Kommunikation & Recht

Betriebs-Berater für
● Medien ● Telekommunikation ● Multimedia

12
K&R

21. Jahrgang **Dezember 2018** Seiten 741 – 812

dfv Mediengruppe · Frankfurt am Main

auf der Blockchain, ist aber ohne Möglichkeit der Entschlüsselung nicht personenbezogen und außerdem ohne Transaktions-ID schwerlich auffindbar. Sofern sowohl Speicherort auf der Blockchain als auch öffentlicher Schlüssel anderweitig veröffentlicht beziehungsweise kompromittiert werden, gilt auch hier der Löschungsanspruch nur bezüglich dieser beiden Daten.

VI. Hin zur Selbstverantwortlichkeit

Bisher hat sich das Recht noch immer der Wirklichkeit angepasst, und sei es durch langsame iterative Transformation.[75] Recht und seine Auslegung sind dem stetigen Wandel unterworfen und es steht außer Frage, dass auch Lösungen im Umgang mit DLT gefunden werden. In Bezug auf Datenschutz wäre aber gar ein ganz anderer Ansatz wünschenswerter: Nicht der Schutz der Daten durch den Staat und seine Gesetze, sondern durch die umfassende Kontrolle des Nutzers selbst (sog. *Self-Sovereign Digital Identity*).[76] Wie dies dank DLT gelingen könnte, zeigen momentan verschiedene Ideen. Am vielversprechendsten erscheint dabei die Möglichkeit, die Daten des Nutzers verschlüsselt auf einer Blockchain zu sichern. Nur der Nutzer selbst verfügt über den Schlüssel. Er ist Betroffener und Verantwortlicher bezüglich seiner eigenen Daten. Natürlich gibt es auf dem Weg zu einer solchen Utopie noch genug technische und rechtliche Probleme zu lösen. Die eigentlichen Ziele des Datenschutzrechts sind allerdings nur dann realisierbar, wenn die Möglichkeiten der Kontrolle durch den Einzelnen gegeben ist. Auf Dauer wird dies nur über DLT erreichbar sein, auf der der Nutzer seine Daten verwaltet und eine Form der Selbstverantwortlichkeit entsteht. Die vorliegende Analyse zeigt, dass viele Regelungen der DSGVO nur schwerlich mit dezentralen Netzwerken vereinbar sind. Bis hier durch Gesetzesänderungen oder Urteile Klarheit geschaffen wird, bleibt ein hohes Maß an Rechtsunsicherheit. Rechtliche Unsicherheit ist seit jeher einer weiteren Innovation abträglich. Wünschenswert wäre daher die Anwendung entsprechender Ausnahmeregelungen und Auslegungen inklusive entsprechender Klarstellungen, seitens Aufsichtsbehörden oder Kommission. Langfristig wäre ein Regulierungsansatz zu präferieren, der nicht ausschließlich auf zentralisierten Lösungen basiert und der zugleich die schrittweise Realisierung des dem Datenschutz immanenten Ziels – Selbstbestimmung – ermöglicht.[77]

75 Im Grundsatz bereits *Kaufmann*, ZVölkR 1908, 419, 438, „Die Theorie kann die Lebenstatsachen nicht ändern und hat kein Recht, jene, wenn sie sich im Widerspruch mit ihr befinden, zu verdrehen oder zu ignorieren. Vielmehr muss […] nach den wirklichen Vorgängen in der Welt die Theorie gestaltet und eventuell umgestaltet werden. Das gilt für alle ehrliche Wissenschaft".

76 Diese Chance herausstellend auch das Europäische Parlament, Entschließung v. 3. 10. 2018 – P8_TA-PROV(2018)0373, Nr. 28 ff.

77 Ähnlich dies anerkennend nunmehr auch das Europäische Parlament, Entschließung v. 3. 10. 2018 – P8_TA-PROV(2018)0373, Nr. 68, das heraushebt, dass versucht werden sollte, „die vorhandenen Hindernisse […]aus dem Wege zu räumen [und] […] eine anwendungsfallbezogene [Regelungs-]Methode zu wählen".

RA Dr. Florian Deusch, Ravensburg und Prof. Dr. Tobias Eggendorfer, Weingarten*

Intrusion Detection und DSGVO

Die DSGVO verlangt vom Verantwortlichen, die Datenströme seines IT-Systems zu kontrollieren, etwa durch Intrusion Detection Systeme (IDS). Gleichzeitig stellen sich zahlreiche Fragen zur Zulässigkeit des IDS-Betriebs.

I. Intrusion Detection zwischen Sicherheit und Datenschutz?

Intrusion Detection Systeme (IDS) sind Softwarelösungen, die Angriffe auf IT-Systeme erkennen und – als Intrusion Prevention Systeme (IPS) ausgestaltet – abwehren können.[1]

Bislang wurde für die Anwendung von IDS ein Zielkonflikt postuliert zwischen IT-Sicherheit und Datenschutz. Nicht in allen bisherigen Darstellungen sind die technischen Sachverhalte eindeutig definiert, die diesem scheinbaren Zielkonflikt zugrunde liegen. Dies gilt insbesondere für Begrifflichkeiten wie zum Beispiel Data Loss bzw. Leakage Prevention, Content Monitoring and Filtering und Deep Packet Inspection sowie SIEM (Sicherheits- und Ereignis-Management) -Systeme, die oftmals in einem Atemzug mit IDS genannt werden. Befürchtet wird dabei eine fortdauernde Echtzeit- und Totalüberwachung, die mit den Grundrechten der betroffenen Systemnutzer nicht vereinbar ist. Deshalb sind für den Einsatz derartiger Systeme in verschiedenster Weise Anforderungen und Grenzen formuliert worden, insbesondere Anonymisierung und Pseudonymisierung.[2]

Die Anforderungen der DSGVO werfen die Frage auf, ob für den Einsatz von IDS eine differenzierte Erhebung und Beurteilung des Sachverhalts erforderlich ist. Die Art. 24 und 33 Abs. 1 DSGVO verpflichten den Verantwortlichen eines IT-Systems, ihre Verarbeitungsvorgänge und Datenflüsse fortlaufend zu überwachen.[3] Erwägungsgrund 87

* Mehr über die Autoren erfahren Sie auf S. VIII. Der Autor *Florian Deusch* ist als Rechtsanwalt, Fachanwalt für Informationstechnologierecht und externer zertifizierter Datenschutzbeauftragter in der Anwaltskanzlei Dr. Gretter tätig; der Autor *Tobias Eggendorfer* ist Professor für IT-Sicherheit an der Hochschule Weingarten, freiberuflicher IT-Berater und ebenso zertifizierter externer Datenschutzbeauftragter. Der Beitrag geht auf einen Vortrag bei der DSRI-Herbstakademie 2018 zurück, der veröffentlicht wurde im Tagungsband von *Taeger* (Hrsg.), Rechtsfragen digitaler Transformation – Gestaltung digitaler