und unter Umständen auch Kunden dieser Provider. Sie nehmen die Rolle der Sensoren beziehungsweise Monitore ein, also jener Beteiligten, die die Informationen über mögliche Spam-Mail liefern. Diesen Teilnehmern steht eine zentrale Stelle gegenüber, die die Informationen empfängt, fusioniert und auswertet.

Dieser organisatorischen Trennung entspricht auch die Trennung hinsichtlich der eingesetzten Software. Während bei den E-Mail-Providern sogenannte Erkennen-von-Anomalien-Agenten (EvA-Agenten) implementiert sind, die die Informationen an MonIKA senden, ist in der MonIKA-Zentralstelle ein entsprechender Empfänger, das EvA-Service-Cluster, installiert. Er nimmt die Daten in Empfang und sorgt für die weitere technologische Behandlung.

Als Beteiligte sind daneben die Kunden des E-Mail-Providers zu berücksichtigen. Sie sind als legitime Eigner der Daten, die Gegenstand des Monitorings sind, am Schutz dieser Daten interessiert, brauchen gleichzeitig aber auch Schutz vor Spam sowie vor Botnetz-Attacken.

Des Weiteren sind die E-Mail-Provider beteiligt. Sie sind die Betreiber des MonIKA-Monitors, der den Spam-Filter als Sensor nutzt. Das Hauptinteresse des E-Mail-Providers gilt dem Schutz der eigenen Infrastruktur sowie der Erfüllung einer eventuellen Schutzpflicht gegenüber dem Kunden.

Daneben treten Sicherheitsdienstleister und Hersteller von IT-Sicherheitsprodukten im erweiterten MonIKA-Kontext (unabhängig von konkreten Anwendungsfällen) gleichzeitig als Konsumenten und als Bereitsteller von MonIKA-Daten auf. Durch sie werden externe (außerhalb des MonIKA-Systems erhobene) Daten zur Korrelation im MonIKA-System verfügbar. Im Gegenzug erhalten sie gegebenenfalls aus dem MonIKA-System umfangreiche Botnetz-Informationen, die neue Erkenntnisse für die Forschung oder die Verbesserung von IT-Sicherheitsprodukten liefern können.

2.2.3 Datenerhebung

Grundlage der Botnetz-Erkennung in diesem Szenario sind Spam-Mails, also als unerwünschte Werbung klassifizierte E-Mails. Die Klassifikation von E-Mails als Spam erfolgt dabei nicht durch das MonIKA-System selbst, sondern durch externe Sensoren, wie etwa durch

- den E-Mail-Provider (automatische lokale Spam-Filter) oder
- den Nutzer (manuell durch Markierung der E-Mails als Spam).

Im weiteren Verlauf der Verarbeitung bilden die als Spam klassifizierten E-Mails die gemeldeten Anomalien. Sie dienen als Datenbasis für die Botnetz-Erkennung durch das MonIKA-System. Die Klassifikation von Spam wird dabei als hinreichend zuverlässig angenommen.

2.2.3.1 Basisdaten

Als grundlegende Datenbasis für das Spam-Kampagnen-Erkennungsszenario dient die Gesamtheit aller als Spam markierter E-Mails sämtlicher Szenario-Teilnehmer. Wann immer eine weitere E-Mail neu als Spam klassifiziert wird, wird sie automatisch in den bestehenden Datenbestand integriert und ihre Klassifikation als Anomalie interpretiert.

Für die Identifikation von Spam-Kampagnen ist es erforderlich, die textuelle Ähnlichkeit großer Mengen von Spam-E-Mails zu bestimmen. Daher kommen für das Feststellen dieser textuellen Ähnlichkeit sämtliche Teile einer Spam-E-Mail in Betracht.

Darüber hinaus ist insbesondere die Information über den originären Absender der Spam-E-Mail relevant. Seine IP-Adresse lässt sich üblicherweise aus dem chronologisch ältesten `Received`-Header der Spam-E-Mail extrahieren, sofern der erste entgegennehmende E-Mail-Server diesen Eintrag korrekt gesetzt und der Spam-Versender keine weiteren Techniken zur Verschleierung seiner Identität genutzt hat. Auch die Existenz eines Header vom Typ `X-Originating-IP` kann zum Feststellen der originären IP-Adresse des Versenders herangezogen werden, wieder unter der Prämisse, dass ein Spam-Versender dies nicht mit anderen Techniken verhindert.

Besonders relevant ist der Zeitpunkt der Initiierung des Sendevorganges, da er sowohl für die Korrelation mit anderen Spam-Mails derselben Kampagne dient als auch in Kombination mit der IP-Adresse des Senders Rückschlüsse auf den tatsächlich befallenen Rechner des Botnetzes erlaubt. Beachtenswert hierbei ist, dass zwischen dem Zeitpunkt des initialen Versendens einer Spam-E-Mail und dem Zeitpunkt der Klassifikation als Spam beim finalen Empfänger eine zeitliche Diskrepanz mit teilweise bedeutsamem Umfang liegen kann. Ein Rückschluss aus dem Zeitpunkt der Klassifikation auf den Zeitpunkt des Versendens ist also nicht immer möglich. Tatsächlich extrahieren lässt sich der Zeitpunkt des Versendens etwa aus dem Header-Feld `Date` oder aus dem chronologisch ersten `Received`-Header.

2.2.3.2 Vorverarbeitung

Aus verschiedenen Erwägungen, unter anderem aus datenschutzrechtlichen Gründen, ist die zentrale Sammlung sämtlicher als Spam klassifizierter E-Mails von allen an einem Szenario beteiligten Teilnehmern bei einer zentralen MonIKA-Auswertungsstelle unrealistisch. Es werden daher nur speziell vorverarbeitete Auszüge aus den tatsächlichen E-Mail-Inhalten an die MonIKA-Zentralinstanz weitergegeben. Die Generierung dieser Auszüge aus den tatsächlichen E-Mails erfolgt stets bei dem MonIKA-Teilnehmer, der eine E-Mail als Spam klassifiziert und der MonIKA-Zentralstelle bereitgestellt hat. Welche Daten im Einzelnen möglicherweise übertragen werden, stellt Tabelle 1 dar.

Tabelle 1: Potentiell übertragene Daten im Botnetz-Monitoring-Szenario

Datum	**Vorverarbeitung bzw. Wert**
IP-Adresse des originären Versenders	Im Klartext
Zeitpunkt des Versendens bzw. der Klassifizierung als Spam	Im Klartext
Liste sämtlicher vorhandenen SMTP-Header-Bezeichnungen, ohne deren jeweilige Werte	Liste im Klartext, Mehrfachnennung bei mehrfachem Auftreten möglich, Sortierung wie in der E-Mail
Anzahl der Zeichen der gesamten E-Mail	Zahlwert
Anzahl der Zeichen der gesamten E-Mail abzüglich Anzahl der nicht sichtbaren Zeichen (Whitespaces)	Zahlwert
Anzahl der Wörter gleicher Länge	Liste mit Zahlwerten, aufsteigend sortiert nach Wortlänge
Anzahl der Zeilenumbrüche	Zahlwert
Art der verwendeten Zeilenumbrüche	Konstante, Wert „CRLF“ oder „LF“
Angabe, ob Zeilenumbrüche innerhalb von Sätzen auftreten.	Konstante, Wert „yes“ oder „no“
Anzahl vorhandener URLs	Zahlwert
Liste der Top-Level-Domains aus den in der E-Mail vorhandenen URLs	Liste im Klartext, Mehrfachnennung bei mehrfachem Auftreten möglich, Sortierung wie in der E-Mail
Liste der Anzahl der Unterverzeichnisse pro URL für alle URLs der E-Mail	Liste von Zahlwerten, Sortierung wie in der E-Mail

2.2.4 Informationsfusion

Die durch die Sensoren als Spam klassifizierten E-Mails werden zusammengeführt und vom MonIKA-System auf inhaltliche und strukturelle Übereinstimmungen verglichen. Dabei wird versucht, Spam-E-Mails in Cluster zu gruppieren, die ihre Zugehörigkeit zu einer Spam-Kampagne ausdrücken.

Die Beschreibung einer E-Mail wird repräsentiert durch einen Vektor, der den deskriptiven Eigenschaften entsprechend Werte zuordnet (siehe Tabelle 1). Die Reduktion der E-Mail auf einen solchen beschreibenden Vektor geschieht bereits aufseiten des E-Mail-Providers. Die durch das EvA-Service-Cluster zu erstellende, als Spam-Kampagnen zu interpretierende Cluster von E-Mails zeichnen sich durch die Übereinstimmung einer Vielzahl von Elementen dieser Vektoren aus.

Im Besonderen werden aufseiten der zentralen MonIKA-Instanz beim Vergleich zweier E-Mails im Rahmen der Clusterung folgende Vergleiche getätigt:

Auf exakte Gleichheit:

- Liste der SMTP-Header;
- Art der verwendeten Zeilenumbrüche;

- Art der Verwendung von Zeilenumbrüchen (im Satz oder nicht);
- Anzahl der URLs.

Auf Differenz kleiner oder gleich einem vordefinierten Schwellwert:

- Zeitpunkt des Versendens;
- Zeichenanzahl bzw. Zeichenanzahl ohne Whitespaces;
- Anzahl Zeilenumbrüche.

Auf Differenz kleiner oder gleich einem vordefinierten Schwellwert für jeden einzelnen Eintrag in einer Liste:

- Anzahl der Wörter gleicher Länge;
- Liste der Top-Level-Domains aus den URLs;
- Liste der Anzahl der Unterverzeichnisse je URL.

Nur falls alle diese Tests erfolgreich verlaufen, werden beide E-Mails als ähnlich genug betrachtet, und in der Folge als zum selben Cluster gehörig klassifiziert. In einem zweiten Schritt wird nun geprüft, ob es sich bei den so generierten Clustern tatsächlich um Spam-Kampagnen handelt. Dazu werden für jedes Cluster zwei weitere Bedingungen abgeprüft: Die Anzahl der Spam-E-Mails pro Cluster muss einen vordefinierten Schwellwert überschreiten, und gleichzeitig muss die Anzahl der aus diesen E-Mails extrahierten unterschiedlichen Sender-IP-Adressen ebenfalls eine vordefinierte Grenze überschreiten, um eine Verwechslung mit intentional versandten Newsletter-Angeboten auszuschließen. Erst wenn diese beiden Tests ebenfalls erfolgreich absolviert werden, wird das zugehörige Cluster als Spam-Kampagne klassifiziert und somit als Anomalie identifiziert.

2.2.5 Informationsverwertung

Die aus den Clustern entnommenen Sender-IP-Adressen werden als zugehörig zu Bot-Rechnern klassifiziert, und können in verschiedener Art und Weise verwertet werden. Beispielsweise werden diese Daten mit existierenden Botnetz-Informationen zusammengeführt und können so bestehende Botnetz-Beschreibungen sowohl um weitere IP-Adressen als auch um eine Beschreibung der Spam-Aktivität des Botnetzes anreichern. Beide Verwertungen sehen vor, die derart gesammelten Listen von Bot-IP-Adressen zu Informationszwecken an die MonIKA-Teilnehmer zu verteilen. Dort bestehen beispielsweise folgende Möglichkeiten zur Nutzung:

- Alle MonIKA-Teilnehmer können die derart gewonnenen IP-Adressen nutzen, um selektiv weitere Schutzmaßnahmen für alle Fälle zu ergreifen, in denen mit IP-Adressen von der Bot-IP-Adress-Liste kommuniziert wird (IP-Adress-Blockade, Intrusion-Detection-Systeme, Deep Packet Inspection etc.).
- MonIKA-Teilnehmer, deren selbstbetriebene Rechner IP-Adressen innehaben, die auf der Bot-IP-Adress-Liste auftauchen, können diese Information nutzen, um laufende Angriffe oder aktuelle Fehlkonfigurationen in ihren eigenen Systemen zu identifizieren.

Neben der Weiterleitung der identifizierten Bot-IP-Adress-Listen besteht eine zweite mögliche Verwertung der Ergebnisse der Datenfusion in diesem MonIKA-Szenario darin, die identifizierten Spam-Kampagnen zur Verbesserung der Spam-Filter bei den MonIKA-Teilnehmern zu nutzen. Hierzu werden die identifizierten Merkmale der zum Spam-Cluster gehörenden E-Mails an alle MonIKA-Teilnehmer verbreitet. Diese haben daraufhin die Möglichkeit, ihre Spam-Filter derart anzupassen, dass neu ankommende E-Mails, die exakt dieselben Merkmale aufweisen, automatisch als Spam klassifiziert werden.

2.3 Globales Internet-Routing

Der MonIKA-Anwendungsfall Monitoring des globalen Internet-Routings betrachtet die Erkennung von Anomalien im Internet-Routing. In den folgenden Abschnitten wird das Anwendungsszenario des BGP-Monitorings näher erläutert. Dazu werden die in diesem Kontext relevanten technischen Voraussetzungen skizziert und die Akteure sowie ihre Rollen beschrieben.

2.3.1 Szenario und technischer Ansatz

Die Zuordnung von Internet-Teilnehmern untereinander erfolgt ausnahmslos durch Verwendung des Internet Protocol (IP). Dieses sieht für jeden Netzteilnehmer eine weltweit eindeutige Identifikationsnummer vor, die IP-Adresse. Eine Reihe von technischen Neuerungen hat hier zwar dazu geführt, dass dieser Bezug nicht immer eindeutig ist; für die Zustellung von Nachrichten im Internet spielen die IP-Adressen aber nach wie vor eine maßgebliche Rolle. Anhand dieser wird die Route zwischen Versender und Empfänger einer IP-Nachricht bestimmt. Dazu wird ermittelt, über welche physikalischen Leitungen, über welche Router und letztendlich über welche Netze von Internet-Dienstleistern ein IP-Paket übertragen werden muss, um vom Sender zum Empfänger zu gelangen. Dieses sogenannte Routing basiert selbst auf dem IP-Protokoll und implementiert eine der Kernaufgaben des heutigen Internets.

Als Verbund administrativ getrennter Autonomer Systeme (AS) ist das Internet auf den kontinuierlichen Austausch von Inter-AS-Routing-Informationen angewiesen. Als De-facto-Standard für diesen Austausch gilt das Border-Gateway-Protocol (BGP). Es dient dazu, Informationen über erreichbare Subnetze (und damit aller in diesen Subnetzen erreichbaren IP-Adressen) zwischen den AS auszutauschen. Soll dann eine Kommunikation zu einer bestimmten IP-Adresse aufgebaut werden, kann der Router des zugehörigen AS aus den per BGP erhaltenen Informationen ermitteln, über welches adjazente AS die Kommunikation zu etablieren ist bzw. über welches Kabel die zugehörige IP-Nachricht idealerweise weiterzuleiten ist. Das BGP ist grundlegender Bestandteil des gesamten Internets. Aus diesem Grund liegt der Fokus für die im MonIKA-Projekt entwickelten Verfahren auf der Beobachtung des Austauschs von Routing-Informationen hinsichtlich des Inter-AS-Routings.

Das Grundprinzip von BGP basiert auf der Annahme, dass alle AS-Router ihren direkten Nachbar-AS-Routern vertrauen. Nur unter solchen direkten Nachbarn werden daher Informationen über neue Verbindungen zwischen autonomen Systemen und sich ergebende neue Routen für IP-Pakete ausgetauscht. Das Grundprinzip funktioniert dabei immer gleich: Ein AS-Router, dessen AS die Zuständigkeit für einen weiteren IP-Bereich übernimmt, aktualisiert zunächst seine eigenen Routing-Tabellen in Bezug auf diese IP-Adressbereiche und informiert dann per BGP seine direkten Nachbarn, dass eben diese IP-Bereiche jetzt bei ihm erreichbar sind. Diese aktualisieren jeweils ihre eigenen Routing-Tabellen und leiten wiederum an ihre direkten Nachbar-AS weiter, welche IP-Adressbereiche sie über welche Route erreichen können.

Analog wird verfahren, wenn eine neue Verbindung zwischen zwei bisher nicht benachbarten AS eingerichtet wird: Beide AS prüfen ihre Routing-Tabellen dahingehend, welche IP-Adressbereiche sie über die neue Verbindung gegebenenfalls besser oder schneller erreichen können, aktualisieren ihre jeweiligen Routing-Tabellen und geben diese Information dann an ihre benachbarten AS weiter.

In beiden Fällen gilt das Prinzip, dass ein AS nur dann seine neuen Routing-Informationen per BGP mit seinen Nachbarn teilt, wenn sich aufgrund einer lokalen Veränderung im AS selbst oder aufgrund einer BGP-Nachricht eines adjazenten AS tatsächlich eine Änderung in der lokalen Routing-Tabelle des AS ergeben hat.

Da es sich bei BGP um ein Protokoll und nicht um eine Implementierung handelt, sind alle Realisierungen, die BGP implementieren, von den Schwachstellen des Protokolls betroffen. Die bekannteste und für dieses Projekt relevante Schwachstelle ist die fehlende Authentifizierung von Routing-Informationen. Durch ein implizites Vertrauensverhältnis zwischen benachbarten AS werden

Informationen eines Nachbarn ohne weitere Prüfung verarbeitet und gegebenenfalls an alle angrenzenden AS verteilt. Inkorrekte Routing-Informationen können somit als Folge von Fehlkonfigurationen oder als Teil eines akuten Angriffs verbreitet werden und so zu Störungen der Konnektivität führen.

Der Monitoring-Ansatz für BGP im Projekt MonIKA besteht nun darin, die Routing-Informationen, die bei einzelnen AS gesammelt wurden, zentral zusammenzuführen und auf Plausibilität zu prüfen. Wird bei dieser Plausibilitätsprüfung eine Abweichung der Netzdarstellung unterschiedlicher AS festgestellt, weil z. B. technisch unmögliche Netztopologien annonciert werden oder mehrere AS Zuständigkeit für dieselben IP-Adressbereiche beanspruchen, kann dies als Anomalie betrachtet und entsprechend bewertet werden.

2.3.2 Stakeholder

Die betroffenen Personen und Rollen für dieses Anwendungsszenario müssen alle am Internet-Routing beteiligt oder darauf angewiesen sein. Aus diesem Grund lassen sich diese in drei große Gruppen aufteilen:

Zunächst sind die Betreiber autonomer Systeme, die nicht MonIKA-Teilnehmer sind, relevant. Durch das Anbieten unterschiedlicher Dienste (z. B. Peering oder Transit) sind sie elementarer Teil des Routing-Systems im Internet und somit potentielle Opfer von Fehlkonfigurationen oder Angriffen.

Des Weiteren sind die Betreiber des MonIKA-Monitors zu berücksichtigen. Die Gesamtheit der MonIKA-Teilnehmer lässt sich dabei unterteilen in AS-Betreiber und sonstige Internet-Teilnehmer. Die teilnehmenden AS-Betreiber können zusätzlich zu den üblichen Routing-Daten möglicherweise weitere Informationen über ihre eigenen Peering-Partner oder Routing-Filter liefern, die in die Auswertung einfließen können.

Schließlich treten im BGP-Routing-Szenario die regulären Internet-Teilnehmer, üblicherweise als Endkunden bezeichnet, auf. Sie haben nur wenig Kontakt mit Routing-Daten. Bei Routing-Anomalien sind sie jedoch ebenfalls betroffen. Es ist denkbar, mit den Erkenntnissen eine Informationsstelle einzurichten, an der Endkunden über Probleme im Inter-AS-Routing informiert werden.

2.3.3 Datenerhebung

Im BGP-Szenario werden Daten aus verschiedenen Quellen genutzt. Neben den existierenden frei verfügbaren Daten zu BGP-spezifischer Kommunikation, die als dedizierte Services bereits im Internet angeboten werden, fließen explizit gesammelte BGP-relevante Daten der MonIKA-Teilnehmer in die Datenbasis dieses Szenarios ein. Dabei werden die frei verfügbaren Daten der bestehenden Internet-Services von der MonIKA-Zentralinstanz direkt eingebunden; die Daten der MonIKA-Teilnehmer werden nach einer Vorverarbeitung separat an die MonIKA-Zentralinstanz übersandt.

2.3.3.1 Basisdaten

Die wichtigste Informationsquelle für das BGP-Szenario besteht in der Menge der ausgetauschten BGP-Nachrichten (sog. BGP-Updates), mit deren Hilfe sich benachbarte AS über Änderungen in ihren lokalen Routing-Tabellen informieren. Wann immer eine Änderung der Topologie oder Erreichbarkeit von autonomen Systemen oder eine Neu-Zuordnung von IP-Adressbereichen zu autonomen Systemen erfolgt, lösen die direkt betroffenen AS neue BGP-Nachrichten an ihre direkten Nachbarn aus, die sich entsprechend durch das Netz weiterpropagieren. Folgerichtig erreichen diese Daten auch Netzbereiche, die von MonIKA-Teilnehmern verwaltet werden. Dort werden diese Update-Nachrichten gesammelt und an die zentrale MonIKA-Instanz weitergeleitet. In dieser Hinsicht unterscheidet sich das Vorgehen der MonIKA-Teilnehmer also nicht von dem der bereits existierenden

BGP-Sammeldienste, außer dass die BGP-Daten explizit nur der MonIKA-Zentralinstanz zur Verfügung gestellt werden.

Neben den gesammelten oder frei verfügbaren BGP-Updates bieten sogenannte Traceroutes eine wichtige Informationsquelle für das BGP-Szenario. Anhand eines aktiv durchgeführten Verbindungsaufbaus auf Basis des IP-Protokolls lassen sich damit diejenigen Router identifizieren, die bei einer Verbindung zwischen zwei IP-Adressen zur Weiterleitung einbezogen werden. Aus der sich so ergebenden Route lassen sich Rückschlüsse auf die zu den einzelnen Routern gehörenden AS ableiten. Diese Kette von AS wiederum kann mit den Angaben aus den BGP-Updates abgeglichen werden, um Hypothesen bezüglich der Netztopologie oder der Existenz von Anomalien zu verifizieren oder zu widerlegen.

Aus solchen aktiv durchgeführten Traceroutes der MonIKA-Teilnehmer ergeben sich – je nach Quell-IP- und Ziel-IP-Adresse – Ketten von IP-Adressen, die als Basisdaten im Kontext des BGP-Szenarios genutzt werden.

2.3.3.2 Vorverarbeitung

BGP-Updates sind weitgehend öffentlich zugängliche Informationen und werden in unveränderter Form an die zentrale MonIKA-Instanz weitergegeben.

Anders sieht es bei den Traceroute-Daten aus. Da hier individuelle IP-Adressen gelistet werden können, ist deren Personenbezug generell unklar. Im MonIKA-Kontext wird deshalb eine entsprechende Vorverarbeitung zur Extraktion des Personenbezugs vorausgesetzt. Dazu werden sämtliche in den Traceroute-Daten enthaltenen IP-Adressen in die diesen IP-Adressen zugeordneten AS aufgelöst. Die AS werden dabei über ihre AS-Nummer identifiziert. Einen Überblick über möglicherweise übertragene Daten gibt Tabelle 2.

Tabelle 2: Potentiell übertragene Daten im Szenario „Globales Internet-Routing“

Datum	Vorverarbeitung bzw. Wert
BGP-Update-Nachricht	Im Klartext
Traceroute-Ergebnis	Liste von AS-Nummern der aus dem Traceroute ermittelten IP-Adressen

2.3.4 Informationsfusion

Zunächst werden verschiedene Arten von Konflikten in den per BGP-Update verbreiteten Routen-Informationen gesucht. Treten Fälle auf, in denen zwei oder mehr verschiedene AS Zuständigkeit für dieselben oder überlappende IP-Bereiche beanspruchen, liegt ein erstes Indiz für eine Anomalie vor. In diesem Fall wird anschließend – soweit möglich – geprüft, ob die Zuständigkeit möglicherweise aus legitimen Gründen tatsächlich zwischen den AS aufgeteilt ist, etwa für Zwecke des Load Balancing oder der besseren regionalen Verfügbarkeit bestimmter Angebote. Kann dies klar verneint werden, oder ist es gar nicht ermittelbar, werden die zugehörigen BGP-Update-Nachrichten, aus denen der Konflikt entstand, als Anomalie klassifiziert.

Eine zweite Fusionstechnik analysiert die sich aus den BGP-Updates ergebenden Netztopologien. Dabei wird gezielt nach AS-Konstellationen gesucht, die nicht konsistente Angaben zu ihren Nachbar-AS oder zu der Liste der durch sie erreichbaren AS machen. Beispielsweise werden Situationen identifiziert, bei denen ein AS *X* angibt, mit einem anderen AS *Y* benachbart zu sein, während AS *Y* zeitgleich behauptet, AS *X* nur über Umwege erreichen zu können. Zwar kann es durchaus Gründe für

AS-Routing-Einwegstraßen geben, dennoch wird eine solche Konstellation stets als Anomalie klassifiziert.

In einer dritten Fusionstechnik werden die von den MonIKA-Teilnehmern bereitgestellten Traceroute-Daten ausgewertet, indem sie auf Konsistenz mit den aus den BGP-Updates gewonnenen Netztopologien geprüft werden. Werden hier Abweichungen zwischen per BGP postulierter Route und tatsächlich genutzter Route identifiziert, wird dies in jedem Einzelfall als Anomalie klassifiziert.

Im Ergebnis ergibt sich also eine Liste der als Anomalie markierten BGP-Updates. Diese werden als Resultat im Rahmen der Informationsverwertung weiterverarbeitet.

2.3.5 Informationsverwertung

Anomalien als Folge illegitimer BGP-Updates, welche in den bereits genannten Schritten erkannt wurden, werden allen MonIKA-Teilnehmern mitgeteilt. Zusätzlich zu den Anomaliedeklarationen selbst können in den von der zentralen MonIKA-Instanz bereitgestellten Informationen auch Handlungsempfehlungen oder Anweisungen an die Teilnehmer verteilt werden, um in kritischen Fällen unmittelbare Maßnahmen zu treffen. Die Entscheidungshoheit über den Versand solcher Zusatzinformationen liegt bei den Betreibern der zentralen MonIKA-Instanz, die Entscheidungshoheit über Art und Umfang der tatsächlichen Reaktion auf solche Bekanntgaben liegt bei den Verantwortlichen der jeweiligen Teilnehmer. Mögliche Reaktionen wären etwa:

- MonIKA-Teilnehmer, die nicht selbst AS-Betreiber sind, könnten für ihre zukünftigen IP-Verbindungen explizite Routen vorgeben, die die aus dem MonIKA-System bekannten Routing-Anomalien umgehen, bzw. andere Routen als die falsch annoncierten Routen verwenden.
- MonIKA-Teilnehmer, die selbst AS-Betreiber sind, könnten entscheiden, ihre eigenen Routing-Tabellen gemäß den identifizierten fehlerhaften Routen anzupassen, um die Fehler dadurch zu kompensieren.
- MonIKA-Teilnehmer, die selbst AS-Betreiber sind, könnten entscheiden, BGP-Updates von bestimmten AS, die im Rahmen einer Anomalie fehlerhafte Angaben gemacht haben, nicht mehr oder zumindest nicht ungeprüft bei der Aktualisierung ihrer Routing-Tabellen zu berücksichtigen.
- MonIKA-Teilnehmer, die selbst AS-Betreiber sind, und von der MonIKA-Zentralinstanz eine Nachricht über fehlerhafte BGP-Updates von ihnen direkt bekannten AS erhalten, könnten entscheiden, Maßnahmen gegenüber den Betreibern dieser AS zu treffen (z. B. Benachrichtigung, Ignorierung, rechtliche Schritte).
- MonIKA-Teilnehmer, die selbst AS-Betreiber sind und von der MonIKA-Zentralinstanz eine Nachricht über fehlerhafte BGP-Updates von ihren eigenen AS erhalten, könnten diese Information nutzen, um laufende Angriffe oder aktuelle Fehlkonfigurationen in ihren eigenen Subnetzen zu identifizieren.

2.4 Enterprise-Monitoring

Beim MonIKA-Anwendungsfall Enterprise-Monitoring geht es um die Erhöhung des Schutzes von Unternehmen vor Bedrohungen aus dem Cyber-Raum durch eine verbesserte Zusammenarbeit zwischen verschiedenen Unternehmen und anderen Organisationen. Dafür sollen die im MonIKA-System vorgesehenen technischen und organisatorischen Maßnahmen verwendet werden. Im Rest dieses Abschnitts wird der Enterprise-Monitoring-Anwendungsfall näher dargestellt. Dazu wird zunächst eine allgemeine Darstellung des Anwendungsfalls gegeben. Anschließend werden die Akteure der verschiedenen beteiligten Arten von Parteien zusammen mit ihren möglichen Rollen im

Kontext des Anwendungsfalls diskutiert. Schließlich werden – soweit möglich – Details zu Datenbasis, Fusion und Verwertung skizziert.

2.4.1 Szenario und technischer Ansatz

Unternehmen stellen immer höhere Anforderungen an die Sicherheit der eigenen Informationsinfrastrukturen sowie die Einhaltung definierter Sicherheitsrichtlinien. Zur Gewährleistung sicherer, insbesondere verlässlicher und verfügbarer, Systeme für den reibungslosen Ablauf von Geschäftsprozessen haben sich unter anderem Security Incident Management und Response-Prozesse, in der Regel in übergeordneten Management-Frameworks eingebettet, etabliert.

Eine effiziente und effektive Durchführung der dort definierten Tätigkeiten bieten sogenannte Cyber Security Operations Center (CSOC), die sich an den Bedürfnissen und den Vorgaben der Unternehmen orientieren. Ein CSOC erbringt Dienstleistungen zur Erhöhung der Sicherheit einer Organisation durch Vorbeugung und Behandlung sicherheitsrelevanter Ereignisse. Eine Aufgabe ist die Minimierung des Sicherheitsrisikos durch kontinuierlich durchgeführte Analysen unter Verwendung menschlicher Ressourcen sowie Techniken der Informatik.

Im Regelfall wird ein CSOC seine Services 24 Stunden täglich und 365 Tage im Jahr erbringen. Das dabei durchgeführte kontinuierliche Monitoring erlaubt die Erkennung von etwaigen Anomalien. Nach deren Analyse können vom CSOC wirkungsvolle und zielgerichtete Gegenmaßnahmen eingeleitet werden. Da es sich hier um eine kostenintensive Tätigkeit handelt, die hochqualifiziertes Personal bindet, ziehen es Unternehmen oft vor, den Dienst auszulagern beziehungsweise an andere Unternehmen zu übertragen, die im Bereich der Informationssicherheit spezialisiert sind.

Der Betreiber des CSOC muss entsprechend die für die Erbringung der Leistung benötigten Ressourcen und Zertifizierungen bereitstellen. Darüber hinaus benötigt er Zugang zu Monitoring-Daten oder Sensoren, um mit geeigneten Verfahren Anomalien und Angriffe auf die Informationsinfrastruktur des Kunden frühzeitig erkennen, Schwachstellen beheben und die Funktionsfähigkeit der Infrastruktur sowie die Integrität bzw. die Vertraulichkeit der Unternehmenswerte gewährleisten zu können. Eine wesentliche Herausforderung ist dabei das Erkennen gezielter und auf das Unternehmen angepasster Angriffe.

Der Anwendungsfall Enterprise-Monitoring untersucht, wie die MonIKA-Konzepte verwendet werden können, um den Informationsaustausch zwischen mehreren Monitoring-Betreibern in Unternehmensnetzen zu gewährleisten. Dabei werden die Abläufe beim Austausch cybersicherheitsrelevanter Informationen zwischen den MonIKA-Teilnehmern analysiert und gemeinsam erzielbare Erkenntnisgewinne identifiziert. Art und Ausprägung der verschiedenen Angriffstechniken und Anomalien sind dabei – anders als bei den beiden vorherigen Anwendungsfällen – nicht fest vorgegeben. Vielmehr können unterschiedliche Arten von Angriffsdaten ausgetauscht werden.

2.4.2 Stakeholder

Für das MonIKA-Szenario des Enterprise-Monitorings lassen sich drei Gruppen von Akteuren unterscheiden: Angreifer, angegriffene Unternehmen (Verteidiger) und unbeteiligte Dritte.

2.4.2.1 Akteure und Rollen auf Angreiferseite

Auf Angreiferseite kommen unter anderem folgende mögliche Akteure in Frage:

- staatliche Einrichtungen/Akteure (insbes. militärischer Art);
- Konkurrenzunternehmen;
- Aktivistengruppen;

- Kriminelle;
- terroristische Gruppierungen.

Jede dieser Gruppen hat ganz eigene Motive, Handlungsmöglichkeiten und Hintergründe, die sie in die Rolle eines Angreifers bringen. Eine Aufzählung möglicher Hintergründe würde dabei den Rahmen dieser Ausarbeitung sprengen, daher werden diese Akteure im Folgenden auf die ihnen bei einem Angriff zukommenden Rollen reduziert. Die Akteure können in einer Vielzahl möglicher Angriffsszenarien diverse Rollen einnehmen:

- *Initiator der Angriffe*: Der eigentliche Initiator der Angriffe, der häufig auch einen Vorteil aus den Angriffen zieht. Die Interessen des Initiators bestimmen maßgeblich die Form der Angriffe und sind daher eine wesentliche Kenngröße für eine effektive Reaktion. Leider ist es meist sehr schwierig, den Initiator eines Angriffs zu identifizieren. So lassen sich oft nur Mutmaßungen über die ursächliche Motivation eines Angriffs feststellen.
- *Ausführender Angreifer*: Derjenige, der die Angriffe unter Nutzung verschiedenster Werkzeuge (u. a. Malware) und Ressourcen tatsächlich durchführt. Er kann dies im Auftrag des Urhebers tun und dabei seinerseits Ressourcen verwenden, die entweder vom Urheber oder von einer dritten Person zur Verfügung gestellt werden.
- *Angriffsinfrastrukturbetreiber*: Betreibt eine Infrastruktur, die als Ressource für Angriffe verwendet werden kann. Hierbei kann es sich um einfache technische Ressourcen handeln, wie z. B. Netzanbindungen oder Server, oder auch um spezifische Cyberangriffsinfrastrukturen, wie z. B. Botnetze.
- *Malware-Entwickler*: Entwickelt Angriffswerkzeuge, insbesondere Malware. Dies kann spezifisch im Auftrag des Urhebers oder des Angreifers passieren, oder aber es können sogenannte „Common-off-the-Shelf“-Werkzeuge genutzt werden, die einsatzfertig eingekauft oder frei bezogen werden können.

2.4.2.2 Akteure und Rollen auf Unternehmensseite

Aufseiten der Verteidiger, d. h. der Unternehmen, die versuchen, sich vor Cyberangriffen zu schützen, gibt es folgende mögliche Akteure:

- *CIO und/oder CISO*: Der Chief Information Security Officer (CISO) ist verantwortlich für alle Belange der Informationssicherheit. Nicht selten fällt unter sein Aufgabenspektrum auch die physische Sicherheit wie z. B. Zutrittssysteme und Alarmanlagen. In vielen Unternehmen existiert die Position eines CISO nicht. In diesen Fällen ist der Verantwortungsbereich des CISO beim Chief Information Officer (CIO) angesiedelt und er handelt somit in Personalunion. Der CIO ist dann insgesamt für das Funktionieren der IT-Infrastruktur des Unternehmens zuständig. Dazu gehört die Funktionalität und Nutzbarkeit der eingesetzten IT-Systeme ebenso wie die Verfügbarkeit und Sicherheit. Dabei kann es einen Zielkonflikt bezüglich dieser Aspekte geben, insbesondere für die Berücksichtigung der Sicherheit. Das Interesse des CIO ist es, die angesprochene Funktionsfähigkeit der IT-Infrastruktur zu gewährleisten und darüber hinaus im Sinne einer Security Compliance wesentliche Regularien mit Bezug zu den IT-Systemen einzuhalten.
- *System- und Netzadministratoren*: Diese sind für den Betrieb der IT-Systeme, Computernetze und Applikationen zuständig. Sie müssen auf der einen Seite Nutzerforderungen im Sinne eines internen Dienstleisters erfüllen, auf der anderen Seite aber auch die wesentlichen Vorgaben vonseiten des CIO/CISO erfüllen, darunter auch die Gewährleistung der Sicherheit. Im Allgemeinen liegt das Interesse der Administratoren daher vor allem auf der Einhaltung der Erwartungen der Nutzer unter Erfüllung der wesentlichen, formal durch Policies vorgegebenen Rahmenbedingungen. Ihrer primären Aufgabe nachkommend, Verfügbarkeit und Funktionalität

von Netz-, System- und Applikationsressourcen sicherzustellen, ist die eigentliche Sicherheit ihrer Systeme, Netze und Applikationen oft eher von untergeordnetem Interesse. Das untergeordnete Sicherheitsinteresse gilt insbesondere dann, wenn bereits Sicherheitskomponenten (z. B. Firewalls) außerhalb ihres Verantwortungsbereichs vorhanden sind und somit ein Gefühl von Sicherheit vermitteln. Verstärkt wird dies noch dadurch, dass Sicherheitsvorfälle vergleichsweise selten auftreten und damit nicht in der direkten Erfahrungswelt des Administrators stehen. Bei Auftreten eines Sicherheitsvorfalls stehen die Administratoren allerdings bei der Reaktion darauf in der ersten Reihe.

- *Datenschutzbeauftragte und Betriebsräte*: Die Aufgabe des Betriebsrates ist die Interessenvertretung der Mitarbeiter eines Unternehmens. In Bezug auf Maßnahmen der IT-Sicherheit übt der Betriebsrat hauptsächlich seine Aufgabe als Kontrollinstanz in Bezug auf die Sammlung und Verwendung von Daten aus. Dabei soll sichergestellt werden, dass diese Daten nicht für Zwecke der Überwachung von Mitarbeitern missbraucht werden können. Dies schlägt sich in der Ausgestaltung und im Abschluss entsprechender Betriebsvereinbarungen nieder, in denen die Möglichkeiten der Datensammlung für IT-Sicherheitsmaßnahmen festgelegt werden. Darüber hinausgehend ist das Interesse des Betriebsrates die Vermeidung oder wenigstens Minimierung der Sammlung von Daten mit Mitarbeiterbezug. Der Datenschutzbeauftragte eines Unternehmens hat speziell die Aufgabe die Einhaltung dieser betriebsinternen Regelungen zu überprüfen, aber vor allem auch die Einhaltung von allgemeinen Datenschutzvorgaben sicherzustellen.
- *Nutzer der IT-Systeme und -Dienste*: Die Nutzer werden in der Regel Mitarbeiter des Unternehmens sein und oft nur sehr rudimentäre Kenntnisse im Themenfeld Sicherheit haben. Sie verwenden die IT-Systeme und Dienste des Unternehmens im Rahmen ihrer täglichen Arbeit. Ihr Interesse besteht sowohl in der ständigen Verfügbarkeit und Nutzbarkeit der für ihre Tätigkeit notwendigen IT-Ressourcen als auch darin, durch Maßnahmen der IT-Sicherheit nicht unverhältnismäßigen Kontrollen ausgesetzt zu sein. Die Nutzer spielen eine wichtige Rolle bei der Erkennung von Bedrohungen, z. B. durch die Meldung ungewöhnlicher Ereignisse.
- *Externe IT-Dienstleister*: Die verschiedenen Akteure dieser sehr breiten Gruppe erbringen eine Dienstleistung im Zusammenhang mit den IT-Ressourcen der Unternehmen, so z. B. die Anbindung des Unternehmensnetzes an das Internet oder andere Netze (Internet Service Provider) oder auch den ausgegliederten Betrieb von Servern. Auch vom Unternehmen in Anspruch genommene Cloud-Dienste fallen unter diese Kategorie. Das Interesse der externen Dienstleister ist die Erbringung des Dienstes gemäß den Erwartungen des Kunden und insbesondere im Rahmen der mit diesem Kunden abgeschlossenen Verträge. Dabei möchte ein externer Dienstleister sein eigenes Risiko und seine eigenen Kosten möglichst gering halten. Die angebotene Dienstleistung kann sich dabei ganz oder teilweise auf Aspekte der IT-Sicherheit beziehen. Handelt es sich dabei vollständig um einen Dienst im Rahmen der IT-Sicherheit, spricht man auch von einem IT-Sicherheitsdienstleister. Diese Untergruppe ist für das MonIKA-System von besonderer Relevanz.

Neben dieser Einteilung anhand der Funktion im Unternehmenskontext lassen sich die Akteure der MonIKA-Verteidigerseite alternativ auch nach ihrer Rolle im MonIKA-Kontext klassifizieren. Dabei können die beteiligten MonIKA-Teilnehmer unter anderem folgende Rollen annehmen:

- *Vertragspartner*: Hierbei handelt es sich um diejenigen Akteure, die für die Aushandlung und Einhaltung der Verträge zwischen verschiedenen kollaborierenden Unternehmen verantwortlich sind. Im Zuge des Anwendungsfalls sollen hier vor allem die Verträge für die Realisierung der Zusammenarbeit im Bereich der IT-Sicherheit verstanden werden. Allerdings ist zu vermuten, dass in der Praxis wohl eher zusätzliche Vereinbarungen für den Austausch von Informationen in bereits bestehende Liefer- oder Rahmenverträge aufgenommen werden würden.

- *Informationslieferanten*: Diese sind dafür verantwortlich, die in den Rahmenverträgen vereinbarten Informationen aus den eigenen Netzen in der festgelegten Form zu liefern. Hierzu werden die Sensoren innerhalb der Unternehmensnetze eingebunden (Logging-Systeme, Intrusion-Detection-Systeme etc.). In der Regel wird eine Vorverarbeitung der erhobenen Daten notwendig sein, die im Verantwortungsbereich der Informationslieferanten liegt.
- *Informationsempfänger*: Hier handelt es sich um diejenigen, die bei den einzelnen MonIKA-Teilnehmern die verarbeiteten Informationen (z. B. Alarme oder aggregierte Lagebilder) entgegennehmen und entsprechende Aktionen innerhalb des Unternehmens in die Wege leiten (z. B. Durchführung einer Reaktion auf einen aufgetretenen Sicherheitsvorfall).
- *Informationsverarbeiter*: Dies sind die Instanzen, die für den Abgleich von Informationen aus verschiedenen Quellen (d. h. in der Regel von verschiedenen Unternehmen) zuständig sind, inklusive Anwendung der entsprechenden Fusions-, Korrelations-, Klassifikations- bzw. Analyseverfahren. Je nach Ausprägung des eingesetzten MonIKA-Systems (siehe nächster Abschnitt) kann diese Rolle von Mitarbeitern eines Unternehmens oder von einem externen (neutralen) IT-Sicherheitsdienstleister übernommen werden.
- *Kontrollinstanzen*: Hierbei handelt es sich um Entitäten, die die Funktionsfähigkeit des MonIKA-Systems und die Konformität mit Anforderungen zu verschiedenen Teilaspekten wie z. B. Datenschutz überprüfen.

2.4.3 Datenerhebung

Bei Betrachtung der Möglichkeiten zum Austausch sicherheitsrelevanter Informationen zwischen verschiedenen Parteien kann man diverse Kategorisierungen vornehmen. Eine mögliche Kategorisierung bezieht sich auf den Zweck des Datenaustauschs in Bezug auf die Vorgänge zum Umgang mit auftretenden Bedrohungen und Vorfällen. Hier unterscheidet man üblicherweise drei verschiedene Phasen:

1. Entdeckung von Anomalien, bei denen es sich um auftretende Bedrohungen handeln könnte;
2. Klassifikation und Bewertung dieser Anomalien (irrelevant oder Bedrohung von Typ X mit Schwere Y) mit nachfolgender Entscheidung zur Einleitung von Reaktionen;
3. Durchführung der Reaktionen.

Prinzipiell können in jeder dieser Phasen relevante Daten mit anderen Parteien ausgetauscht werden. Dabei unterscheiden sich die Arten ausgetauschter Daten stark zwischen diesen Phasen. Das MonIKA-Projekt beschäftigt sich prinzipiell mit dem Datenaustausch in den ersten beiden Phasen. Kollaborative Durchführung der Reaktion ist nicht Gegenstand des Projekts und dieser Ausarbeitung. Betrachtet man die erste genannte Phase, so kann man feststellen, dass für die Entdeckung von Anomalien detaillierte Daten der einzelnen Sensoren in den überwachten Netzen notwendig sind. Beim Enterprise-Monitoring handelt es sich bei den kollaborierenden Parteien um Unternehmen. In aller Regel werden diese nicht bereit sein, die Sensordaten aus ihren Netzen mit anderen Parteien auszutauschen.

Der Enterprise-Monitoring-Anwendungsfall wird sich aus den oben genannten Gründen auf den Austausch von Daten im Zuge der Klassifikation bzw. Bewertung von Anomalien konzentrieren. Dort sind eine ganze Reihe möglicher Anwendungsfelder denkbar. Gemeinsam ist diesen, dass Informationen über Anomalien ausgetauscht werden, die in den einzelnen Teilnehmernetzen detektiert wurden (im Folgenden als Alarme bezeichnet). Die Erkennung der Anomalien geschieht in der Regel durch die teilnehmereigenen Monitoring-Systeme (sog. SIEM). Die in diesem Szenario für den Austausch nutzbaren Daten sind die von den SIEMs in den einzelnen SOCs der Teilnehmer erzeugten Alarme mit den dazugehörigen Informationen. Die Ausprägung der auszutauschenden Daten hängt stark von den zugrundeliegenden Methoden der Anomaliedetektion ab. Diese können in ihrem Informationsgehalt sehr unspezifisch (simple Meldung, dass ein bestimmtes Ereignis eingetreten ist)

bis sehr spezifisch (genaue Daten über Art des Ereignisses, Ziele, Angreifer-IP-Adresse) sein. Tabelle 3 gibt einen Überblick über mögliche Anwendungen mit den zugehörigen Detektionsmethoden und die grobe Beschreibung des Informationsgehalts der nutzbaren Daten, die mit der Detektion verbunden sind. Die Tabelle stellt dabei nur einen Auszug möglicher Detektionsmethoden dar. Weitere Methoden sind denkbar.

Tabelle 3: Detektionsmethoden und die darauf aufbauenden Daten

Anomalie	Detektionsmethode	Informationsgehalt
Scanning	Erkennung von durchgeführten Netz- und Schwachstellenscans durch Abgleich von Logdaten verschiedener Serversysteme, Intrusion Detection Systems (IDS) und evtl. Firewalls	Art des Scans, Art der Ziele, IP-Adressen des Verursachers, Häufigkeit und Ausmaß des Auftretens, Muster beim Vorgehen, Besonderheiten, Konfidenz und Priorität
Phishing	Detektion und Charakterisierung von Phishing-Mails mit maliziösem Anhang oder Web-Link; Detektion durch automatisierte Malware-Analyse (z. B. mittels FireEye Mail MPS) oder Nutzerhinweise	Zielpersonen mit verschiedenen Charakteristika, Herkunft der A-Mails, Häufigkeit des Auftretens, Art des Anhangs oder Links, E-Mail-Patterns
C&C-Verkehr	Erkennung von Command & Control-Verkehr zwischen einem C&C-Server und befallenen Rechnern (Backdoors, Bots etc.); auch Daten-Exfiltration	Quell-IP-Adressen, Ziel-IP-Adressen, Ports, verwendetes Protokoll, Umfang ausgetauschter Daten, Verschlüsselung und Kodierung, besondere Merkmale, Konfidenz/Priorität
(Distributed) Denial-of-Service	Erkennung von (D)DoS-Angriffen durch Monitoring von Verfügbarkeiten und/oder Erkennung von ungewöhnlichem Netzverkehr; insbesondere interessant bei „intelligentem DoS“, das gezielt Schwachstellen ausnutzt	Quell-IP-Adressen, Art der Ziele, Ausmaß der Angriffe, Muster in den Angriffen, Konsequenzen beim Angegriffenen, Konfidenz und Priorität

2.4.4 Informationsfusion

Die geeigneten Analyseverfahren hängen vom erwarteten Nutzen des Datenaustauschs ab. Dieser richtet sich natürlich grundsätzlich nach den zugrundeliegenden Detektionsmethoden und soll daher im Allgemeinen die Bewertung der entsprechenden Ereignisse im Gesamtverbund der Teilnehmer verbessern. Eine Möglichkeit zum Abgleich der Daten aus den verschiedenen Teilnehmernetzen sind regelbasierte Verfahren. Diese vergleichen einzelne Datenfelder der ausgetauschten Daten auf Wertübereinstimmungen (Patternmatching) und können so identische Datenfelder finden. Dies könnte z. B. beim Vergleich von IP-Adressen interessant sein, die eindeutig einen Angreifer identifizieren können. Regelbasierte Verfahren sind allerdings nur dann hilfreich, wenn sich überhaupt direkte Übereinstimmungen finden lassen, was nur dann der Fall ist, wenn ein Angreifer sich tatsächlich durch eindeutige Charakteristika ausprägt.

In vielen Fällen sind statistische bzw. heuristische Verfahren besser geeignet. Diese können Ähnlichkeiten zwischen einzelnen Datenfeldern oder Gruppen von Datenfeldern erfassen und so die von den einzelnen Teilnehmern gewonnenen Daten vergleichbar machen, auch wenn keine direkten

Wertübereinstimmungen vorhanden sind. Die Spanne anwendbarer Verfahren reicht von rein statistischen Verfahren und Modellen bis zu Verfahren des maschinellen Lernens und der künstlichen Intelligenz. Letztere eignen sich häufig zusätzlich noch dazu, vorhandene Unsicherheiten in den Daten zu quantifizieren. Die weitere Auswahl und Ausgestaltung der anzuwendenden Analyseverfahren für die entsprechenden Szenarien des Enterprise-Monitorings muss einem konkreten Beispiel vorbehalten bleiben.[1]

2.4.5 Informationsverwertung

Der Mehrwert des Datenaustauschs liegt hier im Allgemeinen in einer beschleunigten und verbesserten Klassifikation aufgetretener Anomalien. Die Vorteile können im Einzelnen die folgenden sein:

- Verbesserte Priorisierung für die Bewertung von Anomalien durch den automatisierten Abgleich mit Daten der Teilnehmer;
- verkürzte Zeit, bis eine Grundlage für eine Entscheidung zur Verfügung steht;
- verringerter Ressourcenbedarf durch effektivere Bewertung und Klassifikation;
- Möglichkeit des Einsatzes sensitiverer Detektionsverfahren mit erhöhter Fehlalarmrate, die durch den automatisierten Abgleich wieder ausgeglichen werden kann;
- Erkennung großangelegter Angriffe bzw. übergreifender Bedrohungen;
- mögliche Frühwarnung der Teilnehmer.

Insgesamt können die ausgetauschten Informationen bei einem einzelnen Teilnehmer sowohl dazu genutzt werden, um auf mögliche Bedrohungen vorbereitet zu sein, die momentan noch nicht in seinem Netz aufgetreten sind, als auch die Bewertung bereits aufgetretener Ereignisse durch Abgleich mit Teilnehmerinformationen zu vereinfachen. Für die in Abschnitt 2.4.3 dargestellten Detektionsverfahren ist der mögliche Nutzen durch Datenaustausch in Tabelle 4 näher dargestellt.

Tabelle 4: Nutzen des Datenaustauschs beim Enterprise-Monitoring

Detektionsart	Erwarteter Nutzen
Scanning-Detektion	Erkennung der Vorbereitung großangelegter bzw. übergreifender Angriffe; höhere Priorisierung von Gegenmaßnahmen; Warnung der Teilnehmer
Phishing-Erkennung	Erkennung großangelegter bzw. übergreifender Phishing-Kampagnen; Warnung der Teilnehmer über erfolgte oder mögliche Angriffe; Abwehr von Angriffen bei den Teilnehmern durch Blockieren der entsprechenden E-Mails; gezielte Priorisierung
C&C-Verkehr-Detektion	Vereinfachte Klassifikation von Anomalien im Netzverkehr durch Abgleich mit Teilnehmerdaten; verbesserte übergreifende Detektion von Bots und Backdoors
Denial-of-Service	Warnung der Teilnehmer vor möglichen DoS-Angriffen; Abgleich der Angriffsdaten zur Erkennung von Bots und Botnetzen; Warnung vor möglichen Schwierigkeiten beim angegriffenen Teilnehmer; Erkennung übergreifender Bedrohungen

[1] Siehe dazu die Details zum Proof-of-Concept in Abschnitt 6.

2.5 Schnittstellen zwischen den Anwendungsfällen

Trotz des unterschiedlichen Charakters und der unterschiedlichen Zielsetzungen der Anwendungsfälle existieren einige Schnittstellen, an denen der Austausch von Informationen zwischen den Anwendungsfällen möglich und sinnvoll ist. Diese Schnittstellen stellen eine Erweiterung des Potentials des MonIKA-Systems dar, da hier deutlich wird, dass das MonIKA-System nicht nur zur Behandlung isolierter Anwendungen geeignet ist, sondern diese Anwendungen auch durch den informationellen Austausch untereinander weiter bereichern kann.

2.5.1 Informationsaustausch zwischen Botnetz-Monitoring und BGP-Monitoring

Anomalien im globalen Internet-Routing und Aktivitäten von Botnetzen unterscheiden sich in vielen Eigenheiten grundlegend. Somit existieren auch starke Unterschiede in den jeweiligen Detektionsmethoden. Trotz der Differenzen bei Datenerhebung und -verarbeitung bietet sich ein gewisses Maß an Datenaustausch zwischen diesen Anwendungen durchaus an. Sowohl bei Botnetzen als auch beim Internet-Routing steht die Aufdeckung der tatsächlichen Ausprägung von Netzstrukturen sowie deren Abweichungen von einem Soll-Zustand im Fokus.

Ein Beispiel für anwendungsübergreifende Informationsfusion sind sogenannte Darknets: Hierbei handelt es sich um IP-Adressbereiche, die nicht offiziell vergeben sind. Diese können durch manipulierte Routing-Informationen von Angreifern zur Kommunikation genutzt werden. Da solche ungenutzten Adressen sonst nicht in Erscheinung treten und damit auch nicht auf Blacklists auftauchen, werden solche Darknets auch von Botnetz-Betreibern zum Versand von Spam genutzt, um auf diese Weise gängige Filtermechanismen zu umgehen.

Vom Austausch von Informationen zwischen den zu den Zwecken Botnetz-Monitoring und BGP-Anomalieerkennung im EvA-Service-Cluster aktiven Anwendungen profitieren dabei beide Seiten: Als solche erkannte Darknets geben Hinweise auf Botnetze, sofern von den enthaltenen Adressen Kommunikation ausgeht. Umgekehrt kann die Erkenntnis über die Zugehörigkeit bestimmter IP-Adressen zu Botnetzen Anhaltspunkte geben, die dabei helfen, erkannte Anomalien korrekt zu klassifizieren.

2.5.2 Informationsaustausch zwischen BGP-Monitoring und Enterprise-Monitoring

Die Kommunikation der am Enterprise-Monitoring beteiligten Unternehmen findet in vielen Fällen über das Internet statt. Die Ergebnisse der BGP-Anomalieerkennung sollten daher auch innerhalb des Enterprise-Monitorings berücksichtigt werden, um die anomaliefreie Kommunikation zu gewährleisten. So können Unternehmen zum Beispiel erkennen, wenn ihre Kommunikation über ungewöhnliche Routen durch das Internet geleitet wird. Dies kann ein Anzeichen für einen Versuch etwa durch Konkurrenzunternehmen oder staatliche Stellen sein, Informationen abzufangen oder zu manipulieren. Im Gegenzug können am Enterprise-Monitoring beteiligte AS-Betreiber BGP-Monitore betreiben und die lokale Sicht auf das globale Internet-Routing zur Klassifikation zur Verfügung stellen.

2.5.3 Informationsaustausch zwischen Enterprise-Monitoring und Botnetz-Monitoring

Die Schnittmenge zwischen Enterprise-Monitoring und Botnetz-Monitoring ist beträchtlich: Aus Sicht des Botnetz-Monitoring lassen sich im Rahmen des Enterprise-Monitorings betriebene SIEM-Systeme als Sensorik nutzen, die bereits vorklassifizierte, aggregierte Sicherheitsinformationen aus den internen Netzen von Unternehmen bereitstellt. Das Enterprise-Monitoring profitiert wiederum von den

im Rahmen des Botnetz-Monitoring gewonnenen Erkenntnissen, welche die lediglich das eigene Unternehmen umfassende Sicht des Enterprise-Monitorings erweitern.

3 Allgemeine Fragen des Datenschutzes bei Anomalie erkennenden Infrastrukturen

Allen Anwendungsszenarien sind bestimmte Rechtsfragen aus Datenschutzsicht gemein. Diese Fragen werden vorrangig untersucht und dahingehend erörtert, welchen datenschutzrechtlichen Vorgaben der Einsatz eines MonIKA-Systems unterliegt. Zudem werden die grundsätzlichen Herausforderungen in Bezug auf Personenbezug und Datensparsamkeit abstrakt analysiert.

3.1 Rechtsfragen bezüglich der Teilnehmer

Zunächst sind die Teilnehmer, seien es Provider, Unternehmen, Betreiber autonomer Systeme oder andere Datenlieferanten, im Fokus. Hier geht es um die Einordnung, welche Daten dem Datenschutzrecht unterfallen, auf welcher Grundlage eine möglicherweise stattfindende Datenverarbeitung bei diesen Beteiligten möglich ist und welche rechtlichen Bedingungen und Grenzen zu beachten sind.

3.1.1 Personenbezug

Zuerst ist die grundlegende Frage zu klären, welche der bei den einzelnen Teilnehmern aufgezeichneten und geloggten Daten überhaupt personenbezogen sind, um so den Anwendungsbereich des Datenschutzrechts zu bestimmen.

Der Personenbezug als zentrales Merkmal des Datenschutzrechts wird in § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG) selbst durch das Gesetz als

> *„Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“*

definiert. Es macht in diesem Zusammenhang keinen Unterschied, ob die hinter dem Datum stehende Person bestimmt oder nur bestimmbar ist.[2] Das BDSG ist in beiden Fällen gleichermaßen anwendbar. Diese Beschreibung über den Begriff „Einzelangaben“ ist daneben keine Einschränkung[3], der Begriff ist vielmehr weit auszulegen. Die gesamte Fragestellung steht dabei unter dem Eindruck der Rechtsprechung des Bundesverfassungsgerichts, das in seinem Volkszählungsurteil[4] bereits ausführte, dass es

> *„unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses‘ Datum mehr“*

gibt. Dies ist in allen Szenarien von Anomalie erkennenden Verfahren umso mehr der Fall, als dass die Fusion von möglicherweise isoliert wenig sensibler Einzelangaben dahingehend bezweckt wird, dass durch die Korrelation und Fusion Erkenntnisse geschaffen werden soll, die vorher aufgrund der Einzelangaben nicht möglich war.

Als personenbezogene Daten kommen insgesamt die in Tabelle 5 aufgeführten Daten in Betracht.

[2] *Dammann*, in: Simitis, BDSG, § 3, Rn. 23.
[3] Kühling/Seidel/Sivridis, Datenschutzrecht, S. 79.
[4] BVerfGE 65, 1.

Tabelle 5: Potentiell personenbezogen Daten in den MonIKA-Szenarien

Szenario	Daten mit möglichem Personenbezug
Botnetz-Abwehr	▪ E-Mail-Header, Betreffzeile ▪ Inhalt und Anhänge ▪ IP-Adressen ▪ Zeitpunkte der Versendung und Markierung als Spam ▪ URLs
Routing-Anomalien	▪ IP-Bereiche in Routing-Tabellen autonomer Systeme ▪ AS-Nummern ▪ IP-Adressen, die durch Traceroutes adressiert werden ▪ Zeitpunkte der Ereignisse
Enterprise-Monitoring	▪ IP-Adressen von unternehmensinternen und externen Rechner ▪ Portnummern ▪ Daten aus dem genutzten Protokoll ▪ Zeitpunkte der Ereignisse ▪ Angesprochene URLs

In jedem Fall zu klären ist der Personenbezug von IP-Adressen. Sie stellen in jedem Szenario ein relevantes Datum dar, um durch ein Botnetz infizierte Rechner zu identifizieren, Routing-Anomalien zu erkennen oder Angriffe auf Unternehmen zu blockieren. Untrennbar verknüpft mit den IP-Adressen sind in aller Regel Daten über den Zeitpunkt der verdächtigen Ereignisse. Oft wird auch erst über einen Vergleich von Zeitpunkten oder -abschnitten eine Summe von Einzelereignissen als Anomalie erkennbar sein. Auch Zeitpunkte oder Zeitabschnitte der Ereignisse sind damit von großer Bedeutung für jede Art von Anomalieerkennung.

Die sogenannten statischen IP-Adressen sind dabei ohne Weiteres als Einzelangaben über Personen zu werten, weil sie über persönliche und sachliche Verhältnisse, nämlich den benutzten Rechner und den Zeitpunkt der Nutzung, Aufschluss geben. Diese Einzelangaben müssten aber auch einer Person zuordenbar sein. Das Merkmal der Zuordenbarkeit war jedenfalls bei IP-Adressen lange Zeit umstritten, ist aber mittlerweile durch die Rechtsprechung weitgehend geklärt[5] und auch in der allgemeinen Rechtslehre nicht weiter strittig.[6] Die Zuordenbarkeit oder Bestimmbarkeit einer Person ist bereits erfüllt, wenn der Personenbezug über mehrere Zwischenschritte und die Zuordnung zur konkreten Personen objektiv und ohne unverhältnismäßigen Aufwand möglich ist.[7] Dies ist bei statischen IP-Adressen durch die Internet Service Provider regelmäßig möglich, da die Provider statische IP-Adressen einem bestimmten Anschluss und damit einer natürlichen Person zuordnen können.

Weniger deutlich ist die Rechtslage bei dynamischen IP-Adressen, weil dort die Zuordnung möglicherweise schwieriger wird oder mangels vorhandener Aufzeichnungen über die jeweiligen Sessions überhaupt nicht mehr möglich ist. Der Europäische Gerichtshof hat in seinem Urteil vom 24. November 2011[8] zuletzt aber nicht mehr zwischen statischer und dynamischer IP-Adresse unter-

[5] Ganz herrschende Ansicht in der Rechtsprechung, vgl. zuletzt BGH, Urteil vom 13. Januar 2011, Az. III ZR 146/10 und OLG Frankfurt, Urteil vom 28.08.2013, Az. 13 U 105/07.
[6] *Dammann*, in: Simitis, BDSG, § 3, Rn. 63.
[7] *Weichert*, in: Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, § 3, Rn. 13.
[8] Urteil des Europäischen Gerichtshofs vom 24. November 2011, - C 70/10 -, Rn. 51.

schieden und damit den Schluss nahegelegt, dass die dynamische Adresse mit der (zuordenbaren) statischen IP-Adresse gleichzusetzen ist. Das Oberlandesgericht Frankfurt ist in seinem Urteil vom 28.08.2013[9] genauer auf die dynamischen IP-Adressen eingegangen und hat dort dargelegt, dass jedenfalls so lange, wie der Provider über die Zuordnungsdaten verfügt, eine Zuordenbarkeit und damit auch der Personenbezug besteht. Darüber hinaus weist die Artikel-29-Datenschutzgruppe darauf hin, dass die Zuordenbarkeit einer IP-Adresse (dynamisch oder statisch) nicht nur durch den Provider, sondern auch durch den Diensteanbieter oder Website-Betreiber möglich ist, sofern die Zugriffe auf die Seite ein solches Maß erreichen, dass kumuliert eine Zuordnung der IP-Adresse zu einer Person möglich ist. Dies soll in aller Regel bei allen Betreibern solcher Dienste der Fall sein, da dort alle Zugriffe über das Hypertext Transfer Protocol aufgezeichnet werden.[10] Auch das Europäische Parlament geht in seinen offiziellen Dokumenten bezüglich der geplanten Datenschutz-Grundverordnung selbstverständlich davon aus, dass IP-Adressen unabhängig von „statisch oder dynamisch" personenbezogen sind[11], so dass insgesamt der Personenbezug auch von dynamischen IP-Adresse als herrschende Ansicht betrachtet werden muss.

In der Literatur wurde zwar noch vereinzelt die Gegenansicht vertreten. So verweisen *Krüger* und *Maucher*[12] darauf, dass jedenfalls Content-Provider unmittelbar keine Möglichkeit hätten, die hinter der dynamischen IP-Adresse stehende Person zu identifizieren. Neben technischen Verharmlosungen verkennen die Autoren dabei aber insbesondere die bereits zitierte Rechtsprechung des Bundesverfassungsgericht seit dem Volkszählungsurteil, das mit klaren grundrechtlichen Erwägungen darlegt, dass in Zeiten von Big Data, Data-Mining und hochgradigen Korrelationsmöglichkeiten die dynamische IP-Adresse in nahezu allen Fällen einer Person zuordenbar ist und zwar ohne Mithilfe der Provider.

In gleicher Weise ist damit auch der Zeitpunkt der Nutzung zuordenbar. An dieser Einschätzung ändert im Übrigen auch der Umstand nichts, dass die IP-Adressen vor der Übersendung an die Zentralstelle einer Pseudonymisierung unterzogen werden könnten. Die Zuordenbarkeit bleibt nämlich im Verhältnis zu der verantwortlichen Stelle so lange erhalten, wie die verantwortliche Stelle die Zuordnungsregel kennt.[13] Die Teilnehmer an MonIKA-Netzen werden in aller Regel auch nach Übersendung der Daten über die Zuordnungsregel verfügen, da nur so die spätere Auflösung der durch die MonIKA-Zentralstelle gewonnenen Erkenntnisse möglich ist.[14]

Ohne weitere Überlegungen wird zudem auch der Personenbezug der Daten aus der Spam-Erkennung zu bejahen sein. E-Mail-Header, Betreffzeilen, Inhalte sowie Absender und Empfänger liegen vor der weiteren Verwertung und Abstrahierung im Klartext vor und sind damit in aller Regel Personen zuordenbar.

Auch eine unter Umständen angesprochene URL kann Personenbezug aufweisen. Im Bereich des Enterprise-Monitorings kann beispielsweise ein Angriff auf Dateien von Mitarbeitern erfolgen. Die Adresse dieser URL kann neben dem Pfand unter Umständen auch einen Identifikator des Mitarbeiters, wie etwa im Beispiel https://www.Gaertner24.de/index/resources/Rechnungen/Peter-Jansen/docs.htm den Namen eines Mitarbeiters enthalten. Gleiches gilt für URLs, die in E-Mails enthalten sind.

Im Bereich der Erkennung von Routing-Anomalien kommt ein Personenbezug am wenigsten in Betracht. Die Routing-Tabellen der autonomen Systeme enthalten keine konkreten IP-Adressen,

[9] OLG Frankfurt am Main, Urteil vom 28. August 2013, - 13 U 105/07 -, Rn. 78 ff.
[10] Artikel-29-Datenschutzgruppe, WP 136, S. 19.
[11] Background Note Q&A on EU Data Protection Reform, http://www.europarl.europa.eu/sides/getDoc.do?type=IM-PRESS&reference=20130502BKG07917&secondRef=0&language=EN.
[12] *Krüger*/*Maucher*, in: IP-Adresse wirklich ein personenbezogenes Datum? – Ein falscher Trend mit großen Auswirkungen auf die Praxis, MMR 2011, S. 433 ff.
[13] Kühling/Seidel/Sivridis, Datenschutzrecht, S. 85.
[14] Für eine ausführliche Untersuchung der Pseudonymisierungen siehe Abschnitt 3.2.2.

sondern nur Bereiche von IP-Adressen, die mehrere (zehn-)tausend einzelne IP-Adressen abdecken können. Andererseits definiert sich der Personenbezug über die Möglichkeit, einer Person bestimmte sachliche und persönliche Umstände zuzuordnen. Dies ist auch bei Routing-Tabellen grundsätzlich der Fall, denn sie geben Auskunft darüber, welche Personen über welche autonomen Systeme wie erreichbar sind. Vor dem Hintergrund, dass bestimmte organisatorische Einheiten wie Universitäten oder Unternehmen eigene AS-Nummern haben, besteht aus datenschutzrechtlicher Perspektive auch für AS-Nummern ein Personenbezug. So wie die Postleitzahl, die zwischen wenigen Tausend und mehreren Zehntausend Personen eine bestimmte Auflösung bietet[15], kann auch aus der Zuordnung der AS-Nummer zu einer bestimmten Person auf deren persönliche Verhältnisse geschlossen werden. Im Rahmen von Traceroutes wäre etwa denkbar, dass die Zugehörigkeit eines bestimmten Anschlusses zu dem autonomen System eines bestimmten Anbieters bekannt wird. Die Daten, die im Anwendungsszenario rein zu dem Zweck gedacht sind, Anomalien im Routing zu erkennen, würden deshalb auch Werbetreibenden erlauben, bestimmte IP-Adressen zu kontaktieren und Werbung dahingehend zu verbreiten, dass die Teilnehmer eines autonomen Systems des Anbieters *X* besser zu Anbieter *Y* wechseln, weil dieser die IP-Adresse z. B. von YouTube besser erreicht. Gleichermaßen könnte über einen Traceroute auf ein mobiles Gerät herausgefunden werden, dass sich der Inhaber aktuell in dem autonomen System der Universität *A* oder Firma *B* befindet.

Die des Weiteren bei Traceroutes ohnehin anfallenden IP-Adressen sind daneben zweifelsohne personenbezogen. Diese Daten haben in dieser Ausarbeitung aber keine Bedeutung, weil Traceroutes nur derart verwendet werden sollen, dass die konkreten IP-Adressen stets den verantwortlichen autonomen Systemen zugeordnet werden, bevor sie ins MonIKA-System gegeben werden. Insgesamt ist im Szenario „Routing-Anomalien“ also das Vorliegen personenbezogener Daten zu bejahen.

Insgesamt sind damit bei allen Anwendungsszenarien des MonIKA-Vorhabens personenbezogene Daten betroffen.

3.1.2 Verantwortliche Stelle, Dritte und Auftragsdatenverarbeitung

Für die weitere Betrachtung ist neben der Frage des Personenbezugs die rechtliche Einordnung bezüglich der einzelnen Beteiligten von grundsätzlicher Bedeutung. Das BDSG unterscheidet allgemein gemäß § 3 Abs. 7 und Abs. 8 BDSG zwischen „verantwortlicher Stelle“ und „Dritten“. Die verantwortlichen Stellen sind die primären Adressaten der datenschutzrechtlichen Bestimmungen im BDSG, insbesondere der Verantwortlichkeit für die Einhaltung des Datenschutzes. Die Unterscheidung zwischen verantwortlicher Stelle und Dritten spielt dabei in diesem Sachverhalt eine wesentliche Rolle, weil sich daran die Frage anknüpft, welchen rechtlichen Einschränkungen die Weitergabe der Daten von den Teilnehmern an die MonIKA-Zentralstelle unterliegen. Die besonderen Voraussetzungen der Datenübermittlung aus §§ 28a ff. BDSG sind nämlich nur dann zu beachten, wenn die MonIKA-Zentralstelle als Dritte im Sinne des BDSG und nicht als Auftragsdatenverarbeiter einzuordnen ist.

Das BDSG definiert in § 3 Abs. 7 BDSG die verantwortliche Stelle als

> *„jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt”*

und als Dritten in § 3 Abs. 8 BDSG

> *„jede Person oder Stelle außerhalb der verantwortlichen Stelle.“*

[15] Zum Personenbezug der Postleitzahl vergleiche *Weichert*, Neue Postleitzahlen und Datenschutz, DANA 2-1993, S. 5.

3.1.2.1 Verantwortlichkeit der Teilnehmer

Ungeachtet der detaillierten Betrachtung in den weiteren Abschnitten dieser Ausarbeitung ist zunächst festzuhalten, dass die Teilnehmer des MonIKA-Systems in aller Regel verantwortliche Stellen sein werden, da dort jedenfalls durch die Aufzeichnung der ankommenden Daten der Webserver und IT-Sicherheitssysteme eine Datenverarbeitung erfolgt.[16] Die Annahme und Speicherung der dortigen Daten ist notwendige Voraussetzung des MonIKA-Systems.

Eine Ausnahme stellen hier möglicherweise private Teilnehmer dar, die im Anwendungsszenario Botnetz-Bekämpfung über die Meldefunktion ihres E-Mail-Programms oder direkt in den Web-Applikationen der E-Mail-Provider Spam markieren und so als Erkenntnisquelle im MonIKA-System in Erscheinung treten können. Diese Datenverarbeitung unterfällt zwar grundsätzlich der Definition des § 3 Abs. 7 BDSG, weil auch ein Privater eine verantwortliche Stelle ist, solange er nicht ausschließlich eigene Daten über die eigene Person verarbeitet[17], allerdings erklärt § 1 Abs. 2 Nr. 3 BDSG, dass die Datenverarbeitung von Privaten nicht den Vorgaben des BDSG unterliegt, wenn

> *„sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten“*.
>
> (Unterstreichung durch den Bearbeiter)

Der Anwendungsbereich dieser Ausnahmeregelung ist jedoch begrenzt und greift bereits dann nicht, wenn

> *„die Datenverarbeitung jedenfalls zum Teil zu Zwecken [erfolgt], die nicht persönlich oder familiär sind“*.[18]

Die Weitergabe von für Spam gehaltener E-Mail ist kein Zweck, der rein als persönlich oder familiär zu bewerten ist. Private sind im Rahmen einer Mitwirkung am Botnetz-Szenario also ebenfalls verantwortliche Stelle im Sinne des BDSG.

Als Sonderfall ist in Bezug auf die Teilnehmer der Fall zu untersuchen, in dem die Teilnehmer nicht selbst Daten erheben, sondern die zentrale MonIKA-Einheit die Daten direkt bei den Teilnehmern abgreift. Diese Fälle sind etwa im Enterprise-Monitoring denkbar, wenn die teilnehmenden Unternehmen über keine ausreichende IT-Ausstattung verfügen, um die für das MonIKA-System nötigen Daten zu ermitteln. Denkbar ist in diesen Fällen, dass die MonIKA-Zentralstelle eigene Sensoren auf Veranlassung der Teilnehmer im System der Teilnehmer installiert und die Daten direkt selbst ermittelt. Dieses in Anlehnung an die beschriebenen Security Operation Center (SOC) als „managed SOC“ bezeichnete Szenario stellt einen Sonderfall des Enterprise-Monitorings dar und wird später als Sonderfall ausführlicher untersucht.[19]

Für die grundsätzliche Auslegung von § 3 Abs. 7 BDSG ist die Datenschutzrichtlinie 95/46/EG maßgeblich. Diese sieht in Art. 2 d) eine Verantwortlichkeit bei jedem gegeben, der

> *„über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“*.

Abgesehen von Sonderfällen entscheiden die teilnehmenden Unternehmen sowohl über die eingesetzten Mittel als auch die Zwecke, indem sie die Infrastruktur aufbauen und die Daten der Nutzer oder Kommunikationspartner aufzeichnen.

---

[16] Ausführlich im Anschluss unter Abschnitt 3.1.3.
[17] *Dammann*, in: Simitis, BDSG, § 3, Rn. 226.
[18] *Plath*, in: Plath, BDSG Kommentar, § 1, Rn. 30.
[19] Siehe Abschnitt 5.1.

Um nun insgesamt Auskunft darüber geben zu können, wie die anschließende Weitergabe der geloggten Daten von den Teilnehmern an die MonIKA-Zentralstelle rechtlich einzuordnen ist, ist im Anschluss zu klären, ob die MonIKA-Zentralstelle nur Auftragsdatenverarbeiter für die Teilnehmer ist oder als Dritte auftritt.

3.1.2.2 Verantwortlichkeit der Zentralstelle

Die zentrale Stelle ist nur dann eine verantwortliche Stelle, wenn sie im Verhältnis zu den Teilnehmern ein „Dritter" im Sinne des BDSG ist. Ein Dritter ist gemäß § 3 Abs. 8 S. 2 und S. 3 BDSG, wer nicht verantwortliche Stelle, Betroffener oder Auftragsdatenverarbeiter ist. Besonders relevant ist bei dem MonIKA-System dabei die Voraussetzung, dass die zentrale Stelle „nicht verantwortliche Stelle" sein kann. Hier stellt sich die Frage, ob die zentrale Stelle als Auftragsdatenverarbeiter für die Teilnehmer auftritt.

Die erste Voraussetzung bedeutet, dass der Dritte nicht mit der datenerhebenden Stelle identisch sein kann. Die MonIKA-Zentralstelle kann also dann nicht selbst verantwortliche Stelle sein, wenn sie juristisch mit den Teilnehmern identisch ist. Dies ist dann relevant, wenn die Teilnehmer die MonIKA-Zentralstelle über gesellschaftsrechtliche Konstruktionen wie etwa einen Verein realisieren. Denkbar wäre es etwa, dass alle Teilnehmer als Mitglieder einem Verein beitreten, dessen Zweck die Durchführung des MonIKA-Systems ist. Folge eines solchen MonIKA e. V. wäre möglicherweise, dass der Zentralverein gegenüber seinen Mitgliedern, den Teilnehmern, kein Dritter ist, sondern unabhängig von der Art der Arbeitsteilung keine selbstständige verantwortliche Stelle ist. Aufgrund der gesellschaftsrechtlichen Verknüpfung zwischen Mitgliedern und Verein würde eine Weitergabe der bei den Mitgliedern erhobenen Daten an den Zentralverein keine Übermittlung im Sinne des BDSG darstellen.[20] Eine solche Konstruktion dürfte aber die Ausnahme sein. In überschaubaren Unternehmensverbänden ist eine solche Lösung denkbar.[21] In Systemen, die auf deutlich höheren Teilnehmerbestand und Unabhängigkeit von den Teilnehmern angewiesen sind, wird die gesellschaftsrechtliche Unabhängigkeit der Zentralstelle allerdings die Regel sein.

Im Großteil der MonIKA-Szenarien ist daher die zweite der obigen Fragen relevant: Ist die zentrale Auswertungsstelle lediglich Auftragsdatenverarbeiter für die Teilnehmer oder selbst verantwortliche Stelle? Die Auftragsdatenverarbeitung regelt das BDSG in § 11 BDSG. Ein Auftragsdatenverarbeiter wird durch verschiedene Faktoren definiert. Anzeichen[22] sind etwa

- die Weisungsbefugnis des Auftraggebers gegenüber dem Dienstleister,
- die fehlende eigene Verarbeitungs- und Nutzungsbefugnisse des Dienstleisters in Bezug auf die Daten,
- die uneingeschränkte Verfügungsgewalt des Auftraggebers über die Daten,
- die umfassenden Gestaltungsmöglichkeiten des Vertrags durch den Auftraggeber sowie
- die konkreten Umstände des Einzelfalls bezüglich Zweck- und Mittelentscheidung.

Allgemein liegt eine Auftragsdatenverarbeitung dann vor, wenn der Auftraggeber die Datenverarbeitung lediglich in ihrer „Hilfsfunktion" für die Erfüllung der eigenen Aufgaben auslagert.[23] Der Auftraggeber soll regelmäßig jeden Schritt der Datenverarbeitung vorgeben und kontrollieren können, während

[20] Ähnlich: *Dammann*, in: Simitis, BDSG, § 3, Rn. 238.
[21] Bezüglich der vereinsrechtlichen Zulässigkeit eines Vereins mit entsprechenden Aufgaben siehe das Deliverable 5.1 „Rechtliche Herausforderungen der Informationsfusion und -klassifikation zur Erkennung von Anomalien in Internet-Infrastrukturen unter besonderer Berücksichtigung haftungs- und IT-rechtlicher Fragestellungen" des Projektpartners ITM, dort Abschnitt 4.6.
[22] Vgl. *Wedde*, in: Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, § 11, Rn. 4 bis Rn. 13.
[23] *Petri*, in: Simitis, BDSG, § 11, Rn. 22.

> *„dem Auftragnehmer keinerlei inhaltlichen Bewertungs- und Ermessensspielraum gestattet“*[24]

ist. Käme man unter Berücksichtigung dieser Merkmale zu dem Ergebnis, dass die Teilnehmer voll in Kontrolle über die ausgelagerte Datenverarbeitung bleiben, blieben sie gemäß § 11 Abs. 1 S. 1 BDSG voll verantwortlich für die Einhaltung der Datenschutzvorschriften durch die eigene und die ausgelagerte Datenverarbeitung. Im Gegenzug dazu genießt der Auftraggeber dann die sogenannte „Privilegierung der Auftragsdatenverarbeitung“, was praktisch bedeutet, dass die Weitergabe der Daten an den Auftragnehmer keine Übermittlung darstellt und damit nicht den engeren Grenzen der §§ 28a ff. BDSG unterliegt. In diesen Konstellationen würde die Übertragung der Daten an die MonIKA-GmbH also abermals keine Weitergabe an Dritte darstellen, sondern wäre lediglich als Nutzung der Daten zu bewerten.

Die Auftragsdatenverarbeitung ist gegenüber der sogenannten Funktionsübertragung abzugrenzen. Insoweit ist die fortschreitende technische Arbeitsteilung im Bereich der Cybersecurity zu beachten und insbesondere die Auslegung, die das Europarecht vorgibt, zu berücksichtigen.

Bei der Funktionsübertragung verlässt der Dienstleister den Bereich des reinen weisungsgebundenen Gehilfen und wird rechtlich unabhängiger, eigenständiger Datenverarbeiter. Anhaltspunkte[25] für eine solche datenschutzrechtliche und organisatorische Verselbstständigung sind etwa

- die Weisungsunabhängigkeit des Dienstleisters,
- die fehlende inhaltliche Kenntnis des Auftraggebers von den Prozessen des Dienstleisters oder
- die Eigenständigkeit des Dienstleisters bei Umfang der Verarbeitung und Organisation des Geschäftsablaufs.

In der datenschutzrechtlichen Praxis haben sich dementsprechend Beispiele herausgebildet, die zum Vergleich mit dem MonIKA-System geeignet sind. So betreibt der Gesamtverband der deutschen Versicherungswirtschaft (GDV) ein Hinweis- und Informationssystem (HIS), in welchem – dem MonIKA-System nicht unähnlich – die Einzelerkenntnisse der einzelnen Sachbearbeiter über einzelne Versicherungsnehmer durch den GDV zu einer Gesamtbewertung über diesen konkreten Versicherungsnehmer zusammengefasst werden. Nach Zusammenführung der Daten wird sodann eine Gesamteinschätzung dieses Versicherungsnehmers in Bezug auf sein Verhalten an die einzelnen Sachbearbeiter zurückübersandt. Während die Verarbeitung der Versichertendaten im HIS auch Elemente der Auftragsdatenverarbeitung aufzuweisen scheint, geht *Petri*[26] davon aus, dass derartige

> *„[u]nternehmensübergreifende Informationssysteme zur Sammlung und Verteilung von Warnmeldungen an die angeschlossenen Partnerunternehmen […] in aller Regel nicht über eine Auftragsdatenverarbeitung zu realisieren [sind].“*

Diese Wertung ist mit Blick auf die dargestellten Abgrenzungskriterien im Ergebnis überzeugend. Eine Auftragsdatenverarbeitung kann grundsätzlich nur dort vorliegen, wo der Auftraggeber tatsächlich in der Lage ist, das „Wie“ der Datenverarbeitung zu beeinflussen. Hat er aber von dem Inhalt, also etwa den benutzten Algorithmen oder der eingesetzten Software, nur rudimentäre Kenntnisse, so fehlt es an einer grundlegenden Voraussetzung für die weisungsgebundene Auftragsdatenverarbeitung. Aus dem Fehlen der Weisungsgebundenheit folgt dann denklogisch die eigene Entscheidungsbefugnis der beauftragten Stelle.[27] Diese Weisungsunabhängigkeit ist bei unternehmensübergreifenden Warnsystemen wie dem erwähnten HIS und dem hier untersuchten MonIKA-System ein notwendiges Element. Die Teilnehmer dieser Kooperationsnetze wollen in aller Regeln gerade

[24] *Petri*, in: Simitis, BDSG, § 11, Rn. 20.
[25] Vgl. *Wedde*, in: Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, § 11, Rn. 14.
[26] *Petri*, in: Simitis, BDSG, § 11, Rn. 40, und *Weichert*, in: Datenschutzrechtliche Auswirkungen und Neuordnung des Uniwagnis-Systems, 20. Wissenschaftstagung des Bundes der Versicherten (BdV).
[27] *Eckhardt*, in: Auftragsdatenverarbeitung, DuD 2013, S. 585 (586).

nicht vorgeben, wie die Daten verarbeitet werden, sondern sind vielmehr daran interessiert, dass die Dienstleister aufgrund ihres Fachwissens und der Spezialisierung ihre Ermittlungsmethoden dem Stand der Technik anpassen und aus den erhaltenen Daten das Maximum an verwertbaren Informationen für die Teilnehmer errechnen. Diese Art der Selbstständigkeit verhindert dann aber auch die inhaltliche Kontrollmöglichkeit der Teilnehmer und steht einer Einordnung als Auftragsdatenverarbeitung klar entgegen. Aus eben diesem Grund werden nun etwa in der Literatur[28] auch Dienstleister, die Bonitätsprüfungen mithilfe von Scoringverfahren anbieten, mangels

> *„inhaltlicher Kenntnis von der konkreten Gewichtung der Bewertungskriterien"*

nicht als Auftragsdatenverarbeitung angesehen. Eine derartige Eigenständigkeit der Datenverarbeitung ist mit der Auftragsdatenverarbeitung als schlichte Hilfsfunktion nicht vereinbar.[29]

Weiterhin werden in der Regel auch die organisatorische Unabhängigkeit des Dienstleisters und seine Eigenverantwortlichkeit in der Organisation des Geschäftsablaufs gegen die Einordnung als Auftragsdatenverarbeiter sprechen.[30] Zusätzlich ist der Konzeption des MonIKA-Ansatzes nach auch die Weitergabe der in der Zentralstelle gewonnenen Erkenntnisse an externe IT-Dienstleister oder die IT-Sicherheitsforschung vorgesehen, was dazu führt, dass das Kriterium der alleinigen Verfügungsgewalt des Auftragsgebers ebenfalls nicht greift.

Nach dem bereits zitierten Wortlaut des Art. 2 d) der Datenschutzrichtlinie

> *„bezeichnet der Ausdruck ‚für die Verarbeitung Verantwortlicher' die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet."*
>
> (Unterstreichung durch den Bearbeiter)

Im Rahmen der Untersuchung der Teilnehmer wurde diesbezüglich bereits mit Blick auf die Stellungnahme der Artikel-29-Datenschutzgruppe dargestellt, dass die Zweckentscheidung ein starkes Indiz für die Verantwortlichkeit darstellt. In Bezug auf die Auftragsdatenverarbeitung hat die Artikel-29-Datenschutzgruppe zusätzlich ausgeführt[31], dass die Mittelentscheidung weniger entscheidend ist:

> *„The determination of the 'means' of processing can be delegated by the controller, as far as technical or organisational questions are concerned."*

Mit der „delegation", also der Übertragung der Datenverarbeitung, ist dabei die Auftragsdatenverarbeitung gemeint. Überträgt der Zweckbestimmer die Datenverarbeitung, so kann er dem Auftragsdatenverarbeiter die Wahl der Mittel oder des „Wie" überlassen. Im Falle des MonIKA-Systems tun die einzelnen Teilnehmer grundsätzlich genau dies, indem sie die Daten an die MonIKA-Zentralstelle weiterleiten und lediglich den Zweck der Datenverarbeitung derart vorgeben, dass Erkenntnisse über die Gefährdung des eigenen Netzes und IT-Anlagen zurückfließen sollen. Die Frage ist dabei, ob diese Übertragung noch als reine Übertragung der technischen und organisatorischen Ausführung zu bezeichnen ist. In diesem Fall wäre die MonIKA-Zentralstelle nur „processor", also Auftragsdatenverarbeiter, und würde reine Hilfsfunktion für die IT-Abteilungen der einzelnen MonIKA-Teilnehmer ausüben.

Die Artikel-29-Datenschutzgruppe hat zu diesem Aspekt derart Stellung genommen, dass auf den Auftragsdatenverarbeiter nur unwesentliche Elemente des „Wie" übertragen werden dürfen, während Fragen, die den essentiellen Kern der Datenverarbeitung in Bezug auf Rechtmäßigkeit der

---

[28] *Petri*, in: Simitis, BDSG, § 11, Rn. 27.
[29] *Petri*, in: Simitis, BDSG, § 11, Rn. 22.
[30] So auch *Petri*, in: Simitis, BDSG, § 11, Rn. 23.
[31] Opinion 1/2010 on the concepts of „controller" and „processor", 00264/10/EN WP 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf, Fn. 21, S. 15.

Verarbeitung angehen, nicht aus der Hand gegeben werden dürfen. Werden diese Elemente doch aus der Hand gegeben, so muss der so Beauftragte selbst als „controller“, also als verantwortliche Stelle, angesehen werden. In der Stellungnahme heißt es deshalb im direkten Anschluss an die obigen Zitate:

> „*Substantial questions which are essential to the core of lawfulness of processing are reserved to the controller. A person or entity who decides e.g. on how long data shall be stored or who shall have access to the data processed is acting as a 'controller' concerning this part of the use of data, and therefore has to comply with all controller's obligations.*“
>
> (Unterstreichung durch den Bearbeiter)

Aus den Ausführungen der Artikel-29-Datenschutzgruppe ergibt sich damit insgesamt, dass die Festlegung des Zweckes nur dann auch die abschließende Einordnung als verantwortliche Stelle zur Folge haben kann, wenn jedenfalls die wesentlichen Fragen der Gesetzmäßigkeit der Verarbeitung und der Organisation ebenfalls in den Händen des „Zweckbestimmers“ verblieben. Ist dies nicht der Fall, so führt die Zweckbestimmung nicht dazu, dass der Zweckbestimmer alleiniger Verantwortlicher ist. Die Stelle, die daneben ihrerseits diese wesentlichen Fragen festlegt, muss ebenfalls selbst verantwortliche Stelle sein. Die Artikel-29-Datenschutzgruppe formuliert es derart, dass die Zweckbestimmung in jedem Fall die Qualifikation als verantwortliche Stelle auslöst, während die Bestimmung der Mittel dies nur tut, wenn es sich um essentielle Mittel handelt:

> „*Against this background, while determining the purpose of the processing would in any case trigger the qualification as controller, determining the means would imply control only when the determination concerns the essential elements of the means.*“[32]

Als „essential means“, also essentielle Mittel, nennt die Stellungnahme drei Beispiele, nämlich die Frage,

- welche Daten verarbeitet werden sollen,
- für wie lange die Daten verarbeitet werden sollen und
- wer Zugriff auf diese Daten haben soll.[33]

Eine endgültige Antwort auf die Frage, wann eine MonIKA-Zentralstelle dieses Niveau an Eigenständigkeit erreicht hat, ist allgemein nicht möglich. Trotzdem wird sich für den Großteil der Anwendungsfälle feststellen lassen, dass die Bestimmung dieser Faktoren einzig durch die Auswertungszentralstelle bestimmbar ist, da nur diese Stelle entscheiden kann, welche Daten nötig sind, um die durch den Teilnehmer gewünschten Auswertungen vornehmen zu können. Im MonIKA-System wird daher insgesamt eher die Zentralstelle den Teilnehmern bestimmte Anforderungen hinsichtlich der benötigten Daten auferlegen, als dass die Teilnehmer die Verarbeitung bestimmter Daten verlangen können. Es dürfte damit regelmäßig keine reine Hilfsfunktion im obigen Sinne vorliegen. Diese Sichtweise entspricht auch den bisherigen Ansichten in der datenschutzrechtlichen Literatur, die aus eben diesen Gründen auch den GDV als Betreiber des HIS oder Scoring-Dienstanbieter als verantwortliche Stellen eingeordnet haben. Auch in diesen Fällen muss der Dienstleister, der zwar den Zweck seiner Datenverarbeitung von dritter Stelle vorgegeben bekommt, aber die wesentlichen Fragen des „Wie“ der Datenverarbeitung und der damit zusammenhängenden Organisation der Abläufe eigenmächtig festlegt, selbst als verantwortliche Stelle angesehen werden

Nach alledem ist festzuhalten, dass die MonIKA-Zentralstelle im Rahmen ihrer Monitoring- und Auswertungsaufgaben als Dritte im Sinne des § 3 Abs. 8 BDSG auftritt und kein Auftragsdatenverarbeiter im Sinne des § 11 BDSG ist. Damit werden in den meisten Anwendungsszenarien sowohl

[32] Opinion 1/2010 on the concepts of „controller“ and „processor“, 00264/10/EN WP 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf, Fn. 21, S. 14.
[33] Opinion 1/2010 on the concepts of „controller“ and „processor“, 00264/10/EN WP 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf, Fn. 21, S. 14.

die Teilnehmer des MonIKA-Systems als auch die zentrale MonIKA-Einrichtung als verantwortliche Stellen anzusehen sein.

3.1.2.3 „Joint controllership“ nach derzeitiger Rechtslage

Die in den vorigen Abschnitten dargestellte Konstellation, in der mehrere Stellen im Rahmen eines zusammenhängenden Datenverarbeitungsprozesses als Verantwortliche auftreten, ist dem deutschen BDSG bisher eher fremd. Jedenfalls wird in der datenschutzrechtlichen Literatur, etwa bei *Dammann*[34], noch darauf hingewiesen, dass die ursprüngliche Konzeption des BDSG für jede Datenverarbeitung nur eine einzige verantwortliche Stelle vorsah. *Dammann* weist aber selbst zu Recht darauf hin, dass die moderne komplexe Arbeitsteilung der IT-Wirklichkeit nicht mehr durch eine derartig isolierte Betrachtung abgebildet werden kann. *Dammann* formuliert[35]:

> *„Weder für das Gesamtbild noch für Erkenntnisse, die sich erst aus der Kombination von Daten unterschiedlichen Ursprungs ergeben, lässt sich die Verantwortung einzelnen Beteiligten zuschreiben. Von dieser Problematik betroffen sind behördenübergreifende Informationssysteme […], konzernweite oder branchenspezifische Informationssysteme […]. Jede Stelle soll verantwortlich sein, wenn und soweit sie in tatsächlicher Hinsicht über Mittel und Zwecke der Datenverarbeitung verantwortlich bestimmen kann“.*

Dass diese gleichzeitige Bestimmung jeweils bei Teilnehmern und Zentralstelle des MonIKA-Systems gegeben ist, wurde bereits gezeigt. *Dammann* vertritt insgesamt deshalb auch die Ansicht, dass das Gesetz

> *„weder ausdrücklich noch sinngemäß aus[schließt], dass mehrere natürliche oder juristische Personen mit personenbezogenen Daten in gemeinsamer Verantwortung umgehen.“*[36]

In gleicher Weise bejaht auch *Weichert*[37] eine „kumulative“ Verantwortlichkeit bei eng verquickten Verarbeitungsvorgängen. *Schreiber*[38] verweist schließlich auf die Vorgaben der Europäischen Datenschutzrichtlinie und mahnt eine europarechtskonforme Auslegung des Begriffs der verantwortlichen Stelle an. Er kommt sodann zu dem Ergebnis, dass eine gemeinsame Verantwortung gegeben ist, wenn

> *„alle Stellen über Zweck und Mittel der Datenverarbeitung gemeinsam entscheiden oder an der Entscheidung beteiligt sind“.*[39]

Die Artikel-29-Datenschutzgruppe hat diese Realität ebenfalls in ihrer bereits zitierten Stellungnahme zu dem Begriff der Verantwortlichkeit erkannt und rechtlich den Begriff „joint controllership“ benutzt. Als Beispiel führt sie dazu etwa EU-weite Datenbanken an, deren Inhalt aus den einzelnen Mitgliedstaaten stammt. In der Stellungnahme heißt es dazu:

> *„Another possible structure is the ‘origin-based approach’, which arises when each controller is responsible for the data it introduces in the system. This is the case of some EU-wide databases, where control – and thus the obligation to act on requests for access and rectification – is attributed on the basis of the national origin of personal data.“*[40]

Diese derart gemeinsam verantwortlichen Stellen sind nach richtiger Ansicht[41] dann gemeinsame Schuldner gegenüber den Betroffenen (§ 7 BDSG) und Aufsichtsbehörden (§ 38 Abs. 5 BDSG).

---

[34] *Dammann*, in: Simitis, BDSG, § 3, Rn. 226.
[35] *Dammann*, in: Simitis, BDSG, § 3, Rn. 2.
[36] *Dammann*, in: Simitis, BDSG, § 3, Rn. 226.
[37] *Weichert*, in: Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, § 3, Rn. 62.
[38] *Schreiber*, in: Plath, BDSG Kommentar, § 3, Rn. 66 ff.
[39] *Schreiber*, in: Plath, BDSG Kommentar, § 3, Rn. 69.
[40] Opinion 1/2010 on the concepts of „controller“ and „processor“, 00264/10/EN WP 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf, Fn. 21, S. 21.
[41] So auch *Dammann*, in: Simitis, BDSG, § 3, Rn. 226.

Hinzuweisen ist in diesem Zusammenhang auch auf das Rechtskonstrukt der „Gemeinsamen Verfahren“. Dieser Begriff beschreibt in einigen deutschen Landesdatenschutzgesetzen wie beispielsweise in § 8 Abs. 1 Landesdatenschutzgesetz Schleswig-Holstein (LDSG S-H) und § 15 Abs. 1 Hessisches Datenschutzgesetz (HDSG) die Möglichkeit, dass mehrere öffentliche Stellen auf einen, an einer zentralen Stelle gepflegten, Datenbestand zugreifen. Voraussetzung dieser gemeinsamen Verfahren ist allerdings, dass alle Beteiligten einen gemeinsamen Zweck (wie etwa Gewässerschutz) verfolgen und dazu auf eine gemeinsame Datenbank (z. B. bezüglich Altlasten) zurückgreifen, die eine vorher bestimmte Stelle vorhält. Diese gemeinsamen Verfahren sind aber aus zweierlei Gründen für das MonIKA-System wenig relevant: Erstens sind die Regelungen der Landesdatenschutzgesetze nicht auf nicht-öffentliche Stelle und nicht auf öffentliche Stellen des Bundes anwendbar. Der Großteil der hier beschriebenen Anwendungsszenarien wird daher nicht in den Anwendungsbereich der genannten Normen fallen. Zweitens entsprechen die „gemeinsamen Verfahren“ auch inhaltlich nicht den hier diskutierten „joint controllerships“, weil anders als bei den „joint controllerships“ dort ein gemeinsamer Zweck bestehen muss. Die Zwecke der Datenverarbeitung sind im MonIKA-System aber durchaus unterschiedlich. Die Teilnehmer bezwecken den Schutz eigener IT-Infrastruktur, während die MonIKA-Zentralstelle die Förderung eigener Geschäftszwecke, die Mitwirkung an IT-Sicherheitsforschung oder den Schutz der IT-Infrastruktur im Allgemeinen zum Zweck hat. Anders als bei den gemeinsamen Verfahren ist ein gemeinsamer Zweck bei „joint controllership“ nämlich nicht notwendig. Voraussetzung ist entsprechend den obigen Ausführungen nur, dass alle Beteiligten eine Zweck- und Mittelentscheidung treffen. Die Zwecke müssen dabei aber nicht komplett deckungsgleich sein.

3.1.2.4 Verantwortlichkeit in Konzernverbänden

Als letzte Bemerkung zu der Verteilung der Verantwortlichkeiten in koordinierten Auswertungssystemen ist auf die Umsetzung in Konzernverbänden einzugehen.[42] Gerade im Bereich des Enterprise-Monitorings sind Konstruktionen denkbar, in denen alle Teilnehmer Teil eines Konzerns sind, also vertikal oder horizontal durch schuldrechtliche oder gesellschaftsrechtliche Verpflichtungen derart eng verzahnt sind, dass sie aus Sicht des Datenschutzrechts möglicherweise nicht mehr als Dritte untereinander agieren.

Denkbar wäre etwa, dass eine Muttergesellschaft im Verlagswesen im Wege der klassischen vertikalen Konzernstruktur an allen vorgelagerten Unternehmen der Produktionsstufen wie Druck- und Papierlieferung beteiligt ist. Zum Schutz der gesamten Verlagsarbeit unterhält die Muttergesellschaft nun eine MonIKA-Zentralstelle, an dem alle Konzernteile als Datenlieferanten teilnehmen. Die Übersendung der Daten an die Konzernmutter wäre dann möglicherweise mangels Qualifikation als „Dritte“ gegenüber den übrigen Teilnehmern unter Umständen keine „Übermittlung“ im Sinne des BDSG.

Wie bereits bei den Erwägungen zur Verantwortlichkeit der Zentralstelle dargestellt, knüpft die Verantwortlichkeit rein an die rechtliche Selbstständigkeit der einzelnen Stellen an.

> *„Wirtschaftliche Verflechtungen oder faktischer Einfluss spielen für die Festlegung des Stellenbegriffs keine Rolle. […] Rechtlich selbstständige Unternehmen sind demnach jeweils eigene verantwortliche Stellen, auch wenn sie im Konzernverbund stehen“*.[43]

Daraus folgt die griffigere Formulierung, dass das BDSG kein „Konzernprivileg“ kennt. Unabhängig von der Beteiligung der Muttergesellschaft an den Tochterunternehmen ist allein relevant, dass die einzelnen Beteiligten getrennte juristische Personen sind. Überschreitet eine Datenverarbeitung die Grenzen einer juristischen Person, so ist die Datenverarbeitung als Übermittlung zwischen Dritten zu werten, solange keine Auftragsdatenverarbeitung stattfindet. Die bereits beschriebene „Vereins-

[42] Eine ausführlichere Untersuchung von MonIKA-Systemen in Konzernverbänden findet sich in Abschnitt 5.2.
[43] Kühling/Seidel/Sivridis, Datenschutzrecht, S. 100.

lösung“[44] unterscheidet sich davon insofern, als dass dort die Datenverarbeitung innerhalb des Vereins erfolgt und lediglich durch dessen Mitglieder ausgeführt wird. Allerdings zeigen diese Überlegungen zu konzernrechtlichen Szenarien, dass auch diese „Vereinslösung“ ihre Grenzen hat. Im Einzelfall wird genau zu untersuchen sein, ob die Datensammlung der Teilnehmer als Vereinsmitglieder noch als Datenerhebung innerhalb des Vereins oder als eine solche außerhalb des Vereins angesehen werden muss. Hier wird es maßgeblich darauf ankommen, welchem Verantwortungskreis die Datenerhebung der Mitglieder des Vereins zuzurechnen ist.

3.1.3 Erheben, Verarbeiten und Nutzen

Nachdem bisher untersucht wurde, wann in Monitoring-Systemen personenbezogene Daten betroffen sein können und welche Beteiligten als verantwortliche Stellen anzusehen sind, ist im Folgenden zu klären, wie die konkreten Vorgänge hinsichtlich Datenerhebung, -verarbeitung und -nutzung einzuordnen sind.

Das BDSG erfasst zunächst gemäß § 1 Abs. 1 BDSG jeden „Umgang“ mit Daten. Die nichtöffentlichen Stellen, also der Großteil der möglichen Beteiligten, unterliegen den Vorgaben des BDSG gemäß § 1 Abs. 2 Nr. 3 BDSG nur,

> *„soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben […]“*.

Die Merkmale „automatisierte Verarbeitung“ sowie die einzelnen Varianten „Verarbeiten, Nutzen, Erheben“ werden in § 3 Abs. 2 ff. BDSG näher definiert.

3.1.3.1 Erheben

Das Aufzeichnen der Logdaten von Webserver, Firewall, IDS sowie die Aufzeichnung des E-Mail-Verkehrs sind zuerst mit Hinblick auf das Merkmal „Erhebung“ zu untersuchen, das in § 3 Abs. 3 BDSG definiert wird als

> *„Beschaffen von Daten über den Betroffenen“*.

Dabei reicht es zunächst aber nicht aus, dass die Daten den Stellen ohne eigene aktive Handlungen zufallen, etwa indem die Daten der Stelle aufgedrängt oder sonst wie unaufgefordert zugesandt werden. Das Beschaffen setzt vielmehr ein gezieltes Tätigwerden der Stelle voraus.[45] Die Teilnehmer des MonIKA-Systems erlangen die Rohdaten in aller Regel durch die Logging-Automatismen der von ihnen eingerichteten Soft- und Hardware. Dabei ist das entscheidende Differenzierungskriterium nun, ob das Logging der Sensoren den MonIKA-Teilnehmern als bewusstes und zielgerichtetes Einrichten technischer Anlagen zugerechnet wird oder ob das Logging ein passiver, quasi-aufgedrängter Vorgang ist und kein aktives Beschaffen darstellt.

Dazu ist ein genauer Blick auf die eingesetzten Techniken nötig, der im Einzelfall sehr unterschiedliche Ergebnisse liefern kann. Grundsätzlich bieten aber alle gebräuchlichen Webserver oder Firewalls derartige Logging-Automatismen an. Es liegt regelmäßig an den Nutzern derartiger Systeme, das Ausmaß der anfallenden Logdaten festzulegen. Es mag zwar durchaus Systeme geben, die keinerlei Möglichkeiten eröffnen, das Logging umfänglich zu reduzieren. In derartigen Konstellationen, in denen die Logdaten gewissermaßen durch die Software aufgedrängt werden, ohne dass der Nutzer Änderungen vornehmen kann, wäre dann durchaus die Argumentation vertretbar, dass mangels Einflussmöglichkeit auch kein aktives Beschaffen der Daten vorliegt.

[44] Siehe Abschnitt 3.1.2.2.
[45] Kühling/Seidel/Sivridis, Datenschutzrecht, S. 89.

In den relevanten Anwendungsszenarien stellen die Daten der einzelnen Logfiles der jeweiligen Sensoren allerdings gerade das ausgesprochene Ziel der Nutzer dar. Es ist notwendiges Kernelement des gesamten MonIKA-Systems, dass die bereits beschriebenen Datenkategorien aufgezeichnet werden, um überhaupt in der Lage zu sein, diese Daten auszuwerten und zur weiteren Behandlung an die Zentralstelle zu versenden. Im hier zu untersuchenden Fall des Enterprise-Monitorings ist also bei allen Teilnehmern ein starkes subjektives Element vorhanden. Dabei ist es nun anerkannt, dass ein Beschaffen auch dann vorliegt, wenn eine Stelle Interesse an bereits vorhandenen Daten kundtut, die ohne ein aktives Tun dieser Stelle beschafft wurden.[46] Das bedeutet, dass ein nur geringer aktiver Beitrag zusammen mit einem klaren subjektiven Element im Ergebnis auch als Beschaffen gewertet werden muss. Dies überzeugt auch im Ergebnis. So sehr die Einwirkungsmöglichkeiten eines IT-Mitarbeiter oder gar Nutzers auf den Umfang des Loggings auch beschränkt sein mögen, so ist das Betreiben dieser Sensoren doch erklärtes Ziel des Nutzers, und bei den geloggten Daten handelt es sich nicht lediglich um aufgedrängte Daten. Da aber ohnehin alle großen Webserver-Produkte über vielfältige Einstellungsmöglichkeiten verfügen, sind diese Überlegungen sehr theoretischer Natur. In den allermeisten Fällen geht dem Betrieb der diversen loggenden Sensoren eine bewusste und aktive Errichtung und Konfiguration vorweg, so dass bereits insoweit ein Beschaffen zu bejahen ist.

Zusätzlich setzt das „Beschaffen“ im Sinne des BDSG auch voraus, dass die Stelle

> *„Verfügung über die Daten begründet hat. Dazu genügt es, wenn [die Stelle] Datenträger in Besitz oder Daten zur Kenntnis genommen hat“.*[47]
>
> (Ergänzung durch den Bearbeiter)

Anhand dieser Voraussetzungen ist auch das Aufzeichnen der Logdaten zu beurteilen. Die Logs der Webserver, Firewalls und IDS sowie sonstiger Applikationen speichern ihre Datenbestände grundsätzlich dauerhaft auf physischen Datenträgern innerhalb der Zugriffssphäre der einzelnen Unternehmen. Selbst dort, wo technisch keine dauerhafte Speicherung erfolgt, erfordert die EvA-Software, dass die Logdaten doch zumindest vorübergehend in flüchtigen Zwischenspeichern vorgehalten werden, um die Vor-Ort-Auswertung durchführen zu können, die notwendig ist, um später die so aufbereiteten Daten an die MonIKA-Zentralstelle zu senden. Diese sendebereit aufbereiteten Daten sind damit jedenfalls kurzfristig in der Verfügungsgewalt des jeweiligen Betreibers der EvA-Software. Dieses Ergebnis muss auch aus einer teleologischen Betrachtung des § 3 Abs. 3 BDSG folgen. Ziel des BDSG ist gemäß § 1 Abs. 1 BDSG der Schutz der Persönlichkeitsrechte durch den Schutz persönlicher Daten vor dem unkontrollierten Zugriff Unbefugter.[48] Dieser Zweck gebietet es, bei der Auslegung einer Norm immer dann den Anwendungsbereich des BDSG als eröffnet zu betrachten, wenn ein solcher Zugriff möglich ist. Da der Zugriff auf die Daten im Arbeitsspeicher auch unbefugten Dritten möglich ist, muss im Umkehrschluss auch derjenige, der dieses Risiko überhaupt erst durch seine Datenerhebung erschafft, verpflichtet werden, das Datenschutzrecht zu beachten. Dies geschieht durch die Anwendung der §§ 3 ff. BDSG. Der Betreiber einer Software, die lediglich Logdaten in Arbeitsspeichern zwischenverarbeitet, muss damit auch als eine Stelle angesehen werden, die Verfügungsgewalt über die Daten erlangt.

Auch diese Aspekte sind bezüglich des Großteils aller denkbaren Einsatzgebiete eines MonIKA-Systems eher theoretischer Natur. Dies folgt bereits daraus, dass die Teilnehmer eines Auswertungsnetzes die eigentlichen Logdaten in den allermeisten Fällen auch nach Übersenden an die zentrale Logstelle nicht löschen werden. Zum einen erfordern viele Geschäftsprozesse irgendeine Form der Qualitätskontrolle. Diese ist aber nur durchführbar, wenn später ein Abgleich der zurückempfangenen Daten mit den ursprünglich gesendeten Daten möglich ist. Zum anderen sollen die auszuwertenden Logdaten pseudonymisiert übersandt werden. Um später die Zuordnung der pseudonymisiert

[46] *Dammann*, in: Simitis, BDSG, § 3, Rn. 104.
[47] *Dammann*, in: Simitis, BDSG, § 3, Rn. 108.
[48] Vgl. *Simitis*, in: Simitis, BDSG, § 1, Rn. 23.

verarbeiteten Daten zu ermöglichen, müssen die Originaldaten aufbewahrt werden. Soll etwa eine Menge von E-Mail-Domains auf ihre Wahrscheinlichkeit überprüft werden, dass sie durch ein Botnetz für Spam-Versand eingesetzt werden, so werden diese Domains pseudonymisiert an die Zentralstelle übersandt und nach Korrelation mit anderen Daten auch nur in gleicher pseudonymisierter Form zusammen mit den Auswertungsergebnissen zurückgesandt. Damit beim ursprünglichen Absender die Möglichkeit besteht, diese Erkenntnisse einer bestimmten Domain im Klartext zuzuordnen, müssen diese Klartexte noch vorhanden sein. Ansonsten sähe sich ein Empfänger dieser Daten nicht in der Lage, seinen E-Mail-Server derart zu konfigurieren, bestimmte Adressen oder Domains zu blockieren.

Daneben sieht der MonIKA-Ansatz eine Art Live-Preview vor.[49] Zuständige Mitarbeiter, zumeist die betrieblichen Datenschutzbeauftragten, sollen die Möglichkeit haben, in Echtzeit die aktuell übersandten Daten zu sichten. Selbst wenn die Logdaten nur flüchtig im Arbeitsspeicher zwischengelagert und sodann ohne dauerhaftes Speichern an die Auswertungszentralstelle übersandt werden, so würde doch in jedem Fall zumindest die Möglichkeit der Kenntnisnahme bestehen. Gerade der letztere Aspekt führt also dazu, dass auch nur in Arbeitsspeichern verarbeitete Daten der Verfügungsgewalt der MonIKA-Teilnehmer unterliegen.

Diese Kriterien erwägend, stellt sich das Aufzeichnen der Logdaten in den IT-Abteilungen der MonIKA-Teilnehmer insgesamt also als gezieltes, aktives Beschaffen und damit als Erheben im Sinne des § 3 Abs. 3 BDSG dar.

3.1.3.2 Verarbeiten

Neben der ursprünglichen Beschaffung der Daten erfasst das BDSG die Verarbeitung von personenbezogenen Daten als Kernbegriff der Datenverarbeitung im Allgemeinen. Als Verarbeitung wird gemäß § 3 Abs. 4 BDSG

> *„das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten“*

definiert.

Eine Speicherung wird bereits bejaht, wenn es sich nur um eine

> *„Zwischensicherung bei der Dateneingabe“*[50]

handelt, womit in Übereinstimmung mit der obigen Bewertung bei dem Merkmal „Verfügungsgewalt erlangen“ auch die Zwischenspeicherung im Arbeitsspeicher ausreichend sein könnte. Um eine Speicherung handelt es sich nur dann nicht, wenn

> *„Daten technikbedingt für kürzeste Momente‚zwischengespeichert/umgespeichert‘ werden“*.[51]

Die Grenzen sind insoweit fließend. Der Begriff ist dabei nicht identisch mit der IT-Fachsprache.[52] Entscheidender Blickwinkel ist auch hier vielmehr der Schutz personenbezogener Daten. Je weniger die zwischengespeicherten Daten dem Zugriff des Menschen und damit dem Missbrauch ausgesetzt sind, umso mehr wird man eine Speicherung und damit den Schutz des BDSG verneinen können.

Einengend unterfällt eine Speicherung weiterhin nur dem BDSG, wenn sie mit der

> *„Zielrichtung auf eine weitere Verarbeitung“*[53]

erfolgt. Das Merkmal der Speicherung ist damit begrifflich eng mit den anderen Varianten des § 3 Abs. 4 BDSG verknüpft, so dass vorgreiflich zu prüfen ist, ob der weitere Umgang mit den Daten nach

[49] Details finden sich in Abschnitt 6.4.3.
[50] *Weichert*, in: Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, § 3, Rn. 33.
[51] Kühling/Seidel/Sivridis, Datenschutzrecht, S. 90.
[52] *Dammann*, in: Simitis, BDSG, § 3, Rn. 118.
[53] *Weichert*, in: Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, § 3, Rn. 33.

der Speicherung eine Verarbeitung darstellt. Während die Europäische Datenschutzrichtlinie (DSRL)[54] in Art. 2 b) DSRL einen sehr weiten Verarbeitungsbegriff benutzt und das Erheben und Nutzen von Daten mit in den Begriff einschließt, zählt das BDSG zu der Verarbeitung nur die in § 3 Abs. 4 BDSG aufgezählten Schritte. Für die rechtliche Bewertung bedeutet dies, dass die Speicherung der ursprünglich erhobenen Daten nur dann eine Speicherung im Sinne des BDSG darstellt, wenn diese Speicherung mit dem Ziel erfolgt, die Daten zu verändern, zu übermitteln, zu löschen, zu sperren (§ 3 Abs. 4 S. 1 BDSG) oder auf andere Art zu nutzen (§ 3 Abs. 4 S. 2 Nr. 1 i. V. m. § 3 Abs. 5 BDSG).

Als eine Veränderung von Daten wird das

> *„inhaltliche Umgestalten gespeicherter Daten“*[55]

verstanden. Dazu gehört neben einer inhaltlichen Verknüpfung mit anderen Daten auch die Pseudonymisierung.[56] Beides liegt im MonIKA-System vor. Die Auswertung der Logfiles zu einer ersten Voreinschätzung durch den EvA-Agenten in den SOCs der einzelnen Teilnehmer verknüpft die einzelnen Logdaten. Die sich daran anschließende Pseudonymisierung stellt ebenfalls eine inhaltliche Umgestaltung dar. Damit ist der Umgang mit den gespeicherten Logfiles eine Veränderung der Daten und das Speichern der Logfiles zu diesem Zweck auch ein Speichern im Sinne der BDSG.

Neben der Veränderung ist auch die Übermittlung der gespeicherten Daten eine Verarbeitung, die als Zweck für die Speicherung in Betracht kommt. Eine Übermittlung wird dabei durch das BDSG selbst in § 3 Abs. 4 Nr. 3 BDSG definiert als

> *„das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass*
>
> *a) die Daten an den Dritten weitergegeben werden oder*
>
> *b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft“*.

Im vorliegenden Fall senden die einzelnen Teilnehmer die Daten an eine zentrale MonIKA-Stelle und geben die Daten damit grundsätzlich im Sinne der Alternative 3a) weiter. Untersucht wurde daneben auch bereits die Frage, ob die Zentralstelle für die Teilnehmer ein „Dritter“ ist. Da dies regelmäßig der Fall ist, stellt die Weitergabe der Daten eine Übermittlung im Sinne des § 3 Abs. 4 Nr. 3a oder 3b BDSG dar. Die dem vorweggehende Speicherung zum Zweck dieser späteren Übermittlung ist damit auch eine Speicherung im Sinne des BDSG.

Nachdem nun geklärt wurde, dass der Umgang mit den Daten unter den Aspekten der Veränderung, der Speicherung und der Übermittlung als Verarbeitung zu klassifizieren ist, bleibt zu untersuchen, ob es sich auch um ein Löschen im Sinne des BDSG handelt.

Die Löschung im Sinne des § 3 Abs. 4 Var. 5 BDSG ist

> *„jede Form der Unkenntlichmachung“*.[57]

Eine solche Löschung setzt dabei voraus, dass der zuvor gespeicherte Text nicht mehr lesbar ist, und richtet sich angesichts der vielfältigen Möglichkeiten der Rekonstruktion von überschriebenen Datenträgern nach dem Stand der Technik.[58] Im Falle der Teilnehmer an diesem MonIKA-System werden nicht alle erhobenen und gespeicherten Daten zwangsweise genutzt. Stattdessen werden nach der Erstauswertung durch den EvA-Agenten durchaus Daten als unnötig eingestuft und werden damit nicht mehr benötigt. Von der Vielzahl an gespeicherten IP-Adressen kann daher ein Großteil nach der Erhebung und Speicherung gelöscht werden. Einzelheiten sind hier jedoch sehr von den konkreten

[54] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.
[55] *Dammann*, in: Simitis, BDSG, § 3, Rn. 129.
[56] *Weichert*, in: Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, § 3, Rn. 35.
[57] *Weichert*, in: Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, § 3, Rn. 44.
[58] *Weichert*, in: Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, § 3, Rn. 44.

Anwendungsszenarien abhängig. So kann zumindest nicht ausgeschlossen werden, dass der Bereich der IT-Sicherheitsforschung auch an (vermeintlich) unauffälligen IP-Adressen interessiert ist.

3.1.3.3 Nutzen

Schließlich ist in Bezug auf die Teilnehmer des MonIKA-Systems zu erörtern, ob der dortige Datenumgang als „Nutzen" im Sinne des § 3 Abs. 5 BDSG einzuordnen ist. Die Nutzung von Daten ist ein Auffangmerkmal und umfasst alle sonstigen Formen der Verwendung von Daten.[59] Jedenfalls das Kopieren von Daten fällt dabei zum Beispiel unter keine der in § 3 Abs. 3 und 4 BDSG genannten Varianten und wird daher zur Datennutzung gerechnet.[60] Da die MonIKA-Teilnehmer die durch die EvA-Agenten vorausgewerteten Logdaten nicht nur an die MonIKA-Zentralstelle weiterleiten, sondern regelmäßig auch in Kopie speichern müssen, findet damit in jedem Fall auch eine Datennutzung im Sinne des § 3 Abs. 5 BDSG statt. Dabei ist es unerheblich, inwieweit diese kopierten Daten genauso wie die zur Weitergabe vorgesehenen Daten bereits weitgehend pseudonymisiert sind, denn die Pseudonymisierung hebt den Personenbezug nicht auf. Solange aus der pseudonymisierten IP-Adresse noch der Klartext rückerrechenbar ist oder eine andere Form der Zuordnung möglich ist, bleibt der Personenbezug vorhanden.[61]

3.1.4 Rechtsgrundlage für die Datenerhebung

Die Teilnahme an Monitoring-Netzen unterfällt nach den bisherigen Erkenntnissen damit klar dem Regelungsbereich des Datenschutzrechts. Die vorhergehenden Abschnitte haben dargelegt, dass es sich bei den Teilnehmern um verantwortliche Stellen handelt und die Teilnahme am MonIKA-System personenbezogenen Daten betrifft, die einer Datenverarbeitung unterzogen werden.

Dies hat nun zwingend zur Folge, dass sich für die Datenverarbeitungsschritte die Frage nach der Rechtsgrundlage stellen lassen muss.

Das BDSG weist in § 4 Abs. 1 BDSG ausdrücklich darauf hin:

> *„Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat."*

Jede Datenverarbeitung steht damit unter dem grundsätzlichen Verbot mit Vorbehalt der Erlaubnis. Diese Erlaubnis kann aus Einwilligung und Gesetz stammen. Im Rahmen der gesetzlichen Erlaubnisnormen wird zudem zu untersuchen sein, welche Gesetze anwendbar sind.

3.1.4.1 Einholung einer Einwilligung

Als erste Möglichkeit der Rechtfertigung von Datenverarbeitungen kennt das Datenschutzrecht die Einwilligung. Regelungen über die Einwilligung finden sich sowohl im BDSG als auch in Sondergesetzen und stellen stellenweise unterschiedliche Anforderungen an die Wirksamkeit einer Einwilligung.

3.1.4.1.1 Die Einwilligung nach BDSG

Das BDSG selbst regelt die Einwilligung des Betroffenen in § 4a BDSG. Die Betroffenen sind die in den jeweiligen Anwendungsszenarien beschriebenen externen Parteien, also allgemeine Internet-Nutzer, Kunden des E-Mail-Providers, Geschäftspartner oder Kunden der teilnehmenden Unternehmen. Aber auch die Angreifer, die auf die Netze zugreifen, sind solche externen Parteien und grundsätzlich auch Betroffene, da dieser Begriff gemäß § 3 Abs. 1 BDSG alle natürlichen Personen

[59] Kühling/Seidel/Sivridis, Datenschutzrecht, S. 95.
[60] Kühling/Seidel/Sivridis, Datenschutzrecht, S. 95.
[61] Kühling/Seidel/Sivridis, Datenschutzrecht, S. 95.

erfasst, über deren persönliche und sachliche Verhältnisse die Einzelangaben Aufschluss geben. Das MonIKA-System loggt und speichert schließlich grundsätzlich alle Zugriffe. Es findet also keine Differenzierung zwischen solchen Nutzern statt, deren Zugriff gewünscht ist (Mitarbeiter, die per Fernzugriff auf Netzbereiche zugreifen), und solchen, deren Zugriff unerwünscht ist (E-Mail-Absender von Spam-E-Mails). Eine Einwilligung ist unabhängig davon bezüglich aller Datenverarbeitungen nötig.

Die Anforderungen an eine wirksame Einwilligung aller Betroffenen legt § 4a Abs. 1 BDSG fest. Besonders schwer lässt sich in Monitoring-Netzen das Erfordernis der Schriftform gemäß § 4a Abs. 1 S. 3 BDSG einhalten. Im Enterprise-Monitoring-Szenario wäre es zwar denkbar, in die Arbeitsverträge der einzelnen Mitarbeiter der jeweiligen Unternehmen eine Einwilligung bezüglich des Loggings aufzunehmen. Diese Art der Einwilligung versagt aber spätestens bei allen unternehmensfremden Personen, so auch bei den Angreifern, da über deren Identität nichts bekannt ist und erst recht keine arbeitsrechtlichen Beziehungen bestehen müssen. Davon abgesehen ist die Frage der datenschutzrechtlichen Einwilligung in Arbeitsverträgen aber auch grundsätzlich sehr umstritten. So zweifelt *Gola*[62] mit Verweis auf *Wohlgemuth*[63] in nachvollziehbarer Weise daran, ob im Verhältnis zwischen Arbeitnehmer und Arbeitgeber aufgrund des Arbeitsverhältnisses überhaupt von einer Einwilligung gesprochen werden kann, die „auf freier Entscheidung" beruht. In der Praxis hat der Arbeitnehmer oft nur die Wahl, aufgrund des Abhängigkeitsverhältnisses die „Einwilligung" entweder zu erteilen oder den Arbeitsvertrag im Ganzen abzulehnen. Dementsprechend sieht auch *Simitis*[64] existentielle Leistungen wie eben das Arbeitsverhältnis als Beispiel für größtmögliche Sorge um die Vereinbarkeit mit der Autonomie der Entscheidung. Die Artikel-29-Datenschutzgruppe kritisierte[65] zudem,

> *„dass es in den Fällen, in denen ein Arbeitgeber zwangsläufig aufgrund des Beschäftigungsverhältnisses personenbezogene Daten verarbeiten muss, irreführend ist, wenn er versucht, diese Verarbeitung auf die Einwilligung der betroffenen Person zu stützen. Die Einwilligung der betroffenen Person sollte nur in den Fällen in Anspruch genommen werden, in denen der Beschäftigte eine echte Wahl hat und seine Einwilligung zu einem späteren Zeitpunkt widerrufen kann, ohne dass ihm daraus Nachteile erwachsen."*

Dieses Problem stellt sich auch im Enterprise-Monitoring, da die Zugriffe der Mitarbeiter auf Netzelemente in jedem Fall geloggt werden und daher die Einwilligung keine Ausübung einer Wahlmöglichkeit darstellt, sondern in irreführender Weise suggerieren könnte, dass ein Loggen unterlassen würde, falls die Einwilligung nicht erteilt wird.[66] Die Einwilligung des BDSG lässt über den Umweg des bürgerlichen Rechts gemäß § 4a BDSG i. V. m. § 126a BGB zwar auch den Ersatz der Schriftform durch eine qualifizierte elektronische Signatur zu. Die Möglichkeit ist aufgrund der nach wie vor mangelnden Verbreitung aber regelmäßig keine wirkliche Option[67] und hilft nicht über das Erfordernis der zeitlichen Abfolge hinweg.

Das Erfordernis Schriftform wird in § 4a Abs. 1 S. 3 BDSG allerdings stark aufgeweicht. So ist dann nicht notwendig, wenn besondere Umstände dem entgegenstehen. Die juristische Literatur spricht diesbezüglich Sachverhalte wie ärztliche Notfälle oder langwierigen Geschäftskontakt an und betont, dass ein Verzicht auf die Warnfunktion der Einwilligung umso möglicher ist, wie es sich nur um geringe Datenbestände handelt.[68] Vor diesem Hintergrund ist der Verzicht in den MonIKA-Szenarien eher fraglich.

---

[62] *Gola*, in: Die Einwilligung als Legitimation für Verarbeitung von Arbeitnehmerdaten, RDV 2002, S. 109, 110.
[63] *Wohlgemuth*, in: Datenschutz für Arbeitnehmer, Rn. 120 ff.
[64] *Simitis*, in: Simitis, BDSG, § 4a, Rn. 62.
[65] Artikel-29 Datenschutzgruppe, 5062/01/DE/endg.,WP 48, S. 3,
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48de.pdf.
[66] Vgl. *Simitis*, in: Simitis, BDSG, § 4a, Rn. 62.
[67] *Rogosch*, DFN-Infobrief Recht 2, 2011, S. 5.
[68] Zu allem: Kühling/Seidel/Sivridis, Datenschutzrecht, S. 125 m. w. N.

Die eigentliche Problematik liegt aber in den Voraussetzungen der zeitlichen Abfolge und der Informiertheit. Eine nachträgliche Einwilligung ist ausgeschlossen[69], und schon aus praktischen Gründen ginge es nicht, etwa den Besuchern der Website eines Unternehmens oder dem Absender einer E-Mail vor einem Logging durch den Web- oder E-Mail-Server eine Einwilligung abzuverlangen. Bevor der Browser des Besuchers die dafür nötigen Informationen anzeigen könnte, wäre der Zugriff seines Rechners auf dem Server des Unternehmens bereits verarbeitet worden. Letztlich darf auch an der Möglichkeit gezweifelt werden, die Nutzer vorher in ausreichendem Maße über die verfolgten Zwecke und den Umfang der Datenverarbeitung informieren zu können.[70]

3.1.4.1.2 Die Einwilligung nach TKG und TMG

Besondere Regelungen zur datenschutzrechtlichen Einwilligung finden sich in § 94 Telekommunikationsgesetz (TKG) und § 13 Abs. 2 Telemediengesetz (TMG). Die besondere Regelung im TKG gilt nur im Verhältnis zwischen Nutzer und Telekommunikationsdiensteanbieter und erlaubt die Einwilligung auch in elektronischer Form, wenn

> *„der Teilnehmer oder Nutzer seine Einwilligung bewusst und eindeutig erteilt hat, die Einwilligung protokolliert wird, der Teilnehmer oder Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und der Teilnehmer oder Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann“*.

Beide Normen senken die Voraussetzungen für eine elektronische Einwilligung derart herab, dass auch eine Einwilligung in Form von E-Mails oder Interaktionen mit Websites möglich ist. Das TKG greift allerdings nur zwischen Nutzer und Anbieter eines Telekommunikationsdienstes. Ob die einzelnen Teilnehmer als solche zu qualifizieren sind, hängt von dem jeweiligen Anwendungsszenario ab und wird später geklärt. Im Rahmen der Einwilligung kann dies dahinstehen, da eine solche Einwilligung ebenfalls vor böswilligem Zugriff auf eine Website oder vor Versenden der Spam-E-Mail abgegeben werden müsste. Eine solche Einwilligung würde aber auch nur solche Betroffenen erreichen, die die vor Aufrufen einer Website oder vor Versenden einer E-Mail tatsächlich Kontakt mit dem Teilnehmer des Monitoring-Netzes haben. Ein Angreifer im Enterprise-Monitoring-Szenario hat aber üblicherweise ebenso wenig wie ein normaler Nutzer im Bereich von Routing-Anomalien Kontakt mit dem MonIKA-Teilnehmer. Selbst bei aktivem Aufrufen etwa einer Website ist die elektronische Einwilligung in das Geloggt-Werden nur eine rein theoretische Möglichkeit und praktisch ausgeschlossen.

Gleiche Bedenken ergeben sich bei § 13 Abs. 2 TMG, der daneben auch nur zwischen Nutzern und Anbietern von Telemediendiensten greift.

Insgesamt ist damit festzuhalten, dass die Einwilligung im MonIKA-System keine Grundlage für Datenerhebung sein kann. Sie scheitert zuallererst an der faktisch unerreichbaren Schriftform beziehungsweise an der praktischen Unmöglichkeit, von unbekannten Dritten auch nur eine elektronische Einwilligung zu erhalten und führt zudem in Verbindung mit Arbeitsverträgen zu Problemen bezüglich der Freiwilligkeit. Vor allem aber sind die zeitliche Abfolge sowie die Informiertheit kaum erreichbar.

3.1.4.2 Rechtfertigung durch Gesetz

Die Rechtsgrundlage muss damit aus anderen Quellen stammen. Das BDSG sieht als Alternative in § 4 Abs. 1 BDSG nur die Möglichkeit der Datenerhebung vor, wenn

> *„dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt“*.

[69] *Plath*, in: Plath, BDSG Kommentar, § 4a, Rn. 11.
[70] *Däubler*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 4a, Rn. 8.

Damit kann eine Rechtsgrundlage nur aus nationalem oder europäischem Recht stammen. Zur weiteren Verdeutlichung wird im Folgenden ein kurzer Überblick über die möglichen nationalen und europäischen Rechtsquellen gegeben.

3.1.4.2.1 Aktuelle Rechtslage in Deutschland

Die Erhebung personenbezogener Daten wird derzeit durch eine Reihe von Spezialgesetzen und dem allgemeinen Bundesdatenschutzgesetz erfasst.

3.1.4.2.1.1 BSI-Gesetz vom 14. August 2009

Dort findet sich in § 5 BSIG eine Rechtsgrundlage für die Datenverarbeitung zum Zweck der Erkennung von Gefahren für die Sicherheit der Kommunikation des Bundes. Das BSIG erlaubt damit aber zum einen nur die Datenerhebung bei Bundeseinrichtungen und zum anderen auch nur eine Auswertung zum Schutz der Kommunikationsnetze des Bundes. Es erlaubt weder die Erhebung von Daten bei privaten Unternehmen noch bei Landesbehörden noch die Datenverarbeitung von anderen als dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Sein Anwendungsbereich ist streng limitiert auf das BSI.

3.1.4.2.1.2 Telekommunikationsgesetz vom 22. Juni 2004

Im TKG findet sich in § 100 Abs. 1 TKG eine Rechtsgrundlage für die Verarbeitung von Bestandsdaten und Verkehrsdaten durch den Dienstleister bei Störungen oder Fehlern an Telekommunikationsanlagen. Sein Anwendungsbereich erstreckt sich allerdings ausschließlich auf Telekommunikationsdienstleister und ist hinsichtlich seiner Reichweite stark umstritten. Nach verbreiteter Ansicht in der juristischen Literatur werden beispielsweise als „Störung oder Fehler“ nur solche Beeinträchtigungen verstanden, die sich auf die Übertragung der Nachrichten auswirken.[71] Die Nutzung der Netze zum Versand von Spam-E-Mails, zur Unterhaltung von Botnetzen oder zur Durchführung Unternehmenssabotage stört aber die Übertragung selbst nicht.

Zwar verstand der BGH in seinem umstrittenen Urteil zur Speicherung dynamischer IP-Adressen[72] den § 100 TKG weiter, nämlich im Sinne jeder Beeinträchtigung seines Kommunikationsnetzes, und erlaubt die Datenerhebung und 7-Tage-Speicherung, um derartigen Bedrohungen zu begegnen. Aber auch der BGH legt den § 100 Abs. 1 TKG bisher nur derart aus, dass die Daten zur Verwendung für die Abwehr von Bedrohungen gegen das eigene Netz und eigene Anlagen verarbeitet werden. Für kooperatives Monitoring stellt sich deshalb die Frage, ob die Heranziehung des TKG auch zur Abwehr von Gefahren für andere Teilnehmer des Netzes oder gar für das „Internet selbst“ möglich ist.

3.1.4.2.1.3 Telemediengesetz vom 26. Februar 2007

Das TMG regelt die Erbringen von Telemediendiensten, die keine Versorgungsdienste nach TKG sind (z. B. soziale Netzwerke, Online-Banking, Online-Shops usw.). Es enthält in den §§ 14, 15 TMG zwei Grundlagen für die Verarbeitung von personenbezogenen Daten. Während § 14 Abs. 1 TMG die Verarbeitung von Bestandsdaten für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung erlaubt, sieht § 14 Abs. 2 TMG eine Sonderregelung für die Mitwirkung an behördlichen oder geheimdienstlichen Tätigkeiten vor. Die Teilnahme an einem kooperativen System wie dem MonIKA-System müsste also entweder für die Nutzung des Dienstes nötig sein oder sich unter einen der Fälle in § 14 Abs. 2 TMG rechnen lassen. In § 15 TMG ist schließlich eine weitere enge Erlaubnis enthalten, die eine Datenverarbeitung erlaubt, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Zu klären ist in Bezug auf die verschiedenen MonIKA-Anwendungs-

[71] *Braun*, BeckTKG-Komm, § 100 TKG, Rn. 11 m. w. N.
[72] BGH NJW 2011, 1509.

szenarien also, ob die jeweiligen Umstände als Dienstleistung im Sinne des TMG einzuordnen ist und welche Rechte aus dem TMG im Einzelfall folgen könnten.

3.1.4.2.1.4 Bundesdatenschutzgesetz vom 14. Januar 2003

Das BDSG ist immer dann anwendbar, wenn keine spezielleren Gesetze eingreifen. Das BSI-Gesetz, das TKG und das TMG gehen ihm vor, soweit dort Regelungen getroffen sind. Aus Sicht der MonIKA-Beteiligten ist ein Rückgriff auf das BDSG also ausgeschlossen, solange der Anwendungsbereich eines spezielleren Gesetzes eröffnet ist. Für Telekommunikations- und Telemedienanbieter nach dem TKG bzw. TMG ist die Anwendbarkeit des BDSG damit also bereits deutlich eingeengt. Grundlegende Regelungen wie die besondere Zweckbindung des § 31 BDSG[73] gelten zwar auch für kooperative Monitoringsysteme. Aber selbst dort, wo der Rückgriff auf das BDSG eröffnet ist, ist die Teilnahme an einem kooperativen Auswertungssystem wie bei MonIKA bisher nicht ausdrücklich erfasst. Den teilnehmenden Unternehmen bliebe daher derzeit nur der Rückgriff auf bestehende Rechtsgrundlagen zur Datenverarbeitung. Da aber die Teilnahme an einem Monitoring-Netz kein Zweck ist, der bisher im BDSG berücksichtigt wurde, wird nur die Nutzung sinnähnlicher oder allgemeiner Rechtsgrundlagen in Betracht kommen.

3.1.4.2.2 Derzeitige Rechtslage in Europa

In europarechtlicher Hinsicht ist die Teilnahme an derartigen Kooperationsnetzen derzeit ebenfalls nicht ausdrücklich erfasst.

3.1.4.2.2.1 Verordnung zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit (460/2004/EG)

Thematisch kommt zunächst die ENISA-Verordnung dem vorliegenden MonIKA-System näher. Diese Verordnung stellt jedoch keine Rechtsgrundlage dar, sondern ist eine reine Aufgabennorm. Mit ihr wurde die Europäische Agentur für Netz- und Informationssicherheit (ENISA) gegründet. Sie hat das Ziel, die Fähigkeit der Europäischen Union zu verbessern, Probleme im Bereich der Netz- und Informationssicherheit zu verhüten, zu bewältigen und zu beheben (Art. 2 Abs. 1) und hat informierende und beratende Aufgaben (Art. 3). Konkrete Regelungen oder gar Ermächtigungen zur Erhebung von personenbezogenen Daten im Bereich des kooperativen Monitorings enthält diese Verordnung nicht.

3.1.4.2.2.2 Richtlinie über den elektronischen Geschäftsverkehr (2000/31/EG)

Die Richtlinie über den elektronischen Geschäftsverkehr beinhaltet einheitliche Regeln u. a. für die Transparenz und Informationspflichten von Online-Service-Providern, für die kommerzielle Kommunikation, für elektronische Verträge und für die Haftungsbegrenzung für Vermittler. Diese Richtlinie drückt in Erwägungsgrund 14 aber deutlich aus, dass die Verarbeitung personenbezogener Daten ausschließlich Gegenstand der Richtlinie 95/46/EG und der Richtlinie 97/66/EG bleiben soll, und trifft darüber selbst keine Aussagen.

3.1.4.2.2.3 Richtlinie über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (2002/21/EG)

Mit dieser Richtlinie wurde ein einheitlicher Telekommunikationsmarkt geschaffen, und die Vergabe von Funkfrequenzen wurde normiert. Sie ersetzt die Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation (97/66/EG). Die Richtlinie 2002/21/EG sieht in Art. 8 Abs. 4 f) zwar vor, dass die nationalen Regulierungsbehörden eine Gewährleistung von Integrität und Sicherheit der öffentlichen Netze sicherstellen. Einige Regelungen des bereits angesprochenen deutschen TKG haben nun auch ihren Ursprung in

[73] Vgl. hierzu Abschnitt 3.1.5.6.

dieser Richtlinie (genauer: Art. 8 Abs. 4 f) der Richtlinie); eine über die Pflicht zur IT-Sicherheit hinausgehende, dem § 100 Abs. 1 TKG vergleichbare Pflicht zur Verarbeitung von Verkehrsdaten zum Schutz der unternehmereigenen Infrastruktur findet sich in der Richtlinie allerdings nicht. Eine Grundlage für die Erhebung personenbezogener Daten zum Zweck der Teilnahme an einem gemeinsamen Monitoring-Netz sieht die Richtlinie dementsprechend nicht vor.

3.1.4.2.2.4 Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (2002/58/EG)

Auf Ebene des EU-Rechts findet sich erst in der Datenschutzrichtlinie für elektronische Kommunikation (E-Privacy-Richtlinie) ein größerer Ansatzpunkt. Diese Richtlinie regelt den Datenschutz in der elektronischen Kommunikation und richtet sich an Telekommunikationsdienstleister. Im Erwägungsgrund 29 dieser Richtlinie wird die Datenverarbeitung zu dem Zweck, technische Versehen oder Fehler bei der Übertragung von Nachrichten zu ermitteln, erwähnt. Allgemein gilt allerdings, dass sich aus Erwägungsgründen selbst keine Rechte und Pflichten ableiten lassen, da sie unverbindlich sind.[74] In den einzelnen Normen der Richtlinie selbst hat sich dieser Erwägungsgrund nicht niedergeschlagen. Darüber hinaus ist der Zweck in dem Erwägungsgrund auch deutlich enger gefasst als im inhaltlich ähnlichen § 100 Abs. 1 TKG. Wo das deutsche TKG allgemeiner auf Störungen oder Fehlern an Telekommunikationsanlagen abstellt, enthält der Erwägungsgrund nur eine sehr spezifische Berufung auf Fehler in der Nachrichtenübertragung.

3.1.4.2.2.5 Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (95/46/EG)

Schließlich bleibt auch auf europäischer Ebene nur der Rückgriff auf die allgemeine Datenschutzrichtlinie. Anders als im deutschen Recht mit den drei „Schichten“ BDSG, TMG und TKG gibt es im EU-Recht neben dieser grundlegenden Richtlinie nur die oben erwähnte Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG), die grundsätzlich nur Telekommunikationsanbieter adressiert. Für Anbieter von sonstigen Diensten der Informationsgesellschaft (Telemediendienste im Sinne des deutschen Rechts) gelten damit die Vorschriften der Datenschutzrichtlinie 95/46/EG. Insoweit bliebe nur die grundsätzliche Möglichkeit, für die Verarbeitung personenbezogener Daten im MonIKA-System auf Art. 7 DSRL zurückzugreifen.

3.1.4.2.3 Aktuelle Rechtsentwicklung in Europa und Deutschland

Neben den soeben dargestellten Regelungen befinden sich derzeit mehrere Gesetzesvorhaben in der Entwicklung, die kooperatives Monitoring jedenfalls in Teilbereichen erfassen.

3.1.4.2.3.1 Vorschlag für eine Richtlinie zur Erhöhung der Netz- und Informationssicherheit in der Union vom 07.02.2013 (2013/0027 (COD))

Der Vorschlag für eine neue Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union[75] (Cybersecurity-Richtlinie) hat das Ziel, einen europaweiten Mindeststandard des Infrastrukturschutzes einzuführen. Erreicht werden soll dieses durch die Einführung einer Meldepflicht an nationale Sicherheitsbehörden, die Errichtung nationaler IT-Notfallteams und ein Kooperationsnetz aller Teilnehmer unter europäischer Führung. Kernelement ist dabei das umfassende Erheben, Abgleichen und Verarbeiten von Daten zur unionsweiten Identifizierung von Gefahren für die Netze und Informationssysteme.

[74] Siehe dazu den Gemeinsamen Leitfaden des Europäischen Parlaments, des Rates und der Kommission für Personen, die in den Gemeinschaftsorganen an der Abfassung von Rechtsakten mitwirken, http://eur-lex.europa.eu/de/techleg/10.htm.
[75] Vorschlag für eine Richtlinie zur Erhöhung der Netz- und Informationssicherheit in der Union vom 07.02.2013 2013/0027 (COD)), im Internet: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1666.

Der Vorschlag enthält damit viele Elemente eines gemeinsamen Monitorings und einer Informationsfusion, wie sie auch im MonIKA-System geplant ist. Der Vorschlag der Richtlinie enthält in seiner jetzigen Form aber keine ausdrückliche Rechtsgrundlage und ist auch im Übrigen bezüglich des Datenschutzes noch sehr vage.[76]

3.1.4.2.3.2 Vorschlag für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

Die Datenschutz-Grundverordnung (DSGVO) wurde am 25.01.2012 durch die Kommission vorgestellt und scheiterte im Sommer 2013 im Europäischen Rat. Ende Oktober 2013 nahm der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres einen Kompromissvorschlag an.[77] Die Datenschutz-Grundverordnung würde alle Rechtsgrundlagen aus der Richtlinie 95/46/EG ersetzen und als Verordnung gemäß Art. 288 S. 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) unmittelbar in allen Mitgliedstaaten gelten. Das BDSG wäre damit ebenfalls unwirksam.

Gegenüber der aktuell geltenden Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (95/46/EG) enthält die DSGVO einige Änderungen, die auch für den Einsatz von verteilten Monitoring-Netzen relevant sind. Insbesondere die dort in den Gesetzestext aufgenommenen Prinzipien der Datensparsamkeit („Data Protection by Design“) und Datenschutz durch Voreinstellungen („Data Protection by Default“). Diese Prinzipien beeinflussen die im MonIKA-System stattfindenden Datenübertragungen erheblich. Zudem soll die Verordnung ohne nationale Umsetzungsgesetze europaweit gelten und damit europaweit ein gleichmäßiges Schutzniveau gewährleisten, was den europaweiten Einsatz eines grenzüberschreitenden MonIKA-System betrifft. Eine ausgesprochene Erwähnung finden verteilte Auswertungsnetze auch in der DSGVO allerdings nicht. Die beim MonIKA-System nötigen Datenverarbeitungen würden sich nach den allgemeinen Artikeln in Art. 6 DSGVO richten.

3.1.4.2.3.3 Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vom 05.03.2013

Das Bundesministerium des Innern hat im März 2013 den Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) veröffentlicht, welches in weiten Teilen Inhalte der oben genannten Cybersecurity-Richtlinie vorwegnimmt und eine Umsetzung dieser darstellt. Es sieht im Wesentlichen Änderungen des BSI-Gesetzes dahingehend vor, dass das Bundesamt für Sicherheit in der Informationstechnik zur zentralen Meldestelle für Sicherheitsvorfälle bei Betreibern kritischer Infrastrukturen in Deutschland wird. Zusätzlich regelt es eine eigene Kompetenz des BSI zur Sammlung und Auswertung derjenigen Informationen, die zur Abwehr von Gefahren für die IT-Sicherheit notwendig sind. Zwar liest sich der geplante neue § 8b BSIG – ähnlich wie die Richtlinie über die Errichtung der ENISA – eher wie eine Aufgabenbeschreibung denn eine Rechtsgrundlage zur Datenerhebung. Fernab der Frage nach der Rechtsgrundlage für das BSI ist aber in jedem Fall kritisch, dass es im geplanten BSI-Gesetz an einer Rechtsgrundlage für die Erhebung und Weitergabe der Daten bei den meldepflichtigen Unternehmen und Behörden fehlt.

Für den MonIKA-Ansatz ergeben sich aus dem geplanten Entwurf Auswirkungen auf den Einsatz in Monitoring-Netzen, die durch das BSI betrieben würden.[78]

[76] Vgl. hierzu Abschnitt 5.4.
[77] Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments: Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Plenarsitzungsdokument, A7-0402/2013, 21.11.2013.
[78] Vgl. hierzu Abschnitt 5.3.

3.1.4.2.4 Die konkrete Rechtsgrundlage

Als Rechtsquellen kommen damit nationale sowie europäische Regelungen in Betracht.

3.1.4.2.4.1 § 100 TKG

In der Darstellung der rechtlichen Rahmenbedingungen wurde bereits das deutsche Telekommunikationsgesetz angesprochen. Die dort in § 100 Abs. 1 TKG enthaltene, für das MonIKA-System relevante Rechtsgrundlage lautet:

> *„Soweit erforderlich, darf der Diensteanbieter zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden."*

Der dort festgelegte Zweck passt zunächst durchaus auf den MonIKA-Sachverhalt. Genauso wie die Anbieter von Telekommunikationsdienstleistungen Störungen und Fehler in ihren Anlagen abwehren wollen, erhoffen sich die Teilnehmer am MonIKA-System die Abwehr von Störungen an der IT ihrer Unternehmen. Damit diese Rechtsgrundlage aber auf die Teilnehmer im MonIKA-System anwendbar ist, müssen mehrere Voraussetzungen erfüllt sein.

Zum einen müsste das TKG überhaupt anwendbar sein, die Teilnehmer müssten also unter den Anwendungsbereich des § 92 TKG fallen. Zum anderen müsste die Rechtsfolge des § 100 Abs. 1 TKG auch die Datenverarbeitung im MonIKA-System decken.

Die MonIKA-Teilnehmer als Telekommunikationsanbieter

Der gesamte Teil 7 Abschnitt 2 des TKG ist gemäß § 91 Abs. 1 TKG anwendbar auf

> *„Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste in Telekommunikationsnetzen, einschließlich Telekommunikationsnetzen, die Datenerfassungs- und Identifizierungsgeräte unterstützen, erbringen oder an deren Erbringung mitwirken"*.

Diese Definition passt zunächst problemlos auf solche Teilnehmer in einem Monitoring-Netz, die klassische Telekommunikationsdienstleister sind, also insbesondere E-Mail-Provider und Internet-Provider. In den Anwendungsfällen des Botnetz-Monitorings und beim BGB-Routing sind also Beteiligte sehr wahrscheinlich, die in den Anwendungsbereich der § 91 ff. TKG fallen.

Für alle Beteiligten, die diese Voraussetzungen nicht erfüllen, eröffnet das TKG keine Rechtsgrundlage. Wenn also in den Szenarien Private oder fremde Dienstleister wie Sicherheitsunternehmen Daten erheben und zuliefern wollen, so fallen diese aus dem Bereich des TKG heraus.

Einen Sonderfall stellen Unternehmen dar, die zwar nicht primär geschäftsmäßig Telekommunikationsdienstleistungen erbringen, aber doch zumindest gegenüber ihren Mitarbeitern für deren Aufgabenerfüllung Internet-Zugänge oder E-Mail-Dienste vorhalten. Dabei herrscht in der juristischen Literatur[79] nämlich weitgehende Einigkeit darüber, dass bereits dann,

> *„wenn Mitarbeiter mit der betriebs- bzw. behördeneigenen Telekommunikationsanlage Privatgespräche führen dürfen, […] ein geschäftsmäßiges Angebot von Telekommunikationsdiensten [vorliegt]"*.

In diesen Fällen finden dann auch die Regelungen in Abschnitt 2 und damit auch § 100 TKG Anwendung. Diesbezüglich würde § 100 TKG die Vorschriften des BDSG verdrängen. Sollte die private Nutzung erlaubt sein, ist zu beachten, dass nach § 87 Abs. 1 Nr. 6 BetrVG der Betriebsrat, soweit eine gesetzliche oder tarifliche Regelung nicht besteht, bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, ein Mitbestimmungsrecht hat. Da die Logs der Internet-Kommunikation nicht allein

[79] Siehe *Braun*, in: BeckTKG-Komm, § 91, Rn. 12.

zur Analyse auf Bedrohungen für die IT-Infrastruktur verwertbar sind, sondern auch über das Nutzungsverhalten der Mitarbeiter Aufschluss geben können, unterfällt das Logging von Mitarbeiteranschlüssen regelmäßig dem Mitbestimmungsrecht des Betriebsverfassungsgesetzes (BetrVG).[80]

Die Reichweite des § 100 Abs. 1 TKG

Sollte die private Nutzung des Internets betrieblich zugelassen werden oder nehmen Telekommunikationsdienstleister am MonIKA-System teil, so stellt sich nun die viel wichtigere Frage, welche Reichweite der § 100 Abs. 1 TKG tatsächlich hat.

Seinem Wortlaut nach gestattet er eine Datenverarbeitung *„zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen“*. Die Einzelheiten dieser Rechtsgrundlage sind dabei jedoch höchst umstritten. Umstritten sind insbesondere die Fragen, ob auch verdachtsunabhängig Daten erhoben und gespeichert werden dürfen, wie lange diese Daten gespeichert werden dürfen, welche Art von Auffälligkeiten unter den Begriff der „Störung“ fallen und zu welchem Zweck die derart erlangten Daten zusätzlich verwendet werden dürfen.

In der Rechtsprechung[81] hat sich mittlerweile die allgemeine Ansicht durchgesetzt, dass § 100 Abs. 1 TKG auch eine verdachtsunabhängige Vorratsspeicherung der Verkehrsdaten, insbesondere der IP-Adressen, abdeckt. Der BGH erklärte etwa in seinem Urteil zur Speicherung dynamischer IP-Adressen[82], den Störungsbegriff des § 100 TKG im Sinne jeder Beeinträchtigung des Kommunikationsnetzes zu verstehen, und hielt die Datenerhebung und 7-Tage-Speicherung, um derartigen Bedrohungen zu begegnen, für rechtmäßig. Im Ergebnis werden deshalb auch der Betrieb von Botnetzen und der Versand von Spam-E-Mail als Störungen angesehen, obwohl diese die Funktionsfähigkeit der Anlagen selbst nicht betreffen, sondern nur das Netz insgesamt belasten. Auf den MonIKA-Ansatz angewandt, folgt daraus, dass die Unternehmen für solche Daten, die als Verkehrsdaten ihrer Telekommunikationsdienste oder Verkehrsdaten ihrer Mitarbeiter anzusehen sind, eine 7-Tage-Speicherung der Daten vornehmen dürfen und diese Daten nicht bloß zum „Schutz der Anlagen“, sondern auch zur allgemeinen Verhinderung von ungewolltem Netzverkehr nutzen dürfen.

Nach verbreiteter Ansicht in der juristischen Literatur werden als „Störung oder Fehler“ hingegen nur solche Beeinträchtigungen verstanden, die sich auf die Übertragung der Nachrichten auswirken.[83] Die Nutzung der Netze zum Versand von Spam-E-Mails oder zur Unterhaltung von Botnetzen stört die Übertragung selbst nicht, sondern stellt schlicht eine ungewollte Übertragung dar. Damit wäre der § 100 Abs. 1 TKG in den meisten Anwendungsszenarien keine Grundlage, da das Ziel des MonIKA-Systems nicht der Schutz von technischen Anlagen, sondern der Schutz des Vorgangs der Datenverarbeitung ist. Zudem umfasst der § 100 TKG nach seiner jetzigen Konzeption auch nur den Schutz eigener Netze, nicht jedoch den Schutz fremder Netze. Das MonIKA-System beabsichtigt aber den Schutz einer weitergehenden Infrastruktur unabhängig davon, wo potentielle Angriffe sich tatsächlich auswirken. Auch der BGH legt den § 100 Abs. 1 TKG bisher nur derart aus, dass die Daten zur Verwendung für die Abwehr von Bedrohungen gegen das eigene Netz und eigene Anlagen verarbeitet werden. Für die Weiterleitung eigener Daten an zentrale Dienstleister zur koordinierten Gefahrenerkennung oder zur Bekämpfung von Bedrohungen fremder Netze finden sich in § 100 Abs. 1 TKG bisher keine Anhaltspunkte.

Im Ergebnis ist damit selbst unter Zugrundelegung der weniger datenschutzfreundlichen Ansicht der Rechtsprechung der § 100 Abs. 1 TKG im koordinierten Monitoring keine taugliche Rechtsgrundlage. Zwar mag mit der Rechtsprechung das Überwachen der Unternehmensnetze oder die Erkennung von Spam-E-Mail abgedeckt sein; die Nutzung dieser Daten für ein kooperatives

[80] Siehe z. B. Beschluss des ArbG Hamburg vom 07.11.2012, 27 BVGa 3/12, veröffentlicht bei juris.
[81] Vgl. OLG Frankfurt am Main, Urteil vom 16.06.2010 - Az. 13 U 105/07, m. w. N.
[82] BGH NJW 2011, 1509.
[83] *Braun*, BeckTKG-Komm, § 100 TKG, Rn. 11 m. w. N.

Auswertungs- und Fusionssystem wie im MonIKA-Kontext wird aber nur schwer unter § 100 Abs. 1 TKG zu subsumieren sein.

3.1.4.2.4.2 § 109 TKG

In § 109 Abs. 2 TKG wird daneben die Pflicht festgelegt,

> *„erforderliche technische Vorkehrungen und sonstige Maßnahmen zu treffen*
>
> *1. zum Schutz des Fernmeldegeheimnisses und*
> *2. gegen die Verletzung des Schutzes personenbezogener Daten."*

Zu diesen technischen Maßnahmen wird man aber nicht die Verarbeitung persönlicher Daten zählen können. Das folgt aus § 96 Abs. 1 S. 2 TKG, der klarstellt, dass eine Datenverarbeitung nur zu solchen Zwecken gestattet ist, die § 96 Abs. 1 S. 1 TKG ausdrücklich vorsieht oder durch andere gesetzliche Vorschriften gestattet sind. Zu diesen anderen Vorschriften zählt etwa auch der soeben dargestellte § 100 TKG, nicht jedoch § 109 TKG.[84] In § 109 Abs. 2 TKG ist nämlich gerade keine Datenverarbeitung, sondern nur technischer IT-Schutz vorgesehen.

Die Norm stellt keine Ermächtigungsgrundlage zur Verarbeitung neuer personenbezogener Daten dar, sondern ist eine Verpflichtung zum Schutz bestehender Daten. Die Norm würde ansonsten das sinnwidrige Ergebnis haben, dass personenbezogene Daten durch Erhebung neuer Daten geschützt werden sollen, deren Schutz abermals die Erhebung neuer Daten verlangt. So weist auch *Breyer*[85] zu Recht darauf hin, dass selbst der BGH nicht von einer Pflicht zur Vorratsdatenspeicherung der Provider ausgeht, was aber notwendige Folge der Norm wäre, wenn man das Loggen von E-Mail- oder Netzverkehr als eine Maßnahme ansehen würde, die von § 109 TKG erfasst wird.

Interessant ist im Rahmen des § 109 TKG allerdings die Pflicht zu Berücksichtigung des „Stands der Technik". Dieses mit der TKG-Novelle 2012 neu in § 109 Abs. 1 S. 2 TKG eingeführte Erfordernis soll bezwecken, dass die Verpflichteten ihre Vorkehrungen ständig an die gängigen Standards anpassen. Interessant ist dies insoweit, als dass die Teilnahme an koordinierten Monitoring-Netzen eine zunehmende Verbreitung findet. Allerdings enthält § 109 Abs. 1 S. 2 TKG keinen Verweis auf den Stand der Wissenschaft, so dass noch nicht in der Praxis umgesetzte Verfahren nicht berücksichtigt werden müssen.[86] Zudem muss der Stand der Technik auch lediglich „berücksichtigt", nicht aber umgesetzt werden.[87] Insgesamt wird sich aus § 109 TKG derzeit also keine Verpflichtung zur Umsetzung von Systemen wie MonIKA ableiten lassen.

3.1.4.2.4.3 §§ 14 und 15 TMG

Wie dargestellt wurde, enthält auch das Telemediengesetz Ermächtigungsgrundlagen für die Erhebung von personenbezogenen Daten. Das TMG entfaltet allerdings nur Wirkung für Anbieter von elektronischen Informations- und Kommunikationsdiensten, die das TMG selbst in § 1 Abs. 1 TMG negativ abgrenzt als solche Dienste, die

> *„nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind (Telemedien)"*.

[84] Vgl. *Eckhardt*, in: BeckTKG-Komm, § 109, Rn. 9.
[85] *Breyer*, in: (Un-)Zulässigkeit einer anlasslosen, siebentägigen Vorratsdatenspeicherung – Grenzen des Rechts auf Anonymität MMR 2011, S. 573.
[86] Vgl. *Eckhardt*, in: BeckTKG-Komm, § 109, Rn. 31.
[87] *Eckhardt*, in: BeckTKG-Komm, § 109, Rn. 31.

Der klassische Webauftritt etwa eines Unternehmens, wie er für viele der MonIKA-Teilnehmer im Normalfall vorhanden sein wird, stellt unbestritten ein Telemedium im Sinne des TMG dar.[88] Dazu zählen die Aspekte der Unternehmenspräsentation durch Bild, Text und Video und die Eröffnung von Kontaktmöglichkeit via Kontaktformular. All diese Angebote stellen im Regelfall keine reine Übertragung von Telekommunikationssignalen dar, und sie sind auch nicht als Rundfunk einzuordnen. Das TMG erlaubt nun in § 14 Abs. 1 TMG,

> *„personenbezogene Daten eines Nutzers nur [zu] erheben und verwenden, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind (Bestandsdaten)“*.

Von den bisher im Rahmen des MonIKA-Projekts untersuchten Anwendungsszenarien trifft das TMG am ehesten auf das Enterprise-Monitoring zu, wo beispielsweise verhindert werden soll, dass Unbefugte auf geschützte Bereiche des Firmennetzes zugreifen. In solchen Fällen setzt die Rechtsgrundlage des § 14 Abs. 1 TMG voraus, dass die Nutzung des Telemediums, hier der Website des Teilnehmers am MonIKA-System, Gegenstand eines Vertragsverhältnisses ist. Dies ist bezüglich des Verhältnisses zwischen den Unternehmen und dem Besucher der Website aber nur höchst selten der Fall, so dass § 14 Abs. 1 TMG insoweit keine Rechtsgrundlage für die Datenverarbeitung auf Basis der Logfiles darstellt. Darüber hinaus sind die in solchen Fällen relevanten Daten, etwa Zugriffszeitpunkte und IP-Adresse auch keine Bestandsdaten, sondern Nutzungsdaten.[89]

Deshalb spielt insoweit auch eher § 15 TMG eine Rolle, wonach der

> *„Diensteanbieter […] personenbezogene Daten eines Nutzers nur erheben und verwenden [darf], soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten). Nutzungsdaten sind insbesondere*
>
> 1. *Merkmale zur Identifikation des Nutzers,*
> 2. *Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und*
> 3. *Angaben über die vom Nutzer in Anspruch genommenen Telemedien“*.

Der Betreiber der Website wird damit grundsätzlich ermächtigt, beispielsweise die IP-Adresse und die Zugriffszeitpunkte der Besucher zu speichern, sofern dies erforderlich ist, um dem Besucher den Besuch der Website zu ermöglichen. Dies ist bezüglich der IP-Adresse regelmäßig der Fall, da ohne diese die Verbindung zwischen dem Rechner des Besuchers und dem Servers des Website-Hosters nicht hergestellt werden kann. Allerdings erlaubt § 15 Abs. 1 TMG nur die Verarbeitung insoweit und vor allem so lange, wie dies zu Ermöglichung der Nutzung nötig ist. Damit unterfällt eine weitergehende Verarbeitung zu Zwecken der IT-Sicherheit nicht dem TMG. Das Loggen von Besucherdaten, um Angriffe auf den Server oder – im Fall des MonIKA-Systems – auf die IT-Infrastruktur im Übrigen aufzudecken, steht in keinem Bezug dazu, den Besuch der Website zu ermöglichen. Die zu diesem Zweck aufgezeichneten Daten dürfen auch nicht zu diesen Zwecken zweitverwendet werden, da nach Ende der Nutzung diese Daten zu löschen sind, sofern sie nicht für Abrechnungszwecke benötigt werden. Dies folgt im Umkehrschluss daraus, dass nur Abrechnungsdaten gemäß § 15 Abs. 4 S. 1 TMG über das Ende des Nutzungsvorgangs hinaus verwendet werden dürfen.[90]

In vielen Fällen wird es sich nicht um die öffentliche Webpräsenz der Unternehmen handeln. Die für die Unternehmen sensiblen Systeme sind auch nicht in jedem Fall als Telemediendienste zu qualifizieren. So werden zwar geschlossene Intranets, wie etwa universitäre Netze, regelmäßig aufgrund ihrer weitgehend unbestimmten Nutzerbasis noch als Telemediendienste angesehen. Innerbetriebliche Kommunikationsnetze, wie etwa Verwaltungs- und Managementdatenbanken, sind

[88] *Heckmann*, in: jurisPK-Internetrecht, Kapitel 1.1, Rn. 54.
[89] *Heckmann*, in: jurisPK-Internetrecht, Kapitel 1.15, Rn. 8.
[90] So auch: *Heckmann*, in: jurisPK-Internetrecht, Kapitel 1.15, Rn. 14 f.

hingegen aufgrund ihrer Abgeschlossenheit regelmäßig keine Telemediendienste.[91] Die weitere Einstufung hängt danach aber von der Ausgestaltung des internen Netzes ab.

Insgesamt ist das TMG in seinen datenschutzrechtlichen Ermächtigungsgrundlagen nicht auf die Teilnahme an einem Monitoring-Netz angelegt. Aspekte der IT-Sicherheit finden sich eher im TKG oder in allgemeinerem Gewand im Bundesdatenschutzgesetz.

3.1.4.2.4.4 § 28 BDSG

Im BDSG stellt § 28 BDSG die zentrale Ermächtigungsgrundlage für Datenverarbeitungen von nicht-öffentlichen Stellen dar. Sie umfasst eine Reihe von Einzelermächtigungen.

Subsidiarität des BDSG

Bereits im Kontext des rechtlichen Hintergrundes wurde die Subsidiarität des BDSG angesprochen. Überall dort, wo TKG und TMG bestimmte Sachverhalte bereits durch eigene Normen erfassen, ist die Anwendbarkeit des BDSG gesperrt. Die Verdrängung gilt aber nicht für das gesamte BDSG, sondern nur für die Fälle, für die die Sondergesetze eigene Regelungen treffen. In allen Bereichen, wie etwa der Auftragsdatenverarbeitung oder der Definition der personenbezogenen Daten, über die das TKG und das TMG keine Aussagen treffen, bleibt das BDSG anwendbar. Die Ermächtigungsgrundlagen des § 28 BDSG regeln in Teilbereichen Sachverhalte, die auch vom TKG und TMG erfasst werden. Dort ist der Rückgriff ausgeschlossen für alle MonIKA-Teilnehmer, für die diese Spezialregelungen gelten.

§ 28 Abs. 1 Satz 1 Nr. 1 BDSG

Zunächst erlaubt § 28 Abs. 1 S. 1 Nr. 1 BDSG die Datenverarbeitung,

> *„wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist“.*

Dieser Zweck ist jedoch äußert eng an die Erbringung der vertraglichen Leistung geknüpft. Nur solche Datenverarbeitungen, die in einem „unmittelbaren sachlichen Zusammenhang“ mit dem Zweck des Schuldverhältnisses stehen, sind zulässig.[92] Datenverarbeitungen, die lediglich die Durchführung des Vertrags erleichtern, werden nicht erfasst.[93] Es könnte zwar argumentiert werden, dass die Verarbeitung der Logdaten und die Teilnahme an einem kooperativen Monitoring-Netz die Unternehmen allgemein vor Schaden bewahrt, damit ihre eigene Leistungsfähigkeit erhält und so in einem sehr weiten Sinne auch dabei hilft, ihre vertraglichen Pflichten gegenüber ihren Kunden zu erfüllen. Bezüglich der MonIKA-Anwendungsszenarien ist es in diesem Sinne sicherlich nicht zu leugnen, dass ein Vertrag über die Anbietung von E-Mail-Diensten oder generell Internet-Zugang gegenüber den einzelnen Kunden nur möglich ist, wenn die Netze des Providers überhaupt funktionieren. Genauso kann ein Unternehmen aus dem fertigenden Gewerbe nur dann an seine Kunden liefern, wenn die IT der Fertigungsprozesse funktioniert. Allerdings verlangt § 28 Abs. 1 S. 1 Nr. 1 BDSG eben einen konkreten Bezug zu den einzelnen Leistungen. Gefordert wird, dass die Erfüllung der Leistungspflicht ohne Kenntnis der Daten unmöglich wird.[94] Allerdings dürfte dies in den allermeisten Fällen den Regelungsbereich des § 28 Abs. 1 S. 1 Nr. 1 BDSG klar überdehnen, weil ein Bezug zu konkreten Leistungspflichten aus dem Schuldverhältnis fehlt. *Simitis*[95] weist hier darauf hin, dass ein Verweis auf so allgemeine vertragsimmanente Zwecke wie die grundsätzliche Funktionsfähigkeit des Unternehmens letztlich bewirken würde, dass die Verantwortlichen die

[91] *Heckmann*, in: jurisPK-Internetrecht, Kapitel 1.2, Rn. 7. m. w. N.
[92] *Simitis*, in: Simitis, BDSG, § 28, Rn. 57.
[93] *Wedde*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 28, Rn. 15.
[94] Kühling/Seidel/Sivridis, Datenschutzrecht, S. 142.
[95] *Simitis*, in: Simitis, BDSG, § 28, Rn. 105.

Verwendung der Daten selbst bestimmen könnten. Den E-Mail-Verkehr seiner Kunden auf Bedrohung für die Netze hin auszuwerten, mag insgesamt im Interesse der Unternehmen sein. Für die eigentliche vertragliche Verpflichtung, E-Mails zuzustellen, ist an Daten aber bis auf die E-Mail-Adresse des Kunden konkret nichts erforderlich. Dies ist nur dann anders, wenn die vertraglich zugesicherte Leistung nicht nur die Zustellung von E-Mails ist, sondern wenn auch darüber hinausgehende Dienstleistungen wie beispielsweise Spam-Erkennung geschuldet werden. Die Abwehr von Spam ist ohne gewisse Kenntnis des Inhalts tatsächlich nicht möglich oder, etwa bei Filterung rein aufgrund der Absenderadresse, höchst fehleranfällig.

In solchen Fällen, in denen gewissermaßen Aspekte der IT-Sicherheit Gegenstand der vertraglichen Beziehungen sind, kann also § 28 Abs. 1 S. 1 Nr. 1 BDSG durchaus eine Ermächtigungsgrundlage sein, wenn die Daten zur Erfüllung der konkreten Leistungspflichten nötig sind.[96] Im Bereich der Erkennung von BGB-Routing-Anomalien und insbesondere auch im Bereich des Enterprise-Monitorings bestehen aber entweder überhaupt keine vertraglichen Beziehungen zwischen den Betroffenen und den Verantwortlichen, oder diese Beziehungen beziehen sich auf Aspekte fernab der IT-Sicherheit.

Damit ist die Anwendung des § 28 Abs. 1 S. 1 Nr. 1 BDSG lediglich im Bereich der Spam-Erkennung zur Bekämpfung von Botnetzen denkbar. Hier stellen sich anschließend aber drei Fragen: Erstens ist die Frage der Erforderlichkeit zu klären, zweitens ist gegenüber der in solchen Situationen ebenfalls denkbaren Einwilligung abzugrenzen, und drittens muss der Umgang mit Daten Dritter untersucht werden.

Hinsichtlich der Erforderlichkeit reicht das Niveau an Durchdringung der E-Mail von oberflächlicher Auswertung der Absender- oder Betreffdaten bis hin zur Auswertung des Inhalts und aller Metadaten im Rahmen von „Deep Packet Inspection“. Die Grenzen der Erforderlichkeit sind dabei allgemein bereits von der Artikel-29-Datenschutzgruppe in der Stellungnahme WP 118 umrissen worden.[97] Dabei ist zunächst die Erkenntnis, dass auch elektronische Nachrichten, also E-Mails, unter das durch Art. 8 Abs. 1 ERMK geschützte Recht auf Achtung des Privat- und Familienlebens fallen[98], kaum bestreitbar. Die Artikel-29-Datenschutzgruppe gibt bezüglich der Filterung auf Spam einige Empfehlungen.[99] So soll der Nutzer stets die Möglichkeit behalten, als Spam erkannte E-Mails manuell zu sortieren oder gar komplett eigene Filter zu erstellen. Daneben mahnt sie, dass stets über die Filterung informiert werden müsse und dass Vertraulichkeit und Zweckbindung der gescannten Daten gewährleistet bleiben müssen. Die Artikel-29-Datenschutzgruppe

> *„befürwortet ferner die Suche nach anderen, möglicherweise weniger stark in die Privatsphäre eingreifenden Instrumenten zur Bekämpfung von Spam“.*

Damit triff die Artikel-29-Datenschutzgruppe den Kern der Erforderlichkeit. Für die Spam-Erkennung muss stets das mildeste, gleich geeignete Mittel gewählt werden, das die Erkennung von Spam erlaubt.[100] Technisch ist die Überprüfung aller Daten im OSI-Schichtenmodell möglich, von der bloßen Adressauswertung bis zur Auswertung der Nutzerdaten auf der siebten Ebene.[101] Da eine effektive Spam-Erkennung ohne Auswertung des Nachrichteninhalts auf die bloße Listung bestimmter IP-Adressen hinausläuft, ist die Auswertung des Nachrichteninhalts kaum zu umgehen. Hier ist vielmehr die konkrete Verfahrensgestaltung gefragt, die gewährleisten muss, dass die Privatsphäre der Nutzer gewahrt bleibt und Nachrichteninhalte nicht zweckentfremdet werden. Denkbar ist hier etwa die in

[96] So auch die Artikel-29-Datenschutzgruppe, in: Stellungnahme 2/2006 zu Datenschutzfragen bei Filterdiensten für elektronische Post, 00451/06/DE WP 118, Seite 6, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp118_de.pdf.
[97] Stellungnahme 2/2006 zu Datenschutzfragen bei Filterdiensten für elektronische Post, 00451/06/DE WP 118.
[98] Stellungnahme 2/2006 zu Datenschutzfragen bei Filterdiensten für elektronische Post, 00451/06/DE WP 118, S. 3.
[99] Stellungnahme 2/2006 zu Datenschutzfragen bei Filterdiensten für elektronische Post, 00451/06/DE WP 118, S. 8.
[100] Vgl. *Plath*, in: Plath, BDSG Kommentar, § 28, Rn. 19 ff.
[101] *Bedner*, Rechtmäßigkeit der “Deep Packet Inspection”, S. 6 und 7, http://kobra.bibliothek.uni-kassel.de/bitstream/urn:nbn:de:hebis:34-2009113031192/5/BednerDeepPacketInspection.pdf.

Abschnitt 2.2.3.2 beschriebene, auf Hashwerten basierende Analyse nach Ähnlichkeit hinsichtlich Wortanzahl, Zeichenanzahl und allgemeinen Texteigenschaften, die auf Spam-Muster untersuchen kann, ohne notwendigerweise den Klartext der E-Mail verarbeiten zu müssen.

Da in den Fällen des § 28 Abs. 1 S. 1 Nr. 1 BDSG stets ein gewisses Maß an vertraglichen Beziehungen zwischen dem Betroffenen und der verantwortlichen Stelle besteht, ist eine rechtliche Nähe zur Einwilligung gegeben. Ist die Gewährleistung eines bestimmten Niveaus an IT-Sicherheit und E-Mail-Filterung Teil des Vertrags zwischen E-Mail-Nutzer und -Provider, so lässt sich leicht argumentieren, dass in solchen Fällen eine Einwilligung in die Verarbeitung der Daten der E-Mails vorliegen könne. Dagegen sprechen zunächst die ausführlich dargestellten hohen Anforderungen an eine Einwilligung. Insbesondere die Schriftform ist bei den allermeisten E-Mail-Provider-Diensten nicht eingehalten. Daneben setzt die Einwilligung auch ein sehr konkretes Maß an Informiertheit hinsichtlich Art und Ausmaß der verarbeiteten Daten voraus, während § 28 Abs. 1 S. 1 Nr. 1 BDSG die Datenverarbeitung als

> *„Hilfsmittel bei der Verwirklichung bestimmter für die verantwortliche Stelle wichtiger Zwecke“*[102]

spezifiziert. Die Abgrenzung erfolgt also auch auf einer Wertungsebene zwischen Kernelement der Einwilligung und Nebenerfolg des Hauptziels der Vertragserfüllung. Kernelement der Provider-Verträge ist aber nicht Spam-Filterung, sondern reibungsloser E-Mail-Verkehr.

Schließlich wird sich nicht vermeiden lassen, dass die Filterung der E-Mails auch Daten Dritter betrifft, also solcher Beteiligten, die weder E-Mail-Provider noch Kunde sind. Regelmäßig wird dies der Empfänger oder Sender der E-Mail sein, die an oder von dem Kunden des Providers versandt wird. Grundsätzlich wird diese Notwendigkeit in der datenschutzrechtlichen Literatur akzeptiert, solange die Zweckerfüllung ohne Bezug zu den Daten unmöglich ist, was für Spam-Filterung grundsätzlich nicht zu bestreiten ist.[103] Allerdings ist auch insoweit eine strenge Zweckbindung notwendig, und es sind solche technischen Verfahren zu wählen, die die Privatsphäre der Unbeteiligten nur im Nötigsten betreffen. Eine weitergehende Auswertung der Inhalte der E-Mails etwa hinsichtlich werberelevanter Profile ist klar zu verhindern.

Insgesamt ist § 28 Abs. 1 S. 1 Nr. 1 BDSG damit jedenfalls im Bereich Botnetz-Abwehr für kooperative Monitoring-Systeme eine denkbare Ermächtigungsgrundlage für die Auswertung der E-Mails.

§ 28 Abs. 1 Satz 1 Nr. 2 BDSG

Als nächste Ermächtigungsgrundlage wird in § 28 Abs. 1 S. 1 Nr. 2 BDSG eine Datenverarbeitung gestattet,

> *„soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.“*

Im Sinne dieser gemeinhin als Generalklausel des Datenschutzrechts bezeichneten Ermächtigungsgrundlage sind berechtigte Interessen jedoch nur „eigene Belange“ der verantwortlichen Stelle, und „weder die Interessen Dritter noch öffentliche Belange rechtfertigen“ eine Datenverarbeitung nach dieser Norm.[104] Das führt zu der Frage, wie die Teilnahme an kooperativen Sicherheitsnetzen einzuordnen ist. Wie bereits angesprochen, dient die Teilnahme am MonIKA-System mehreren Zwecken. In erster Linie wird die Stärkung der eigenen Infrastruktur und Abwehr von Cyberangriffen gegen die eigene IT-Sicherheit angestrebt. Dieses Interesse stünde also nicht im Widerspruch zu der gerade genannten Auslegung des § 28 Abs. 1 S. 1 Nr. 2 BDSG, da insoweit auf eigene, nicht auf

[102] *Simitis*, in: Simitis, BDSG, § 28, Rn. 30.
[103] *Simitis*, in: Simitis, BDSG, § 28, Rn. 62.
[104] *Simitis*, in: Simitis, BDSG, § 28, Rn. 105.

fremde Belange abgestellt wird. Darüber hinaus ist notwendige Folge aber auch, dass die gewonnenen Daten nicht in jedem Fall Anomalien aufdecken, die eigene Systeme betreffen, sondern gegebenenfalls nur die zentrale Stelle dabei unterstützen, Anomalien in Bezug auf andere Teilnehmer des Kooperationsnetzes aufzudecken. In einem letzten Gedankenschritt muss darauf aufbauend dann die Frage gestellt werden, ob diese unmittelbare Verwendung zum Schutz anderer Teilnehmer nicht in mittelbarer Hinsicht doch wieder dem Selbstschutz dient. Schließlich dient die Teilnahme an dem Kooperationsnetz ja insgesamt dem Ziel, alle Beteiligten und damit auch das eigene Unternehmen zu schützen. Ob dies in jedem Einzelfall darüber erfolgt, dass unmittelbar Auswirkungen auf das eigene Netz begegnet wird oder dieser Effekt nur mittelbar über den Schutz des Verbunds der Teilnehmer erfolgt, mag als künstliche Differenzierung kritisiert werden. Die datenschutzrechtliche Literatur ist zu dem Begriff des „berechtigten Interesses“ wenig aussagekräftig.

So stellt etwa *Kühling*[105] schlicht fest:

> *„Der Begriff ist also so weit zu verstehen, dass sich ein entsprechendes Interesse der verantwortlichen Stelle in aller Regel ohne Weiteres finden lässt“*

und scheint damit die Ansicht zu unterstützen, dass ein nur mittelbares Eigeninteresse, wie es beim MonIKA-Ansatz oft vorhanden sein wird, einem berechtigten Interesse nicht entgegensteht. Auch *Simitis*, der, wie oben bereits zitiert[106], ausdrücklich darauf verweist, dass es sich nur um eigene Belange handeln kann, führt im Verlauf seiner Kommentierung[107] aber aus, dass die Regelung

> *„der verantwortlichen Stelle helfen soll, ihre Aufgaben zu verwirklichen“,*

und sieht den Bereich der „eigenen Belange“ nur dann verlassen, wenn die Datenverarbeitung ohne Selbstbezug ausschließlich abstrakten Drittinteressen dient.[108] Auch *Simitis* scheint daher nicht streng zwischen mittelbaren und unmittelbaren Eigeninteressen zu differenzieren und akzeptiert Interessen so lange als berechtigt, wie sie sich konkret in der Unterstützung der eigenen Aufgabenerfüllung niederschlagen. Dies dürfte bei der Teilnahme an einem kooperativen Sicherheitsnetz wie dem MonIKA-System nicht zu bestreiten sein. Eindeutiger formuliert es schließlich *Plath*[109], der zu Recht den Vergleich zu datenverarbeitenden Steuerberatern und Anwälten zieht. Auch dort, so *Plath*, stellt das Interesse der Mandanten ein mittelbares Eigeninteresse der Anwälte und Steuerberater dar. Wo diese Berufsgruppen also aufgrund ihrer Kernaufgaben die Interessen Dritter mitfördern, weil dies notwendigerweise aus der beratenden Tätigkeit folgt, ist die Förderung der Drittinteressen in kooperativen Sicherheitsnetzen weit weniger dominant und dürfte damit ebenso wenig der Einordnung als „eigene Interessen“ entgegenstehen. Im Ergebnis sprechen damit die besseren Gründe dafür, dass auch die mittelbare Förderung von Interessen Dritter als notwendiges Nebenprodukt der Datenverarbeitung als eigenes Interesse gewertet werden muss, sofern das Endziel immer die unmittelbare Förderung konkreter Eigeninteressen ist.

Akzeptiert man diese Einordnung, stellt § 28 Abs. 1 S. 1 Nr. 2 BDSG grundsätzlich eine Rechtsgrundlage für die Teilnehmer des MonIKA-Netzes zur Erhebung der Daten dar. Bedingung dafür, dass diese Datenerhebung auch als rechtmäßig anzusehen ist, ist im Schwerpunkt die in § 28 Abs. 1 S. 1 Nr. 2 BDSG verlangte Interessenabwägung. Während § 28 Abs. 1 S. 1 Nr. 1 BDSG die Erforderlichkeit ausreichen lässt, also bereits dann die Datenverarbeitung rechtfertigt, wenn kein milderes Mittel zur Erreichung des Vertragsziels besteht, verlangt § 28 Abs. 1 S. 1 Nr. 2 BDSG, dass die Interessen der Betroffenen die berechtigten Interessen der verantwortlichen Stellen nicht überwiegen.

Dass die Teilnahme an koordinierten Monitoring-Netzen zur Stärkung der eigenen IT-Sicherheit ein berechtigtes Interesse darstellt, ist ohne Weiteres anzunehmen. Die darauf aufbauende Abwägung

[105] Kühling/Seidel/Sivridis, Datenschutzrecht, S. 143.
[106] *Simitis*, in: Simitis, BDSG, § 28, Rn. 105.
[107] *Simitis*, in: Simitis, BDSG, § 28, Rn. 105.
[108] *Simitis*, in: Simitis, BDSG, § 28, Rn. 105.
[109] *Plath*, in: Plath, BDSG Kommentar, § 28, Rn. 48.

ist hingegen nicht nur höchst vielseitig und kaum ohne konkrete Einzelfälle möglich, sondern wird sogar insgesamt aufgrund der begrifflichen Unbestimmtheit als fast nicht handhabbar angesehen.[110] Fernab dieser Schwierigkeiten lassen sich in den MonIKA-Anwendungsszenarien aber zunächst klar die Interessen der Beteiligten herausstellen:

Die MonIKA-Teilnehmer haben in den meisten Anwendungsszenarien zunächst wirtschaftliche Interessen, nämlich den Schutz eigener Anlagen, Netze und damit oft die Funktionsfähigkeit des eigenen Unternehmens. Dazu zählt ebenfalls das Interesse an der Integrität der Daten sowie der Vertraulichkeit der Daten und Geschäftsgeheimnisse. Darüber hinaus zielt die Datenverarbeitung auch auf den Erhalt der Stabilität und Leistungsfähigkeit des Internets im Allgemeinen ab. Beispiele aus dem Bereich der Botnetz-Abwehr zeigen zudem, dass sogar der Zugang zum Internet selbst ein treibendes Interesse an verbessertem Monitoring sein kann. So werden teilweise ganze IP-Bereiche bei einzelnen Providern als Spam markiert und so die Zustellung jedweder E-Mails an Kunden des sperrenden Providers verhindert.[111]

Aufseiten der Betroffenen sind die Meinungs- und Informationsfreiheit, das Fernmeldegeheimnis die Unverletzlichkeit der Wohnung und insbesondere auch die richterrechtlich anerkannten Grundrechte auf informationelle Selbstbestimmung[112] und auf Integrität und Vertraulichkeit informationstechnischer Systeme[113] sowie das allgemeine Persönlichkeitsrecht betroffen. In dieser Hinsicht besteht also ein enormes Interesse daran, Details über die Benutzung und die Inhalte der Kommunikation vor Zugriff zu schützen und den diese Interessen verbriefenden Rechtsnormen Geltung zu verschaffen. Die Eingriffe in diese Rechte wiegen umso schwerer, wenn wie im Botnetz-Szenario nicht nur ein „Mitlesen“ bei den MonIKA-Teilnehmern bezweckt wird, sondern die Daten des Betroffenen grundsätzlich auch mit anderen Daten der anderen Teilnehmern fusioniert werden und so die Erstellung weitreichender Nutzungsprofile über den Betroffenen möglich wäre. Im Bereich des BGP-Monitorings wäre die Sammlung einer großen Zahl von IP-Adressen sowie Routen denkbar, die Ortsdaten vieler Betroffener enthalten würden. Im Bereich des Enterprise-Monitorings ist über den Abgleich der Logfiles der einzelnen Unternehmen abermals eine sehr weitgehende Profilbildung über Kunden, Konkurrenten und Dritte möglich.

Es stehen sich also zwei Rechtsgüter von schwerem Gewicht gegenüber. Eine grundsätzliche Gewichtung hin zu einer der Seiten gibt es nicht. Zwar sind die Ermächtigungsgrundlagen im BDSG als Ausnahmen vom generellen Verbot der Datenverarbeitung konzipiert und stellen die Rechte der Betroffenen grundsätzlich auf eine höhere Stufe als die Interessen der verantwortlichen Stelle. Andererseits formuliert § 28 Abs. 1 S. 1 Nr. 2 BDSG die Gewichtung derart, dass

> *„kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt“*.

Damit senkt das BDSG den Prüfungsmaßstab etwas ab und verlangt nicht in jedem Fall eine ausführliche Interessenabwägung, sondern eine summarische Abwägung[114] dahingehend, ob Gründe vorliegen, die darauf hinweisen, dass die Rechte der Betroffenen überwiegen. Die verantwortliche Stelle muss also die möglichen Verarbeitungsfolgen für die Betroffenen prüfen und darf nur dann die Daten verarbeiten, wenn die bisherige Erfahrung und die vorliegenden Informationen keine Anhaltspunkte dafür liefern, dass die Interessen der Betroffenen nicht überwiegen.[115] Die Teilnehmer des Monitoring-Systems müssen damit vor Teilnahme an dem Monitoring-Netz prüfen, welche Daten betroffen sind, zu welchem Zweck diese verarbeitet werden sollen und welche Risiken dabei für die Betroffenen

[110] *Simitis*, in: Simitis, BDSG, § 28, Rn. 126.
[111] Heise.de, GMX landet auf Spam-Liste, http://heise.de/-1974706.
[112] BVerfG Urteilvom 15. Dez. 1983, 1 BvR 209/83, – Volkszählung –, online: http://openjur.de/u/268440.html.
[113] BVerfG Urteil vom 27. Feb. 2008, 1 BvR 370/07 und 1 BvR 595/07 – Onlinedurchsuchung –, online: http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html.
[114] *Plath*, in: Plath, BDSG Kommentar, § 28, Rn. 53, *Simitis*, in: Simitis, BDSG, § 28, Rn. 129 m. w. N.
[115] *Simitis*, in: Simitis, BDSG, § 28, Rn. 130.

entstehen. Allgemein ist mit Blick auf den Zweck des BDSG, nämlich den Schutz der informationellen Selbstbestimmung, im Zweifel ein Abwägungsergebnis zu berücksichtigen, das die Situation der Betroffenen am wenigsten beeinträchtigt.[116]

Fernab dieser allgemeinen Vorgaben enthält das BDSG aber einige Grenzen, die auch § 28 Abs. 1 S. 1 Nr. 2 BDSG nicht zu überwinden vermag. Insbesondere sind hier die besonderen Datenkategorien in § 3 Abs. 9 BDSG zu nennen. Daten, die

> *„Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben“*

betreffen, unterliegen den engeren Voraussetzungen des § 28 Abs. 6 BDSG und sind ohne Einwilligung nur dann einer Verarbeitung zugänglich, wenn

> *„1. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,*
>
> *2. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,*
>
> *3. dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, oder*
>
> *4. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.“*

Während derlei Datenkategorien im Bereich des BGP-Monitorings abermals wenig Relevanz haben, ist der gesamte Bereich der E-Mail-Überwachung zur Spam- und Botnetz-Abwehr durchaus kritisch zu betrachten. Daten der genannten Kategorien werden jedenfalls in textbasierten Filtermethoden nicht zu vermeiden sein. E-Mails zwischen Privatpersonen, die derart sensible Daten enthalten, müssen daher im Rahmen einer Spam-Filterung grundsätzlich unberücksichtigt bleiben oder erfordern eine noch strengere Einwilligung nach § 4 Abs. 3 BDSG. Technisch ist diese Anforderung nicht einfach umzusetzen, da gerade Spam-E-Mails beispielsweise nicht selten sexuelle Stichworte aufweisen. Hier muss im Zusammenspiel der Filtermethoden sichergestellt werden, dass im Regelfall keine sensiblen Daten erfasst werden.

§ 28 Abs. 1 Satz 1 Nr. 3 BDSG

Mit § 28 Abs. 1 S. 1 Nr. 2 BDSG sieht das BDSG schließlich eine Ermächtigungsgrundlage vor, die den Teilnehmern an einem koordinierten Monitoring-Netz einen weiteren Spielraum zugesteht,

> *„wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt“*.

Auch hier ist eine Verwendung nur für berechtigte Interessen möglich, und es ist nach wie vor eine Abwägung nötig. Allerdings sind diese Voraussetzungen jedenfalls hinsichtlich des Abwägungsmaßstabs leichter. Zwingend ist allerdings, dass die für die Anreicherung der Monitoring-Informationen bestimmten Daten allgemein zugänglich sind. Das ist der Fall, wenn die Daten

[116] *Simitis*, in: Simitis, BDSG, § 28, Rn. 21 m. w. N.

> *„sich sowohl ihrer Zielsetzung als auch ihrer Publikationsform nach dazu eignen, einem **individuell nicht bestimmbaren Personenkreis** Informationen zu vermitteln“.*[117]
> *(Fettung im Original)*

Inwiefern in den einzelnen Anwendungsszenarien solche Daten vorhanden sind, hängt von den jeweiligen Zielsetzungen der Monitoring-Verbände ab. Es kommen jedenfalls Datenbanken der DENIC oder RIPE RIS und Route Views[118] im Bereich des BGP-Monitorings und Listen wie die „Domain Name System Blacklists“[119] in Spam-Szenarien in Betracht. Hierbei ist aber zu beachten, dass der § 28 Abs. 1 S. 1 Nr. 2 BDSG nur die Verwendung der Primärdaten, nicht die Anreicherung mit Sekundärdaten erfasst.[120] Da sich die Datenverarbeitung in Anomalie erkennenden Verfahren aber gerade auf die Fusion der Daten mit anderen Daten konzentriert, erweitert diese Rechtsgrundlage den Handlungsspielraum nur begrenzt. Für die Kerntätigkeit der MonIKA-Systeme wird daher auf die vorher genannten Rechtsgrundlagen zurückzugreifen sein.

3.1.4.2.4.5 Rechtsgrundlagen aus geltendem Europarecht

Neben bundesdeutschen Rechtsquellen kommen europarechtliche Vorgaben als Grundlage für die Verarbeitung von Daten in koordinierten Monitoring-Netzen in Betracht. Von größter Relevanz ist dabei zunächst die allgemeine Europäische Datenschutzrichtlinie.

Diese Richtlinie 95/46/EG ist die Vorlage für das deutsche BDSG, und der Art. 7 DSRL ist Vorbild für die §§ 28 ff. BDSG und ähnelt ihnen inhaltlich. Wegen der inhaltlichen Nähe ergeben sich aus einem Rückgriff auf die allgemeine Europäische Datenschutzrichtlinie keine weitergehenden Handlungsspielräume. Unabhängig davon bestünde zwar die grundsätzliche Möglichkeit, für die Verarbeitung personenbezogener Daten zu MonIKA-Zwecken auf Art. 7 b) oder 7 f) zurückzugreifen. Beide Normen begegnen aber den gleichen Bedenken wie ihre deutschen Umsetzungen, und für die unmittelbare Anwendung von Richtlinien ergeben sich hohe Hürden.

Der Art. 7 b) stellt wie der deutsche § 28 Abs. 1 S. 1 Nr. 1 BDSG auf die Erforderlichkeit zur Durchführung des Vertrags ab und begegnet damit den gleichen Bedenken. Dort ergeben sich somit keine weitergehenden Möglichkeiten.

Der Art. 7 f) stellt als Vorlage für § 28 Abs. 1 S. 1 Nr. 2 BDSG auf ein berechtigte Interesse ab und setzt damit stets eine konkrete Interessenabwägung zugunsten der verantwortlichen Stelle voraus und formuliert:

> *„Die Mitgliedstaaten sehen vor, dass die Verarbeitung personenbezogener Daten lediglich erfolgen darf, wenn eine der folgenden Voraussetzungen erfüllt ist: […]*
>
> *f) die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 geschützt sind, überwiesen.“*

Insoweit ergibt sich aus der Datenschutzrichtlinie ein Unterschied nur dahingehend, dass auch die Übermittlung an Dritte mit aufgeführt ist. Selbst wenn man also das BDSG als teilweise enger gefasst ansieht, stellt sich die Frage nach der unmittelbaren Anwendung von Europarecht. Eine solche ist gemäß Artikel 288 des Vertrags über die Arbeitsweise der EU (AEUV) nur für Verordnungen vorgesehen. Für Richtlinien hat sich zwar eine detaillierte Rechtsprechung entwickelt für Fälle, in denen Mitgliedstaaten Richtlinien nicht rechtzeitig oder inhaltlich weitgehend genug umgesetzt

[117] *Simitis*, in: Simitis, BDSG, § 28, Rn. 151.
[118] Siehe D3.4, S. 17.
[119] http://www.dnsbl.info/.
[120] *Simitis*, in: Simitis, BDSG, § 28, Rn. 164.

haben.[121] Eine solche unmittelbare Anwendung setzt aber unter anderem voraus, dass der Mitgliedstaat die Richtlinie nicht rechtzeitig umgesetzt hat, was hier nicht der Fall ist, wie das ursprünglich vor dem EuGH angestrengte, dann aber fallengelassene Vertragsverletzungsverfahren zeigt.[122] Selbst wenn die Richtlinie aber nicht rechtzeitig umgesetzt wäre, so ist einhellige Auffassung, dass die unmittelbare Wirkung einer Richtlinie nur das Verhältnis zwischen Bürger und Staat betreffen kann. Einzelne Bürger untereinander können daraus keine Rechte ableiten. So würde dann auch die unmittelbare Anwendung einiger Normen aus der Europäischen Datenschutzrichtlinie keine Ermächtigungsgrundlage für ein Unternehmen gegen einen Bürger darstellen können.

Ebenfalls von Relevanz für die MonIKA-Szenarien ist die Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG). Dort findet sich ein Verweis auf eine Möglichkeit der Einzelstaaten, Rechtsvorschriften zu erlassen,

> *„die die Rechte und Pflichten [der Richtlinie 95/46/EG] beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist."*

Diese Regelung stellt aber selbst keine Rechtsgrundlage dar, sondern ermächtigt lediglich zum Erlass einer Rechtsgrundlage, wie sie etwa in Deutschland durch den § 100 Abs. 1 TKG geschaffen wurde. Ob die einzelnen nationalen Normen aber die Datenerhebung und -weiterleitung für Zwecke eines Monitoring-Netzes rechtfertigen, ist damit genauso wenig geklärt wie die Frage, wann welche Eingriffe in die persönliche Privatsphäre „angemessen und verhältnismäßig" sind. Die dafür notwendigen Konkretisierungen finden sich in der Richtlinie selbst nicht. Nicht zuletzt der Blick auf den bereits angesprochenen deutschen § 100 Abs. 1 TKG zeigt, dass Art. 15 Abs. 1 der Richtlinie 2002/58/EG eben keineswegs bedeuten muss, dass hier die Teilnahme an einem gemeinsamen Auswertungsnetz begründet wird. Letztlich würde eine solche Ermächtigungsgrundlage abermals lediglich Kommunikationsdienstleister erfassen und in vielen MonIKA-Szenarien keine Regelungskraft entfalten.

3.1.4.2.4.6 Zukünftige Rechtsgrundlagen aus der Datenschutz-Grundverordnung

In europarechtlicher Hinsicht zeichnet sich mit der geplanten Datenschutz-Grundverordnung eine Rechtsquelle ab, die nicht nur aufgrund ihrer Qualität als Verordnung unmittelbar in Deutschland und der gesamten EU gelten wird, sondern in vielen Bereichen auch konkreter und strenger als die geltende Datenschutzrichtlinie 95/46/EG ist.

Im aktuellen Kompromissentwurf des Europäischen Parlaments[123] findet sich in Art. 6 Nr. 1 DSGVO eine dem § 28 Abs. 1 S. 1 Nr. 2 BDSG und dem Art. 7 f) DSRL entsprechende Regelung. Sie lautet:

> *„1. Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist: […]*
>
> *f) Die Verarbeitung ist zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen – oder, im Fall der Weitergabe, der berechtigten Interessen eines Dritten, an den die Daten weitergegeben wurden –, die die berechtigten Erwartungen der betroffenen*

[121] *Grabitz/Hilf*, Das Recht der Europäischen Union, Art. 249 EGV, Rn. 155 ff.
[122] Vgl. *Simitis*, in: Simitis, BDSG, Einleitung, Rn. 96.
[123] Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments: Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Plenarsitzungsdokument, A7-0402/2013, 21.11.2013.

> *Person, die auf ihrem Verhältnis zu dem für die Verarbeitung Verantwortlichen beruhen, erfüllen, erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. […]“*

Insoweit hängt der Einsatz von koordinierten Monitoring-Netzen auch unter der Geltung der DSGVO an einer Abwägung im Einzelfall. Inwieweit sich daraus Erweiterungen oder Einschränkungen der Befugnisse von möglichen MonIKA-Teilnehmern ergeben, bleibt der weiteren Ausfüllung der DSGVO durch Gerichte und Literatur überlassen. Die Aufnahme der Formulierung „die berechtigten Erwartungen der betroffenen Person, die auf ihrem Verhältnis zu dem für die Verarbeitung Verantwortlichen beruhen,“ eröffnet jedenfalls einen weiten Auslegungsspielraum, der abhängig von dem gesellschaftlichen Stellenwert der IT-Sicherheit entweder zu einer weiten Akzeptanz von Netzen zu Anomalieerkennung führen oder derartige Datenverwendungen als ungewollt einordnen kann. Die fortschreitende kritische Befassung der Informationsgesellschaft mit Themen der Datensammlung und Auswertung könnte hier durchaus zu Einschnitten in der Akzeptanz solcher Systeme führen und damit auch unter Geltung der DSGVO deren Rechtmäßigkeit beeinflussen.

Hinsichtlich der übrigen rechtlichen Veränderungen durch die DSGVO ist mit Hinblick auf das MonIKA-System insbesondere relevant, dass die Weitergabe von Daten an Drittländer erschwert wird (Art. 42 DSGVO), was die Implementierung internationaler Systeme zur Anomalieerkennung betrifft.

3.1.4.3 Zusammenfassung bezüglich der Teilnehmer

Insgesamt zeigt sich hinsichtlich der rechtlichen Zulässigkeit der Datenerhebung bei den Teilnehmern eines koordinierten Auswertungssystems, dass eine Erhebung personenbezogener Daten grundsätzlich zulässig ist. Die konkrete Rechtmäßigkeit richtet sich nach den verfolgten Zwecken und den eingesetzten Mitteln. Abhängig von den einzelnen Szenarien finden sich Ermächtigungsgrundlagen im TKG und BDSG. Die erwartete Datenschutz-Grundverordnung ändert an der grundsätzlichen Zulässigkeit wenig, birgt allerdings neue Unsicherheitsfaktoren.

3.1.5 Anwendung des BDSG bei den Teilnehmern

Nachdem die grundsätzliche Frage der Zulässigkeit der Erhebung der Daten beantwortet ist, ist zu untersuchen, welche sonstigen Voraussetzungen das BDSG an kooperierende Auswertungs- und Fusionssysteme stellt.

3.1.5.1 Direkterhebung und Informationspflichten nach § 4 Abs. 2 und 3 BDSG

Gemäß § 4 Abs. 2 S. 1 BDSG ist eine Erhebung der Daten grundsätzlich nur bei den Betroffenen selbst zulässig:

> *„Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn […]“.*

Diese Norm hat im Laufe der technischen Entwicklung nach allgemeiner Ansicht den Anschluss an die tatsächlichen Umstände verloren und ist in Zeiten der hochvernetzten Informationsstrukturen nur bedingt handhabbar.[124] Sinn der Norm ist es, den Betroffenen die Möglichkeit zu geben, ihr Recht auf informationelle Selbstbestimmung auszuüben, indem die Daten direkt bei den Betroffenen erhoben werden. Dies soll idealerweise dazu führen, dass die Daten einerseits korrekt sind und andererseits der Betroffenen weiß, wer welche Daten über ihn erhebt.

In MonIKA-Systemen werden die Daten aber in den allermeisten Fällen ohne jede Mitwirkung der Betroffenen erhoben, da die Daten und Logdaten von Servern oder Systemen der Teilnehmer weitergeleitet werden. Während E-Mail-Provider in vielen Fällen zumindest grundsätzlich transparent

[124] *Simitis*, in: Simitis, BDSG, § 4, Rn. 23.

machen, dass auf den Inhalt der E-Mails zu Zwecken der Spam-Filterung zugegriffen wird, ist dies in allen anderen Szenarien nicht der Fall. Weder beim BGP-Monitoring noch im Enterprise-Monitoring erhält der Betroffene Auskunft darüber, dass und welche Daten durch Logfiles und durch die bloße Teilnahme am Routing aufgezeichnet und später korreliert werden. Selbst wenn die Art und der Umfang der Datenaufzeichnung stets transparent gemacht würde, so scheitert es doch in jedem Fall an der „Direktheit", denn die Daten werden praktisch nie in Gegenwart des Betroffenen auf seinem heimischen Rechner oder sonstigem Endgerät erhoben. Stattdessen werden Spuren auf Servern und in Logfiles Dritter ausgewertet. Die Durchsetzung dieser Norm ist daher praktisch kaum möglich.

In § 4 Abs. 2 S. 2 BDSG trägt das BDSG diesen Umständen insoweit Rechnung, als dass diverse Ausnahmen von der Direkterhebung hingenommen werden:

> *„Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn*
>
> *1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder*
>
> *2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder*
>
> *b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde*
>
> *und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden."*

Die erste Alternative hat keinen eigenen Regelungsgehalt, da der Vorrang bereichsspezifischer Regelungen bereits durch die generelle Subsidiarität des BDSG gegenüber dem TKG und TMG erreicht wird. Da die Eingriffsbefugnisse durch das TKG nur einen kleinen Teil der Anwendungsmöglichkeiten des MonIKA-Systems abdecken[125], können diese Fälle unberücksichtigt bleiben. Weitergehende Möglichkeiten zur Erhebung von Daten bei Dritten ergeben sich jedoch aus den Alternativen 2a) und 2b). Allerdings ist hierbei zu beachten, dass das Grundrecht auf informationelle Selbstbestimmung im Kern das Recht darstellt, darüber zu entscheiden, wem in welcher Situation welche Daten preisgegeben werden.[126] Folglich müssen die Ausnahmevorschriften, die eine Erhebung ohne Mitwirkung des Betroffenen erlauben, verfassungskonform und somit restriktiv ausgelegt werden.[127] Dies wird vor allem durch die notwendige Verhältnismäßigkeitsabwägung zwischen den Interessen der verantwortlichen Stelle und schutzwürdigen Interessen des Betroffenen erreicht (§ 4 Abs. 2 S. 2 Nr. 2 letzter Halbsatz BDSG).

Dennoch kann die Anwendung der Alternative 2a) gerade im Bereich des Enterprise-Monitorings und im begrenzten Maße im Bereich des Botnetz-Monitorings in Betracht kommen. Die Anwendungsszenarien verbindet, dass durch die Sammlung verschiedener Daten Angriffe auf Netzsysteme verhindert werden sollen. Für diesen Zweck ist es teilweise notwendig, die Betroffenen – insbesondere die „Angreifer" – nicht über Monitoring-Aktivitäten zu informieren und so die Kenntnisse über mögliche Angriffe preiszugeben. Dieses Szenario kann mit der Arbeit einer Detektei verglichen werden, deren Geschäftszweck eine Datenerhebung ohne Mitwirkung rechtfertigt.[128]

Darüber hinaus könnte auch die Ausnahmevorschrift der Ziffer 2b) eine Erhebung ohne Mitwirkung des Betroffenen rechtfertigen. Wie oben bereits diskutiert, haben die technischen Entwicklungen der letzten Jahre eine Direkterhebung in diesem Bereich enorm schwierig werden lassen. Folglich erscheint eine Direkterhebung im Umfeld des MonIKA-Netzes nur mit unverhältnismäßigem Aufwand möglich. Deshalb wird in vielen Fällen, soweit eine einzelfallbezogene Abwägung die Verhältnismäßigkeit ergibt, eine Datenerhebung ohne Mitwirkung des Betroffenen gerechtfertigt sein.

---

[125] Siehe Abschnitte 3.1.4.2.1.2 und 3.1.4.2.1.3.
[126] BVerfG, Urteil vom 15.12.1983, 1 BvR 209/83; 1 BvR 269/83; 1 BvR 362/83; 1 BvR 420/83; 1 BvR 440/83; 1 BvR 484/83, Rn. 172 f.
[127] *Sokol,* in: Simitis, BDSG, § 4, Rn. 35.
[128] *Sokol,* in: Simitis, BDSG, § 4, Rn. 34 m. w. N.

Eine weitere Herausforderung ergibt sich aus der Tatsache, dass, selbst wenn keine Direkterhebung notwendig ist, § 33 BDSG eine grundsätzliche Benachrichtigungspflicht an die Betroffenen statuiert. Demzufolge ist der Betroffene über die Speicherung, die Art der Daten, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung sowie die Identität der verantwortlichen Stelle zu informieren.

> *„Die Benachrichtigung setzt voraus, dass der verantwortlichen Stelle Name und Anschrift der betroffenen Personen bekannt sind. Ist dies nicht der Fall, so besteht grundsätzlich keine Benachrichtigungspflicht. Unter Berücksichtigung des Schutzzwecks der Vorschrift ist es regelmäßig nicht geboten, ausschließlich zur Durchführung der Benachrichtigung Namen und Anschrift zu ermitteln und zu speichern und damit potenzielle Risiken für die Betroffenen zu erhöhen.“*[129]

Auch wenn diese Ansicht in der Literatur nicht unumstritten ist, scheint sie jedenfalls im Einklang mit der neuen Datenschutz-Grundverordnung zu stehen. Der aktuelle Kompromissentwurf des Europäischen Parlaments zur Verordnung enthält in Art. 10 Nr. 1 die folgende Regelung:

> *„Kann der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter anhand der von ihm verarbeiteten Daten eine natürliche Person weder direkt noch indirekt bestimmen, oder bestehen die von ihm verarbeiteten Daten nur aus pseudonymisierten Daten, so ist es ihm nicht gestattet, zur bloßen Einhaltung einer Vorschrift dieser Verordnung zusätzliche Daten zu verarbeiten oder einzuholen, um die betroffene Person zu bestimmen.“*[130]

Wie die Tabellen über die betroffenen Daten in den Abschnitten 2.2, 2.3 und 2.4 über die potentiell erhobenen personenbezogen Daten in den MonIKA-Szenarien zeigen, wird den MonIKA-Teilnehmern in keinem der Szenarien Name und Anschrift der Betroffenen unmittelbar bekannt. Folglich wären weitere Ermittlungen zusätzlicher Daten notwendig, um die Betroffenen zu informieren. Selbst der möglicherweise geringe Aufwand, die Pseudonyme mithilfe der MonIKA-Teilnehmer aufzulösen, ändert daran nichts, da nach dem Kompromissvorschlag des Europäischen Parlaments zur DSGVO auch derartige Maßnahmen nicht gestattet wären. Im Endergebnis wird daher nicht gefordert werden können, dass weitergehende personenbezogene Daten ermittelt werden, um einer Benachrichtigungspflicht nachzukommen.[131] Hierfür spricht auch, dass für die Ermittlungen die bisher gespeicherten Daten ohne Rechtsgrundlage genutzt werden müssten.

3.1.5.2 Rechte der Betroffenen

Basierend auf dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) gewährleistet das BDSG den Betroffenen einige Rechte, die einerseits Voraussetzung für eine wirksame Ausübung des Grundrechtes sind und andererseits die Ausübung des Grundrechtes selbst darstellen.

Den einzelnen Rechten ist jedoch die Frage vorgelagert, gegenüber wem Betroffene ihre Rechte geltend machen können. Grundsätzlich verpflichten §§ 34 f. BDSG die „verantwortliche Stelle“, d. h. die datenerhebenden und -verarbeitenden Teilnehmer des MonIKA-Netzes.[132] Um jedoch eine wirksame Wahrnehmung der Betroffenenrechte zu gewährleisten, enthält § 6 Abs. 2 BDSG eine Ausnahmevorschrift für Fälle, in denen durch Datenverarbeitung in sogenannten Verbundnetzen bzw. vernetzten Systemen nicht ohne Weiteres nach außen erkennbar ist, wer für die einzelnen Daten die „verantwortliche Stelle“ ist. Somit kann es in Monitoring-Netzen für die Gewährleistung der Betroffenenrechte in Fortführung des „joint controllerships“ dazu führen, dass sich die Betroffenen an

[129] *Dix*, in: Simitis, BDSG, § 33, Rn. 20.
[130] Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments: Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Plenarsitzungsdokument, A7-0402/2013, 21.11.2013.
[131] Vgl. *Dix*, in: Simitis, BDSG, § 33, Rn. 20.
[132] Siehe Abschnitt 3.1.2.

jede speicherungsberechtigte Stelle wenden können, um ihre Rechte auszuüben. Festzuhalten bleibt somit, dass sowohl die einzelnen Teilnehmer als auch die Zentralstelle Ansprechpartner bezüglich der Geltendmachung von Betroffenenrechten sind.

Dennoch muss für das weitere Verfahren immer noch zwischen speicherungsberechtigter und verantwortlicher Stelle unterschieden werden.

> *„Das Gesetz geht in [§ 6] Abs. 2 [BDSG] davon aus, dass hinsichtlich einer Datei grundsätzlich (nur) eine ‚verantwortliche Stelle' besteht, die Verpflichtete hinsichtlich der in [§ 6] Abs. 1 [BDSG] bezeichneten Rechte ist, dass aber mehrere Stellen speicherungsberechtigt sind. Die Vorschrift weist also nicht quasi gesamtschuldnerisch allen speicherungsberechtigten Stellen die Verantwortung einer verantwortlichen Stelle hinsichtlich aller in der gemeinsamen Datei gespeicherten Daten zu; die Verantwortlichkeit bleibt vielmehr getrennt."*[133]

Hieraus ergibt sich, dass jede „verantwortliche Stelle" erst einmal für die Daten verantwortlich bleibt, die sie in das gemeinsame System eingeführt hat, während sich Betroffene jedoch auch an jede andere speicherungsberechtigte Stelle wenden können, um eine möglichst datenschutz- und betroffenenfreundliche Ausübung der Rechte zu gewährleisten. § 6 Abs. 2 S. 2 BDSG verpflichtet speicherungsberechtigte, aber nicht verantwortliche Stellen, Vorbringen von Betroffenen an die jeweils zuständige verantwortliche Stelle weiterzuleiten. Diese hat wiederum nach den §§ 34 f. BDSG zu verfahren. Im MonIKA-System sind sowohl Teilnehmer als auch Zentralstelle jedenfalls für die durch die EvA-Agenten generierten und an das EvA-Service-Cluster weitergeleiteten Daten speicherungsberechtigt und daher nebeneinander auskunftspflichtig.

§ 34 Abs. 1 BDSG statuiert ein Auskunftsrecht des Betroffenen. Auf sein Verlangen ist dem Betroffenen Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. den Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

Die Auskunft ist gemäß § 34 Abs. 6 und 8 BDSG in der Regel in Textform und unentgeltlich zu erteilen. In Einzelfällen kann von diesen Grundsätzen abgewichen werden, falls die Auskunftserteilung aufgrund besonderer Umstände in anderer Form angemessen erscheint.

Weitere Betroffenenrechte enthält § 35 BDSG. Soweit die verantwortliche Stelle ihren Pflichten zur Berichtigung, Löschung oder Sperrung nicht ausreichend nachkommt, können diese von dem Betroffenen verlangt werden. Personenbezogene Daten sind gemäß Abs. 1 unverzüglich – d. h. ohne schuldhaftes Zögern – zu berichtigen, wenn sie unrichtig sind. Unrichtig sind Daten nicht nur dann, wenn sie nicht mit der Realität übereinstimmen, sondern auch, wenn eine Information durch einen Kontextverlust wahrscheinlich Fehlvorstellungen verursachen wird.[134] Wird die Richtigkeit von Daten durch den Betroffenen bestritten und das Bestreiten ist nicht offensichtlich fehlerhaft, so sind die Daten unverzüglich zu sperren (Abs. 4). Stellen sich die Daten als falsch heraus, sind sie zu berichtigen. Lässt sich weder die Richtigkeit noch die Unrichtigkeit feststellen, verbleiben die Daten gesperrt (Abs. 4). Die Sperrung hat ein relatives Nutzungsverbot zur Folge, so dass Nutzung und Übermittlung nur in strikten Ausnahmefällen (Abs. 8) möglich sind, welche jedoch im Kontext des MonIKA-Netzes irrelevant erscheinen.

[133] *Mallmann*, in: Simitis, BDSG, § 6, Rn. 28 m. w. N.
[134] *Däubler*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 35, Rn. 5.

Darüber hinaus enthält Abs. 2 S. 2 enumerativ aufgezählte Löschungspflichten. Dementsprechend sind Daten insbesondere dann zu löschen, wenn

1. ihre Speicherung unzulässig ist oder
2. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist.

Weiterhin wurde im Jahr 2001 mit Rücksicht auf Art. 14 Buchstabe a der EG-Datenschutzrichtlinie ein Widerspruchsrecht in § 35 Abs. 5 BDSG eingeführt:

> *„Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. […]“*

Zuletzt ist noch auf die sogenannte Nachberichtspflicht des § 35 Abs. 7 BDSG hinzuweisen. Hiernach ist die verantwortliche Stelle verpflichtet, all diejenigen Stellen zu unterrichten, an die Daten zur Speicherung weitergegeben wurden – insbesondere an die MonIKA-Zentralstelle –, wenn unrichtige Daten berichtigt, bestrittene Daten gesperrt oder Daten wegen der Unzulässigkeit der Speicherung gelöscht oder gesperrt wurden. Die Teilnehmer des MonIKA-Netzes sind also dazu verpflichtet, Fehler in ihren übersandten Daten aufzuklären.

3.1.5.3 Die Schadensersatzpflicht nach § 7 BDSG

Bei § 7 BDSG handelt es sich um eine eigenständige datenschutzrechtliche Haftungsnorm. Anspruchsberechtigt ist der Betroffene, d. h. eine natürliche Person, deren personenbezogene Daten unzulässig oder unrichtig erhoben, verarbeitet oder genutzt wurden.

Anspruchsgegner sind die verantwortlichen Stelle oder ihre Träger, hier die Teilnehmer des MonIKA-Systems. Sofern von Auftragsdatenverarbeitung auszugehen ist, bleibt die Verantwortung beim Auftraggeber. Der Auftragnehmer wird im Falle des Verstoßes gegen die Weisungen selbst zur verantwortlichen Stelle, so dass er dann auch nach § 7 BDSG dem Betroffenen gegenüber haftet.[135] Sofern im Rahmen eines MonIKA-Systems mehrere Teilnehmer als verantwortliche Stellen anzusehen sind und erst durch ihr Zusammenwirken der Schaden entstanden ist, haften sie dem Betroffenen als Gesamtschuldner (§ 840 S. 1 BGB).[136]

Die verantwortliche Stelle muss gegen die Vorschriften über den Datenschutz verstoßen haben. In Betracht kommen hier sowohl Verstöße gegen das BDSG selbst, wie etwa die Übermittlung von Daten ohne Einwilligung, als auch Verstöße gegen datenschutzrechtliche Normen des TMG und des TKG oder etwa gegen Betriebsvereinbarungen zum Umgang mit Arbeitnehmerdaten.[137] Irrelevant ist, ob die Datenverarbeitung automatisiert oder nicht-automatisiert erfolgt.[138]

Dem Betroffenen muss hierdurch ein Schaden entstanden sein. Nach vorherrschender Meinung in der juristischen Literatur[139] werden lediglich materielle Schäden erfasst, d. h. solche, die „wirtschaftlich zu beziffern“ sind. Immaterielle Schäden werden nicht erfasst. Ein Anspruch auf Schmerzensgeld wegen des Bekanntwerdens die Intimsphäre verletzender Informationen besteht nach § 7 BDSG mithin nicht. In den einzelnen Anwendungsszenarien können also alle Schäden in Betracht, kommen, die dadurch entstehen, dass zum Beispiel fehlerhafte Botnetz-Säuberungen zu defekten

[135] *Simitis*, in: Simitis, BDSG, § 7, Rn. 11.
[136] *Simitis*, in: Simitis, BDSG, § 7, Rn. 37.
[137] *Däubler*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 7, Rn.10.
[138] *Simitis*, in: Simitis, BDSG, § 7, Rn. 15.
[139] *Däubler*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 7, Rn. 3, 19 f.; Simitis, BDSG, § 7, Rn. 5, 32.

Rechnern führen. Rufschädigende Auswirkungen für zu Unrecht als Spam-Versender erkannte Betroffene wären hingegen nicht ersatzfähig.

Bei Vorliegen der o. g. Voraussetzungen wird das Verschulden der verantwortlichen Stelle bzw. ihres Trägers vermutet. Es besteht für sie lediglich die Möglichkeit, sich zu exkulpieren, d. h. nachzuweisen, dass sie „die nach den Umständen des Falles gebotene Sorgfalt" beachtet hat (§ 7 S. 2 BDSG). Dem klaren Wortlaut nach sind damit die Anforderungen an die zu treffenden Vorkehrungen umso höher, je größer die potentiellen Gefahren für die Betroffenen sind.[140] Ob der Verstoß auf ein Fehlverhalten von Beschäftigten der verantwortlichen Stelle oder ihres (internen) Datenschutzbeauftragten oder auf einen internen Organisationsmangel zurückzuführen ist, ist im Verhältnis zum Betroffenen irrelevant, da § 7 BDSG die verantwortliche Stelle als Einheit betrachtet.[141] Bei technischen Störungen, die belegbar nicht zu vermeiden waren, kommt indes eine Exkulpation in Betracht.[142]

Die praktische Bedeutung des § 7 BDSG ist eher gering. Es sind keine erfolgreichen Klagen auf Grundlage des § 7 BDSG bekannt, die nicht auch unter Berufung auf allgemeine haftungsrechtliche Normen zum Erfolg geführt hätten.[143] Insofern wird vollumfänglich auf das Gutachten „Rechtliche Herausforderungen der Informationsfusion und -klassifikation zur Erkennung von Anomalien in Internet-Infrastrukturen unter besonderer Berücksichtigung haftungs- und IT-rechtlicher Fragestellungen" des Projektpartners ITM verwiesen.

3.1.5.4 Technische und organisatorische Maßnahmen nach § 9 BDSG

Das BDSG verpflichtet verantwortliche Stellen in § 9 BDSG auf einen Standard für erforderliche technische und organisatorische Maßnahmen zur Gewährleistung des Schutzes personenbezogener Daten, unabhängig davon, ob diese automatisiert oder nicht-automatisiert verarbeitet werden. Der Standard ist auch von Auftragnehmern im Rahmen der Auftragsdatenverarbeitung einzuhalten. Die verantwortliche Stelle hat sich hiervon zu überzeugen.[144] Für die Teilnehmer eines MonIKA-Systems sind lediglich die Anforderungen an automatisierte Datenverarbeitung und -nutzung von Belang. Für diesen Bereich ist in der Anlage 1 zu § 9 S. 1 BDSG ein Maßnahmenkatalog zur Umsetzung der Datensicherheit enthalten, der das „Mindestmaß des Notwendigen"[145] bestimmt.

Teilnehmer eines MonIKA-Systems sind in aller Regel ohnehin bereits verantwortliche Stellen i. S. d. BDSG und sollten damit die erforderlichen technischen und organisatorischen Maßnahmen getroffen haben. Der Umgang mit MonIKA-Daten bedeutet für die Teilnehmer abstrakt zunächst keine Änderung der an ein ausreichendes Datenschutzsystem zu stellenden Voraussetzungen.

Die geforderten Maßnahmen stehen gem. § 9 S. 2 BDSG unter dem Vorbehalt der Verhältnismäßigkeit, d. h. eine Maßnahme ist stets daraufhin zu überprüfen, ob sie im Einzelfall geeignet, erforderlich und angemessen ist. Geeignet ist sie, wenn sie den angestrebten Zweck – Datensicherheit – erfüllt. Erforderlich ist sie, wenn sich der gleiche Schutzzweck nicht mit einem weniger aufwendigen (z. B. kostengünstigeren) Mittel erreichen lässt. Für die Beurteilung der Angemessenheit ist die Intensität des Eingriffs in (Grund-)Rechte Betroffener mit der Bedeutung der Sache abzuwägen. Angesichts des Ausmaßes der Datenverarbeitung durch die Teilnehmer und die Zentralstelle und der möglichen Risiken für die Betroffenen dürften sich die Anforderungen an die entsprechenden Maßnahmen aber im oberen Bereich des § 9 BDSG befinden.

[140] *Däubler*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 7, Rn.15.
[141] *Däubler*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 7, Rn. 15; *Simitis*, in: Simitis, BDSG, § 7, Rn. 26.
[142] *Däubler*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 7, Rn. 15.
[143] *Däubler*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 7, Rn. 3.
[144] *Wedde*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 9, Rn. 11.
[145] *Wedde*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 9, Rn. 3.

3.1.5.5 File-Trennung nach § 30 BDSG

Das Gebot der File-Trennung gemäß § 30 BDSG ist für die MonIKA-Anwendungsszenarien von untergeordneter Bedeutung, solange die Daten als Klardaten von den Teilnehmern an die Zentralstelle weitergegeben werden. Lediglich die dargestellte Umwandlung des Klartexts von E-Mails in eine Art Fingerabdruck, der nur noch statistische Angaben bezüglich Worthäufigkeit, Anzahl der Zeichen usw. enthält, kann als Anonymisierung in Betracht kommen.[146] Dennoch zeigt das MonIKA-Projekt, dass das Gebot der File-Trennung in ähnlichen Einsatzszenarien von Bedeutung sein könnte. Insbesondere die Verarbeitung von IP-Adressen, URLs und AS-Nummern z. B. mit den von Kerschbaum[147] entwickelten Techniken zur distanzerhaltenen Hashwertbildung[148] können zu einer Übermittlung von anonymisierten Daten führen, was eine Auseinandersetzung mit § 30 BDSG verlangt.

Der Anwendungsbereich des § 30 BDSG wurde durch die Einführung des § 30a BDSG stark eingeschränkt, und viele Stimmen in der datenschutzrechtlichen Literatur haben die Ansicht einer gänzlichen Funktionslosigkeit von § 30 BDSG vertreten.[149] Das MonIKA-Projekt hat jedoch gezeigt, dass weiterhin Szenarien möglich erscheinen, in denen § 30 BDSG einschlägig ist und die Spezialregelung des § 30a BDSG gerade nicht ausreicht, da zweifelsfrei die Tätigkeit eines MonIKA-Systems nicht der Meinungs- oder Marktforschung im klassischen Sinn zuzuordnen ist. Problematischer erscheint die Frage, ob die Teilnehmer eines MonIKA-Netzes Daten geschäftsmäßig erheben und speichern, um sie in anonymisierter Form zu übermitteln (§ 30 Abs. 1 S. 1 BDSG). Dies erscheint aus zwei Gründen problematisch: Zum einen stellt sich die Frage, ob die Daten in anonymisierter Form übermittelt werden, zum anderen ist fraglich, ob die Daten zu diesem Zweck erhoben und gespeichert werden.

In Abschnitt 3.1.1 wurde der Personenbezug der erhobenen Daten ausführlich diskutiert und klargestellt, dass eine Pseudonymisierung von Daten nichts an ihrer Einstufung als personenbezogene Daten ändert. Diese Einschätzung ergab sich aus der Tatsache, dass die Zuordenbarkeit der Daten im Verhältnis zu der verantwortlichen Stelle insbesondere so lange erhalten bleibt, wie die verantwortliche Stelle die Zuordnungsregel kennt.[150] Die Teilnehmer an MonIKA-Netzen werden in aller Regel auch nach Übersendung der Daten an die Zentralstelle über die Zuordnungsregel verfügen, da nur so die spätere Auflösung der durch die Zentralstelle gewonnenen Erkenntnisse möglich ist. Hier ist jedoch deutlich zwischen den Teilnehmern und der Zentralstelle zu unterscheiden. Wenn sichergestellt wird, dass nur die einzelnen Teilnehmer Zugriff auf ihre jeweiligen Zuordnungsregeln haben, bleiben die Daten für diese pseudonymisiert, während sie für die Zentralstelle und alle anderen Teilnehmer anonymisierte Daten darstellen.[151] Dies ergibt sich aus der Tatsache, dass nur der einzelne Teilnehmer die Daten von der pseudonymisierten Form mithilfe seiner Zuordnungsregel in Klardaten zurückführen kann. Somit würden ausschließlich anonymisierte Daten an die Zentralstelle weitergeleitet.

Weiterhin stellt sich jedoch die Frage, ob diese Übermittlung Zweck der Speicherung ist, da die Daten von den Teilnehmern auch für eigene andere Zwecke genutzt und gespeichert werden. Da die Teilnahme an einem Netz zur Anomalieerkennung aber dazu dient, von verschiedenen Stellen Daten zu sammeln und so einen erhöhten Informationsgewinn zu erlangen, wird sich die Übermittlung jedenfalls als Mitzweck jedes MonIKA-Systems einstufen lassen. Damit wäre auch § 30 BDSG anwendbar.

Als Folge hiervon wären die Teilnehmer zur File-Trennung verpflichtet.

---

[146] Siehe dazu Abschnitt 3.2.2.
[147] *Kerschbaum*, Distance-Preserving Pseudonymization for Timestamps and Spatial Data, ACM Workshop on Privacy in the Electronic Society (WPES), 2007, http://www.fkerschbaum.org/wpes07.pdf. Weitere Details siehe in Abschnitt 6.5.4.
[148] Siehe hierzu Abschnitt 3.2.2.
[149] *Ehmann*, in: Simitis, BDSG, § 30, Rn. 1.
[150] Kühling/Seidel/Sivridis, Datenschutzrecht, S. 85.
[151] Vgl. *Ehmann*, in: Simitis, BDSG, § 30, Rn. 50 f.

> *„Der Ablauf der File-Trennung gestaltet sich folgendermaßen: Der Datensatz, der zum einzelnen Betroffenen gehört, wird nicht als Einheit gespeichert, sondern in zwei Teile zerlegt. Der erste Teil enthält lediglich solche Einzelangaben, die aus sich heraus (also ohne Beiziehung weiterer Daten/der Merkmale des zweiten Teils) weder auf den Betroffenen bezogen sind noch auf ihn bezogen werden können [d. h. die gehashten IP-Adressen]. Der zweite Teil besteht dagegen aus personenbezogenen Merkmalen, die dazu dienen können, die im ersten Teil enthaltenen Angaben wieder dem Betroffenen zuzuordnen [d. h. IP-Adressen als Klardaten] […]. Die Einzelangaben im ersten Teil und die Merkmale im zweiten Teil werden in zwei getrennten Dateien gespeichert (daher die übliche Bezeichnung ‚File-Trennung').“*[152]
>
> (Auslassungen und Ergänzungen für den MonIKA-Kontext durch den Bearbeiter)

Die File-Trennung hat grundsätzlich unmittelbar bei der Speicherung zu erfolgen. Dies ist dem Zweck der Regelung geschuldet und gilt auch dann, wenn ein baldiges, aber späteres Zusammenführen bereits absehbar ist.[153]

> *„Allerdings darf dies nicht dazu führen, dass unzumutbare Abläufe gefordert werden. Solche Aspekte sind weniger eine Frage der technischen Möglichkeiten (sie bestehen prinzipiell) als der Zumutbarkeit.“*[154]

Dementsprechend kann davon ausgegangen werden, dass eine Pseudonymisierung, die ohne schuldhaftes Verzögern nach der Speicherung vorgenommen wird, noch die Voraussetzungen des § 30 Abs. 1 BDSG erfüllt.

3.1.5.6 Zweckbindung nach § 28 Abs. 1 Satz 2 und § 31 BDSG

Gemäß § 28 Abs. 1 S. 2 BDSG ist der Zweck, für den personenbezogene Daten verarbeitet oder genutzt werden sollen, bereits bei der Erhebung konkret festzulegen. § 31 BDSG bestimmt ergänzend, dass personenbezogene Daten, die ausschließlich zum Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, auch nur für diese Zwecke verwendet werden dürfen. Die für ein MonIKA-System zu erhebenden und verarbeitenden Daten dienen in aller Regel mehr Zwecken als den in § 31 BDSG genannten. Die Übersendung an eine zentrale Auswertungsstelle ist bereits nicht in jedem Fall den Zwecken zuzuordnen, Daten zu sichern, die Einhaltung des Datenschutzes zu kontrollieren oder einen ordnungsgemäßen Betriebsablauf zu garantieren. Gerade letzterer Punkt kann, muss aber nicht ausschließliches Ziel der Teilnahme an MonIKA sein. Die Erkennung von Botnetzen hat etwa regelmäßig keinen konkreten Bezug zu eigenen Betriebsabläufen. Ziele wie die Förderung der Forschung können weitere Zwecke der Übersendung sein und heben die Anwendung des § 31 BDSG auf. Sofern allerdings in kleinen Anwendungsszenarien die Ziele eines MonIKA-Systems allein die Erreichung von Zwecken im Sinne des § 31 BDSG sind, ist die besondere Zweckbindung zu beachten.

Wie bereits in Abschnitt 3.1.4.2.4.4 zur Rechtsgrundlage der Datenerhebung ausgeführt, dient die Datenerhebung und -verarbeitung in den zu untersuchenden Szenarien Botnetz-Erkennung, BGP-Monitoring und Enterprise-Monitoring abstrakt immer der Erhaltung der Arbeitsfähigkeit und damit letztlich der Leistungsfähigkeit eines Unternehmens. Die IT-Sicherheit dient dem Schutz der eigenen Anlagen und garantiert damit die Möglichkeit, eigene vertragliche Verpflichtungen Geschäftspartnern, Kunden und Angestellten gegenüber einzuhalten. Die Definition des genauen Zwecks muss jedoch grundsätzlich dem konkreten Anwendungsszenario vorbehalten bleiben.

[152] *Ehmann*, in: Simitis, BDSG, § 30, Rn. 49.
[153] *Ehmann*, in: Simitis, BDSG, § 30, Rn. 54.
[154] *Ehmann*, in: Simitis, BDSG, § 30, Rn. 55.

Die verantwortliche Stelle hat die Zweckbestimmung schriftlich niederzulegen. Dies ergibt sich aus einer Zusammenschau des § 28 Abs. 1 S. 2 BDSG mit § 9 BDSG (technische und organisatorische Maßnahmen).[155]

3.1.5.7 Beschäftigtendatenschutz nach § 32 BDSG

Einen besonders weitgehenden Schutz persönlicher Daten statuiert das BDSG im Verhältnis zwischen Arbeitnehmern und Arbeitgebern. Dies begründet vor allem im Szenario des Enterprise-Monitorings vielfältige Besonderheiten. Anerkannt ist, dass Unternehmen als Arbeitgeber Verbindungsdaten über die Internet-Nutzung erheben und verwenden können, falls die Daten soweit anonymisiert sind, dass einem einzelnen Arbeitnehmer keine bestimmte Nutzung zugeordnet werden kann.[156] Die Datenerhebung in den MonIKA-Anwendungsszenarien, insbesondere das Enterprise-Monitoring, geht über dieses Maß allerdings hinaus, da auch konkrete IP-Adressen, URLs und Portnummern erhoben und verarbeitet werden.

Diese geplante Nutzung erscheint problematisch, ist jedoch für verschiedene Situationen differenziert zu betrachten:

Die erste Variante basiert auf der Annahme, dass der Arbeitgeber seinen Arbeitnehmern die private Nutzung des Internets, E-Mails usw. erlaubt bzw. nicht ausdrücklich verboten hat. Wie in Abschnitt3.1.4.2.4.1 3.1.4.2.4.1 ausgeführt, hätte dies zur Folge, dass Arbeitgeber als Anbieter im Sinne des TKG zu qualifizieren sind. Dies würde dazu führen, dass das in § 88 TKG geregelte Fernmeldegeheimnis zu beachten ist. In Einklang mit § 88 Abs. 3 S. 1 TKG ist es Arbeitgebern somit untersagt, sich Kenntnis von Inhalten und näheren Umständen der Telekommunikationsvorgänge im Internet bzw. im E-Mail-System zu verschaffen.[157] Jeder Zugriff auf diese Daten bedarf der ausdrücklichen Erlaubnis durch den Arbeitnehmer.

> *„Grundsätzlich können bestimmte Zugriffe auf Kommunikations- und E-Mail-Inhalte durch Betriebsvereinbarungen geregelt werden, die als andere Rechtsvorschrift gemäß § 4 Abs. 1 [BDSG] zu qualifizieren sind. Allerdings ist es den Betriebsparteien mit Blick auf § 75 Abs. 2 BetrVG verwehrt, weitgehende Zugriffe in die Persönlichkeitsrechte der Beschäftigten zu legitimieren. Arbeitgeber und Betriebsräte dürfen allerdings durch kollektivrechtliche Regelungen nur solche Eingriffe zulassen, die im Ergebnis einer Interessenabwägung unumgänglich sind und bei denen die Persönlichkeitsrechte der Beschäftigten maximal gewahrt bleiben.“*[158]

Die zweite Alternative bezieht sich auf die Situation, dass Beschäftigten die private Nutzung von Kommunikationssystemen verboten ist. Dies führt dazu, dass das TKG keine Anwendung findet und § 32 BDSG den Beschäftigtendatenschutz abschließend regelt.

> *„Hieraus folgt indes nicht, dass damit unbegrenzte Zugriffsmöglichkeiten von Arbeitgebern auf die Daten von Beschäftigten bestehen. Auch nach einem Verbot der privaten Nutzung bleibt der Zugriff auf Daten aus dem persönlichen dienstlichen Bereich in jedem Fall unzulässig.“*[159]

Im Ergebnis kann damit festgehalten werden, dass, falls die Daten dem persönlichen Bereich zugerechnet werden können bzw. die Möglichkeit besteht, dass u. U. auch Daten aus dem persönlichen Bereich gespeichert werden, eine einzelvertragliche Regelung oder Betriebsvereinbarung notwendig ist. Insbesondere für den Bereich des Enterprise-Monitorings ist es somit nötig, dass alle Beschäftigten diesem zugestimmt haben.

---

[155] *Wedde*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 28, Rn. 64.
[156] *Wedde*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 32, Rn. 111.
[157] *Wedde*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 32, Rn. 115.
[158] *Wedde*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 32, Rn. 117.
[159] *Wedde*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 32, Rn. 118.

3.1.5.8 Der betriebliche Datenschutzbeauftragte nach §§ 4f, 4g BDSG

Gemäß § 4f Abs. 1 BDSG sind nicht-öffentliche Stellen, d. h. private Unternehmen, verpflichtet, einen Datenschutzbeauftragten zu bestellen, wenn sie personenbezogene Daten automatisiert verarbeiten und in der Regel mehr als neun Personen beschäftigen, die ständig personenbezogene Daten automatisiert verarbeiten. Sowohl von den MonIKA-Teilnehmern als auch der MonIKA-Zentralstelle werden personenbezogene Daten automatisiert verarbeitet. Dementsprechend können sie, abhängig von ihrer Größe, zur Bestellung eines betrieblichen Datenschutzbeauftragten verpflichtet sein. Die Bestellung hat gemäß § 4f Abs. 1 S. 2 BDSG innerhalb eines Monats nach Aufnahme der Tätigkeit bzw. Erreichung des Grenzwerts von über neun Personen zu erfolgen. Der betriebliche Datenschutzbeauftragte ist zwar dem Leiter der verantwortlichen Stelle direkt zu unterstellen (§ 4f Abs. 3 S. 1 BDSG), jedoch im Bereich des Datenschutzes nicht seinen Weisungen unterworfen (§ 4f Abs. 3 S. 2 BDSG).

Als Anforderungen an den betrieblichen Datenschutzbeauftragten nennt § 4f Abs. 2 S. 1 BDSG zwar die für die Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit, definiert diese Begriffe aber nicht genauer. Folglich müssen sie in Hinblick auf den konkreten Einzelfall ausgelegt werden.

> *„Die Trias rechtlicher, organisatorischer und technischer Kenntnisse ist Leitlinie und Maßstab sämtlicher Überlegungen zur gesetzlich geforderten Fachkunde (§ 4f Abs. 2 Satz 1) des Beauftragten. […] Ein festes Anforderungsprofil gibt es […] nicht. Ebenso wie die Bedingungen, unter denen sich die Verarbeitung abspielt, variieren, verändern sich auch die Erwartungen an den Beauftragten. Welchen Anforderungen er im Einzelnen genügen muss, lässt sich deshalb, ganz im Sinne des § 4f Abs. 2 Satz 2, nur sagen, wenn die je spezifischen Umstände seiner Tätigkeit feststehen.“*[160]

Allerdings lassen sich einige generelle Punkte zusammenfassen. Erstens ist zu beachten, dass sich das Anforderungsprofil durch eine ständige Weiterentwicklung der technischen Möglichkeiten fortlaufend ändert.[161] Aus dieser Tatsache ergibt sich die Pflicht des Datenschutzbeauftragten, sich ebenfalls fortlaufend fortzubilden.[162] Weiterhin hat der Beauftragte über genügend technische Kenntnisse zu verfügen, um die Verarbeitungsprozesse, die er beaufsichtigt, zu umreißen.[163] Jedoch dürfen die Anforderungen an seine rechtlichen oder technischen Kenntnisse nicht überstrapaziert werden und daher nicht mit ausgeprägten Spezialkenntnissen gleichgesetzt werden. Die Stellung des Datenschutzbeauftragten ist nicht ausschließlich Juristen oder Informatikern vorbehalten.[164]

Die Anforderung der Zuverlässigkeit lässt sich in eine subjektive und eine objektive Komponente zerlegen, die gleichwertig nebeneinander stehen. Der subjektive Teil bezieht sich auf die persönlichen Eigenschaften des Beauftragten und kann aus seinem bisherigen Verhalten geschlossen werden.[165] Bei der objektiven Komponente geht es hauptsächlich darum, Interessenskollisionen zu vermeiden. Eine vertrauenswürdige und verlässliche Datenschutzkontrolle setzt eine klare Trennung zwischen der verantwortlichen Stelle und dem Datenschutzbeauftragten voraus. Folglich müssen alle Personen ausscheiden, die direkt an dem Unternehmen beteiligt sind (z. B. Inhaber, Alleinaktionäre) oder aufgrund ihrer

> *„Position und Funktion nach berechtigt sind, die Grundsätze festzulegen, nach denen sich die verantwortliche Stelle bei ihrer Tätigkeit richten muss“*.[166]

[160] *Simitis*, in: Simitis, BDSG, § 4f, Rn. 84.
[161] *Simitis*, in: Simitis, BDSG, § 4f, Rn. 85.
[162] *Simitis*, in: Simitis, BDSG, § 4f, Rn. 87.
[163] *Simitis*, in: Simitis, BDSG, § 4f, Rn. 92.
[164] *Simitis*, in: Simitis, BDSG, § 4f, Rn. 93.
[165] *Simitis*, in: Simitis, BDSG, § 4f, Rn. 95.
[166] *Simitis*, in: Simitis, BDSG, § 4f, Rn. 98.

Darüber hinaus können sich auch aus der Bestellung von leitenden Angestellten zu nebenamtlichen Datenschutzbeauftragten Probleme ergeben. Vieles ist hier wiederum abhängig vom konkreten Einzelfall. Dennoch kann allgemein gesagt werden, dass

> *„eine Unvereinbarkeit […] grundsätzlich immer dann zu bejahen [ist], wenn es um Tätigkeiten geht, die mit der Verarbeitung personenbezogener Daten zusammenhängen oder sich auf sie auswirken.“*[167]

Dementsprechend dürften die Leiter der EDV-Abteilung, der Rechtsabteilung oder der Marketing-Abteilung im Allgemeinen als nebenamtliche Datenschutzbeauftragte ausscheiden.

Die Aufgaben des Beauftragten sind hauptsächlich in § 4g Abs. 1 S. 1 BDSG geregelt und zusammengefasst mit der allgemeinen Formulierung:

> *„Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin.“*

Darüber hinaus werden die zwei wichtigsten Pflichten konkret bezeichnet. Der Beauftragte hat die Datenverarbeitung zu überwachen und die hiermit beschäftigten Personen zu schulen (§ 4g Abs. 1 S. 4 Nr. 1 und 2 BDSG). Die Kontrollpflicht beinhaltet einerseits die Pflicht, die Gestaltung von Datenverarbeitungsprogrammen sowie deren ordnungsgemäße Anwendung unter Umständen durch unangemeldete Kontrollen zu überwachen. Andererseits ist der Beauftragte auch bei der Neugestaltung bzw. -einführung von Verarbeitungsprogrammen frühzeitig hinzuzuziehen, um evtl. datenschutzrechtlich gebotene Korrekturen vorzunehmen. Insbesondere der zweite Teil der Kontrollpflicht korreliert mit der Pflicht zur Vorabkontrolle gemäß § 4d Abs. 6 S. 1 BDSG. § 4d Abs. 5 BDSG definiert die Vorabkontrolle wie folgt:

> *„Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). Eine Vorabkontrolle ist insbesondere durchzuführen, wenn*
>
> 1. *besondere Arten personenbezogener Daten (§ 3 Abs. 9) verarbeitet werden oder*
> 2. *die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens,*
>
> *es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.“*

Beide Kontrollpflichten setzen eine umfassende Information des Datenschutzbeauftragten voraus. Diese darf sich nicht auf das konkrete Verarbeitungsprogramm beschränken, sondern muss ebenfalls Angaben über die Verwendungszwecke, Verarbeitungsabsichten, Geschäftszwecke und Organisation der verantwortlichen Stelle umfassen.[168] Je nach Anwendungsszenario erfordert dies von dem Beauftragten also durchaus weitgehende Auseinandersetzungen mit der Spam-Filterung, dem Internet-Routing und den Zielen der Teilnahme an dem MonIKA-Netz.

Die Schulungspflicht bezieht sich auf alle Personen, deren Tätigkeit mit der Verwendung personenbezogener Daten verbunden ist, und bezweckt, dass der Datenschutzbeauftragte die erforderlichen Kenntnisse an die Beschäftigten weitergibt.[169]

[167] *Simitis*, in: Simitis, BDSG, § 4f, Rn. 99.
[168] *Simitis*, in: Simitis, BDSG, § 4g, Rn. 84.
[169] *Simitis*, in: Simitis, BDSG, § 4g, Rn. 50, 51.

3.1.5.9 Die Meldepflicht nach § 42a BDSG

Eine nicht-öffentliche Stelle ist nach § 42a BDSG verpflichtet, die zuständige Aufsichtsbehörde (§ 38 BDSG) und die Betroffenen zu informieren, wenn bestimmte bei ihr gespeicherte Daten unrechtmäßig übermittelt oder auf sonstige Weise unrechtmäßig zur Kenntnis gelangt sind und schwerwiegende Beeinträchtigungen für die Rechte und schutzwürdigen Interessen der Betroffenen drohen. Die Informationspflicht ist nicht zu verwechseln mit der allgemeinen Meldepflicht nach § 4d BDSG für verantwortliche Stellen, die Verfahren zur automatisierten Datenverarbeitung anwenden wollen. Diese soll lediglich eine Zulässigkeitsprüfung der Anwendung automatisierter Verfahren ermöglichen[170] und kann unter den dort genannten Voraussetzungen entfallen.

Die Informationspflicht gem. § 42a BDSG entfällt unter keinen Umständen. Auch die Teilnahme an einem MonIKA-System beseitigt die Informationspflicht nicht. Ebenso ersetzt eine entsprechende Meldung an die MonIKA-Zentralstelle nicht die Meldung gegenüber der Aufsichtsbehörde.

Das BDSG bezieht sich in § 42a BDSG nur auf besonders sensible Daten. Bei den relevanten personenbezogenen Daten handelt es sich um solche

- besonderer Art nach § 3 Abs. 9 BDSG, d. h. solche über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben,
- die einem Berufsgeheimnis unterliegen,
- die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder
- zu Bank- und Kreditkartenkonten.

Wie bereits in Abschnitt 3.1.4.2.4.4 erwähnt, besteht bei den untersuchten Szenarien am ehesten im Rahmen des Spam-Filterns zur Botnetz-Erkennung die Notwendigkeit, derlei personenbezogene Daten zu verarbeiten. Für die unrechtmäßige Übermittlung anderer als der genannten Daten gilt die Informationspflicht nicht. Es finden sich jedoch spezialgesetzliche Regelungen für Bestands- und Verkehrsdaten nach § 3 Nr. 3 und Nr. 30 TKG sowie für Bestands- und Nutzungsdaten nach §§ 14, 15 TMG.

Die Informationspflicht besteht, sobald der verantwortlichen Stelle tatsächliche Anhaltspunkte dafür vorliegen, dass Daten unrechtmäßig übermittelt wurden oder auf andere Weise Nichtberechtigten zur Kenntnis gelangt sind und schwerwiegende Beeinträchtigungen für die Betroffenen drohen. Solche schwerwiegenden Beeinträchtigungen drohen, wenn über das bloße Offenbaren der Daten hinaus die Weitergabe, Veröffentlichung oder Nutzung in schädlicher Form, wie etwa zum Identitätsbetrug, droht.[171] Der betriebliche Datenschutzbeauftragte ist in die Prüfung des Vorliegens der schwerwiegenden Gefahr einzubeziehen.[172]

Neben der Information der Aufsichtsbehörde sind grundsätzlich ebenso unverzüglich die Betroffenen zu benachrichtigen. § 42a S. 2 BDSG schränkt dies jedoch insofern ein, als zunächst angemessene Datensicherungsmaßnahmen zu treffen sind. Es soll also zunächst die Schwachstelle beseitigt werden, um gegebenenfalls weitere Offenlegungen zu verhindern.[173] Sicherzustellen ist weiterhin zunächst, dass eine eventuelle Strafverfolgung durch die Benachrichtigung nicht mehr gefährdet wird. Sofern die Strafverfolgungsbehörden hierzu nicht in angemessener Frist Stellung nehmen, muss die

[170] *Klebe*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 4d, Rn. 3.
[171] *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 42a, Rn. 6.
[172] *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 42a, Rn. 5.
[173] *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 42a, Rn. 8.

verantwortliche Stelle sie dazu auffordern, um dann bis zum Eingang einer Antwort die Benachrichtigung aussetzen zu dürfen.[174]

Eine bestimmte Form der Information bzw. Benachrichtigung ist gesetzlich nicht normiert. Inhaltlich muss die Information der Aufsichtsbehörde die Möglichkeit geben zu überprüfen, ob auf den Datenschutzverstoß angemessen reagiert wird. Die Betroffenen müssen aufgrund der Benachrichtigung den Vorfall erkennen, verstehen sowie die Konsequenzen für sie persönlich abschätzen und gegebenenfalls geeignete Maßnahmen ergreifen können.[175]

3.2 Rechtsfragen bezüglich der Übermittlung der erhobenen Daten

Neben der eigentlichen Datenerhebung bei den Teilnehmern eines MonIKA-Systems ist immanent, dass diese Daten nicht nur erhoben und vorverarbeitet werden, sondern auch zur Fusion und Korrelation weitergeleitet werden. Hier stellen sich insbesondere Fragen der Pseudonymisierung und Anonymisierung.

3.2.1 Rechtsgrundlage für die Übermittlung an die zentrale Stelle

Jedes Stadium der Datenverarbeitung braucht eine Rechtsgrundlage[176], so dass zunächst untersucht werden muss, unter welchen Umständen auch die Weitergabe der Daten von einer Rechtsgrundlage gedeckt ist.

Die Übermittlung bereits erhobener Daten regelt das BDSG in § 28 Abs. 2 BDSG.

> *„Die Übermittlung oder Nutzung für einen anderen Zweck ist zulässig*
>
> 1. *unter den Voraussetzungen des Absatzes 1 Satz 1 Nummer 2 oder Nummer 3,*
> 2. *soweit es erforderlich ist,*
>
> a) *zur Wahrung berechtigter Interessen eines Dritten oder*
> b) *zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten*
>
> *und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat, oder*
>
> 3. *wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.“*

Die Übermittlung ist also immer dann zulässig, wenn bereits die Datenerhebung durch die Abwägung des § 28 Abs. 1 S. 1 Nr. 2 BDSG gerechtfertigt war. Da dies im MonIKA-Ansatz grundsätzlich der Fall sein kann, wären derart erhobene Daten auch an die Zentralstelle rechtmäßig zur weiteren Korrelation übermittelbar. Auch die Weitergabe von Daten aus allgemein zugänglichen Quellen, die besonders im Anwendungsszenario des BGB-Monitorings relevant sind, wäre danach zulässig.

Die weiteren Grundlagen der Übermittlung hängen von konkreten Faktoren ab. So ist eine Übermittlung nach § 28 Abs. 2 S. 1 Nr. 2 a) BDSG davon abhängig, wie das Monitoring-Netz ausgestaltet ist. Eine Übermittlung nach dieser Norm könnte zulässig sein

> *„soweit es erforderlich ist, zur Wahrung berechtigter Interessen eines Dritten […]“.*

[174] *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 42a, Rn. 10.
[175] *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 42a, Rn. 11.
[176] Kühling/Seidel/Sivridis, Datenschutzrecht, S. 106.

Die Einordnung in diese Alternative erscheint deshalb fraglich, weil Dritte im allgemeinen Sinne aller Rechtsnormen regelmäßig jedenfalls individualisierbar sein müssen.[177] Auch die einschlägige Kommentierung zum BDSG zählt stets konkrete Dritte als Beispiel auf.[178] Je nach Zielsetzung oder Ausformung der konkreten Systeme kann es an dieser Voraussetzung durchaus fehlen. Im Bereich der Erkennung von BGP-Routing-Anomalien wäre es etwa problematisch, wenn allein die Verbesserung der globalen Routing-Informationen bezweckt wird. Die gesichtslose Allgemeinheit im Sinne aller zu schützenden Netznutzer oder gar die völlig unverkörperte IT-Infrastruktur lassen sich nämlich kaum individualisierbaren Dritten im Sinne der Norm zuordnen.

Kaum anwendbar erscheint der § 28 Abs. 2 S. 1 Nr. 2 b) BDSG. Die Abwehr von Gefahren für die öffentliche Sicherheit ist weder Ziel eines der Anwendungsszenarien, noch lassen sich Anomalien im BGP-Routing, Botnetz-Verkehr oder die Absicherung von Unternehmensnetzen regelmäßig als Aspekte der öffentlichen Sicherheit verstehen. Für eine enge Auslegung des Begriffs der „öffentlichen Sicherheit“ spricht auch, dass das BDSG in diesem Aspekt von der früheren Formulierung „öffentliches Interesse“ zu der konkreten Bezeichnung „öffentliche Sicherheit“ gewechselt ist und so dem extensiven Gebrauchs der Rechtfertigung über „öffentliches Interesse“ begegnen wollte.[179]

Die Möglichkeit, die Daten zu Zwecken der wissenschaftlichen Forschung zu übermitteln, regelt schließlich § 28 Abs. 2 S. 1 Nr. 3 BDSG. Voraussetzung für eine solche Übermittlung an Beteiligte der IT-Sicherheitsforschung ist, dass die Forschungsinteressen die Interessen der betroffenen Person überwiegen und dass die Forschungszwecke nicht auch ohne diese personenbezogenen Daten verfolgt werden können. Aufgrund des grundsätzlichen Bedürfnisses der IT-Sicherheitsforschung nach mehr als synthetischen Daten ist ein solches Interesse nicht von der Hand zu weisen. Es muss aber stets geprüft werden, in welchem Maß die Daten ohne Personenbezug oder in pseudonymisierter Form ausreichen.

3.2.2 Datensparsamkeit, Pseudonymisierung und Anonymisierung

Ein wichtiges Element des MonIKA-Projekts ist die Verwirklichung von Datensparsamkeit und Datenvermeidung bei gleichzeitiger Bewahrung der Fähigkeit zur effizienten Korrelation der gesammelten Daten.

Das BDSG enthält in § 3 Abs. 6 und Abs. 6a Regelungen über die Pseudonymisierung und Anonymisierung. Zusätzlich verweist § 3a BDSG auf diese Verfahren als Werkzeuge der Datensparsamkeit. Beide Prinzipien sind damit Ausfluss des Prinzips der Datensparsamkeit[180], das allgemein verlangt, dass das Entstehen vermeidbarer Datensammlungen verhindert wird, insbesondere durch gezielten Einsatz datenschutzfreundlicher Technik.[181]

Die im BDSG enthaltenen Regelungen zur Datensparsamkeit sowie Pseudonymisierung und Anonymisierung sind zwar verpflichtende Vorschriften[182], sie schreiben aber nicht vor, in welchen Einzelfällen welche Art der Datenbehandlung zu erfolgen hat. Genauso wenig sieht die datenschutzrechtliche Literatur für diese Normen Durchsetzungsmöglichkeiten durch die Aufsichtsbehörden oder Rechte der Betroffenen auf Nutzung solcher datensparsamer Mechanismen gegeben.[183] Verbindlich vorgesehen ist beispielsweise die Anonymisierung nur in Einzelvorschriften wie bezüglich der Markt- und Meinungsforschung (§ 30, § 30a BDSG) oder der wissenschaftlichen Forschung (§ 40 BDSG).

[177] Vgl. etwa die Kommentierung zu § 328 BGB von *Grüneberg*, in: Palandt, § 328, Rn. 1.
[178] *Simitis*, in: Simitis, BDSG, § 28, Rn. 174 ff.
[179] *Simitis*, in: Simitis, BDSG, § 28, Rn. 190.
[180] *Plath*, in: Plath, BDSG Kommentar, § 28, Rn. 56.
[181] *Scholz*, in: Simitis, BDSG, § 3a, Rn. 3.
[182] *Scholz*, in: Simitis, BDSG, § 3a, Rn. 57.
[183] *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3a, Rn. 4.

Beide Mechanismen sind damit primär Gestaltungsprinzipien, die immer dort zum Tragen kommen, wo im Rahmen einer Abwägung eine Erforderlichkeitsprüfung verlangt wird.[184] Erst wenn sich im Rahmen einer solchen Erforderlichkeitsprüfung zeigt, dass das Ziel der Datenverarbeitung mit anonymisierten oder pseudonymisierten Daten erreichbar ist, werden entsprechende Verfahren auch rechtlich relevant. Unterbliebe nämlich eine mögliche Maßnahme der Datenminimierung, so wäre die Datenverarbeitung unangemessen und somit rechtswidrig. Die Rechtsgrundlagen im MonIKA-Szenario sind vor allem in § 109 Abs. 2 TKG, § 28 Abs. 1 S. 1 Nr. 1 BDSG und § 28 Abs. 1 S. 1 Nr. 2 BDSG zu finden. Diese Normen erlauben allesamt nur eine Verarbeitung im erforderlichen Maße, so dass im Bereich von Verfahren der Anomalieerkennung in verteilten Verfahren die Fragen der Datensparsamkeit von großer Relevanz sind. Die Regelungen des BDSG bezüglich Datensparsamkeit finden im Übrigen mangels speziellerer Normen im TKG auch auf die Datenverarbeitungsprozesse durch Telekommunikationsanbieter Anwendung.[185]

Auch die Datenschutz-Grundverordnung sieht in ihrer Entwurfsfassung in Artikel 23 weitergehende Verpflichtungen dahingehend vor, dass verantwortliche Stellen die Grundsätze des „Data Protection by Design“ (Datenschutz durch Technik) und „Data Protection by Default“ (datenschutzfreundliche Voreinstellungen) berücksichtigen müssen.

Schließlich ist dieses Prinzip auch in Gesetzen der deutschen Bundesländer verankert. Die Landesdatenschutzgesetze sind nur auf den öffentlichen Bereich anwendbar, so dass diese Gesetze insbesondere bei Monitoring-Netzen unter Führung oder Mitwirkung einzelner Bundesländer relevant werden. Im schleswig-holsteinischen Landesdatenschutzgesetz (LDSG S-H)[186] regelt etwa § 4 LDSG S-H diese Grundsätze. Darüber hinaus verlangt § 5 Abs. 1 LDSG S-H auch die Einhaltung von technischen und organisatorische Maßnahmen, zu denen die Einhaltung von sechs Schutzzielen gehört. Unter anderem wird dort die Nicht-Verkettbarkeit als Schutzziel definiert, wozu sich ebenfalls der möglichst minimale Einsatz von personenbezogenen Daten zählen lässt.

In diesem Abschnitt werden die angewandten Datenveränderungen auf ihre rechtliche Einordnung hin untersucht, um sie im Rahmen des Gebots der Datensparsamkeit beurteilen zu können.

3.2.2.1 Angewandte Datenveränderungen

Wie in Abschnitt 2 dargestellt, werden in den jeweiligen Szenarien ganz bestimmte Datenkategorien erhoben, die besonders geeignet sind, um nach einer Fusion und Korrelation Auffälligkeiten auszumachen. Tabelle 6 zeigt noch einmal zusammengefasst die erhobenen Daten in den jeweiligen Szenarien.

Tabelle 6: Bei den Teilnehmern erhobene Daten

Anwendungsszenario	Verarbeitete Daten
Botnetz-Erkennung	▪ Zeitpunkt der Registrierung als Spam ▪ Absender und Empfänger, Inhalt des Headers ▪ kompletter Nachrichteninhalt ▪ alle enthaltenen URLs
BGP-Routing	▪ Routing-Tabellen autonomer Systeme ▪ Traceroutes

[184] *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3a, Rn. 3.
[185] Kühling/Seidel/Sivridis, Datenschutzrecht, S. 72.
[186] Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen (Landesdatenschutzgesetz – LDSG –) vom 9. Februar 2000.

Enterprise-Monitoring	▪ IP-Adressen der Angreifer und Zielrechner ▪ angesprochene Ports ▪ genutzte Anwendung (FTP, HTTP, SMTP) ▪ sonstige Daten der Logfiles

Diese Daten werden der bei den Teilnehmern installierten MonIKA-Software zugänglich gemacht und dort vor der Weiterversendung an die Zentralstelle behandelt. Die folgenden Tabellen zeigen, wie die Daten vor ihrer Weiterleitung durch die MonIKA-Software verändert werden (Tabelle 7 für das Botnetz-Szenario, Tabelle 8 für das BGP-Routing sowie Tabelle 9 für das Enterprise-Monitoring).

Tabelle 7: Durch die MonIKA-Software durchgeführte Datenveränderung im Botnetz-Szenario

Datenveränderung im Botnetz-Szenario	
Inhalt des Headers	Löschung aller Daten bis auf Absender-IP-Adresse und Menge der verwendeten Schlüsselwörter
Inhalt der Nachricht	Berechnung der Zeichenanzahl, Worthäufigkeit nach Länge und Zeilenumbrüche und weitere Wortstatistiken
Enthaltene URLs	Anzahl der enthaltenen URLs, Top-Level-Domains und Unterverzeichnisse

Tabelle 8: Durch die MonIKA-Software durchgeführte Datenveränderung im BGP-Routing

Datenveränderung im BGP-Routing-Szenario	
AS-Routing-Tabellen	Update-Nachrichten im Klartext
Traceroutes	Zuordnung der IP-Adressen zu ihren AS-Nummern

Tabelle 9: Durch die MonIKA-Software durchgeführte Datenveränderung im Enterprise-Monitoring

Datenveränderung im Enterprise-Monitoring	
IP-Adressen	Klartext
Portnummern	Klartext
Zeitpunkt des Ereignisses	Klartext
Verwendete Protokolle	Klartext
Angesprochene Ressource	Klartext

Kritisch ist in diesem Zusammenhang insbesondere die fehlende Pseudonymisierung der IP-Adressen zu sehen. Auch die fehlende Behandlung von URLs oder AS-Nummern muss sich einer kritischen Überprüfung unterziehen lassen.

3.2.2.2 Rechtliche Würdigung der Datenveränderungen

Der Grundsatz der Datensparsamkeit verlangt von den Beteiligten eines Monitoring-Netzes also, so wenige personenbezogene Daten wie möglich zur Erreichung der Zwecke zu nutzen. Wie oben ausgeführt, besteht zwar keine Durchsetzungsmöglichkeit der Pflicht zur Anonymisierung oder Pseudonymisierung; bei Nichtnutzung dieser Techniken droht die Datenverarbeitung aber rechtswidrig zu werden. Die verantwortlichen Stellen im MonIKA-System haben daher bei der Datenverarbeitung zu prüfen, ob bestimmte Daten überhaupt erhoben werden müssen und in welcher Tiefe eine Verarbeitung notwendig ist.[187]

3.2.2.2.1 Anonymisierung

Das BDSG sieht zur Minimierung des Personenbezugs zwei Mechanismen vor: die Anonymisierung und die Pseudonymisierung. Ersteres minimiert den Personenbezug nicht nur, sondern hebt ihn gänzlich auf. Anonymisierte Daten sind nicht mehr personenbezogen.[188]

Eine Anonymisierung kommt bei den MonIKA-Anwendungsfällen insbesondere bei den Zahlwerten der Spam-Filter in Betracht. Wie dargestellt, wird aus dem Klartext der E-Mails eine Art Fingerabdruck für die Spam-Filter errechnet, der nur noch statistische Angaben bezüglich Worthäufigkeit, Anzahl der Zeichen usw. enthält. Während der Klartext also ohne Weiteres bestimmten Personen zuordenbar ist, ist dies bei den Zahlwerten möglicherweise nicht mehr der Fall.

Diese Fingerabdrücke der E-Mails sind dann anonymisiert, also ohne Personenbezug, wenn das Risiko, den Betroffenen zu bestimmen,

> *„so gering ist, dass es praktisch irrelevant erscheint“*.[189]

Ein Personenbezug bleibt hingegen so lange bestehen, wie mit Zusatzwissen wieder ein Bezug zu Personen hergestellt werden kann. Bezüglich der aus E-Mails errechneten statistischen Werte, ist damit also in zwei Schritten zu prüfen, ob es erstens überhaupt Zusatzwissen gibt, das den Personenbezug wiederherstellen kann, und zweitens, wie groß die Wahrscheinlichkeit ist, dass dieses Zusatzwissen auch eingesetzt wird. Die erste Frage lässt sich je nach Gestaltung der Verfahren durchaus bejahen: Die Möglichkeit einer Zuordnung zu Personen besteht zunächst über die Provider, die die Klartexte vor der Weitergabe an die MonIKA-Zentralstelle in die Zahlwerte umwandeln. Je nach Einsatzzweck der später zurückgesandten Ergebnisse wird in aller Regel das Original nicht gelöscht werden. Dies mag aus Gründen der Qualitätssicherung geschehen, um die Korrelationstechniken der MonIKA-Zentralstelle auf ihre Wirksamkeit hin zu untersuchen. Ein anderer Grund wäre darin denkbar, dass die Provider oder sonstige Teilnehmer nicht bloß daran interessiert sind, durch die zurückerhaltenen Muster ihre eigenen Filter zu verbessern, sondern die als Spam klassifizierten Muster wieder den ursprünglichen E-Mails zuzuordnen, um etwa die IP-Adresse des Absenders zu ermitteln oder um den Absender darüber zu informieren, dass von seiner Adresse aus Spam verschickt wird. Was auch immer die Gründe sein mögen: Solange die Absender dieser Zahlwerte die Originale vorhalten und Zuordnungsmöglichkeiten vorhanden sind, existiert für die Teilnehmer unproblematisch ein Zusatzwissen, das die Zuordnung der Zahlenwerte zu einer Person ermöglicht.

Für die Zentralstelle führt dieses Zusatzwissen aber nur dann zu einem Personenbezug, wenn sie

> *„aus objektiver Sicht und mit nicht unverhältnismäßig großem Aufwand auf dieses Wissen zugreifen kann“*.[190]

---

[187] *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3a, Rn. 3.
[188] *Dammann*, in: Simitis, BDSG, § 3, Rn. 23.
[189] *Dammann*, in: Simitis, BDSG, § 3, Rn. 23.
[190] *Plath/Schreiber*, in: Plath, BDSG Kommentar, § 3, Rn. 59.

Ob dies der Fall ist, hängt sowohl von den vertraglichen als auch den faktischen Einflussmöglichkeiten der Zentralstelle auf die Teilnehmer ab. In solchen Szenarien, in denen die Zentralstelle die Daten nicht bloß vorverarbeitet und empfängt, sondern auch im Rahmen einer weitergehenden Dienstleistung die Betreuung der IT-Systeme bei den Teilnehmern übernimmt[191], ist dies vorstellbar. Ganz allgemein ist das Zusatzwissen Dritter in jedem Fall bei der Frage des Personenbezugs zu berücksichtigen, wobei hier nur solches Zusatzwissen berücksichtigt werden soll, das „vernünftigerweise“[192] eingesetzt werden kann und wird.

Eine andere Quelle für Zusatzwissen, das den Personenbezug wiederherstellt, kann für die Zentralstelle daraus resultieren, dass über die Fusion und Korrelation der einzelnen spezifischen Zahlwerte ein persönlicher Schreibstil oder Ähnliches extrapoliert wird. Es sind etwa Szenarien vorstellbar, in dem ein Provider die Aufgabe der Zentralstelle wahrnimmt. In solchen Fällen ist es durchaus denkbar, dass der E-Mail-Verkehr der Kunden in ähnliche Zahlenwerte aufgeschlüsselt wird und mit den Daten der Teilnehmer korreliert wird. Auf diese Weise könnte eine Zentralstelle die gemeldeten Daten einer Person zuordnen, ohne dass die eigentlichen Zuordnungstabellen der Teilnehmer dafür herangezogen werden müssten. Die Entscheidung pro oder contra Personenbezug richtet sich hier abermals danach, mit welchem Aufwand mögliches Zusatzwissen erlangt werden kann.

Unerheblich ist dabei, ob die Zuordenbarkeit zu einer Person beabsichtigt ist. Relevant ist allein der Aufwand, mit dem dies möglich wäre. In Zeiten von Big Data und hochgradigen Verschneidungsmöglichkeiten sind Systeme wie die im MonIKA-Projekt untersuchten Monitoring-Netze in großem Maße geeignet, auch aus scheinbar belanglosen Einzeldaten Erkenntnisse zu gewinnen. Dies gehört – für den Fokus auf Netzsicherheit – nicht zuletzt auch zu den Zielen des MonIKA-Projekts. Vor dem Hintergrund des bereits zitierten Volkszählungsurteils des Bundesverfassungsgerichts[193], das bereits 1983 feststellte, dass es vor dem Hintergrund der automatischen Massendatenverarbeitung kein belangloses Datum mehr gibt, muss die Frage nach tauglichen Anonymisierungstechniken in jedem Einzelfall neu gestellt werden.

3.2.2.2.2 Pseudonymisierung

Vor dem Hintergrund der soeben dargestellten Ergebnisse wird in vielen Fällen also statt einer Anonymisierung höchstens eine Pseudonymisierung vorliegen. Eine solche ist dann gegeben, wenn sich der Personenbezug unter Verwendung von Zusatzwissen – wie beispielsweise der Zuordnungsfunktion zwischen Pseudonym und Klartext – herstellen lässt.[194] Pseudonymisiert sind die Daten aber nur im Verhältnis zu der Stelle, die nicht über diese Zuordnungsfunktion verfügt. Im MonIKA-Szenario sind die Daten trotz Pseudonymisierung für die Teilnehmer also stets in vollem Maße personenbezogen. Der datenminimierende Effekt der Pseudonymisierung, insbesondere vor dem Hintergrund der Pflicht zu Datensparsamkeit, würde also nur für die Zentralstelle greifen, die nicht über die Zuordnungsfunktion verfügt.

Die Probleme, dass die Zuordnungsfunktion problemlos durch Korrelationsmöglichkeiten anderer Art ersetzt werden kann, sind bereits im Bereich der Anonymisierung angesprochen worden. Auch hier gilt, dass der Personenbezug von bestimmten Daten nur ausgeschlossen werden kann, wenn die

> *„Wahrscheinlichkeit, dass sie einer bestimmten Person zugeordnet werden können, so gering ist, dass sie nach der Lebenserfahrung oder der wissenschaftlichen Prognose praktisch ausscheidet“*.[195]

[191] Dieses Szenario wird unter dem Begriff „managed SOC“ in Abschnitt 5.1 aufgegriffen.
[192] Vgl. Erwägungsgrund 26 zur Datenschutzrichtlinie 95/46/EG sowie *Dammann*, in: Simitis, BDSG, § 3, Rn. 26 m. w. N.
[193] BVerfGE 65, 1.
[194] *Dammann*, in: Simitis, BDSG, § 3, Rn. 26.
[195] *Roßnagel/Scholz*, Datenschutz durch Anonymität und Pseudonymität – Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, S. 725.

Jede Pseudonymisierungstechnik muss sich daher dem Test stellen, mit welcher Wahrscheinlichkeit der Klartext zugeordnet werden kann. Für die bezüglich der Zahlwerte der E-Mail-Inhalte angewandten Umwandlungen mag diese Wahrscheinlichkeit gering sein. Die Rückrechnung pseudonymisierter IP-Adressen ist hingegen aufgrund der geringen Verteilung von IPv4-Adressen ohne weitere kryptographische Techniken sehr einfach und damit auch sehr wahrscheinlich.[196] Da der IPv4-Standard aufgrund der 32-Bit-Struktur maximal 4.294.967.296 mögliche IP-Adressen zulässt, wird die Aufdeckung durch einen Brute-Force-Angriff begünstigt.[197]

Die Artikel-29-Datenschutzgruppe diskutierte dementsprechend bereits in ihrer Stellungnahme WP 148, ob und wann gegebenenfalls die Entfernung einzelner Octets aus der IP-Adresse den Personenbezug aufheben kann.[198]

3.2.2.2.3 Resultate im MonIKA-Projekt

Dem Gebot der Datensparsamkeit durch Anonymisierung und Pseudonymisierung zu entsprechen, werden die MonIKA-Anwendungsszenarien bisher nur teilweise gerecht. Insbesondere die Verarbeitung der IP-Adressen, der URLs und AS-Nummern im Klartext bietet Raum für datensparsamere Techniken. Vor dem Hintergrund, trotz Pseudonymisierung noch die Vergleichbarkeit zu erhalten, ist die Frage nach weniger invasiven Verarbeitungsmethoden aber nicht trivial. Erste Erkenntnisse der Wissenschaft, wie die von Kerschbaum[199] entwickelten Techniken zu distanzerhaltenen Hashwertbildung, sind vorhanden.

3.3 Rechtsfragen bezüglich der Zentralstelle

Kernelemente des MonIKA-Systems sind die Fusion und die Korrelation der von den Teilnehmern erhaltenen Daten. Dabei ergeben sich zunächst die gleichen Fragen wie bei den Teilnehmern, also etwa der anhaltende Personenbezug oder die Rechtsgrundlage für die Verarbeitung. Darüber hinaus stellt die Anreicherung der Daten aus den einzelnen Quellen aber auch eine zusätzliche Herausforderung aus datenschutzrechtlicher Sicht dar. Diese Konzentration von Daten verlangt sodann auch ein höheres Maß an Vorkehrungen der IT-Sicherheit.

3.3.1 Bleibender und neuer Personenbezug

Die der Zentralstelle übersandten Daten sind bereits durch die Teilnehmer vorsortiert und vor allem nach Möglichkeit pseudonymisiert beziehungsweise anonymisiert. Bezüglich der durch eine MonIKA-Zentralstelle durchgeführten Berechnungen auf dieser Datenbasis ist bereits dargestellt, in welchem Umfang der Personenbezug durch Anonymisierung aufgehoben werden kann und inwieweit eine Pseudonymisierung dem Gebot der datensparsamen Verarbeitung in der Zentralstelle entgegenkommt.[200]

Soweit die Daten nach der Erhebung durch die Teilnehmer im Klartext an die Zentralstelle weiterübersandt werden, ist der Personenbezug unzweifelhaft auch für die Zentralstelle gegeben. Sofern der Personenbezug durch Anonymisierung effektiv aufgehoben wurde, so ist er zunächst auch für die Zentralstelle nicht vorhanden. Besonders interessant ist der ebenfalls soeben beleuchtete Fall, dass die Zentralstelle erst durch die angewandten Korrelationsmöglichkeiten die Daten auf bestimmte Personen beziehen kann, ohne dass dies vorher aufgrund der Einzeldaten möglich war.

---

[196] Vgl. hierzu *Xu, Fan, Ammar, Moon*, in: Prefix-Preserving IP Address Anonymization: Measurement-based Security Evaluation and a New Cryptography-based Scheme, Computer Networks 2002, S. 280-289.
[197] Zu Brute-Force-Angriffen als Zuordnungsfunktion vergleiche *Scholz*, in: Simitis, BDSG, § 3, Rn. 217b.
[198] Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen, 00737/DE WP 148, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_de.pdf, S. 20.
[199] *Kerschbaum*, Distance-Preserving Pseudonymization for Timestamps and Spatial Data, ACM Workshop on Privacy in the Electronic Society (WPES), 2007, http://www.fkerschbaum.org/wpes07.pdf.
[200] Siehe Abschnitt 3.2.2.

Hier ist in Bezug auf die konkret erhobenen und übersandten Daten im jeweiligen Einsatzszenario zu untersuchen, welche Möglichkeiten der Zentralstelle gegeben sind.

3.3.2 Rechtsgrundlage für die Verarbeitung in der Zentralstelle

So wie die Datenerhebung der Teilnehmer und die Weiterleitung an die Zentralstelle erfordert auch die dortige Datenverarbeitung eine eigene gesetzliche Grundlage oder die Einwilligung der Betroffenen.

Hinsichtlich einer möglichen Einwilligung ergibt sich nichts Abweichendes gegenüber den einleitenden Darstellungen.[201] Hinsichtlich der gesetzlichen Erlaubnistatbestände ist ebenfalls weitgehend auf die dortigen Ausführungen zu verweisen. Besonderheiten ergeben sich insoweit allerdings in zweierlei Hinsicht.

Zum einen dürfte der Rückgriff auf das TKG ausscheiden. Selbst wenn ein MonIKA-Netz gegeben wäre, das nicht nur aufseiten der Datenlieferanten Telekommunikationsdienstleister beinhaltet, sondern deren zentralen Auswertungsaufgaben ebenfalls durch einen solchen wahrgenommen würde, greift das TKG als Rechtsgrundlage nicht. Die entscheidende Norm, § 100 Abs. 1 TKG, rechtfertigt nämlich nur die Erhebung von

> *„Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer“.*

Der Rückgriff auf das TKG würde insoweit die zentrale Auswertung auf Daten von Telekommunikationsteilnehmern und Nutzern beschränken. Daten aus anderen Quellen deckt die Grundlage nicht. Im Rahmen von Enterprise-Monitoring-Szenarien wäre dies nachteilig. Zudem ist fraglich, inwieweit § 100 Abs. 1 TKG neben der Erhebung eigener Bestands- und Verkehrsdaten auch die Auswertung und Korrelation von fremden Bestands- und Verkehrsdaten umfasst. Die datenschutzrechtliche Literatur verneint dies tendenziell.[202] Die Sonderregelungen in § 100 Abs. 3 S. 3 und S. 4 TKG erwähnen zwar die Erstellung pseudonymisierter Datenzusammenfassungen, erlauben dies aber nur im Kontext von unrechtmäßiger Inanspruchnahme und Leistungserschleichung, nicht jedoch im Rahmen der Netzsicherheit. Da § 100 Abs. 3 S. 3 und S. 4 TKG keine Regelungen über Datensammlungen zu MonIKA-Zwecken enthalten, steht die Norm einer subsidiären Anwendung des BDSG auch nicht entgegen. Damit ist für die Datenverarbeitung der Zentralstelle der Rückgriff auf das BDSG möglich und nötig.

Zum anderen wird im Rahmen der Datenverarbeitung der Zentralstelle die Interessenabwägung des § 28 Abs. 2 S. 1 Nr. 1 i. V. m. § 28 Abs. 1 S. 1 Nr. 2 BDSG maßgeblich sein. Insoweit gleichen sich die gegenüberliegenden Interessen der verarbeitenden Stelle und der Betroffenen weitgehend. Hinzu kommt bei der zentralen Stelle natürlich das wirtschaftliche Interesse, die eigenen vertraglichen Verpflichtungen im MonIKA-Netz zu erfüllen. Aufseiten der Betroffenen kommt dem Interesse, im Rahmen der Datenfusion nicht Gegenstand von kaum greifbaren Profilbildungen zu werden, besondere Bedeutung zu. Die Grundsätze der Zweckbindung, Datensparsamkeit und Transparenz sind auch bezüglich der Datenverarbeitung bei der Auswertungszentralstelle zu berücksichtigen und können die Einschnitte in die Betroffenenrechte minimieren und so zu einer angemessenen und damit rechtmäßigen Umsetzung führen.

3.3.3 Rechtsgrundlage für die Rücksendung

Schließlich ist nach erfolgter Fusion und Korrelation auch die Rücksendung der Daten an die jeweiligen Teilnehmer von einer diesbezüglichen Ermächtigungsgrundlage abhängig. Hinsichtlich der Rechtsgrundlage ist die Rücksendung nicht anders zu bewerten als die ursprüngliche Übersendung. Grundlage für die Rücksendung ist ebenfalls § 28 Abs. 2 S. 1 Nr. 1 i. V. m. § 28 Abs. 1 S. 1 Nr. 2 BDSG.

---

[201] Siehe Abschnitt 3.1.4.1.
[202] *Braun*, BeckTKG-Komm, § 91, Rn. 19 und 20.

Es ergeben sich aber bezüglich der Abwägung einige Besonderheiten. Die ursprüngliche Datenerhebung und die nachfolgende Fusion der Daten in der Zentralstelle bargen insbesondere die Gefahr, dass Betroffene Gegenstand von Datenaggregationen zu vielfältigen Zwecken werden. Im Zusammenhang mit der Rücksendung der Erkenntnisse an die Teilnehmer, besonders im Bereich der Botnetz-Erkennung und des Enterprise-Monitorings, sind Reaktionen möglich, die den Einzelnen deutlich beeinträchtigen können. Denkbar wäre etwa, dass der Zugang der Betroffenen zu den Netzen bestimmter Provider gesperrt oder dessen IP-Adresse in den Firewalls der teilnehmenden Unternehmen in eine Sperrliste eingetragen wird. Das „Ob“ und „Wie“ solcher Reaktionen ist zwar nicht Gegenstand des MonIKA-Projekts, es ist aber zumindest allgemein ein Faktor, der im Rahmen der Abwägung der Interessen bei der Rücksendung relevant wird. Es muss gewährleistet werden, dass die Betroffenen nicht intransparent und ohne Kontroll- und Interveniermöglichkeiten Gegenstand solcher Reaktionen werden.

Relevant ist in diesem Zusammenhang auch die Frage, welche Erkenntnisse die Teilnehmer überhaupt erhalten. Die ursprünglich an die Zentralstelle übersandten Daten enthalten nur Daten aus dem eigenen Herrschaftsbereich: aus den eigenen Logfiles im Unternehmen, aus den E-Mail-Servern der Provider oder aus sonstigen eigenen Quellen. Diese werden aufseiten der Zentralstelle mit vergleichbaren Daten der anderen Teilnehmer angereichert und erlauben den Abgleich und die Verdichtung der ursprünglichen Daten auf hohem Niveau. Die danach zurückgesandten Daten enthalten also möglicherweise mehr Informationen als die ursprünglich erhaltenen Daten. Dies birgt unter Umständen die Gefahr, dass Unternehmen nicht nur die üblichen Einblicke in den Netzverkehr haben, sondern diesen Verkehr in einem viel größeren Maße in eine Beziehung zu ihren Nutzern oder Konkurrenten setzen können.

Diese Risiken und das daraus folgende Interesse der Betroffenen sind Folge der Zielsetzung des MonIKA-Ansatzes im Allgemeinen und damit grundsätzlich bereits bei der ursprünglichen Erhebung zu berücksichtigen. Sie treten aber besonders bei der Rücksendung zu Tage und sind deshalb in diesem Schritt mit besonderem Augenmerk abzuwägen. Eine enge Zweckbestimmung der Datenverwendung aufseiten der Teilnehmer und Datensparsamkeit können hier entschärfend wirken.

3.3.4 Anwendung des BDSG bei der Zentralstelle

Auch bezüglich der Datenverarbeitung der zentralen Stelle sind die weiteren Vorgaben des BDSG zu berücksichtigen. Dort haben insbesondere die Vorgaben der technischen und organisatorischen Maßnahmen sowie Fragen der Zweckbindung Bedeutung. Zur Vermeidung von Redundanzen wird soweit möglich auf die entsprechenden Ausführungen bezüglich der Teilnehmer in Abschnitt 3.1.5 verwiesen.

3.3.4.1 Direkterhebung und Informationspflichten nach § 4 Abs. 2 und 3 BDSG

Während bei den Teilnehmern die Direkterhebung jedenfalls noch teilweise denkbar ist, ist dies bei der Verarbeitung in der Zentralstelle systembedingt ausgeschlossen. Die Daten werden bei niemandem direkt erhoben, sondern von anderen Quellen gesammelt und an die Zentralstelle zur gemeinsamen Verarbeitung übersandt. Insoweit muss das Abweichen von dem Gebot der Direkterhebung in jedem Fall ebenso wie bei den Teilnehmern durch die Ausnahmebestimmungen des § 4 Abs. 2 S. 2 Nr. 2 b) BDSG gerechtfertigt werden.

Auch die Ausnahmen von der Benachrichtigungspflicht des § 33 BDSG werden aus denselben Gründen wie bei den Teilnehmern, d. h. keine Pflicht zur Namen- und Adressermittlung, zu bejahen sein. Aus diesen Gründen kann für eine genauere Darstellung auf Abschnitt 3.1.5.1 verwiesen werden.

3.3.4.2 Rechte der Betroffenen nach § 6 BDSG

Bereits in Abschnitt 3.1.2.2 wurde erarbeitet, dass in den meisten Anwendungsszenarien sowohl die Teilnehmer des MonIKA-Systems als auch die zentrale MonIKA-Einrichtung im Rahmen ihrer Monitoring- und Auswertungsaufgaben als verantwortliche Stellen anzusehen sind. Der Begriff der verantwortlichen Stelle ist vor allem auch Anknüpfungspunkt für die Verpflichtung zur Einräumung der Betroffenenrechte gemäß §§ 34 f. BDSG. Folglich können Betroffene auch gegenüber der Zentralstelle ihre Rechte geltend machen. Die Einzelheiten der konkreten Betroffenenrechte wurden bereits in Abschnitt 3.1.5.2 herausgearbeitet, auf den hier verwiesen wird.

Erwähnenswert an dieser Stelle ist zudem, dass die Zentralstelle gemäß § 6 Abs. 2 BDSG auch Ansprechpartner bezüglich Beschwerden ist, die sich auf Sachverhalte vor der Übermittlung an sie selbst, d. h. vor allem bei der ursprünglichen Datenerhebung durch die Teilnehmer, beziehen. Derartige Beschwerden hat sie an die jeweils zuständigen Teilnehmer weiterzuleiten.

Zuletzt ist auf die sogenannte Nachberichtspflicht des § 35 Abs. 7 BDSG hinzuweisen. Hiernach ist die MonIKA-Zentralstelle verpflichtet, all diejenigen Stellen zu unterrichten, an die Daten zur Speicherung weitergegeben wurden, wenn unrichtige Daten berichtigt, bestrittene Daten gesperrt oder Daten wegen der Unzulässigkeit der Speicherung gelöscht oder gesperrt wurden.

3.3.4.3 Die Schadensersatzpflicht nach § 7 BDSG

Es gelten gegenüber der Schadensersatzpflicht der Teilnehmer keine Besonderheiten, so dass grundsätzlich auf die Ausführungen in Abschnitt 3.1.5.3 verwiesen werden kann. Erläuternd sei erwähnt, dass die Zentralstelle auch verantwortliche Stelle entsprechend der Definition des § 3 Abs. 7 BDSG ist bzw. wird, sobald sie die ihr übermittelten Daten selbst verarbeitet oder nutzt und damit haftungspflichtig gem. § 7 BDSG ist.

3.3.4.4 Technische und organisatorische Maßnahmen nach § 9 BDSG

Bei Errichtung einer Zentralstelle für ein MonIKA-System sind die in § 9 BDSG sowie in der Anlage zu § 9 S. 1 BDSG normierten technischen und organisatorischen Maßnahmen zu beachten. Wie bereits in Abschnitt 3.1.5.4 erläutert, sind jeweils die „erforderlichen“ Maßnahmen zu treffen. Die konkreten Anforderungen der einzelnen Anwendungsszenarien müssen den konkreten Umsetzungen überlassen werden.

In Bezug auf die Zentralstellen ist von erhöhter Relevanz, dass nach Nr. 8 Anlage 1 zu § 9 BDSG grundsätzlich Maßnahmen zu treffen sind, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Diese Maßnahmen können jedoch unterbleiben, wenn Zweckänderungen gesetzlich zulässig sind.[203] Eine MonIKA-Zentralstelle, die gegenüber mehreren Teilnehmergruppen als Diensteanbieter auftritt und unter Umständen auch unterschiedliche Ziele verfolgt, müsste dementsprechend sicherstellen, dass die Daten getrennt gespeichert und analysiert werden. Daten von Teilnehmern aus dem Bereich Botnetz-Erkennung sollen daher nicht mit Daten aus dem Bereich Enterprise verschnitten werden, da ansonsten eine zweckwidrige Fusion von zu getrennten Zwecken erhobenen Daten droht. Insbesondere die Verschneidung von beruflichen Daten der Beschäftigten im Enterprise-Szenario mit kontextuell völlig abweichenden Daten aus privatem E-Mail-Verkehr kann derartige Maßnahmen gebieten.

3.3.4.5 File-Trennung nach § 30 BDSG

Bezugnehmend auf Abschnitt 3.1.5.5, in dem die Übermittlung der Daten von den Teilnehmern an die Zentralstelle und generelle Aspekte der Anwendbarkeit von § 30 BDSG in MonIKA-Systemen

[203] *Wedde*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 9, Rn. 97.

erläutert wurden, werden an dieser Stelle lediglich einige kurze Hinweise zu den Besonderheiten der File-Trennung aus der Sichtweise der Zentralstelle gegeben.

Sinn des MonIKA-Netzes ist es, dass die von einem Teilnehmer an die Zentralstelle mitgeteilten Daten durch die Daten der anderen Teilnehmer ergänzt und angereichert werden, bevor eine Rücksendung von der Zentralstelle an die jeweiligen Teilnehmer stattfindet. Die Daten werden in der Zentralstelle also nicht weitergehend anonymisiert, sondern angereichert und zurückübersandt. Darüber hinaus ist ebenfalls zu bedenken, dass, selbst wenn die Daten anonymisiert oder pseudonymisiert von den Teilnehmern an die Zentralstelle übermittelt werden, die Teilnehmer zumindest in den Fällen den Zuordnungsschlüssel behalten müssen, in denen nach einer eventuellen Rücksendung die Pseudonymisierung rückgängig gemacht werden soll. Aus diesem Grund stellen die von der Zentralstelle übermittelten Daten jedenfalls für die Teilnehmer regelmäßig keine anonymisierte Daten dar, und § 30 BDSG ist für diese Übermittlung nicht anwendbar.

3.3.4.6 Zweckbindung nach § 28 Abs. 5 und § 31 BDSG

Ein Dritter, dem Daten übermittelt worden sind, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Der Zweck ist ihm gemäß § 28 Abs. 5 S. 1 und 3 BDSG durch die übermittelnde Stelle mitzuteilen. Die Zentralstelle eines MonIKA-Systems ist im Verhältnis zu den Teilnehmern zunächst „Dritter“ i. S. d. § 28 Abs. 5 BDSG und muss sich dementsprechend an den von den Teilnehmern vorgegebenen Zweck halten. Allerdings gelten über den Verweis in § 28 Abs. 5 S. 2 BDSG zahlreiche Ausnahmen, auf die der Übermittelnde den Dritten im Zusammenhang mit der Zweckbindung hinzuweisen hat.[204] Bezüglich der Ausnahmeregelungen und ihrer Anwendbarkeit sei auf die Ausführungen zur Rechtmäßigkeit der Verarbeitung der Daten durch die Zentralstelle und zu den Voraussetzungen, unter denen eine Verarbeitung durch den Dritten auch zu anderen Zwecken erfolgen darf, unter Abschnitt 3.3.2 verwiesen. Die Übermittler – hier: die Teilnehmer – haben auch nicht die Möglichkeit, diese Ausnahmen durch einseitige Erklärung der Zentralstelle gegenüber auszuschließen oder zu begrenzen.[205]

3.3.4.7 Beschäftigtendatenschutz nach § 32 BDSG

Im Zusammenhang mit der Zentralstelle ergeben sich keine datenschutzrechtlichen Probleme im Bereich des Beschäftigtendatenschutzes nach § 32 BDSG. Die verschiedenen MonIKA-Szenarien beinhalten keine Monitoring-Aktivitäten bezüglich des internen Netzes der Zentralstelle. Folglich werden auch keine Kommunikationsdaten aus diesem System im Rahmen des MonIKA-Systems verarbeitet, wodurch in den persönlichen Bereich der Mitarbeiter der Zentralstelle eingegriffen werden könnte.

3.3.4.8 Der betriebliche Datenschutzbeauftragte nach § 4f BDSG

Abhängig von ihrer Größe bzw. der Anzahl ihrer Beschäftigten kann auch die Zentralstelle zur Bestellung eines betrieblichen Datenschutzbeauftragten verpflichtet sein. Da die Probleme, die sich im Rahmen der Bestellung ergeben können, identisch sind mit denen bei den Teilnehmern und da die Aufgaben des Beauftragten ausführlich dargestellt wurden, wird zur weiteren Information in Abschnitt 3.1.5.8 verwiesen.

3.3.4.9 Die Meldepflicht nach § 42a BDSG

Auch die Zentralstelle ist informationspflichtig. Es wird insofern auf die Ausführungen in Abschnitt 3.1.5.9 verwiesen.

[204] *Wedde*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 28, Rn. 161.
[205] *Wedde*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 28, Rn. 160.

4 Besondere Rechtsfragen

Neben den allgemeinen Ausführungen in Abschnitt 3 gibt es einige besondere Rechtsfragen, die im Rahmen von koordinierten Auswertungsnetzen Bedeutung erlangen. Diese Aspekte haben in den allgemeinen Rechtsfragen bezüglich der Teilnehmer und der Zentralstelle bereits Anklang gefunden, sind aber von so großer Bedeutung, dass sie an dieser Stelle herausgehoben untersucht werden.

4.1 Rücksendung der IP-Adressen

Grundprämisse des MonIKA-Systems ist ein Geben und Nehmen. Die Teilnehmer übersenden eigens erhobene Daten und erhalten diese Daten unter Anreicherung anderer Daten aufgewertet zurück. Während dies dem Ziel dient, die Erkennung von Anomalien durch eine Verbreiterung des Blicks zu verbessern, führt dies notgedrungen aber auch dazu, dass in den zurückerhaltenen Daten weitere Informationen enthalten sind. Diese waren einerseits vorher nicht zugänglich, und andererseits lassen diese nicht nur Rückschlüsse auf Anomalien in Netzen zu, sondern erlauben weitergehende Erkenntnisse über Mitarbeiter und Konkurrenten. Die damit verknüpften Rechtsfragen sind haftungsrechtlich relevant und von datenschutzrechtlichem Interesse.

Wie in Abschnitt 2 dargestellt, erhalten die Teilnehmer unter anderem die IP-Adresse möglicher Spam-Versender (zur Botnetz-Erkennung) oder sonstiger Angreifer (im Bereich Enterprise-Monitoring). Selbst wenn ein MonIKA-Teilnehmer nicht von einer solchen IP-Adresse aus angesprochen wurde, ist die Adresse in den Daten enthalten, die die Zentralstelle an alle Teilnehmer zurücksendet. Diese IP-Adresse könnte einem bestimmten Unternehmen oder einer Privatperson zugeordnet werden, was Unternehmen in die Lage versetzt, festzustellen, dass aus dem Netz eines Konkurrenten Angriffe durchgeführt werden. Daraus könnte beispielsweise der Schluss gezogen werden, dass dieser Konkurrent unzureichende IT-Sicherheitskonzepte einsetzt, die die Übernahme unternehmensinterner IT zulassen, oder dass er sogar aktiv in verdächtiger Weise auf Netze der übrigen Teilnehmer zugreift. Würde die Zentrale neben den Quell-IP-Adressen auch die Ziel-IP-Adressen zurücksenden, könnten die übrigen Teilnehmer sogar feststellen, welche Rechner der Konkurrenten Angriffen ausgesetzt waren oder welche Mitarbeiter in den eigenen Reihen betroffene Rechner benutzen.

Das Problem ist im Bereich der IP-Adresse deshalb so groß, weil eine Pseudonymisierung der IP-Adressen vor dem Hintergrund der aktuellen Firewall- und sonstiger Informationstechnik kaum sinnvoll möglich ist. Eine mögliche Reaktion auf die Meldung verdächtiger Quell-IP-Adressen wäre im Spam-Szenario etwa, E-Mails dieses Absenders nicht mehr zuzustellen, und im Enterprise-Monitoring, eine bestimmte IP-Adresse in den unternehmenseigenen Netzen über einen entsprechenden Eintrag in einer Firewall zu sperren. Dazu ist in beiden Fällen aber die IP-Adresse im Klartext notwendig. IT-Systeme, die vollständig auf Basis von pseudonymisierten oder verschlüsselten Daten rechnen, also gewissermaßen „geheim rechnen“, sind noch nicht für die Praxis geeignet. Eine erste funktionsfähige voll homomorphe Verschlüsselung wurde erst im Jahr 2009 entwickelt und verlangt bisher unverhältnismäßigen Rechenaufwand.[206] Auch die Verschlüsselung der IP-Adressen begegnet den gleichen Problemen. Zwar ist diese in Bezug auf die jeweiligen Übertragungen selbstverständlich, muss vor Eintragung in die Firewall aber ohnehin aufgehoben werden.

Um die Zwecke des MonIKA-Systems zu erreichen, ist in Bezug auf die IP-Adressen also an vielen Stellen der Klartext unverzichtbar. Ein Missbrauch dieser Daten ist daher über enge Zweckbindungen und Datensparsamkeit zu verhindern. Eine Maßnahme besteht daher darin, die gemeldeten Ziel-IP-Adressen regelmäßig nicht von der Zentrale zurückzuleiten. Auf diese Weise kann die Zentralstelle zwar eine Korrelation der anvisierten System vornehmen; um den so identifizierten Angreifer zu blockieren, ist diese Information allerdings nicht mehr nötig. Es reicht dort die Rückmeldung der

[206] *Gentry*, Fully homomorphic encryption using ideal lattices, STOC 2009, S. 169-178.

Quell-IP-Adresse. Derartige Prüfungen hinsichtlich Erforderlichkeit der Datenkategorien müssen in jedem konkreten Einsatzszenario eines MonIKA-Systems sowohl in Bezug auf die Notwendigkeit zur Übersendung an die Zentralstelle als auch auf die Notwendigkeit der Rückleitung an die Teilnehmer überprüft werden.

4.2 Pseudonymisierte Erkenntnisse wertlos ohne Zuordnungsschlüssel

Ein ähnliches Problem ergibt sich hinsichtlich der Zuordnung von pseudonymisierten Werten zu ihren entsprechenden Klartexten.

In Abschnitt 3.2.2 wurde dargestellt, dass im Botnetz-Szenario die Klartexte der E-Mails bei den Teilnehmern verbleiben und nur Zahlwerte der Spam-Nachrichten an die Zentralstelle weitergegeben werden. Ebenfalls wurde darauf hingewiesen, dass es für die Teilnehmer trotzdem sinnvoll sein kann, die Klartexte und ihre Zuordnung zu den jeweiligen abstrahierten E-Mail-Fingerabdrücken zu speichern. So könnte ein als Spam erkanntes Zahlenmuster dem Original zugeordnet werden und gegebenenfalls mit weiteren im Original vorhandenen Daten verknüpft werden, um etwa den Absender über eine mögliche Infektion zu informieren.

Dies stellt für ein System wie MonIKA aber insoweit ein Problem dar, als dass nur die Teilnehmer, die die Originale tatsächlich vorliegen haben, diese Zuordnung vornehmen können. Alle anderen Teilnehmer erhalten nur das als Spam erkannte Zahlenmuster und können mit diesen Mustern zwar ihre Spam-Filter anpassen, aber keine weiteren Schritte in Bezug auf E-Mail-Adresse oder Absender-IP-Adresse vornehmen.

Dies führt zu der Situation, dass entweder die Effektivität des Systems beeinträchtigt oder entgegen von Datensparsamkeitserwägungen die Zuordnung auch anderen Teilnehmern ermöglicht wird. Dieses Problem wird umso größer, je stärker der Schutz für den Personenbezug durch die Pseudonymisierung ist. Werden die Daten vor der Übergabe an die Zentralstelle nicht bloß durch Zahlenwerte abstrahiert, sondern durch vergleichbare Hashwerte ersetzt, so bieten die Erkenntnisse für diejenigen Teilnehmer, die nicht über die Zuordnung zu den Originalen verfügen, nicht nur weniger, sondern gar keine Erkenntnisse. Eine auf gehashten IP-Adressen erfolgte Berechnung der Zentralstelle mag Übereinstimmungen erkennen und zu der Erkenntnis gelangen, dass eine Anomalie vorliegt. Ohne die Möglichkeit, diese Erkenntnis einer konkreten IP-Adresse zuzuordnen und dementsprechende Maßnahmen in der lokalen Firewall zu treffen, ist diese Erkenntnis für die Teilnehmer aber in rein gehashter Form wertlos. Eine Datenerhebung und -verarbeitung, die keinen Mehrwert liefert, ist im Rahmen einer Abwägung[207] aber kaum als erforderlich zu bewerten.

4.3 Manipulation von Daten und Ergebnissen

Die Gefahr der Manipulation von Daten ist das Spiegelbild der Probleme in Abschnitt 4.1. Wenn die Zentralstelle aus den erhaltenen Daten eine Gesamtauswertung herstellt, auf deren Basis die Teilnehmer des Systems informiert werden, dann ist notwendige und auch beabsichtigte Folge das in Abschnitt 4.1 untersuchte Problem, dass Teilnehmer mehr Daten erhalten, als sie gesendet haben.

Gleichzeitig eröffnet dieser Mechanismus aber auch die Möglichkeit, dass die Übermittlung manipulierter Daten bestimmte Ergebnisse durch die Zentralstelle provoziert, die an die übrigen Teilnehmer weitergegeben werden, ohne tatsächlich Anomalien zu zeigen. Auf diese Weise könnte ein manipulierender Teilnehmer eine falsche Warnung erzeugen und seine Mitteilnehmer im MonIKA-System zu einer Reaktion veranlassen, beispielsweise die Sperrung einer IP-Adresse oder eines E-Mail-Absenders, die in keinem Bezug zu einer echten Bedrohung steht. So könnte über eine manipulierende Daten-Injektion erreicht werden, dass sich die IT-Systeme aller Konkurrenten etwa gegenüber der Kontaktmöglichkeit durch einen Auftraggeber sperren.

[207] Siehe Abschnitt 3.1.4.2.4.4 zu § 28 Abs. 1 Satz 1 Nr. 2 BDSG.

Derartiges Verhalten ist vor allem im Kontext der schuldrechtlichen Beziehungen von Bedeutung und daher primär eine Haftungsfrage.[208] Aus datenschutzrechtlicher Perspektive kann dies dann relevant werden, wenn die manipulierten Daten personenbezogen sind. Durch die provozierte Reaktion auf solche Falschdaten werden nicht nur die Interessen der Teilnehmer des MonIKA-Systems beeinträchtigt, sondern auch die Betroffenen hinter den missbrauchten Falschdaten. Das BDSG verlangt daher die Gewährleistung der bereits in den Abschnitten 3.1.5 und 3.3.4.2 dargestellten Betroffenenrechte, die in solchen Fällen der Falschmeldung ermöglichen, dass die Betroffenen wissen, welche Daten verarbeitet wurden, und so in die Lage versetzt werden, die Falschmeldung aufzudecken.

Schließlich ist hier auch § 7 BDSG von Bedeutung. Der Missbrauch personenbezogener Daten zur Wettbewerbsverzerrung ist eine nicht durch das BDSG gedeckte Datenverarbeitung, und der dadurch entstandene Schaden wäre nicht nur deliktsrechtlich, sondern auch aufgrund des § 7 BDSG zu ersetzen.

[208] Vergleiche insoweit die Ausführungen in Deliverable 5.1 „Rechtliche Herausforderungen der Informationsfusion und -klassifikation zur Erkennung von Anomalien in Internet-Infrastrukturen unter besonderer Berücksichtigung haftungs- und IT-rechtlicher Fragestellungen“ des Projektpartners ITM.

5 Besondere Anwendungsszenarien

Die Anwendungsszenarien des MonIKA-Projekts konzentrieren sich auf innerdeutsche Netze mit hauptsächlich privatrechtlicher Organisationsform, die zudem die notwendigen Daten selbst erheben. Nicht im Fokus des Projekts standen grenzüberschreitende Monitoring-Netze, Netze unter staatlicher Kontrolle und solche Konstellationen, in denen die Zentralstelle als Dienstleister auch die Datenerhebung bei den Teilnehmern übernimmt. Aufgrund der Bedeutung solcher Szenarien sollen diese hier zumindest dargestellt und um einen Ausblick auf die rechtlichen Herausforderungen ergänzt werden.

5.1 Das „managed SOC“-Szenario

Der erste Sonderfall ist ein Unterfall des Enterprise-Monitorings. Er unterscheidet sich von dem in Abschnitt 2.3 beschriebenen Szenario dadurch, dass die teilnehmenden Unternehmen über keine ausreichende Infrastruktur zur eigenständigen Installation und Wartung der MonIKA-Software in ihrem Unternehmen verfügen. In solchen Fällen ist es möglich, dass die Implementierung der notwendigen Software durch die Zentralstelle als Dienstleistung unternommen wird. Diese Dienste können gleichrangig neben anderen Dienstleistungen, die beispielsweise Server und Informationssicherheitsdienste vorhalten, geschehen; wahrscheinlicher ist aber, dass ein MonIKA-Teilnehmer sowohl die eigentliche Netzinfrastruktur als auch die darauf aufbauenden MonIKA-Systeme erhält. Eine solche Lösung kann als geleitetes Sicherheitscenter („managed Security Operation Center“, „managed SOC“) bezeichnet werden.

Hinsichtlich der allgemeinen datenschutzrechtlichen Beurteilung weicht ein solches Modell in einigen Bereichen von den in Abschnitt 3 dargestellten Ergebnissen ab. Die erste Frage stellt sich im Zusammenhang mit der Einordnung als verantwortliche Stelle. Während in den sonstigen Fällen die jeweiligen Teilnehmer die für die Teilnahme am MonIKA-System nötigen Daten durch ihre Technik selber erheben und im Anschluss an die zentrale Instanz weiterleiten, überlassen die Teilnehmer die Einrichtung und Wartung der Sensoren (Webserver, Firewall) komplett dem MonIKA-Dienstleister.

In diesen Fällen ist fraglich, ob die sich derart weitgehend einer technischen Mitwirkung entziehenden Teilnehmer noch als verantwortliche Stellen bezeichnet werden können. Zwar wird das Loggen des Netzverkehrs durch die MonIKA-Zentralstelle selbst unzweifelhaft eine Datenerhebung sein. Dies erfolgt aber auf den ersten Blick ohne Mitwirkung der Teilnehmer, so dass die datenschutzrechtliche Verantwortlichkeit für diese „fremde Verarbeitung in eigener Sphäre“ näher untersucht werden muss.

Wie die allgemeinen Ausführungen in Abschnitt 3.1.2 gezeigt haben, ist für die Einordnung als „verantwortliche Stelle“ entscheidend, wer über Zweck und Mittel entscheidet. Relevant ist bezüglich des „managed SOC“ nun, welches Maß an Zweck- und Mittelentscheidung zu fordern ist, um den Bereich der eigenen Verantwortlichkeit zu erreichen. Die Artikel-29-Datenschutzgruppe hat in einer Stellungnahme zu dieser wesentlichen Frage ausgeführt:

> *„[…] While determining the purpose of the processing would in any case trigger the qualification as controller, determining the means would imply control only when the determination concerns the essential means.“* [209]

Grundsätzlich ist also die Festlegung des Zwecks der wichtigste Indikator für die Einordnung als verantwortliche Stelle, und diese erfolgt, trotz technischer Durchführung des eigentlichen Loggings, durch den Teilnehmer selbst. Er legt fest, dass er zum Zweck der Teilnahme an einem koordinierten Monitoring-Netz Daten verarbeiten (lassen) möchte. Im MonIKA-System wäre also jeder MonIKA-Teilnehmer eine verantwortliche Stelle, da dieser den Zweck eigenverantwortlich vorgibt. Die reine Fokussierung auf die Zweckentscheidung scheint auf den zweiten Blick allerdings nicht mit der

[209] Opinion 1/2010 on the concepts of „controller“ and „processor“, 00264/10/EN WP 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf, Fn. 21, S. 14.

Vorgabe vereinbar, dass ein „controller“ auch über die Mittel entscheiden muss. Die Artikel-29-Datenschutzgruppe hat dazu im Zusammenhang mit den obigen Ausführungen ergänzend Stellung bezogen. So heißt es in der Stellungnahme des Weiteren:

> *„[…] where there is a good definition of purposes, but little or even no guidance on technical and organizational means […] the data controller should be fully informed about the means used.“*

Daraus lässt sich der Schluss ableiten, dass allein das Wissen um die eingesetzten technischen Mittel bereits als „Wahl der technischen Mittel“ im Sinne der Richtlinie ausreicht. Dieses Ergebnis überzeugt auch wertungstechnisch: Der Teilnehmer kann zwar nicht die eingesetzten Mittel direkt bestimmen. Dies muss er der MonIKA-Zentralstelle überlassen, damit diese ihre zugesicherten Auswertungen durchführen kann. Der Teilnehmer bestimmt die eingesetzten technischen Mittel aber jedenfalls mittelbar, indem er sich für konkrete Dienstleister entscheidet. Die technische Mittelwahl folgt schlicht aus der Wahl eines konkreten Anbieters. Im Sinne der Datenschutzrichtlinie sowie der Artikel-29-Datenschutzgruppe sind damit beide Voraussetzungen erfüllt. Wer an einem Detektionsnetz wie dem MonIKA-System teilnimmt, gibt zum einen das Ziel der Datenverarbeitung vor: Erkennung von IT-Bedrohungen. Zum anderen liegt in der Wahl des MonIKA-Anbieters aber auch die technische Mittelwahl, nämlich die Wahl der Mittel eben dieses Anbieters. Damit ist auch in solchen Fällen, in denen ein Teilnehmer ohne eigene aktive Mitwirkung MonIKA-Technik in seinem Herrschaftsbereich einsetzen will, dieser als verantwortliche Stelle zu qualifizieren.

Die Zentralstelle, die dementsprechend nun noch deutlicher als in den klassischen Anwendungsszenarien über die Schritte der Datenverarbeitung entscheidet, ist in „managed SOC“-Szenarien ebenfalls als „verantwortliche Stelle“ zu klassifizieren. Ein bloße Auslagerung von internen Verarbeitungsschritten kann hier in keinem Fall mehr angenommen werden, da die „managed SOC“-Lösung gerade deshalb gewählt wird, weil die Teilnehmer die IT-Sicherheit eben nicht eigenverantwortlich durchführen können. Für die Einordnung des Dienstleister als reine „Hilfskraft“ bleibt hier also noch weniger Raum als in den Fällen, in denen die Teilnehmer die MonIKA-Software eigenverantwortlich einsetzen und warten.[210] Stattdessen muss man die Wahrnehmung dieser Elemente der IT-Sicherheit als umfängliches Outsourcing[211] ansehen, in welchem das Weisungsrecht der Auftraggeber in einem solchen Maß zurücktritt, dass eine Auftragsdatenverarbeitung ausscheidet.

Demzufolge ist auch die Datenerhebung und -weiterleitung nicht anders zu bewerten, da die Teilnehmer physische Kontrolle über die Datenträger haben, die die Dienstleister in ihren IT-Systemen installieren. Auch ändert die Installation der MonIKA-Software in den Systemen der Teilnehmer nichts daran, dass die Übersendung an die Zentralstelle eine Weitergabe von Daten aus der Sphäre eines Verantwortlichen in die eines anderen darstellt. Insofern ist die Datenerhebung keine rein interne Angelegenheit des Dienstleisters, die sich vermeintlich in einem Beschaffen der Daten erschöpft.

Im Rahmen einer solchen Dienstleistung sind sodann aus Sicht des Datenschutzes gewisse Anforderungen an die zugrundeliegenden Vertragsgestaltungen zu stellen. Zwar gelten die Vorgaben der Auftragsdatenverarbeitung in § 9 BDSG nicht. Dies entbindet die Unternehmen, die sich für den Einsatz eines „managed SOC“-Modell entscheiden, aber nicht davon, die üblichen Anforderungen an Datenschutz und Datensicherheit zu berücksichtigen. Der Einsatz eines „managed SOC“ ist dabei nicht anders zu bewerten als jede andere Maßnahme, die personenbezogene Daten verarbeitet. Der Nutzer einer „managed SOC“-Lösung ist also beispielsweise nach wie vor für die Umsetzung und Einhaltung der in § 9 BDSG geforderten technischen und organisatorischen Maßnahmen verantwortlich. Hier dürfte vor allem im Bereich der Weitergabekontrolle nach Nr. 4 der Anlage zu § 9 S. 1 BDSG eine genaue Prüfung notwendig sein. Besonders vor dem Hintergrund, dass nun nicht mehr eigene

[210] Siehe dazu abermals ausführlich die Darstellung in Abschnitt 3.1.2.
[211] Vgl. zum Outsorcing *Plath*, in: Plath, BDSG Kommentar, § 11, Rn. 37 m. w. N.

Mitarbeiter, sondern fremde Mitarbeiter die Details der Erhebung, Pseudonymisierung und Weiterleitung konfigurieren, ist dies angezeigt.

Besonders interessant ist die Frage, wie damit umgegangen wird, dass im „managed SOC"-Modell Erhebung und Auswertung in einer Hand liegen. Während in den üblichen Anwendungsszenarien der Gefahr der Zweckentfremdung auch dadurch begegnet wird, dass die Zentralstelle nur weitgehend anonymisierte und pseudonymisierte Daten erhält, ist die Zentralstelle im „managed SOC"-Modell jedenfalls theoretisch deutlich eher in der Lage, die pseudonymisierten Daten den Klartexten zuzuordnen. Während ansonsten nur die Teilnehmer die Zuordnung der gelieferten Daten zu den dahinterstehenden Klartexten vornehmen können, obliegt nun die gesamte Erhebung, Zuordnung, Pseudonymisierung, Übersendung und Auswertung einem zentralen Dienstleister. Hier ist also mit größter Sorgfalt sicherzustellen, dass die Zentralstelle nicht mehr Daten erhält, als sie benötigt, und dies durch organisatorische und technische Maßnahme in den Einrichtungen und Systemen der Teilnehmer realisiert. Auf eine Pseudonymisierung und Anonymisierung sollte auf jeden Fall nicht deshalb verzichtet werden, nur weil die Zentralstelle auch technisch an der Erhebung mitwirkt.

5.2 Monitoring-Netze im Konzernverbund

Bereits im Zusammenhang mit Rechtsfragen um die „verantwortliche Stelle"[212] wurde darauf hingewiesen, dass der Einsatz von Monitoring-Netzen in Konzernverbänden rechtliche Sonderfragen aufwirft.

Hinsichtlich der allgemeinen Umsetzung ändert sich zunächst nichts, mit der Ausnahme, dass die zentrale Auswertungsstelle zu den Teilnehmern in einem konzernrechtlichen Vertragsverhältnis steht. Diese Konstellation ähnelt der des „managed SOC" im vorhergehenden Abschnitt. Hier wie dort ist der Einsatz der Software in den IT-Bereichen der Teilnehmer nicht vollständig unter der Kontrolle der Teilnehmer. Zwischen einer völlig autarken Implementierung, wie sie in den Anwendungsszenarien beschrieben ist, und einer vollständig fremdbestimmten Implementierung, wie sie beim „managed SOC" durchgeführt wird, steht die Umsetzung in einem Konzernverbund in der Mitte. Die einzelnen Teilnehmer können durchaus eigene IT-Abteilungen haben, die die MonIKA-Software eigenverantwortlich einsetzen. Je nach Ausformung der konzernrechtlichen Abhängigkeiten und Einflussmöglichkeiten der Konzernmutter sind aber auch Elemente des „managed SOC" enthalten.

Je nach Ausprägung des konzernrechtlichen Beherrschungsverhältnisses ergeben sich also durchaus die gleichen datenschutzrechtlichen Bedenken, was die Trennung der Datenbestände und die Möglichkeit der Zuordnung angeht. Hier ist ebenfalls besonders darauf zu achten, dass die Konzernmutter nicht mehr Daten erhält, als sie zu MonIKA-Zwecken benötigt. In diesem Zusammenhang ist festzuhalten, dass die Konzerntöchter trotz ihrer konzernrechtlichen Verknüpfung datenschutzrechtlich selbstständig sind und insbesondere selbst verantwortliche Stellen bleiben. Die Weitergabe der in ihren Systemen erhobenen Daten an die Konzernmutter muss daher stets eigenverantwortlich überwacht und abgesichert werden.

Hinsichtlich der Rechtsgrundlage der Datenerhebung in den Konzerntöchtern kommt bei einer Anwendung des BDSG hinzu, dass die Rechtfertigung der Datenerhebung allein aus Interessen des Konzernwohls nicht ausreicht.[213] Es gibt kein Konzernprivileg im Datenschutzrecht.[214] Ähnliche Anmerkungen sind bezüglich des Interesses an der Versendung der Daten an die Konzernmutter zu machen. Auch hier reicht der Verweis auf den Konzern als „homogene Datenschutzzelle"[215] nicht aus.

[212] Siehe Abschnitt 3.1.2.4.
[213] *Schulz*, in: Die (Un-)Zulässigkeit von Datenübertragungen innerhalb verbundener Unternehmen, BB 2011, S. 2554.
[214] *Plath*, in: Plath, BDSG Kommentar, § 28, Rn. 73 m. w. N.
[215] *Simitis*, in: Simitis, BDSG, § 28, Rn. 177.

5.3 Bundesweite Monitoring-Netze unter staatlicher Kontrolle

Das Bundesministerium des Innern hat bereits im März 2013 den Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz[216]) erarbeitet, das in weiten Teilen Inhalte der ebenfalls geplanten Cybersecurity-Richtlinie[217] vorwegnimmt und eine Umsetzung dieser darstellt. Es sieht im Wesentlichen die Änderung des BSI-Gesetzes dahingehend vor, dass das Bundesamt für Sicherheit in der Informationstechnik zur zentralen Meldestelle für Sicherheitsvorfälle bei Betreibern kritischer Infrastrukturen in Deutschland wird. Zusätzlich regelt es eine eigene Kompetenz des BSI zur Sammlung und Auswertung derjenigen Informationen, die zur Abwehr von Gefahren für die IT-Sicherheit notwendig sind.

Der Entwurf enthält als zentrale Änderung die Einführung des § 8b des geplanten Gesetzes. Danach wird das BSI zur zentralen Meldestelle für Betreiber kritischer Infrastruktur. Nach § 8b Abs. 2 des Entwurfs hat das Bundesamt

> *„zur Wahrnehmung dieser Aufgabe die […] wesentlichen Informationen […] zu sammeln und auszuwerten“.*

Diese Norm kann je nach Lesart als Ermächtigungsgrundlage für das Sammeln und Fusionieren von Daten angesehen werden, wie sie in Monitoring-Netzen nach MonIKA-Art vorgesehen sind. Diese Norm bezieht sich aber nicht auf die Erhebung personenbezogener Daten. Wenn diese Vorschrift als Ermächtigungsgrundlage im Sinne des § 4 Abs. 1 BDSG gelten soll, muss sie eine „andere Rechtsvorschrift“ im dortigen Sinne sein. Die datenschutzrechtliche Literatur verlangt dafür allerdings die Einhaltung enger Voraussetzungen. So schreibt *Weichert*[218]:

> *„Aus der Aufgabe allein kann noch nicht auf eine Befugnis zum Grundrechtseingriff geschlossen werden. Reine Aufgabennormen zur Informationsverarbeitung oder zur Zusammenarbeit oder zur Amtshilfe genügen nicht. Ein Mindestmaß an Bestimmtheit bzgl. Zweck, verarbeitende Stelle und Art der Verarbeitung muss aus der Rechtsvorschrift hervorgehen. Je sensibler die Verarbeitung für die Betroffenen ist und je präziser die Verarbeitung beschrieben werden kann, desto klarer muss die Norm sein.“*

Vor diesem Hintergrund muss sich der Entwurf des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme klar die Kritik gefallen lassen, dass der geplante § 8b Abs. 2 BSIG weder den Zweck der Verarbeitung nennt oder überhaupt auf einen etwaigen Personenbezug der Daten eingeht noch die Verarbeitungsschritte in irgendeiner Form beschreibt. Damit muss der Abs. 2 als Aufgabennorm hingenommen, als Ermächtigungsgrundlage aber abgelehnt werden. Dies ist umso erstaunlicher vor dem Hintergrund des bereits bestehenden § 5 BSIG. Dort regelt das BSIG sehr detailliert und unter Berücksichtigung eines möglichen Personenbezugs der Daten die automatische Erhebung von Protokolldaten sowie die automatische Auswertung von Kommunikationsschnittstellen des Bundes. Eine ähnliche Regelungsdichte lässt der Entwurf der Änderungen des BSIG in Bezug auf die geplante Einbindung von Betreibern kritischer Infrastrukturen leider vermissen. In der Begründung zu dem Entwurf heißt es dazu schlicht, dass die Meldungen regelmäßig rein technischer Natur sein würden, ein Personenbezug deshalb praktisch nicht bestehe und notfalls auf die normalen Regelungen des Datenschutzes zurückzugreifen sei.[219]

---

[216] Referentenentwurf des Bundesministeriums des Innern, Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vom 05.03.2013, im Internet: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_it-sicherheitsgesetz.pdf?__blob=publicationFile.

[217] Siehe dazu gleich im Anschluss in Abschnitt 5.4.

[218] *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 4, Rn. 3.

[219] Referentenentwurf des Bundesministeriums des Innern, Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vom 05.03.2013, S. 21, im Internet: https://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_it-sicherheitsgesetz.pdf?__blob=publicationFile.

Mit § 8b Abs. 2 regelt das geplante Gesetz zudem auch nur die eine Seite des Systems, nämlich die der Zentralstelle. Über eine mögliche Ermächtigungsgrundlage für die meldepflichtigen Stellen zu Erhebung und Weitergabe der für das BSI interessanten Daten schweigt der geplante Entwurf, soweit es Daten mit Personenbezug betrifft.

Als Ermächtigungsgrundlage können im IT-Sicherheitsgesetz am ehesten die geplanten § 8b Abs. 4 und Abs. 5 angesehen werden. Dort werden die Betreiber kritischer Infrastrukturen verpflichtet,

> *„über die Warn- und Alarmierungskontakte nach Absatz 3 schwerwiegende Beeinträchtigungen ihrer informationstechnischen Systeme […] unverzüglich an das Bundesamt zu melden" (Abs. 4),*

oder, falls solche Verpflichtungen bereits in Bezug auf andere Stellen oder Behörden bestehen,

> *„Meldungen zu erheblichen IT-Sicherheitsvorfällen im Sinne von Absatz 4 unverzüglich an das Bundesamt weiterzuleiten" (Abs. 5).*

Beide Normen beziehen sich abermals nicht auf die Meldung personenbezogener Daten. Vor dem Hintergrund der soeben dargestellten Voraussetzungen stellt sich die Frage, warum § 8b Abs. 4 und 5 weder den Zweck der Verarbeitung nennen noch überhaupt auf einen möglichen Personenbezug der Daten eingehen oder die Verarbeitungsschritte in irgendeiner Form beschreiben. Mangels klarer Regelungen im geplanten IT-Sicherheitsgesetz bliebe nur der Rückgriff auf § 28 Abs. 2 Nr. 2b BDSG, der zwar die Verarbeitung zu Zwecken der öffentlichen Gefahrenabwehr regelt, aber zwei Schwachpunkte aufweist: Zum einen sattelt er die Berechtigung zur Übermittlung nur auf eine vorherige rechtmäßige Erhebung auf, und zum anderen ist fraglich, ob das IT-Sicherheitsgesetz nur solche Fälle erfassen will, die unter die Abwehr von Gefahren für die staatliche Sicherheit fallen. Letzteres würde den Anwendungsbereich des IT-Sicherheitsgesetzes wohl über die eigene Zielsetzung hinaus einengen.

Der Entwurf sieht weiter einzelne Änderungen anderer Gesetze vor, so etwa die Einfügung eines § 109a Abs. 4 TKG, wonach Telekommunikationsdiensteanbieter Beeinträchtigungen von Telekommunikationsnetzen und -diensten, die zu einer Störung der Verfügbarkeit der Dienste oder zu einem unerlaubten Zugriff führen können, der Bundesnetzagentur mitteilen müssen und die Bundesnetzagentur zur Unterrichtung des BSI verpflichtet wird. Auch diese Norm hat allerdings mehr Charakteristika einer Aufgabennorm als einer bestimmten Rechtsgrundlage zur Erhebung und Weiterleitung von personenbezogenen Daten. Der geplante Abs. 4 gibt nicht einmal grob darüber Auskunft, welche Daten in diesen „Mitteilungen" enthalten sein können und müssen. Der geplante § 109a Abs. 4 TKG zeigt zudem, dass das oben dargestellte Credo des Entwurfs, es würden regelmäßig keine personenbezogenen Daten betroffen sein, nicht konsequent ist. In Satz 3 der geplanten Erweiterung des § 109 TKG wird den Diensteanbietern die Pflicht auferlegt, ihre Nutzer über die Störungen zu informieren, wenn diese Störung von Systemen der Nutzer ausgehen. Die zeigt deutlich, dass in vielen Fällen ein Personenbezug herstellbar ist, und steht im Widerspruch zu den Erwägungen in der Begründung des Entwurfs.

Aus Gründen der Rechtssicherheit wäre es insgesamt sinnvoll, entsprechende Ermächtigungsgrundlagen samt konkreter Zweckbindung und Verfahrensbeschreibungen jeweils bezüglich des BSI als auch der meldepflichtigen Stelle in den Entwurf des Gesetzes aufzunehmen, anstatt derartige Rechtsgrundlagen im BDSG und TKG zu ergänzen.

5.4 Monitoring-Netze im europaweiten Einsatz

Der soeben dargestellte Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme fußt in vielen Bereichen auf einem Vorschlag für eine Richtlinie zur Erhöhung der Netz- und Informationssicherheit in der Union[220], der ein europäisches Cybersecurity-Netz etablieren will.

[220] Vorschlag für eine Richtlinie zur Erhöhung der Netz- und Informationssicherheit in der Union vom 07.02.2013 2013/0027 (COD)), im Internet: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_de.pdf.

Der aktuell diskutierte Vorschlag sieht in dem Cybersecurity-Netz die folgenden Beteiligten und Rollen vor:

Auf unterster Ebene befinden sich die Marktteilnehmer, Diensteanbieter und öffentlichen Stellen, die Sicherheitsvorfälle melden müssen und zu Maßnahmen für IT-Sicherheit verpflichtet werden. Zu diesen Stellen zählt die Richtlinie nach Art. 3 Abs. 8 Anbieter von Diensten der Informationsgesellschaft und Betreiber kritischer Infrastrukturen. Ausgenommen von den in Art. 14 vorgesehenen Sicherheitsanforderungen einschließlich einer Meldepflicht sind dabei nach Art. 1 Abs. 3 sowohl Unternehmen, die öffentlichen Kommunikationsnetze betreiben, als auch sogenannte Vertrauensdiensteanbieter nach Art. 3 Abs. 11, also Anbieter von Diensten im Zusammenhang mit elektronischen Signaturen, elektronischen Dokumenten, elektronischen Zustelldiensten o. Ä. Für diese gibt es jeweils Sonderregelungen. Nach Art. 14 Abs. 8 gelten die Sicherheitsanforderungen inklusive Meldepflicht nicht für Kleinstunternehmen.[221]

Auf der nächsten Ebene sieht die Richtlinie in Art. 6 die Einrichtung zentraler, nationaler Behörden vor. Diese Zentralstellen sammeln die gemeldeten Informationen, sollen die Einhaltung von Sicherheitsstandard bei den meldepflichtigen Stellen überwachen und durchsetzen und werten die gesammelten Informationen für eine übergeordnete Gefahrenanalyse für die nationale Infrastruktur aus. Ihnen soll nach Art. 15 der Richtlinie darüber hinaus auch die Befugnis eingeräumt werden, von den meldepflichtigen Stellen Auskünfte zu verlangen. Alle Mitgliedstaaten sollen nach Art. 7 IT-Notfallteams (Computer Emergency Response Teams, CERTs) einrichten. Diese Teams können nach Konzeption der Richtlinie innerhalb der zuständigen nationalen Behörden eingerichtet werden, unterstehen aber in jedem Fall ihrer Aufsicht (Art. 7 Abs. 5). Aufgabe der CERTs ist die aktive Begegnung der durch die nationalen Stellen erkannten Sicherheitsvorfälle.

Des Weiteren sieht die Richtlinie in Art. 8 als ganz wesentliches Kernelement eine Zusammenarbeit aller nationalen zuständigen Behörden vor. Über ein Kooperationsnetz sollen die nationalen Behörden Frühwarnungen nach Art. 10 und koordinierte Reaktionen nach Art. 11 abstimmen. Zu diesem Zweck wird die Kommission in Art. 9 ermächtigt, Rechtsakte für den Informationsaustausch im Kooperationsnetz zu erlassen, insbesondere hinsichtlich des Niveaus der Sicherheit der Kommunikation zwischen den nationalen Stellen.

Die Rolle der Kommission ist darüber hinaus von Bedeutung als zentrale Koordinationsstelle des gesamten Sicherheitssystems der geplanten Richtlinie. Dabei sind ihre Aufgaben, Rechte und Pflichten aber bisher weit weniger konkret gezeichnet als die der Beteiligten der unteren Ebenen. Verstreut über einzelne Erwägungsgründe und Artikel der Richtlinie ergibt sich nur ein fragmentarisches Bild. So soll die Kommission mit allen nationalen Stellen im Kontakt stehen (Art. 8 Abs. 1 und 2) und nach Art. 12 einen Kooperationsplan der Union entwickeln. Dazu gehört auch die Festlegung von Verfahren über den Informationsaustausch mit den nationalen Stellen (Art. 8 Abs. 2 und 3), u. a. zum Zwecke der Verbreitung von Frühwarnungen und Gewährleistung einer koordinierten Reaktion. Daneben soll die ENISA dem Kooperationsnetz beratend zur Seite stehen (Art. 8 Abs. 2), und es sollen das bei Europol angesiedelte Europäische Zentrum zur Bekämpfung der Cyberkriminalität ebenso wie weitere europäische Einrichtungen am Informationsaustausch beteiligt werden (Art. 8 Abs. 3 f)). Die Rolle des

[221] Diesbezüglich weist der Europäische Datenschutzbeauftragte (EDPS) in seiner „Opinion of the European Data Protection Supervisor on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a 'Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace', and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union" vom 14.06.2013, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-06-14_Cyber_security_EN.pdf, zu Recht darauf hin, dass derartige Kleinunternehmen in Einzelfällen aber in ihrem Marktsegment wesentliche Anbieter sein und damit wieder zu wichtigen Anbietern der Informationsgesellschaft werden können.

seit dem 11.09.2012 eingerichteten CERT-EU[222] wird in diesem Zusammenhang nicht weiter spezifiziert.

Die Richtlinie regelt damit eine Situation, in der die Verarbeitung persönlicher Daten unvermeidlich werden wird, und setzt sich somit in Konflikt mit Datenschutzanforderungen. Unter dem Eindruck dieses weitgehenden Regelungsbereichs und vor dem Hintergrund der bereits erörterten deutschen und europäischen Rechtslage ergeben sich fünf große Kritikpunkte an der Cybersecurity-Richtlinie, die in den folgenden Abschnitten erörtert werden.

5.4.1 Fehlende Rechtsgrundlage für die nationalen Zentralstellen

Zunächst ist zu kritisieren, dass es der Richtlinie an einer eindeutigen und in ihren Grenzen klar definierten Rechtsgrundlage für die Verarbeitung personenbezogener Daten bei den nationalen Zentralstellen fehlt.

Je nach der Art der abzuwehrenden Gefährdungen kann es erforderlich sein, dass die zur Meldung verpflichteten Unternehmen eine sehr breite Datenbasis weitergeben müssen, die viele personenbezogene Daten, aber auch geschäftliche Geheimnisse beinhalten kann. Die Verarbeitung dieser Daten durch die nationalen Zentralstellen kann nicht ohne eindeutige und zweckgebundene Rechtsgrundlage erfolgen. Der Vorschlag der Richtlinie geht auf diese zentrale Frage der Rechtsgrundlage jedoch nur äußert oberflächlich ein. Lediglich in Erwägungsgrund 39 findet sich ein Verweis auf die Rechtfertigung für die Datenverarbeitung. Der Vorschlag der Richtlinie führt dort aus:

> *„Diese Verarbeitung personenbezogener Daten ist notwendig, um die mit dieser Richtlinie verfolgten Ziele des öffentlichen Interesses zu erreichen, und somit nach Artikel 7 der Richtlinie 95/46/EG zulässig."*

Dabei macht die Richtlinie zum einen nicht deutlich, welche Variante des Art. 7 der Richtlinie 95/46/EG gemeint ist. Zum anderen sind die Erwägungsgründe – wie bereits erwähnt – auch lediglich unverbindliche Erklärungen und kein Ersatz für eine klare Rechtsgrundlage in der Richtlinie selbst. Dieses Versäumnis des Entwurfs führt zu hochgradiger Unklarheit hinsichtlich der Ermächtigung zur Datenverarbeitung. Diese Unklarheit ist primär an zwei Unzulänglichkeiten festzumachen, die im Folgenden dargestellt werden.

5.4.1.1 Unzureichende Pauschalabwägung

Der Erwägungsgrund ist in seinem Verweis auf Art. 7 der Richtlinie 95/46/EG zu ungenau. Von den Varianten in Art. 7 der Richtlinie 95/46/EG Richtlinie 95/46/EG kommen, wie oben dargestellt wurde[223], sinnvollerweise nur die Buchstaben e) und f) in Betracht. Der EDPS, der in seiner Stellungnahme[224] eine ähnliche Kritik geäußert hat, scheint davon auszugehen, dass Art. 7 e) der Richtlinie 95/46/EG als Rechtsgrundlage heranzuziehen sei.

Der EDPS begründet in seiner Stellungnahme allerdings nicht, weshalb Art. 7 e) der Richtlinie 95/46/EG die Datenverarbeitung der nationalen Behörden für die Zwecke der Cybersecurity-Richtlinie rechtfertigen soll. Der bloße Verweis auf das „öffentliche Interesse" ist kaum geeignet, als abschließende Rechtfertigung zu gelten. Im Sinne der Richtlinie 95/46/EG bezeichnet das „öffentliche Interesse" nämlich kein isoliertes Rechtsgut, sondern muss immer im Verhältnis zu dem Rechtsgut betrachtet werden, zu dessen Lasten das öffentliche Interesse verfolgt werden soll.[225] Bereits die Erwä-

[222] http://cert.europa.eu/cert/plainedition/en/cert_about.html.
[223] Abschnitt 3.1.4.2.2.5.
[224] EDPS, Opinion of the European Data Protection Supervisor on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a 'Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace', and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union.
[225] *Dammann/Simitis*, Kommentar zur EG-Datenschutzrichtlinie, S. 152.

gungsgründe[226] zur Richtlinie 95/46/EG weisen ausdrücklich darauf hin, dass die Verarbeitung personenbezogener Daten nur dann rechtmäßig ist,

> *„wenn sie […] notwendig ist […] zur Wahrnehmung einer Aufgabe im öffentlichen Interesse, […] vorausgesetzt, daß die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen.“*

Damit wird deutlich, dass das schlichte Vorhandensein eines öffentlichen Interesses für sich allein niemals eine Rechtfertigung sein kann. Auch unter Berücksichtigung des notwendigerweise eher abstrakten Niveaus einer Richtlinie muss eine hinreichend konkrete Richtlinie jedenfalls anhand konkret benannter Gefährdungsszenarien konkrete Eingriffe benennen und einzeln die dafür erlaubten Datenverarbeitungen aufführen. Nur so kann der Richtliniengeber seinem Auftrag gerecht werden, eine Rechtsgrundlage zu schaffen, die in ihrem Umfang nicht völlig uferlos ist, sondern konkrete Anwendungsfälle und Eingriffsmodalitäten legitimiert. Eine solche Abwägung findet sich aber nicht in dem Vorschlag der Richtlinie. Die derzeit gewählte Formulierung legt vielmehr nahe, dass jedwede Datenverarbeitung ohne Rücksicht auf konkrete Umstände allein wegen des allgemeinen öffentlichen Interesses zulässig sein soll.

Gleichermaßen ungeeignet ist daneben auch ein Verweis auf Art. 7 f) der Richtlinie 95/46/EG. Dort wird eine Datenverarbeitung gestattet,

> *„zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 geschützt sind, überwiegen.“*
>
> (Unterstreichung durch den Bearbeiter)

Damit ist auch bei Heranziehung des Art. 7 f) als Rechtsgrundlage eine Abwägung gegen die Interessen der Betroffenen notwendig. Diese findet aber weder Grundzügen statt noch scheint sich der bisherige Richtlinienentwurf dieses Erfordernisses überhaupt bewusst zu sein. Die Pauschalerwägung, die die Richtlinie selbst in Erwägungsgrund 39 vornimmt, genügt den Anforderungen an eine tragfähige Interessenabwägung nicht. Relevante Aspekte, die eine Verarbeitung rechtfertigen oder verbieten könnten, werden nicht dargestellt. Der reine Verweis auf das allgemeine Interesse, die europäische IT-Infrastruktur zu sichern, mit dem Ergebnis, dass das Interesse der durch die Datenverarbeitung Betroffenen dahinter stets zurücktreten müsse und die Datenverarbeitung daher rechtmäßig erfolge, ist unzureichend. Daneben fällt auch auf, dass die geplante Richtlinie nicht auf die nach Art. 8 der Richtlinie 95/46/EG besonderen Kategorien personenbezogener Daten eingeht, die ganz besonders strengen Eingriffsbeschränkungen unterliegen. So ist die Verarbeitung von Daten, aus denen die

> *„rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben“*

nur unter sehr engen Bedingungen erlaubt und grundsätzlich untersagt. Trotzdem ist es nicht nur nicht auszuschließen, sondern auch sehr wahrscheinlich, dass bei den durch die nationalen Behörden zu verarbeitenden Daten auch sensible Daten dieser Kategorien verarbeitet werden. Umso dringender ist es, dass die vorgeschlagene Cybersecurity-Richtlinie jedenfalls im Ansatz aufzeigt, zu welchen Zwecken welche Daten verarbeitet werden sollen und wie im Einzelfall etwa durch technische und organisatorische Maßnahmen wie einer Pseudonymisierung ein Ausgleich zwischen den Interessen erreicht werden soll. Der bloße Verweis auf ein (im Grundsatz unbestreitbar vorhandenes) „öffentliches Interesse“ vermag in dieser Form als Grundlage jedenfalls nicht auszureichen.

[226] Erwägungsgrund 30 Satz 1 der Richtlinie 95/46/EG.

5.4.1.2 Fehlendes Abwägungsmaterial

Eine solche Abwägung wäre auch überhaupt nicht in ihrer notwendigen Genauigkeit möglich. Um zwischen gegenläufigen Interessen abwägen zu können, muss der Wert der in ein Verhältnis zu setzenden Rechtsgüter jedenfalls in Grundzügen bekannt sein. Dazu ist es notwendig, das Maß der Sensibilität der Daten für die betroffene Person dazustellen und Verarbeitungsverfahren zumindest grob zu umreißen. Dies ist auf der Regelungsebene einer Richtlinie wegen der notwendigen Abstraktheit nur bedingt zu leisten. Daher ist es jedenfalls erforderlich, einen solchen Detailgrad durch ergänzende Rechtsakte zu schaffen und durch diese Ergänzungsrechtsakte gewisse Leitlinien vorzugeben. Nur durch eine vorherige Betrachtung der Daten, die jeweils übermittelt werden sollen, und des Grades der Gefährdung für die zu schützende Infrastruktur lässt sich nämlich überhaupt erst ein Urteil darüber bilden, welche Daten zu welchen Zwecken verarbeitet werden dürfen. Wenn aber nicht einmal klar ist, welche Daten für welche Sicherheitsvorfälle gemeldet werden sollen, ist es unmöglich zu beurteilen, ob die Verarbeitung der Daten auch angemessen ist.

Genauso unbestimmt, wie die Richtlinie bezüglich der Eingriffsintensität ist, bleibt sie auch in Bezug auf die Ziele der Cybersecurity-Richtlinie. Zwar spricht die Richtlinie vielerorts von einem hohen Schutzniveau für die Infrastruktur (etwa Art. 4 oder Erwägungsgrund 32), benennt dieses Schutzniveau aber an keiner Stelle genauer oder differenziert einzelne Stufen des Schutzbedarfs, wie sie sich etwa in den IT-Grundschutz-Katalogen des BSI anhand der Stufen „normal“, „hoch“ und „sehr hoch“ etabliert haben.[227] Insgesamt ist es deshalb nicht möglich, entsprechend Art. 7 e) und Art. 7 f) der Richtlinie 95/46/EG die beiden Gewichte in der Waage in einen schonenden Ausgleich zu bringen. Dies liegt schlicht an der mangelnden Bestimmtheit der Richtlinie im Ganzen.

Schließlich muss generell in Frage gestellt werden, ob die Richtlinie 95/46/EG mit ihrem Art. 7 überhaupt als Rechtsgrundlage herangezogen werden sollte. Der Regelungsbereich dieser Richtlinie bezog sich 1995 auf die Verarbeitung durch einzelne Marktteilnehmer und öffentliche Stellen; man hatte bei Verabschiedung kein derart umfassendes und einschneidendes Netz im Sinn, wie es nun durch die Cybersecurity-Richtlinie geschaffen werden soll. Hier ist aus Gründen der Normenklarheit und der Transparenz zu fordern, angesichts dieser neuen Dimensionen eine eigene Rechtsgrundlage zur Verarbeitung der Daten direkt und unmittelbar in der neuen Cybersecurity-Richtlinie anzulegen, um diesem neuen Anwendungsfall gerecht zu werden.

Neben den Bedenken hinsichtlich der Rechtsgrundlage bestehen vier weitere große Bedenken bezüglich der Vereinbarkeit mit Datenschutzanforderungen.

5.4.2 Keine Rechtsgrundlage für meldepflichtige Stellen

In ähnlicher Weise für die staatliche Datenverarbeitung ergibt sich auch aufseiten der meldepflichtigen Stellen in den jeweiligen Mitgliedstaaten die Frage nach der Rechtsgrundlage.

Die Cybersecurity-Richtlinie selbst nimmt in Erwägungsgrund 5 zunächst die Anbieter öffentlicher Kommunikationsnetze (im Sinne der Richtlinie 2002/21/EG) von ihrem Anwendungsbereich aus und klammert damit die wohl größten Quellen für Daten aus – wohl in der Annahme, für diese Unternehmen bestünde ohnehin bereits eine Ermächtigungsgrundlage für eine entsprechende Datenverarbeitung. Wie ausgeführt wurde, sieht auf europäischer Ebene die Richtlinie 2002/21/EG zwar eigene IT-Standards für Telekommunikationsanbieter vor und regelt Rechte und Pflichten hinsichtlich der Umsetzung der IT-Sicherheit, nicht jedoch eine Rechtsgrundlage für die Datenverarbeitung zu Zwecken der europaweiten Netzsicherheit. Die Richtlinie klammert diese Unternehmen also zu Unrecht aus der Cybersecurity-Richtlinie aus, da es außerhalb der Richtlinie gerade keine Ermächtigungsgrundlage für eine Meldung von IT-Sicherheitsvorfällen an Dritte zu dem Zweck eines europa-

[227] BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002_pdf.pdf?__blob=publicationFile.

weiten Cybersecurity-Netzes gibt. In dem Umriss der gegenwärtigen Rechtslage auf europäischer Ebene dargestellt befasst sich am ehesten die Richtlinie 2002/21/EG mit der Frage der Datensicherheit bei den Bereitstellern öffentlicher Kommunikationsnetze. Eine Grundlage zur Erhebung und Weitergabe von persönlichen Daten zu Zwecken der koordinierten Cybersicherheit findet sich dort aber nicht. Dies macht das Bedürfnis dafür deutlich, unmittelbar in der Cybersecurity-Richtlinie selbst eine Rechtsgrundlage zu normieren, die die Datenerhebung und -verarbeitung für die Zwecke der Richtlinie einheitlich – auch für die Meldestellen – regelt und den Umfang grundrechtskonform beschränkt.

Aber nicht bloß das grundsätzliche Fehlen einer Rechtsgrundlage ist diesbezüglich Grund zur Besorgnis. Es fehlt daneben auch an einer weiteren Konkretisierung der Datenschutzmaßnahmen, die bei der Verarbeitung und Weitergabe an die nationalen Stellen erforderlich werden. Zu verlangen wäre dabei im Mindestmaß die Aufnahme einer konkreten Zweckbindung, wie sie das deutsche BDSG etwa in § 31 BDSG für personenbezogene Daten zu Zwecken der Datensicherheit festschreibt. Mit größter Besorgnis sind diesbezüglich die Ausführungen in Erwägungsgrund 30 der Richtlinie zu sehen, da dort die Nutzung der übermittelten Daten auch zu Strafverfolgungszwecken vorgesehen ist, ohne konkret darzulegen, unter welchen Voraussetzungen die gemeldeten Daten auch zur Strafverfolgung genutzt werden dürfen. Die Aussicht, durch die gemeldeten Sicherheitsvorfälle Gegenstand von Ermittlungsmaßnahmen und Strafverfolgung zu werden, dürfte die Motivation der meldepflichtigen Unternehmen erheblich mindern, ihrer Meldepflicht vollständig und zeitnah nachzukommen. Hier wäre es empfehlenswert, ähnlich zu der Systematik im Steuerrecht einen Schutz vor Strafverfolgung zu gewährleisten. So wie der Steuerpflichtige als Ausgleich für seine Meldepflichten in der Abgabenordnung (§ 93 AO) auf die Verschwiegenheit der Finanzbehörden aufgrund des Steuergeheimnisses (§ 30 AO) vertrauen kann, sollte die meldepflichtige Stelle darauf vertrauen können, dass die gemeldeten Sicherheitsvorfälle von der nationalen Behörde ebenso verschwiegen behandelt werden. Die für besonders schwere Straftaten in der Abgabenordnung vorgesehenen Ausnahmen (§ 30 Abs. 4 AO) sollten dabei entsprechend übernommen werden. Eine thematisch ähnliche Regelung findet sich bereits in § 42a S. 6 BDSG, wonach bei einer pflichtgemäßen Meldung von Datenschutzverstößen die Verfolgung des Meldepflichtigen wegen Straftaten und Ordnungswidrigkeiten nur nach Zustimmung der Person zulässig ist, deren Daten betroffen sind.

5.4.3 Datenkonzentration bei den Zentralstellen

Als drittes großes Thema ist die Einrichtung der nationalen Zentralbehörden zu hinterfragen. Nach jetziger Konzeption in Art. 6 Abs. 1 der Richtlinie benennt jeder Mitgliedstaat eine „zuständige Behörde“, die die gemeldeten Sicherheitsvorfälle auswertet und entsprechende Maßnahmen einleiten soll. Hier ergibt sich aus Datenschutzperspektive die Gefahr eines zentralen Datensilos mit entsprechend großem Missbrauchspotential.

Um diese Gefahr zu minimieren, sollten bereits aufseiten der Meldestellen die im Zusammenhang mit § 3 Abs. 6 und 6a des BSIG gemachten Ausführungen zur Anonymisierung und Pseudonymisierung[228] der gemeldeten Daten normiert werden. Zudem wäre zu verlangen, innerhalb der zentralen Stelle zu gewährleisten, dass sich der gesamte Datenbestand nicht zur Zusammenführung und Profilbildung von Betroffenen nutzen lässt. Idealerweise würde der Datenbestand auf mehrere Stellen verteilt, um das Risiko einer Gesamtverkettung der Daten zu minimieren. In diesem Zusammenhang wäre auch zu erwägen, den Art. 6 Abs. 1 insoweit abzuändern, dass kein Zwang besteht, für jeden Mitgliedstaat eine eigene Zentralbehörde zu errichten, sondern für kleine Mitgliedstaaten ein gemeinsames Zentrum und in größeren Mitgliedstaaten entsprechend der nationalen Besonderheiten mehrere Behörden zu gestatten. In Anlehnung an die föderale Struktur der Bundesrepublik könnte erwogen werden, die Zentralstellen zunächst auf Landesebene zu errichten und nur dort vorverarbeitete Daten an eine nationale Zentralbehörde weiterzugeben. Auf diese Weise würde auch die Gefahr einer zentralen Sammelstelle für Rohdaten in einer einzelnen Behörde minimiert, da diese Behörde keine

[228] Siehe Abschnitt 3.2.2.

konkreten Klardaten mehr erhielte, sondern nur vorverarbeitete anonymisierte und pseudonymisierte Daten.

5.4.4 Meldepflicht zu unbestimmt

Das vierte Problemfeld wurde vereinzelt bereits in den bisherigen Punkten allgemein angesprochen, stellt aber für sich allein ebenfalls eine große Schwachstelle des Richtlinienvorschlags dar. Zu bemängeln ist weiterhin nämlich auch der Umfang der Meldepflicht der einzelnen Unternehmen und öffentlichen Stellen im Speziellen. Die Richtlinie geht in Art. 14 zwar grundsätzlich auf diese Meldepflicht ein, regelt aber nur, dass die Marktteilnehmer ein gewisses IT-Sicherheitsniveau gewährleisten müssen, und statuiert eine Meldepflicht von Sicherheitsvorfällen. Dabei geht die Richtlinie aber nicht darauf ein, welche Daten zu welchen Zwecken und in welchem Detailgrad in der Meldung übermittelt werden müssen. Ebenso wie Art. 14 Abs. 5 und Abs. 7 die Details der IT-Sicherheit delegierten Rechtsakten und Durchführungsrechtsakten überlassen, muss dort ebenfalls die Meldepflicht unter dem Gesichtspunkt des Datenschutzes konkretisiert und eingerahmt werden.

Hier erlangt zudem der Erwägungsgrund 31 Bedeutung, der für das gesamte Kommunikationsnetz ein einheitliches Muster zur Meldung von Vorfällen präferiert. Die dabei bezweckte Reduzierung des Verwaltungsaufwands ist zwar verständlich, birgt aus Datenschutzsicht allerdings das Risiko, dass im Zweifel mehr Daten als notwendig übermittelt werden. Zum einzelfallgerechten Datenschutz ist die Verwendung getrennter Muster für einzelne Sicherheitsvorfallkategorien zu bevorzugen. Nicht alle Sicherheitsvorfälle verlangen nach den gleichen Daten; die Meldung sollte daher bereits in diesem Stadium die zu übermittelnden Daten auf das notwendige Minimum reduzieren. Nach dem Grundsatz des „Data Protection by Design“ ist es notwendig, auf ganz grundlegendem Niveau die Verfahren derart zu gestalten, dass Daten nur im notwendigen Maße überhaupt in die Verarbeitung gelangen. Mit Blick auf das derzeit verwendete Muster, das die ENISA für freiwillige Sicherheitsmeldungen verwendet[229] und das unter Punkt 11 unabhängig von dem Vorfall stets die Meldung der Host-IP-Adresse vorsieht, ist hier zu befürchten, dass bei unzureichender Konkretisierung der Meldepflichten in großem Umfang Daten gemeldet werden, die für eine Einschätzung der Gefahrenlage gar nicht erforderlich sind und nur deshalb weitergegeben werden, weil für sie ein Datenfeld in dem einheitlichen Muster vorgesehen ist. Um dies zu vermeiden, sollte jedenfalls im Grundsatz in der Richtlinie eine Trennung nach einzelnen Kategorien von Sicherheitsvorfällen erfolgen, und es sollte konkreten Rechtsakten überlassen werden, jeweils passende Meldeformen zu entwickeln, die nur die für die Reaktion erforderlichen Daten enthalten.

5.4.5 Unklare Rolle der Kommission

Als letzter großer Kritikpunkt muss die unklare Rolle der Kommission beziehungsweise einer möglichen zentralen europäischen Stelle angesprochen werden. Wie bereits ausgeführt, bleibt der Vorschlag für die Richtlinie hinsichtlich der Aufgaben und Kompetenzen dieser Einrichtung sehr unspezifisch. Insbesondere ist nicht klar,

- in welchem Maße auf europäischer Ebene selbst eine Datenauswertung erfolgen soll,
- ob diese Daten von den nationalen Stellen nach dortigen Erwägungen freiwillig weitergegeben werden sollen oder ob auch eine europäische Stelle eine eigene Kompetenz besitzen soll, Daten von den nationalen Behörden einfordern zu können, und
- wann eine Frühwarnung durch die Union und wann durch nationale Stellen erfolgt und auf welcher Datengrundlage dies basieren soll.

Je nachdem, welche Rolle für die Kommission oder ein dort angesiedeltes Zentralorgan vorgesehen sein soll, würde es sich um ein dezentralisiertes oder zentralisiertes Kooperationsnetz handeln. Nach

[229] http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_11_002_v2_1.pdf.

dem bisherigen Eindruck scheint die Richtlinie ein dezentralisiertes Netz zu konstruieren, in dem die nationalen Stellen ihre Erkenntnisse unabhängig voneinander auf ihre nationalen Auswertungen stützen, es aber keine zentral organisierte Auswertung aller nationalen Daten geben wird. Zwar ist über das Kooperationsnetz ein Informationsaustausch vorgesehen; es gibt jedoch kein genaues Verfahren, das erklärt, wie aus den einzelnen nationalen Erkenntnissen ein europaweites Lagebild konstruiert werden und wer dieses Lagebild erstellen soll. Ohne zentrale Auswertung bliebe es damit in der Verantwortung jeder einzelnen nationalen Behörde, die Erkenntnisse der jeweiligen Mitgliedstaaten zu erhalten und selbst ein europäisches Lagebild zu erstellen. Die Gefahr, dass einzelne Mitgliedstaaten dabei zu abweichenden Einschätzungen gelangen und eine koordinierte Reaktion bereits an der uneinheitlichen Gefahreneinschätzung scheitern könnte, würde das Ziel der Richtlinie, ein europaweites Cybersecurity-System zu etablieren, erheblich beeinträchtigen. Daneben erscheint die parallele Auswertung der europäischen Bedrohungslage als ineffektive Ressourcennutzung.

Eine zentrale Fusions- und Auswertungsstelle, wie sie das MonIKA-System beschreibt, ist nicht vorgesehen. Das selbst gesteckte Ziel einer einheitlichen und umfassenden Erkennung von Bedrohungen für das gesamte europäische Kommunikationsnetz lässt sich aber nur umsetzen, wenn eine zentrale Stelle auch ein Gesamtbild erhält. In der jetzigen Form ist aus dem Richtlinienvorschlag nicht erkennbar, wie dieses Gesamtbild geformt werden soll. Es ist also bereits mit Hinblick auf die bisherige Konzeption der Richtlinie fraglich, ob das Ziel der europäischen Rechtsgeber so überhaupt erreicht werden kann. Wenn aber das eigentliche Ziel der Richtlinie nach der jetzigen Konstruktion gar nicht erreicht werden kann, steht dem Eingriff in die Persönlichkeitsrechte und die Privatsphäre der durch die Datenverarbeitung Betroffenen kein Interesse mehr gegenüber, das diese Einschnitte rechtfertigen könnte. Die gesamte Richtlinie muss, sofern sie die massive Verarbeitung personenbezogener Daten auch nur im Grundsatz rechtfertigen will, überhaupt erst ein Konzept enthalten, das sich als geeignet zeigt, die Ziele der Richtlinie zu erreichen. Dies tut sie in der bisherigen Form jedoch nur schwerlich, so dass die Hinnahme von Eingriffen in die Grundrechte der Betroffenen nicht gerechtfertigt ist.

5.4.6 Bedeutung für den Einsatz von Monitoring-Netzen

Insgesamt mangelt es dem Richtlinienvorschlag in seiner aktuellen Form an tauglichen Rechtsgrundlagen für die Datenverarbeitung auf Ebene sowohl der nationalen Zentralstellen als auch der meldepflichtigen Stellen. Die bisherige Rechtslage deckt die durch die geplante Richtlinie geplante Datenverarbeitung nur fragmentarisch und unzureichend ab.

Die Verfahren zur Erhebung und Übermittlung sind ebenso unkonkret wie die Auswertung in den nationalen Stellen und der sonstige Umgang mit den Daten. Die äußert unbestimmte Rolle einer möglichen europäischen Zentralstelle lässt die Richtlinie bereits als ungeeignetes Instrument erscheinen und rechtfertigt den Eingriff in die Grundrechte der Betroffenen nicht. Für zentrale Monitoring-Netze, wie sie im Projekt MonIKA untersucht werden, bietet die geplante Richtlinie daher keinen verlässlichen Rechtsrahmen.

6 Beispielszenario Enterprise-Monitoring in einer PKW-Herstellungskette

Das MonIKA-Projekt hat zu konkreten Untersuchungszwecken einen Machbarkeitsnachweis (Proof-of-Concept, kurz PoC) entwickelt, um einige Abläufe technisch exakt nachvollziehbar zu machen. Der PoC stellt das Anwendungsszenario Enterprise-Monitoring anhand eines fiktiven Unternehmensverbunds dar und gibt Gelegenheit, einige abstrakte Rechtsfragen an einem konkreten Versuchsaufbau zu überprüfen.

6.1 Sachverhalt

Der Unternehmensverbund besteht aus vier fiktiven Unternehmen: der McQueer AG, einem Automobilhersteller, und den Zulieferern 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 aufgrund 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 das MonIKA-System dieses isolierte, dezentrale Vorgehen der lokalen IT-Sicherheit um einen kooperativen, zentralen Ansatz.

Dies geschieht durch die Teilnahme der Unternehmen an einem Netz, in dessen Zentrum die MonIKA-GmbH steht. 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 diese zu senden. Die zu übermittelnden Informationen werden durch eine seitens der MonIKA-GmbH bereitgestellte Software, sogenannte Agenten, gewonnen. Diese Agenten werden an die unternehmenseigene, datenliefernde Sensorik angebunden. Über die Agenten erfolgt auch die Kommunikation mit der MonIKA-GmbH. Die Organe der Unternehmen, die mit dem Einsatz des MonIKA-Systems betraut sind, sind die sogenannten „Security Operation Center“ (SOC). Diese beobachten an jedem Tag des Jahres rund um die Uhr den Netzverkehr der unternehmenseigenen IT (Monitoring) und werden eingesetzt, um das aus dem Betrieb von Informationstechnik resultierende Sicherheitsrisiko zu minimieren. In jedem SOC wertet der eingesetzte Agent anfallende Logdaten auf auffällige Ereignisse – insbesondere die Unternehmens-IT gefährdende Anomalien – aus (Klassifikation) und sendet die aufbereiteten Informationen an das sogenannte „Common Security Operation Center“ (CSOC).

Über das CSOC als gemeinsames SOC wird der zentrale Ansatz des MonIKA-Systems organisiert und verwirklicht. Technisch erfolgt dies durch die Einrichtung und den Betrieb eines sog. „Erkennen-von-Anomalien-Service-Clusters“ (EvASC) bei der MonIKA-GmbH. Durch den Betrieb des EvASC werden einerseits die gesammelten Sensordaten aus den einzelnen Unternehmen zusammengeführt, 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 übersandten 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 von Warnungen zur

Verfügung, so dass es diesen möglich ist, sich überhaupt oder bereits in einem frühzeitigen Stadium durch die Bewertung eigener Daten vor Angriffen und Anomalien zu schützen.

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

Ein externer Dritter plant, die Autoproduktion der McQueer AG durch Störung der Lieferkette zu sabotieren. Sein Ziel ist es, die Verwaltung der Lieferkette gezielt lahmzulegen 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 Java-Programmiersprache. 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“ auszunutzen, bei dem eine systembedingte Schwachstelle des Hypertext Transfer Protocols (HTTP) ausgenutzt wird.

Die über HTTP kommunizierenden Teilnehmer in einem Netz nutzen für die Kontaktaufnahme bestimmte Befehle (GET, HEAD, POST etc.), die von dem Gegenüber umgesetzt werden. Um zu verhindern, dass bestimmte Befehle von Unbefugten ausgeführt werden können, sind in gut gepflegten Netzkomponenten erlaubte und verbotene Kommandos für bestimmte Nutzer indiziert (White- und Blacklists). Zum Beispiel soll der Befehl GET nur von zugelassenen, angemeldeten Nutzern ausgeführt werden können. Die Schwachstelle, die sich der Angreifer zunutze machen will, liegt darin, dass teilweise nur die Befehle reglementiert sind, die normalerweise für eine bestimmte Funktion vorgesehen sind. Das HTTP kennt aber eine Vielzahl von Befehlen. So kann es möglich sein, einen nicht-indizierten Befehl (z. B. HEAD) zu nutzen, der zwar nicht diejenige Aktion ausführt, die der Angreifer eigentlich nutzen möchte (GET), jedoch zumindest irgendeine Aktion ausführt und zwar, ohne diese Aktion dahingehend zu prüfen, ob sie von einem berechtigten Nutzer ausgeführt wird, weil der Befehl eben auf keiner White- oder Blacklist geführt wird. Um auf diesem Weg nun aber schädigende Aktionen in der Software der Opfer auszuführen, muss diese Software Schwachstellen derart aufweisen, dass Funktionen beispielsweise auch über den HEAD-Befehl zugänglich werden, die normalerweise nur durch den GET-Befehl vorgesehen sind. Die hier eingesetzte SAP-Netweaver-Anwendung verfügt über eben diese Schwachstellen.[230]

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 Versionen davon betrieben werden und auf welchen Kanälen (Ports) diese mit der Außen(netz)welt kommunizieren. Dazu setzt der Angreifer verschiedene Methoden und Werkzeuge ein. Zunächst nutzt der Angreifer allgemein zugängliche Internet-Suchmaschinen, um sich anhand von öffentlichen Informationen einen Eindruck über das Unternehmensgeflecht rund um den Autohersteller McQueer zu verschaffen. So erfährt er etwa die Internet-Adressen der Lieferanten und damit auch die diesen Adressen entsprechenden IP-Adressbereiche. Nachdem der Angreifer auf diesem Weg einen groben Überblick über die Unternehmensstruktur und die für diese Unternehmen vergebenen IP-Adressen 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, die diese Software versteht. Mit diesem Wissen ausgestattet, plant der Angreifer sein weiteres Vorgehen.

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

All diese Tätigkeiten des Angreifers werden von dem anvisierten Unternehmen registriert: 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. Zusätzliche Angriffserkennungssysteme (Intrusion Detection Systems, IDS) registrieren weitere Daten. All diese Instrumente stellen aus Sicht des Opfers Sensoren dar, mit deren Hilfe die Kommunikation mit dem Internet beobachtet wird. Die dabei anfallenden Daten werden nun in den SOCs der Lieferanten und der McQueer AG gesammelt und nach bestimmten Kriterien bezüglich ihrer Gefährdung für die IT-Sicherheit voranalysiert. Diese Analyse erfolgt dabei zunächst nur isoliert mit Blick auf die Bedrohungen für das jeweils durch das SOC überwachte Einzelunternehmen. Das SOC kommt daraufhin entweder zu dem Ergebnis, dass eine Anomalie vorliegt, oder eben nicht. Um nun den Blick auf die gesamte Lieferkette und Unternehmensgruppe zu erweitern, ist es erforderlich, die Erkenntnisse der einzelnen SOCs auf ihre Relevanz für die gesamte Lieferkette zu analysieren. Dies geschieht, indem die einzelnen SOCs ihre Daten an das CSOC der MonIKA-GmbH weitergeben. Im CSOC werden die Einzelerkenntnisse nun fusioniert. Vorher als vermeintlich unauffällig eingestufte Ereignisse können als planmäßiges Vorgehen gegen die Lieferkette der McQueer AG identifiziert werden. So mag ein begrenzter Portscan bei allen Lieferanten die einzelnen SOCs nicht alarmiert haben. Wird aber über eine fusionierte Auswertung erkannt, dass alle gescannten Ports zu der Software für Liefer- und Warenmanagement gehören, ist die Erkenntnis möglich, dass es sich nicht um Zufälle, sondern um ein strategisches Abklopfen der Schwachstellen innerhalb der Lieferkette handelt.

6.2 Stakeholder

Im PoC sind mehrere Beteiligte und Rollen zu unterscheiden, wie in den folgenden Abschnitten erläutert wird.

6.2.1 Externe

Als MonIKA-Externe lassen sich solche Beteiligte qualifizieren, die keinem der partizipierenden Unternehmen gesellschaftsrechtlich zuzurechnen sind oder die in keinem vertraglichen Verhältnis zu der MonIKA-GmbH (betreffend der Anwendung des MonIKA-Systems) stehen. Dabei handelt es sich zum einen um Kunden, Geschäftspartner und sonstige neutrale Personen, die mit den MonIKA-Beteiligten über das Internet kommunizieren, etwa indem sie die Websites der MonIKA-Teilnehmer aufrufen oder E-Mails an Adressen der McQueer-Lieferantenkette versenden. Zum anderen tritt auch der Angreifer als Externer auf. Er hat keinerlei vertragliche oder gesellschaftsrechtliche Beziehung zu der McQueer AG, den Lieferanten oder MonIKA-Beteiligten im Übrigen.

Eine Sonderrolle nehmen die Programmierer des MonIKA-Systems und das Software-Unternehmen ein, das die entwickelten MonIKA-Komponenten an den IT-Sicherheitsdienstleister verkauft bzw. ihm entsprechende Nutzungsrechte einräumt. Der IT-Sicherheitsdienstleister wiederum ist für den Vertrieb der MonIKA-Komponenten an die Akteure als Endnutzer zuständig. Dies hat jedoch nur für rahmen- und haftungsrechtliche Fragen Relevanz. Im Ergebnis stehen Programmierer und Software-Unternehmen außerhalb des Betriebs des MonIKA-Systems und sind damit Externe im Sinne des Proof-of-Concepts.

6.2.2 MonIKA-Teilnehmer

Innerhalb des MonIKA-Systems treten zunächst die Lieferanten und die McQueer AG als eigenständige juristische Personen auf. Jedes Unternehmen beschäftigt Personal und verfügt über eine eigene IT-Abteilung, in die auch das unternehmenseigene SOC eingegliedert ist. Die Angestellten verfügen über Zugang zum internen Firmennetz sowie 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 das MonIKA-System 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 das MonIKA-System fungiert. Diese bereits angesprochenen Agenten sind an die datenliefernde Sensorik angeschlossen und haben dadurch Zugriff auf die von den Sensoren (Webserver, Firewall, IDS) gewonnenen Rohdaten. Der Agent wertet die Rohdaten selbstständig nach vorgegebenen Parametern auf auffällige Ereignisse aus und sendet so gewonnene Informationen und Daten an das CSOC der MonIKA-GmbH. Die Daten werden zuvor sortiert, strukturiert und aufbereitet und soweit möglich durch Pseudonymisierungs- und Anonymisierungsverfahren verfremdet. Der Agent legt zusätzlich in den einzelnen Unternehmen Zuordnungsmechanismen an, um später eine Zuordnung von pseudonymisiert verarbeiteten Erkenntnissen zu den tatsächlich erhobenen Daten zu ermöglichen. Diese Zuordnung verbleibt bei den Teilnehmern und wird dem CSOC nicht mit übersandt.

All diese Schritte werden von dem Datenschutzbeauftragten der einzelnen Unternehmen begleitet und organisatorisch von den zuständigen Personen des Managements beaufsichtigt. Der Datenschutzbeauftragte hat über eine in der Agenten-Software eingebaute Funktion jederzeit die Möglichkeit, den Strom der an das CSOC weitergesandten Daten einzusehen und sich eine Momentaufnahme der derzeit ausgewerteten und pseudonymisierten Daten anzeigen zu lassen.

Die Teilnehmer sind aber nicht bloß Sender der Daten, sondern treten in doppelter Rolle auch als Empfänger von Daten in Form der Ergebnisse auf. Nach der Fusion, Klassifikation und Auswertung der Daten durch das CSOC der MonIKA-GmbH erhalten die einzelnen Unternehmen diese Daten mit einem zugehörigen Warnungshinweis zurück.

Konkret erlangen die firmeneigenen SOCs und das dortige Fachpersonal Kenntnis von Daten und dem Auswertungsergebnis durch das CSOC. Durch diese Warnungshinweise erhalten die Beteiligten Erkenntnisse über Anomalien und konkrete Gefährdungen. Die Beteiligten sind dann in der Lage, das Bedrohungspotential 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 Software-Updates für das im Fokus stehende SAP-System, die Verbesserung der HTTP-Blacklists oder die Sperrung der betroffenen Ports ist allerdings nicht Teil des im MonIKA-Projekts.

6.2.3 MonIKA-Zentralstelle

Über die Übertragungswege der Agenten erhält das von der MonIKA-GmbH betriebene EvA-Service-Cluster die aufbereiteten Daten. Die MonIKA-GmbH fungiert als gemeinsames, kooperatives Security Operation Center. 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.

Auch bei der MonIKA-GmbH wirkt ein Datenschutzbeauftragter mit.

Die in der MonIKA-GmbH empfangenen sowie die nach der Auswertung vorhandenen Daten werden zur Verbesserung der Dienstleistungen und zu Zwecken des Qualitätsmanagements auch nach Rücksendung an die einzelnen Lieferanten für eine bestimmte Zeit gespeichert.

6.2.4 Schaubild

Insgesamt lassen sich die Beteiligten und ihre Rollen mit Abbildung 1 veranschaulichen.

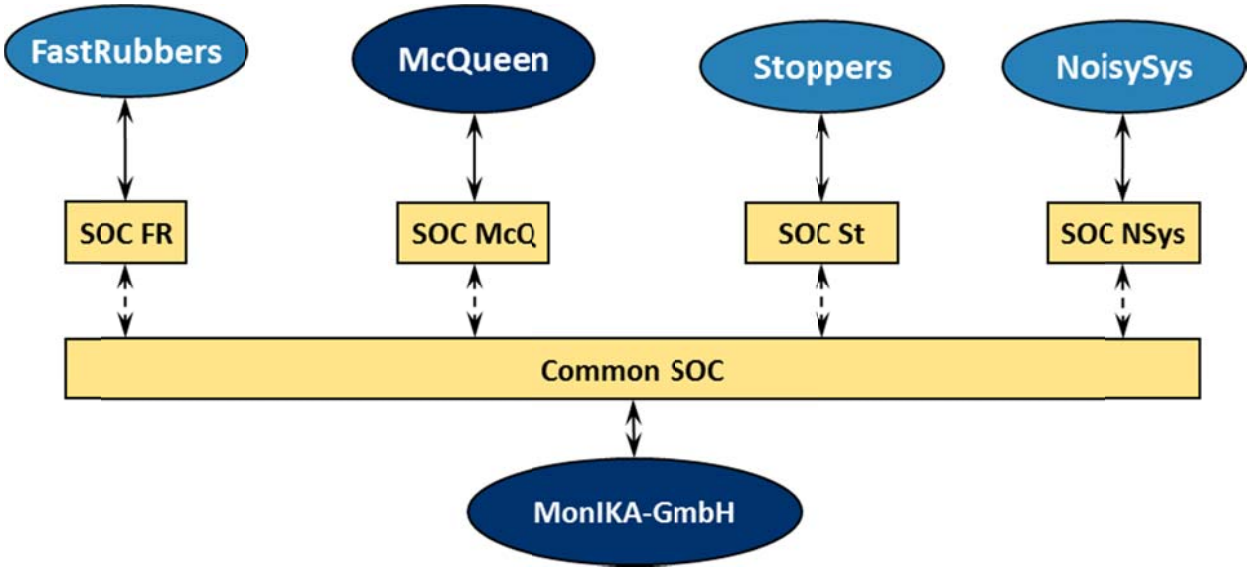

Abbildung 1: Schaubild der Beteiligten im PoC

6.3 Betroffene Daten und Datenkategorien

Den allgemeinen Ausführungen in Abschnitt 3 folgend, soll in diesem Teil abgebildet werden, welche Datenkategorien im Rahmen des PoC relevant werden. Es werden dazu einerseits die Datenkategorien dargestellt, die durch die Sensoren der teilnehmenden Unternehmen aufgezeichnet werden, und andererseits wird die Art und Weise der weiteren Bearbeitung dieser Daten auf ihrem Weg durch das MonIKA-System gezeigt.

Die technische Umsetzung des PoC besteht aus zwei Plugins (shared objects) für das MonIKA-Software-Framework, die die Verfahren zur Erkennung der im Sachverhalt abgebildeten Anomalien implementieren. Hierbei handelt es sich zum einen um das bereits erwähnte Plugin für die EvA-Agenten des Frameworks, das an die in den Unternehmen verwendeten Sensoren (Firewall, Webserver usw.) anbindet, und zum anderen um ein Plugin für das EvA-Service-Cluster bei der MonIKA-GmbH, das auf der Grundlage der von Agenten gelieferten Daten Erkennungsverfahren für die im Sachverhalt beschriebenen Anomalien implementiert und Ergebnisse an die Agenten zurückleitet.

6.3.1 Betroffene Daten und Datenkategorien bei den Teilnehmern

Die Sender, also die Lieferanten und die McQueer AG, sind im hier betrachteten Szenario die einzigen originären Datensammler. Ihre Sensoren, also Webserver, Firewall und sonstige IDS, beobachten die Kommunikation der Systeme und Anwendungen mit dem Internet und zeichnen Informationen zu bestimmten, vorher festgelegten Datenkategorien zur späteren Analyse auf.

Bei den hier verarbeiteten Daten handelt es sich um Meldungen von Firewalls (iptables) und Webservern (apache). Konkret melden die Firewalls durch sie verworfene Pakete (packet drops), der Webserver meldet solche Zugriffe, die nicht korrekt beantwortet werden konnten und daher zur Meldung eines Fehlers an den Client geführt haben (Antwort mit einem HTTP-Code im 400er- oder

500er-Bereich). Im Rahmen des MonIKA-Systems werden solche Webzugriffe als mögliche Verletzung von Zugangsbeschränkungen (access violation) interpretiert.

Die Datenkategorien, die durch die Firewall aufgezeichnet werden, sind in Tabelle 10 exemplarisch aufgeführt.

Tabelle 10: Von der Firewall geloggte Datenkategorien im PoC

Kategorie	Beschreibung	Beispiel
SrcIP	IP-Adresse, von der die Verbindung aufgebaut wurde	192.168.6.27
DestIP	IP-Adresse, zu der die Verbindung aufgebaut wurde	1.2.3.4
Target	Zielsignatur: das Übertragungsprotokoll, in dem das Paket gekapselt ist (innerhalb des IP-Pakets)	TCP, UDP
Src/DestPrt	Port, von dem und zu dem die Verbindung aufgebaut wurde	54789, 23759
Time	Zeitstempel des Ereignisses	2013-09-09T09:47:38Z

Der Agent wertet diese Daten im nächsten Schritt aus und notiert alle verworfenen Pakete. Aus dieser Vorverarbeitung erzeugt die Software eine XML-Datei, um ein einheitliches Format zu schaffen, das für die spätere Fusionierung bei der MonIKA-GmbH geeignet ist. Die XML-Datei wird dazu als Datentyp „packetdrop“ gespeichert. Eine solche XML-Datei kann etwa aussehen wie in Abbildung 2.

```
1 <packetdrop
xmlns="http://itsec.cs.uni-bonn.de/schema/monika/poc">
2 <source>131.220.240.138</source>
3 <destination>131.220.240.142</destination>
4 <target>TCP/139</target>
5 <time>2013-09-09T09:47:38Z</time>
6 </packetdrop>
```

Abbildung 2: XML-Datei über verworfene Pakete nach Zusammenfassung durch den EvA-Agenten

In ähnlicher Weise dokumentiert der Webserver die Anfragen und Antworten, die über die Protokolle der Internet-Kommunikation gesendet werden, also solche Informationen, die etwa in den HTTP- und TCP-Headern enthalten sind, sowie ergänzende Informationen, die der Webserver eigenständig loggt. Tabelle 11 zeigt, welche Kategorien von Daten dabei aufgezeichnet werden.

Tabelle 11: Vom Webserver geloggte Datenkategorien

Kategorie	Beschreibung	Beispiel
SrcIP	IP-Adresse, von der die Verbindung aufgebaut wurde	192.168.6.27
DestIP	IP-Adresse, zu der die Verbindung aufgebaut wurde	1.2.3.4
Date-header/Timestamp	Zeitpunkt der Kommunikation	2013-12-24 19:56:43 CET
Target	Zielsignatur: das Übertragungsprotokoll, in dem das Paket gekapselt ist (innerhalb des IP-Pakets)	TCP, UDP
Src/DestPrt	Port, von dem und zu dem die Verbindung aufgebaut wurde	54789, 23759
Resource	Ort der abgefragten Ressource	www.beispiel.de/SAP154
Protocol	Benutztes Protokoll auf Anwendungsschicht	FTP/HTTP
Protocolmethod	Benutzte Zugriffsmethode	GET, POST, HEAD (HTTP Verbs)
Authtoken	Bei Zugriff verwendetes Merkmal zur Authentifizierung des Clients	Benutzername, Zertifikat
Reason	Protokollunabhängige Begründung, warum der Zugriff als Verletzung einer Zugangsbeschränkung eingestuft wurde	Resource not found, System error

Auch diese Logdaten werden von dem Agenten vorverarbeitet und auf Verletzungen von Zugriffsrechten überprüft. Werden Auffälligkeiten registriert, die auf solche Verletzungen hindeuten, fasst der Agent die Daten ebenfalls in einer XML-Datei zusammen. Ein Beispiel einer solchen Datei des Typs „access violation“ zeigt Abbildung 3.

```
1 <accessviolation
xmlns="http://itsec.cs.uni-bonn.de/schema/monika/poc">
2 <source>203.0.113.37</source>
3 <destination>192.0.2.11</destination>
4 <target>TCP/21</target>
5 <time>2013-02-02T03:26:14Z</time>
6 <protocol>FTP</protocol>
7 <protocolmethod>PWD</protocolmethod>
8 <resource>.</resource>
9 <authtoken>anonymous</authtoken>
10 <reason>Unauthorized</reason>
11 </accessviolation>
```

Abbildung 3: XML-Datei über Zugriffsverletzungen nach Zusammenfassung durch den EvA-Agenten

Neben den technischen Sensoren spielen natürlich auch die Mitarbeiter der Unternehmen eine Rolle bei der Identifizierung auffälligen Netzverkehrs. So ist es beispielsweise denkbar, dass der Inhalt einer E-Mail einem Mitarbeiter verdächtig vorkommt. Als Angriffsszenario ist entsprechend neben dem hier dargestellten Szenario eines Portscans auch vorstellbar, dass ein Angreifer einen vertrauenswürdigen Absender imitiert und per E-Mail Logindaten für das SAP-System erfragt. Der Umgang mit derartige Nachrichten der Mitarbeiter muss selbstverständlich im Sicherheitskonzept der MonIKA-Teilnehmer integriert werden; dies stellt aber kein Element der im PoC zu untersuchenden Rechtsfragen dar. Bezüglich der Eingliederung eines Helpdesks in den Event-Management-Prozess siehe MonIKA-Deliverable 2.3 „Prozess-Framework für kooperatives Monitoring“.[231]

Die derart erlangten Informationen werden an die MonIKA-GmbH versandt. Die dazu nötige Infrastruktur wird von den Internet Service Providern des Senders und des Empfänger gestellt und unterhalten. Die transportierten Daten werden dabei grundsätzlich weder inhaltlich verändert noch ergänzt oder beschnitten.

6.3.2 Betroffene Daten und Datenkategorien im zentralen EvA-Service-Cluster

In der Zentralstelle, der MonIKA-GmbH werden die Daten schließlich entgegengenommen und mit denen der anderen Datensender verglichen. Die einzelnen Datenkategorien werden dazu korreliert und auf auffällige Ereignisse ausgewertet. Dabei werden nicht nur bestehende Datenbestände inhaltlich ausgewertet, sondern auch neue Daten gewonnen. So lässt sich aus der Fusion diverser Angriffe ein deutlich genaueres Bild von der Bedrohung generieren, als es die Einzeldaten erlauben würden.

Software-seitig fungiert ein Server des MonIKA-Software-Frameworks, das EvA-Service-Cluster, als Empfänger. Dieses Cluster empfängt und vergleicht die bei den Sendern erstellten XML-Dateien. Als Beispiel kann hier auf obige Abbildungen 2 und 3 verwiesen werden. Derartige Informationen erhält die MonIKA-GmbH von allen Lieferanten. Sie gleicht beispielsweise die angesprochenen Ports ab und korreliert diese Informationen mit den IP-Adressen der Nutzer und dem Zeitpunkt des Zugriffs. Dadurch lässt sich für eine bestimmte IP-Adresse eine Auflistung der Zeitpunkte und der Art der Zugriffe auf die Systeme der gesamten beteiligten Lieferanten erstellen. Als Ergebnis generiert das EvA-

[231] Insbesondere S. 24 und die Grafik auf S. 25.

Service-Cluster eigene XML-Dateien, die bestimmten Gefährdungen entsprechen. Beispielhaft beschreibt der PoC drei dieser Datentypen: „portscan“, „hostdiscovery“ und „eventsequence“.

Der Datentyp „portscan“ stellt das eingangs beschriebene Ereignis dar, bei dem ein System über eine Netzverbindung systematisch nach solchen Ports abgesucht wird, die Verbindungen entgegennehmen (Portscan). Solche Ereignisse werden durch Korrelation von Meldungen des Typs „packetdrop“ erkannt. Dementsprechend leiten sich die darin enthaltenen Informationen aus denen ab, die dem Datentyp „packetdrop“ entnommen werden können, nämlich

- der Ursprungs-IP-Adressen, einer Liste mit Adressen der Systeme, von denen der Portscan ausging (sources),
- der Zieladresse, der Adresse des gescannten Systems (destination),
- der Zielsignaturen, z. B. gescannter Ports (targets),
- der Anfangszeit (time_begin) und
- der Endzeit (time_end).

Eine solche Datei des Typs „portscan“ ist in Abbildung 4 dargestellt.

```
1 <portscan
xmlns="http://itsec.cs.uni-bonn.de/schema/monika/poc">
2 <sources>
3 <source>203.0.113.37</source>
4 <source>203.0.113.73</source>
5 </sources>
6 <destination>198.51.100.100</destination>
7 <targets>
8 <target>TCP/21</target>
9 <target>TCP/22</target>
10 <target>TCP/23</target>
11 <target>TCP/25</target>
12 <target>TCP/67</target>
13 <target>TCP/68</target>
14 <target>TCP/80</target>
15 <target>TCP/110</target>
16 <target>TCP/143</target>
17 <target>TCP/443</target>
18 </targets>
19 <time_begin>2013-02-02T04:32:15Z</time_begin>
20 <time_end>2013-02-02T04:32:24Z</time_end>
21 </portscan>
```

Abbildung 4: XML-Datei über Portscans nach Zusammenfassung durch das EvA-Service-Cluster

Die im Datentyp „hostdiscovery“ dargestellten Ereignisse ähneln einem Portscan, unterscheiden sich aber dadurch, dass hier nicht ein System auf verschiedene Verbindungsmöglichkeiten hin untersucht wird, sondern mehrere Systeme auf die gleiche Verbindungsmöglichkeit. Bei dem Typ „host-discovery“ geht es also um das Auffinden von Systemen, die eine bestimmte Art von Netzverbindung zulassen. Genau wie der Typ „portscan“ entsteht auch der Typ „hostdiscovery“ durch Korrelation von „packetdrop“-Nachrichten und enthält dementsprechend aus diesem Typ extrahierte Informationen:

- Ursprungsadressen (sources),
- Zieladressen (destinations),
- Zielsignatur (targets),
- Anfangszeit (time_begin) und
- Endzeit (time_end).

Eine beispielhafte XML-Datei des Typs „hostdiscovery“ ist in Abbildung 5 aufgeführt.

```
1 <hostdiscovery
xmlns="http://itsec.cs.uni-bonn.de/schema/monika/poc">
2 <sources>
3 <source>203.0.113.37</source>
4 </sources>
5 <destinations>
6 <destination>192.0.2.1</destination>
7 <destination>192.0.2.2</destination>
8 <destination>192.0.2.3</destination>
9 <destination>192.0.2.4</destination>
10 <destination>192.0.2.5</destination>
11 <destination>192.0.2.6</destination>
12 <destination>192.0.2.7</destination>
13 <destination>192.0.2.8</destination>
14 <destination>192.0.2.9</destination>
15 <destination>192.0.2.10</destination>
16 </destinations>
17 <target>TCP/21</target>
18 <time_begin>2013-02-02T03:26:04Z</time_begin>
19 <time_end>2013-02-02T03:26:13Z</time_end>
20 </hostdiscovery>
```

Abbildung 5: XML-Datei „hostdiscovery“ nach Zusammenfassung durch das EvA-Service-Cluster

Der letzte Datentyp „eventsequence“ enthält schließlich eine Liste von Einzelereignissen, zwischen denen durch Korrelation ein potentieller Zusammenhang festgestellt wurde. Hierzu werden die Dateien „accessviolation“ untereinander sowie mit Nachrichten der Typen „packetdrop“, „portscan“ sowie „hostdiscovery“ korreliert. Die entstehenden „eventsequence“-Dateien listen zusammengehörige Ereignisse in der Reihenfolge ihres Ablaufs auf. Damit ist der Nachrichtentyp „eventsequence“ zum Beispiel dazu geeignet, (verteilte) Angriffe mit Vorbereitungs- und Durchführungsphase zu beschreiben.

Abbildung 6 zeigt beispielhaft eine Datei des Typs „eventsequence“.

```
1 <eventsequence
xmlns="http://itsec.cs.uni-bonn.de/schema/monika/poc">
2 <hostdiscovery>
3 <sources>
4 <source>203.0.113.37</source>
5 </sources>
6 <destinations>
7 <destination>192.0.2.1</destination>
8 <destination>192.0.2.2</destination>
9 <destination>192.0.2.3</destination>
10 <destination>192.0.2.4</destination>
11 <destination>192.0.2.5</destination>
12 <destination>192.0.2.6</destination>
13 <destination>192.0.2.7</destination>
14 <destination>192.0.2.8</destination>
15 <destination>192.0.2.9</destination>
16 <destination>192.0.2.10</destination>
17 </destinations>
18 <target>TCP/21</target>
19 <time_begin>2013-02-02T03:26:04Z</time_begin>
20 <time_end>2013-02-02T03:26:13Z</time_end>
21 </hostdiscovery>
22 <accessviolation>
23 <source>203.0.113.37</source>
24 <destination>192.0.2.11</destination>
25 <target>TCP/21</target>
26 <time>2013-02-02T03:26:14Z</time>
27 <protocol>FTP</protocol>
28 <protocolmethod>PWD</protocolmethod>
29 <resource>.</resource>
30 <authtoken>anonymous</authtoken>
31 <reason>Unauthorized</reason>
32 </accessviolation>
33 </eventsequence>
```

Abbildung 6: XML-Datei über eine Eventsequence nach Zusammenfassung durch den EvA-Service-Cluster

Im EvA-Service-Cluster werden die von den Agenten gelieferten Nachrichten der Typen „packet-drop“ und „accessviolation“ ausgewertet, aggregiert und korreliert. Die Handhabung der einzelnen Nachrichten hängt dabei von deren Typ ab. Eingehende „packetdrop“-Daten werden in einer lokalen Datenbank vorgehalten. Existieren hier bereits Einträge über zuvor eingegangene Nachrichten, werden neu eingehende mit diesen auf Gemeinsamkeiten hin abgeglichen. Miteinander verglichen werden

jeweils die Datenfelder „source“, „destination“ und „target“. Das Datenfeld „time“ dient der Filterung von Kandidaten für den Abgleich, so dass nur Ereignisse miteinander in Beziehung gesetzt werden, die innerhalb eines definierten zeitlichen Abstands zueinander aufgetreten sind. Aus der Korrelation von „packetdrop“-Nachrichten untereinander werden bei Übereinstimmung unmittelbar Ergebnisse produziert. Die Art des Ergebnisses hängt dabei davon ab, in welchem Verhältnis die einzelnen Datenfelder zueinander stehen. Diese Zusammenhänge sind in Tabelle 12 dargestellt.

Tabelle 12: Korrelation von „packetdrop“-Ereignissen

Korrelation	Ergebnis
Portscan	„destination“ gleich, „target“ verschieden
Hostdiscovery	„target“ gleich

Diese Ergebnisse werden sowohl in einer lokalen Datenbank vorgehalten als auch an die angeschlossenen Agenten weitergereicht. „packetdrop“-Ereignisse, die sich nicht mit anderen verbinden oder in „portscans“ oder „hostdiscoveries“ einordnen lassen, werden ebenfalls weiter in der Datenbank vorgehalten, ebenso eingehende „accessviolation“-Nachrichten. Auch die „accessviolation“-Ereignisse werden mit Daten der drei bereits zuvor erhobenen Typen „portscan“, „hostdiscovery“ und „packetdrop“ auf Übereinstimmung bestimmter Datenfelder bei Ereignissen innerhalb einer bestimmten Zeitspanne verglichen. Tabelle 13 fasst die hergestellten Beziehungen zusammen. Die Verknüpfung von Ereignissen wird in Form von „eventsequence“-Nachrichten an die Agenten kommuniziert.

Tabelle 13: Korrelation von „accessviolation“-Ereignissen

Datentyp	Vergleich auf Übereinstimmung in …
Portscan	destination
Hostdiscovery	target
Packetdrop	source, target

6.4 Optionen zu Datensparsamkeit im PoC

Die bei den Sendern des MonIKA-Systems entstehenden Datensammlungen sollen nach ihrer Vorauswertung durch die örtliche MonIKA-Software und die SOC nicht unverändert in ihrer Rohfassung an die MonIKA-GmbH weitergeleitet werden. Sie müssen vor ihrer Weiterverschickung kryptographische und datenminimierende Maßnahmen durchlaufen.

6.4.1 Bildung von Hashwerten

Die Bildung von Hashwerten ist ein gängiges Werkzeug der Informationstechnik, um den Inhalt einer Datei auf eine kleinere Zahlenfolge abzubilden. Dies kann mithilfe verschiedener mathematischer Formeln geschehen. Aus einem fünfseitigen Text lässt sich so beispielsweise (je nach gewählter Formel) ein zehnstelliger Hashwert errechnen, der möglichst einmalig ist und so als eindeutiger Stellvertreter des Ursprungstexts behandelt werden kann, ohne dass der Inhalt des Ursprungstexts noch erkennbar wäre. Ein Nebenerfolg der Bildung von Hashwerten besteht also darin, dass der Inhalt der Ursprungsdatei nicht in seiner ursprünglichen Form im Hashwert vorhanden ist und damit mögliche personenbezogene Informationen nicht aus dem Hashwert unmittelbar erkennbar sind. Dieses Ergebnis kann im

MonIKA-System genutzt werden, um die geloggten Daten nicht im Klartext, sondern in verfremdeter Form zur Auswertung zu übergeben.

Einige Datenkategorien, wie etwa der Zeitpunkt eines Zugriffs auf Netzkomponenten der Unternehmen, müssen durch die MonIKA-GmbH aber derart fusioniert werden, dass eine Einschätzung über die Häufung von Zugriffen in einem bestimmten Zeitfenster möglich bleibt. So sollen beispielsweise die Zugriffe von externen IP-Adressen in einem bestimmten Zeitrahmen miteinander korreliert werden. Die Bildung von Hashwerten aus allen IP-Adressen und Zeitdaten würde grundsätzlich zum Verlust jeder Information über die Daten im Klartext führen und einen Vergleich der IP-Adress-Zugriffe unmöglich machen. Um dies zu verhindern, können moderne Methoden eingesetzt werden, die es ermöglichen, trotz der Bildung von Hashwerten noch immer Vergleiche anstellen zu können. So ist im Ergebnis aus den Hashwerten zweier IP-Adress-Zugriffe zwar nicht mehr erkennbar, wann genau die Zugriffe erfolgten, es bleibt aber möglich, Aussagen darüber zu treffen, ob die Zeitpunkte identisch sind oder in welchem zeitlichen Anstand die Zugriffe stattfanden. Als spezielles System kommt beispielswese die von Kerschbaum[232] entwickelte Methode zur distanzerhaltenden Pseudonymisierung von Zeitstempeln in Betracht, die genau diese Vergleichbarkeit für Timestamps erhält.

Anstatt nun also die Daten über die einzelnen Zugriffszeitpunkte im Klartext an die MonIKA-GmbH zu schicken, erhält diese nur Hashwerte. Diese Werte können aber trotzdem noch mit den Werten der anderen Teilnehmer verglichen und auf Übereinstimmung überprüft werden. So bleibt einerseits der Klartext verborgen, das MonIKA-Service-Cluster kann aber trotzdem auf einzelne Lieferanten verteilte, aber zeitlich verdächtige IT-Angriffe erkennen.

6.4.2 Pseudonymisierung

Diese soeben beschriebene Bildung von Hashwerten stellt damit einen Sonderfall allgemeiner Pseudonymisierung dar. Andere Möglichkeiten sind in Abschnitt 3.2.2 angesprochen und je nach Datenkategorie mit mehr oder weniger Aufwand einsetzbar.

Das Problem, dass eine einfache Pseudonymisierung von IP-Adressen aufgrund der geringen Anzahl von Variationen im IPv4-Standard wenig Schutz vor einer Aufdeckung bietet, stellt sich bei den Portnummern im PoC im gesteigerten Maße. Während es 4.294.967.296 mögliche IPv4-Adressen gibt, ist nach dem Standard RFC 6335 sogar nur ein Portnummern-Bereich von 0 bis 65535 zugeordnet, was die Aufdeckung des Klartexts durch einen Brute-Force-Angriff zusätzlich erleichtert. Hier sind also Verfahren notwendig, die eine Erhebung und Übertragung der nur erforderlichen Daten umsetzen, die aber gleichzeitig eine ausreichend effektive Verwendung zu den Zwecken der Monitoring-Netze ermöglichen.

6.4.3 Manuelle Filterung

Als Besonderheit sieht der PoC eine manuelle Filterung durch einen zuständigen Mitarbeiter, unter Umständen den betrieblichen Datenschutzbeauftragten, vor. Diese manuelle Filterung ist auf zweierlei Art möglich. Zum einen ist vor der ersten Weiterleitung der Daten von dem EvA-Agenten zum EvA-Service-Cluster eine Freigabe durch den zuständigen Mitarbeiter erforderlich. Diese Freigabe wird durch ein Rollenkonzept begleitet, das verlangt, dass sich der berechtigte Mitarbeiter in der Bedienoberfläche des EvA-Agenten einloggt, während die normalen Administratoren diese Rechte nicht haben. Dort können die Klardaten mit den Daten verglichen werden, die nach den datenminimierenden Verfahren an das Service-Cluster gesendet werden sollen. Erst nach Freigabe durch den Mitarbeiter beginnt die Datenversendung. Zum anderen kann der Mitarbeiter in einer Art Live-Preview die aktuellen durch den EvA-Agenten verarbeiteten Daten einsehen. Werden dabei Daten erkannt, die aus Datenschutzsicht – oder beispielsweise zur Wahrung von Geschäftsgeheimnissen – nicht übersandt

[232] *Kerschbaum,* Distance-Preserving Pseudonymization for Timestamps and Spatial Data, ACM Workshop on Privacy in the Electronic Society (WPES), 2007, http://www.fkerschbaum.org/wpes07.pdf.

werden sollen, besteht die Möglichkeit, in den Ablauf einzugreifen und gegebenenfalls die Konfiguration zu ändern. Sollten also trotz der entsprechenden Programmierung der MonIKA-Software Daten übersandt werden, deren Inhalt unnötigerweise personenbezogene Daten enthalten oder auch Geschäftsgeheimnisse offenbaren würde, so kann die Übertragung manuell geprüft und letztlich unterbunden werden.

6.5 Rechtliche Erwägungen zum PoC

Der Proof-of-Concept bietet in einzelnen Punkten abweichende Facetten gegenüber den allgemeinen Ausführungen in Abschnitt 3. Soweit sich keine Besonderheiten ergeben, wird zur Vermeidung von Wiederholungen nach oben verwiesen oder Wesentliches zusammengefasst.

6.5.1 Daten mit Personenbezug

Neben den bereits in den allgemeinen Darstellungen erörterten Kategorien wie IP-Adressen, Zeitpunkte der Ereignisse oder Inhalt von E-Mails kommen im PoC insbesondere zwei neue Kategorien hinzu: die Portnummern und diverse Informationen aus den Protokollen TCP oder HTTP.

Die Portnummern dienen laut der IETF primär der Unterscheidung von verschiedenen Verbindungen, die zwischen zwei IP-Adressen hergestellt werden.[233] Darüber hinaus sind viele Ports aber auch bei der IANA für bestimmte Anwendungen reserviert, was dazu führen kann, dass zusammen mit der geloggten IP-Adresse nicht nur der Absender der Kommunikation für die Teilnehmer erkennbar ist, sondern auch konkrete genutzte Anwendungen identifizierbar sind. So lässt sich über die Portnummer beispielsweise herausfinden, dass bestimmte Hardware genutzt wird. Beispielsweise wird Port 311 für Mac OS X-Server genutzt, und andere Ports erlauben Rückschlüsse auf die Nutzung von VPN-Diensten (OpenVPN nutzt Port 1194), Mediennutzung (Port 1234 ist voreingestellt für UDP/RTP-Streaming im VLC Media Player) oder sogar die Nutzung bestimmter Spiele (Port 666 ist unter anderem dem Ego-Shooter „Doom“ zugewiesen). Die Kenntnis der offenen Ports eines Systems kann also in Einzelfällen durchaus Auskunft über persönliche oder sachliche Verhältnisse einer Person ergeben und ist damit nicht ohne Personenbezug.

Die in TCP und HTTP enthaltenen Informationen sind im PoC daneben vor allem relevant, weil die enthaltenen Authentifizierungsdaten Personenbezug haben können. Das mehrfache fehlgeschlagene Einloggen des Nutzers „HMüller“ lässt den Rückschluss zu, dass der Nutzer mit diesem Pseudonym oder Klarnamen erfolglos versucht hat, auf ein bestimmtes System zuzugreifen.

6.5.2 Verantwortlichkeit der Beteiligten im PoC

In Bezug auf die Einordnung der MonIKA-Beteiligten ergeben sich im PoC keine Besonderheiten. Es handelt sich vielmehr um eine Variante des „joint controllerships“, wie es in Abschnitt 3.1.2.3 dargestellt ist.

Die Teilnehmer sind gemäß Art. 2 d) DSRL verantwortliche Stellen, weil jedes der teilnehmenden Unternehmen im Sinne der Datenschutzrichtlinie

„über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“.

Bei der MonIKA-GmbH verbleiben als Zentralstelle hingegen alle weiteren Entscheidungen. Die Art der Verarbeitung, die Dauer der Speicherung und die Frage, welche Parteien innerhalb der MonIKA-GmbH Zugriff haben, wird faktisch von der GmbH festgelegt, da diese das Produkt entwickelt, gestaltet und bei den Teilnehmern implementiert. Der Einordnung als reine Auftragsdatenverarbeitung durch die MonIKA-GmbH spricht dabei insbesondere entgegen, dass das Monitoring grundsätzlich Aufgabe

[233] Internet Engineering Task Force (Hrsg.): Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry, RFC 6335, BCP 165, August 2011, S. 6.

der einzelnen Teilnehmer ist und der MonIKA-Dienstleister dies lediglich im Sinne der oben bereits angesprochenen Hilfsfunktion abnimmt. Dies mag bei der reinen Unterstützung der eigenen Netzsicherheit noch der Fall sein. Im Falle der Teilnahme an einem kooperativen Netz von datenliefernden MonIKA-Teilnehmern wird der Rahmen der reinen hilfsweisen Aufgabenauslagerung aber verlassen. Dies wird bereits dadurch deutlich, dass die MonIKA-GmbH nicht nur die Daten der einzelnen Teilnehmer getrennt verarbeitet, sondern daneben auch Daten anderer Teilnehmer mit diesen fusioniert und zu neuen Daten vereint. Der einzelne Teilnehmer kann damit auch keinerlei Weisungsrecht über das Verfahren haben, da ein solches Weisungsrecht für die Daten der anderen Unternehmen nicht besteht. Die MonIKA-Zentralstelle wird damit zwangsweise zu einer verantwortlichen Stelle, da das Ziel des MonIKA-Systems überhaupt nur in Unabhängigkeit von den einzelnen Teilnehmern erreicht werden kann.

6.5.3 Einordnung der Verarbeitungsschritte

Hinsichtlich der Verarbeitungsschritte ergibt sich keine Abweichung gegenüber den Aussagen in Abschnitt 3.1.3. Das Aufzeichnen und Speichern der Logdaten ist als Verarbeitung und Speicherung zu bewerten. Da die MonIKA-GmbH gegenüber den Teilnehmern auch als Dritte auftritt, ist hier eine Übermittlung gegeben. Schließlich stellt die Fusion und Korrelation zur Erkennung von Anomalien in dem Netzverkehr des Unternehmensverbundes auch eine Nutzung dar.

Als Besonderheit ist hier darauf hinzuweisen, dass der PoC in Form der Live-Preview-Funktion jederzeit die Kenntnisnahme von den erhobenen Daten ermöglicht, so dass die in Abschnitt 3.1.3.1 diskutierte Frage des „Beschaffens“ klar bejaht werden muss. Ein „Beschaffen“ im Sinne des BDSG setzt, wie ausgeführt, voraus, dass die Stelle

> *„Verfügung über die Daten begründet hat. Dazu genügt es, wenn [die Stelle] Datenträger in Besitz oder Daten zur Kenntnis genommen hat“*.[234]

Dies ist im PoC der Fall, da die Daten der Agenten nicht bloß blind an den CSOC geschickt werden, sondern von den Mitarbeitern der Unternehmen, regelmäßig vom betrieblichen Datenschutzbeauftragten, zur Kenntnis genommen werden können.

6.5.4 Rechtliche Überprüfung der datensparenden Verfahren

Wie auch in den allgemeinen Anwendungsszenarien muss sich die Datenverarbeitung des PoC auf seine Vereinbarkeit mit den Anforderungen der Datensparsamkeit und der Erforderlichkeit hinterfragen lassen. Dabei ist zu berücksichtigen, dass im PoC nicht alle technischen Möglichkeiten dargestellt sind, sondern die Implementierung je nach Zielsetzung der teilnehmenden Unternehmen variieren kann. Die Beschreibung der Klassifikations- und Korrelationstypen in Abschnitt 6.3 enthält in der Umsetzung des PoC zunächst keinerlei datensparende Mechanismen, sondern erhebt, verarbeitet und übermittelt alle Daten im Klartext. Diese Form der Umsetzung wirft in jedem Fall datenschutzrechtliche Bedenken auf und ist in dieser Form mit dem Erforderlichkeitsprinzip kaum vereinbar. Bereits die bloße Bildung von Hashwerten der IP-Adressen und Portnummern ist insofern ein milderes Mittel, allerdings dank seiner leichten Aufdeckbarkeit kaum mehr als ein guter Anfang.

Die Variabilität der Implementierungen aktueller und kommender Verfahren zeigt aber, dass das Potential der MonIKA-Umsetzung groß ist. So zeigt das Hashwertsystem von Kerschbaum, dass das Problem des geringen Zahlenraums bei IP-Adressen lösbar ist und gleichzeitig die Vergleichbarkeit von Zugriffszeitpunkten erhalten bleibt. Um bei den jeweiligen Sendern der Daten später eine Identifizierung der Hashwerte und eine Zuordnung zu den tatsächlichen IP-Adressen und Zeitpunkten zu ermöglichen, ist es zudem erforderlich, dass die Originale und entsprechenden Hashwerte zugeordnet gespeichert werden. Die Stärke des MonIKA-Ansatzes ist dabei seine Offenheit für kommende

[234] *Dammann*, in: Simitis, BDSG, § 3, Rn. 108.

Entwicklungen. Diese ist aber auch nötig, da die unveränderte Verarbeitung der Daten große Risiken für die betroffenen Personen darstellen kann.

Zusammen mit der Implementierung kommender datenminimierender Verfahren muss aber das Problem der Verwertbarkeit der Erkenntnisse gelöst werden. Wie in Abschnitt 4.2 dargestellt, führt die Pseudonymisierung von Logdaten dazu, dass diese zwar – abhängig von den eingesetzten technischen Verfahren – für die Zentralstelle noch fusionierbar und vergleichbar sind, doch nur für diejenigen Teilnehmer Erkenntnisse liefern, die diese Daten den eigentlichen Rohdaten zuordnen können. Würde im PoC etwa die IP-Adresse zusammen mit den Zugriffszeiten nach Kerschbaum gehasht und so an die MonIKA-GmbH übermittelt, wäre dort zwar die Untersuchung auf Gleichheit mit den Daten der anderen Unternehmen möglich. Stellte sich eine bestimmte IP-Adresse als anomale Quelle heraus, etwa weil von dort ein Portscan ausgeführt wurde, oder würden auffällig viele fehlerhafte Logins registriert, dann könnte nur derjenige Teilnehmer diese Anomalien konkreten Quell-IP-Adressen bzw. Logins zuordnen, der diese gehashten Werte mit den Originallogs in Beziehung setzen könnte. Alle anderen Teilnehmer erhielten zwar eine Mitteilung über eine Anomalie, könnten diese Erkenntnisse aber nicht verwerten.

Ein systembedingt ähnliches Problem ergibt sich hinsichtlich der Verarbeitung der Ziel-IP-Adressen. Diese werden, wie Tabelle 10 in Abschnitt 6.3.1 zeigt, zwar erhoben und auch durch das Cluster fusioniert. Diese Datenkategorie wird aber nicht zurückgesandt. Würden diese Daten im Klartext zurückgesandt, wäre für alle Teilnehmer die Erkenntnis möglich, welche Rechner in fremden Unternehmen Opfer einer Anomalie waren. Dies ist aus Datenschutzsicht nicht ideal, da die Erkenntnis über den Angriff auf bestimmte Systeme im Grunde nur dort interessiert, wo diese Angriffe auch stattgefunden haben. Nur diejenigen, in deren Netzen sich betroffene Rechner befinden, können tatsächlich auf die Anomalie reagieren. Für den Fall der Rücksendung der Ziel-IP-Adressen erhielten alle anderen Teilnehmer des PoC Informationen über ihre Konkurrenten, ohne dass damit dem Zweck, die eigene Infrastruktur zu schützen, gedient würde. Aus Sicht der Datensparsamkeit stellt die Ziel-IP-Adresse also ein nicht erforderliches Datum da. Die Entscheidung, sie den Teilnehmern nicht zurückzusenden, ist daher zu begrüßen.

6.5.5 Rechtsgrundlage für der Verarbeitungsschritte

Im Rahmen der Rechtsgrundlage ergeben sich ebenfalls einige Besonderheiten.

Gemäß den Ausführungen in Abschnitt 3.1.4.2.4 ist vorrangig die Anwendbarkeit des TKG zu diskutieren. Da im PoC keines der beteiligten Unternehmen als Telekommunikationsdienstleister im engen Sinne auftritt, ist lediglich interessant, wie die Unternehmen die Kommunikation ihrer Mitarbeiter regeln. Die Erlaubnis zur privaten Nutzung eröffnet, wie ausgeführt, den Anwendungsbereich des TKG. Im PoC ist jedoch per Betriebsvereinbarung eine private Nutzung der Unternehmensnetze ausgeschlossen, so dass insoweit keine Anwendbarkeit des TKG gegeben ist.

Die Anwendung des TMG ist im PoC ebenfalls fraglich. Zwar sind die Internet-Auftritte der einzelnen Teilnehmer grundsätzlich Telemedienangebote und das TMG dort auch anwendbar. Das Angriffsszenario im PoC konzentriert sich allerdings auf die firmeninterne SAP-Software, die nur einem abgeschlossenen und bestimmten Nutzerkreis zugänglich ist, so dass diesbezüglich die Anwendbarkeit des TMG nicht gegeben ist.

Im PoC ist somit das BDSG als Rechtsgrundlage heranzuziehen. Von den in den allgemeinen Ausführungen diskutierten Normen kommt mangels vertraglicher Beziehung zu den Angreifern im Kern für die Datenerhebung durch die Teilnehmer nur § 28 Abs. 1 S. 1 Nr. 2 BDSG in Betracht. Damit ist für die Rechtmäßigkeit der Datenverarbeitung im PoC vor allem die Abwägung zwischen den Zielen der teilnehmenden Unternehmen und denen der Betroffenen relevant. Die bereits in Abschnitt 3.1.4.2.4.4 dargestellten Interessen der Parteien werden im PoC dahingehend konkretisiert, dass insbesondere aufseiten der Betroffenen der Beschäftigtendatenschutz Gewicht erlangt. Die Aufzeichnung

des Internet-Verkehrs betrifft zwangsläufig auch Rechner von Mitarbeitern. Über die Logdaten kann anhand der kontaktierten IP-Adressen, der Zeitpunkte der Ereignisse, der Informationen aus den TCP- und HTTP-Daten und sogar der gescannten offenen Ports ein sehr genaues Profil über die beruflichen und möglicherweise auch über private Umstände des Mitarbeiter erstellt werden. Die Gefahr des Missbrauchs spricht im Rahmen einer Abwägung also ganz klar gegen die Verarbeitung dieser Daten. Dies gilt umso mehr, als dass die Daten auch mit den Daten von anderen Unternehmen und den dortigen Mitarbeitern korreliert werden können.

Demgegenüber steht das Interesse der beteiligten Unternehmen, die Möglichkeiten zu Detektion von Anomalien zu erkennen. Im PoC-Szenario wird dies dahingehend spezifiziert, dass ein Portscan erkannt werden soll. Um das Gewicht dieses Interesses beurteilen zu können, ist die Abwehr des Portscans hinsichtlich seiner Bedeutung für IT-Systeme eines Unternehmens einzuordnen. Portscans stellen oft die erste Ausforschungsstufe eines späteren Angriffs dar und sollen als Ergebnis liefern, ob und welche Ports offen sind, um Schwachstellen der dahinter laufenden Anwendungen auszunutzen. Wie das Klingeln an der Tür, um zu überprüfen, ob jemand im Haus ist, bevor ein Wohnungseinbruch begangen wird, wird der Portscan teilweise als unkritische Vorbereitungshandlung angesehen. Auch das Bundesamt für Sicherheit in der Informationstechnik stufte Anfang der 2000er Jahre einen Portscan vereinzelt noch nicht als Angriff auf Systeme, sondern als bloße Vorbereitungshandlung ein. Aktuelle Studien des BSI sehen in Portscans jedoch einen Angriff.[235] Das lässt sich zum einen deshalb vertreten, weil im Unterschied zum Türklingeln ein Portscan keine sozial-adäquate Handlung ist, sondern für sich selbst bereits die Frage aufwirft, warum ein Dritter alle offenen Ports eines Systems absucht. Zum anderen kann exzessives Portscanning auch selbst eine Beeinträchtigung darstellen, wenn auf diesem Wege dauerhaft und unablässig jeder Port angesprochen und damit die Kommunikation blockiert wird. In solchen Fällen, in denen ein Portscan unter Kontrolle eines Botnetzes einen Denial-of-Service-Angriff gegen ein System unternimmt, stellt der Portscan dann keine reine Vorbereitungshandlung dar, sondern ist selbst der Angriff gegen die Verfügbarkeit des Systems. Das SANS Institute stellte den Zwiespalt zwischen Vorbereitungshandlung und rechtswidrigem Angriff in einem Gutachten wie folgt dar:

> *„A scan is not an attack.“*[236]

Gleichzeitig stellt das Gutachten aber fest:

> *„Port scanning is nearly always considered malicious because of this ability for it to be exploited. Industry professionals consider port scanning an invasive activity that violates the target machine.“*[237]

Schließlich darf auf die Allgemeinen Geschäftsbedingungen vieler Provider hingewiesen werden, die, wie etwa die Telekom Austria[238], Portscan als vertragswidrig festlegen.

Mit diesen Rahmenbedingungen ist keine abschließende Bewertung des Portscans möglich. Allerdings lässt sich insoweit ein Urteil fällen, als dass die Eingriffsintensität eines Portscans unterhalb der eines Angriffs in die Systeme liegt. Es handelt sich meist um einen Ausforschungsvorgang, der den Verdacht weckt, dass schwerwiegendere Beeinträchtigungen drohen. Es stehen sich daher klar definierte Risiken für die Betroffenen und ein Gefahrenverdacht gegenüber. Entsprechend der Praxis in anderen Rechtsgebieten wie etwa im allgemeinen Polizei- und Ordnungsrecht, wo ein Gefahrenverdacht nur Gefahrenerforschungsmaßnahmen rechtfertigt[239], wird man im Portscan wohl ebenfalls auf Maßnahmen verweisen müssen, deren Mittel ein Weniger gegenüber den späteren Erkennungs-

[235] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), in: Studie „Durchführungskonzept für Penetrationstests“, S. 7.
[236] *Jamieson*, in: SANS Institute (Hrsg.), The Ethics and Legality of Port Scanning, S. 3.
[237] *Jamieson*, in: SANS Institute (Hrsg.), The Ethics and Legality of Port Scanning, S. 3.
[238] Telekom Austria AG, Allgemeine Geschäftsbedingungen AGB Mobil, S. 14, Punkt 1.5.2, online unter: https://cdn1.a1.net/final/de/media/pdf/AGB_Mobil_geltende_Fassung.pdf, aufgerufen am 14.02.2014.
[239] OVG Münster, NVwZ 1982, 46.

maßnahmen darstellt. Bezogen auf die Abwägung im Proof-of-Concept würde daher die volle Auswertung der gesamten Logfiles unter Umständen das zulässige Maß des Eingriffs in die Rechte der Betroffenen übersteigen. Stattdessen wären die teilnehmenden Unternehmen darauf zu verweisen, weniger Daten zu erfassen und zwar nur solche, die über das Ja oder Nein eines Portscans unterscheiden. Die Quell-IP-Adressen sowie Authentifizierungsdaten könnten dazu in einem ersten Schritt noch nicht nötig sein.

Vor diesem Hintergrund dürfte die vollständige Erhebung aller im PoC beschriebenen Datenkategorien das durch § 28 Abs. 1 S. 1 Nr. 2 BDSG gerechtfertigte Maß übersteigen, sofern es allein um die Erkennung von Portscans geht.

6.5.6 Sonstige datenschutzrechtliche Besonderheiten

In Ergänzung zu in den Abschnitten 3.1.5 und 3.3.4 dargestellten Rahmenbedingungen des BDSG für den Einsatz von Anomalie erkennenden Monitoring-Netzen weist der Proof-of-Concept einige Besonderheiten auf.

Hinzuweisen ist insbesondere auf den betrieblichen Datenschutzbeauftragten. Der Beauftragte hat die Datenverarbeitung zu überwachen. Diese Kontrollpflicht beinhaltet, die Anwendung der Verarbeitungsprogramme unter Umständen durch unangemeldete Kontrollen zu überwachen. Weiterhin ist der Beauftragte bei der Neugestaltung bzw. -einführung von Verarbeitungsprogrammen frühzeitig hinzuzuziehen, um evtl. datenschutzrechtlich gebotene Korrekturen vorzunehmen.

Im Rahmen des Proof-of-Concepts hat der Beauftragte deshalb insbesondere zwei Aufgaben wahrzunehmen. Er muss einerseits die Policies kontrollieren, die das CSOC für die Datenverarbeitung und -weiterleitung durch die Agenten implementieren will. Dazu gehört insbesondere die Überprüfung der eingesetzten Techniken der Datenminimierung dahingehend, ob die verarbeiteten Daten zur Teilnahme an dem Monitoring-Netz erforderlich sind. Andererseits muss er die Einhaltung dieser Policies später überwachen, wozu er insbesondere über die Live-Preview-Funktion eine ständige Kontrollmöglichkeit erhält.

Da der PoC in einem Unternehmensverbund angesiedelt ist, sind die Zwecke der Datenverarbeitung besonders auf ihre Vereinbarkeit mit dem Beschäftigtendatenschutz zu untersuchen.

7 Verbleibende Forschungsfragen

Aus Sicht des Datenschutzes ergeben sich aus den dargestellten Analysen vielfältige – teilweise grundlegende – Forschungsgebiete und -fragen. Dazu gehören insbesondere:

- Welche technischen Verfahren erlauben die bestmögliche Minimierung der erforderlichen Daten, unterstützen aber gleichzeitig die Fusion und Auswertbarkeit zur effektiven Erkennung von Anomalien?
- Wie sähen Hashverfahren aus, die geeignet sind, konkrete Operationen für komplexe Daten auch auf den Hashwerten anstelle der Originaldaten durchzuführen? Lassen sich derartige Hashverfahren formalisieren?
- Wie kann die Präzision der Spam-Erkennung, insbesondere zur Minimierung falscher Positivmeldungen und Verbesserung der Mustererkennung in Texten, noch verbessert werden?
- Wie lassen sich die einzelnen Hashverfahren hinsichtlich ihrer Eignung für den Datenschutz rechtlich bewerten?
- Wie verändert sich die Performanz des Gesamtsystems mit bzw. ohne Verwendung der genannten Hashverfahren?
- Wo liegen die Grenzen von Personenbezug und Anonymität in der Massendatenverarbeitung? Wie lassen sich diese Grenzen festlegen, und sind sie sinnvoll?
- Wie sind Verantwortlichkeit und „joint controllership“ in IT-gestützten Dienstleistungen vor dem Hintergrund zunehmender Aufgabenteilung zu bewerten?
- Inwieweit sind Rechtsgestaltung und Rechtsfortentwicklung notwendig für einen rechtmäßigem Einsatz von CERTs auf nationaler, europäischer und internationaler Ebene? Wie sollten geeignete Rechtsgrundlagen und Rahmenbedingungen für die Verarbeitung der Daten einschließlich eines potentiell grenzüberschreitenden Transfers aussehen?
- Wie bewertet man die vielfältigen möglichen Reaktionen auf detektierte Anomalien in einem Monitoring-Netz? Welche Auswirkungen ergeben sich aus den verschiedenen Reaktionsmöglichkeiten auf die Rechte der Betroffenen?

Es ist empfehlenswert, diese Fragen interdisziplinär zu bearbeiten, um zu tragfähigen Ergebnissen zu kommen. Gerade in Hinblick auf die wachsende Abhängigkeit der Gesellschaft von funktionierenden IT-Infrastrukturen und die aktuelle Entwicklung von juristischen und technischen Ansätzen für ein höheres Schutzniveau auf nationaler und europäischer Ebene sollten zeitnah Diskussionen über eine faire Gestaltung von Anomalie erkennenden Systemen geführt werden. Das MonIKA-Projekt hat erste Resultate geliefert, um die Diskussionen auf ein valides Fundament zu stellen. Gleichzeitig ist deutlich geworden, wo weiterer Bedarf für Forschung und Entwicklung besteht.

8 Zusammenfassung der Ergebnisse

Diese Ausarbeitung aus Perspektive des Datenschutzes und der Datensicherheit zur Zulässigkeit sowie zum Einsatz und zur Gestaltung von Anomalie erkennenden Verfahren in Internet-Infrastrukturen hat gezeigt, dass die Teilnahme an derartigen Monitoring-Verbänden vielfältige Fragestellung aufwirft.

Von größter Bedeutung sind dabei die Untersuchungen des Personenbezugs der verarbeiteten Daten und der datenschutzrechtlichen Verantwortlichkeit der Beteiligten. Beide Bereiche stehen unter dem Eindruck der immensen technischen Entwicklungen der Kommunikationstechnik und der hochkomplexen, verteilten Massendatenverarbeitung.

Für die Fragen des Personenbezugs ist dabei festzuhalten, dass nicht nur

- statische und dynamische IP-Adressen,

sondern auch

- Portnummern,
- Autonome-Systeme-Nummern sowie
- URLs

einen Personenbezug aufweisen können. Gestaltung und Betrieb der im MonIKA-Projekt untersuchten Monitoring-Netze müssen daher mit den Anforderungen des geltenden Datenschutzrechts vereinbar sein.

Für das Thema der „verantwortlichen Stelle“ hat sich gezeigt, dass in komplexen Systemen, wie sie der MonIKA-Ansatz beschreibt, die Konstruktion der Auftragsdatenverarbeitung kaum noch anwendbar ist. Die teilnehmenden Stellen sowie die Zentralstellen müssen mit Hinblick auf die gleichzeitig verzahnten und doch unabhängigen Datenverarbeitungsprozesse nebeneinander als verantwortliche Stellen angesehen werden.

Gleichermaßen grundlegende Arbeiten waren bezüglich der Rechtsgrundlagen für die Datenverarbeitung nötig. Dabei wurde deutlich, dass heutige Gesetze der Komplexität von verteilten Monitoring-Systemen nicht gerecht werden; auch aktuelle Entwürfe von neuen gesetzlichen Regelungen bieten dafür keine Lösungen. Die anwendbaren Vorschriften des Telekommunikations- und des allgemeinen Datenschutzrechts sind nur unter Auslegung vieler unbestimmter Rechtsbegriffe auf Systeme wie im MonIKA-Projekt beziehbar.

Zentrale Erkenntnisse konnten im Bereich der Datensparsamkeit gewonnen werden. Die Anforderungen der Datensparsamkeit stehen im Spannungsverhältnis zu dem Bedürfnis der Korrelierbarkeit und erfordern sehr genaue Zweckbestimmungen und die Ausnutzung geeigneter kryptographischer Verfahren, um die Balance mit Hinblick auf den Erforderlichkeitsgrundsatz zu halten.

Insgesamt hat sich gezeigt, dass der Einsatz von Anomalie erkennenden Verfahren in Internet-Infrastrukturen datenschutzkonform möglich ist, sofern die Prozesse von vornherein auf die Anforderungen der Datensparsamkeit und -vermeidung hin gestaltet werden und die organisatorischen und technischen Rahmenbedingungen dem besonderen Risiko massenhafter Datenfusion und -korrelation angepasst werden. Hier besteht weiterer Forschungsbedarf.

Literaturverzeichnis

Bücher, Kommentare

Dammann/Simitis	EG-Datenschutzrichtlinie Kommentar 1. Auflage Baden-Baden 1997
Däubler/Klebe/Wedde/Weichert	Bundesdatenschutzgesetz 3. Auflage Frankfurt am Main 2010
Geppert/Schütz	Beck'scher TKG-Kommentar 4. Auflage München 2013
Grabitz/Hilf [Hrsg.]	Das Recht der Europäischen Union Kommentar 26. Ergänzungslieferung München 2005
Graf [Hrsg.]	Beck'scher Online-Kommentar StPO, Auszug TKG 14. Edition Stand 01.06.2012
Heckmann	juris PraxisKommentar Internetrecht – Telemediengesetz, E-Commerce, E-Government 3. Auflage Saarbrücken 2011
Kühling/Seidel/Sivridis	Datenschutzrecht 2. Auflage Heidelberg 2011
Palandt	Beck'sche Kurzkommentare – Bürgerliches Gesetzbuch: BGB 71. Auflage München 2012
Plath [Hrsg.]	Bundesdatenschutzgesetz Kommentar 1. Auflage Köln 2013
Simitis [Hrsg.]	Bundesdatenschutzgesetz 7. Auflage Frankfurt am Main 2011
Wohlgemuth	Datenschutz für Arbeitnehmer 2. Auflage Neuwied 1988

Andere Publikationen

Artikel-29-Datenschutzgruppe	WP 48 – Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Arbeitnehmern, Brüssel 2001
dieselbe	WP 118 – Stellungnahme 2/2006 zu Datenschutzfragen bei Filterdiensten für elektronische Post Brüssel 2006
dieselbe	WP 136 – Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ Brüssel 2007
dieselbe	WP 148 – Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen Brüssel 2008
dieselbe	WP 169 – Opinion 1/2010 on the concepts of „controller“ and „processor“ Brüssel 2010
Bedner	Rechtmäßigkeit der „Deep Packet Inspection“ Projektgruppe verfassungsverträgliche Technikgestaltung Kassel 2009
Breyer	(Un-)Zulässigkeit einer anlasslosen, siebentägigen Vorratsdatenspeicherung – Grenzen des Rechts auf Anonymität MMR 2011, S. 573-578
Bundesamt für Sicherheit in der Informationstechnik (Hrsg.)	BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise Version 2.0 Bonn 2008 abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002_pdf.pdf?__blob=publicationFile
dasselbe	Studie „Durchführungskonzept für Penetrationstests“ Bonn 2003
Eckhardt	Auftragsdatenverarbeitung DuD 2013, S. 585-591

European Data Protection Supervisor (Hrsg.)
Opinion of the European Data Protection Supervisor on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a 'Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace', and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union
Brüssel 2013

abrufbar unter:
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-06-14_Cyber_security_EN.pdf

ENISA (Hrsg.)
Security White Paper 2011-002
CERT-EU Services – Fundamentals, Version 1.0
19.10.2011

abrufbar unter:
http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_11_002_v2_1.pdf

Gentry
Fully homomorphic encryption using ideal lattices
Symposium on Theory of Computing 2009, S. 169-178

Gola
Die Einwilligung als Legitimation für Verarbeitung von Arbeitnehmerdaten
RDV 2002, S. 109-116

Internet Engineering Task Force (Hrsg.)
Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry
RFC 6335, BCP 165
August 2011

Jamieson
The Ethics and Legality of Port Scanning
SANS Institute InfoSec Reading Room
2001

Kerschbaum
Distance-Preserving Pseudonymization for Timestamps and Spatial Data
ACM Workshop on Privacy in the Electronic Society (WPES)
Karlsruhe 2007

abrufbar unter:
http://www.fkerschbaum.org/wpes07.pdf

Krüger/Maucher
IP-Adresse wirklich ein personenbezogenes Datum? – Ein falscher Trend mit großen Auswirkungen auf die Praxis
MMR 2011, S. 433-439

Polyakov — A crushing blow at the heart of SAP J2EE Engine – Architecture and program vulnerabilities in SAP's J2EE engine
ERPScan 2011

Rogosch — Elektronische Einwilligung ist nicht gleich elektronische Einwilligung
DFN-Infobrief 2011, Heft 2, S. 5-6

Roßnagel/Scholz — Datenschutz durch Anonymität und Pseudonymität – Rechtsfolgen der Verwendung anonymer und pseudonymer Daten
MMR 2000, S. 721-731

Schulz — Die (Un-)Zulässigkeit von Datenübertragungen innerhalb verbundener Unternehmen
BB 2011, S. 2552-2557

Weichert — Datenschutzrechtliche Auswirkungen und Neuordnung des Uniwagnis-Systems
20. Wissenschaftstagung des Bundes der Versicherten (BdV) Timmendorfer Strand 2010

abrufbar unter:
https://www.datenschutzzentrum.de/vortraege/20100415-weichert-uniwagnis.html

Weichert — Neue Postleitzahlen und Datenschutz
DANA 2-1993, S. 4-7

Xu/Fan/Ammar/Moon — Prefix-Preserving IP Address Anonymization: Measurement-based Security Evaluation and a New Cryptography-based Scheme
Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP 2002)

abrufbar unter:
http://www.ieee-icnp.org/2002/papers/2002-25.pdf

Abkürzungen

AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Aktiengesellschaft
AO	Abgabenordnung
AS	Autonome Systeme
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BGP	Border Gateway Protocol
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
C&C	Command and Control
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CRLF	Carriage Return Line Feed
CSOC	Cyber Security Operations Center
DENIC	Deutsches Network Information Center
DoS	Denial of Service
DDoS	Distributed Denial of Service
DSGVO	Datenschutz-Grundverordnung; Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Entwurf)
DSRL	Europäische Datenschutzrichtlinie; Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
EDPS	European Data Protection Supervisor; Europäischer Datenschutzbeauftragter
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EMRK	Europäische Menschenrechtskonvention; Konvention zum Schutze der Menschenrechte und Grundfreiheiten
ENISA	European Network and Information Security Agency; Europäische Agentur für Netz- und Informationssicherheit
EU	Europäische Union
EuGH	Europäischer Gerichtshof

EvA	Erkennen von Anomalien
EvASC	Erkennen-von-Anomalien-Service-Cluster
FTP	File Transfer Protocol
GDV	Gesamtverband der deutschen Versicherungswirtschaft
GG	Grundgesetz
GmbH	Gesellschaft mit beschränkter Haftung
HDSG	Hessisches Datenschutzgesetz
HIS	Hinweis- und Informationssystem
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IT	Information Technology; Informationstechnik
LDSG S-H	Landesdatenschutzgesetz Schleswig-Holstein
LF	Line Feed
MonIKA	Monitoring durch Informationsfusion und Klassifikation zur Anomalieerkennung
PoC	Proof-of-Concept
RIPE (NCC)	Réseaux IP Européens (Network Coordination Centre)
RIS	Routing Information Service
RTP	Real-Time Transport Protocol
SANS	SysAdmin, Networking and Security
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol
SOC	Security Operations Center
TCP	Transmission Control Protocol
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network
XML	Extensible Markup Language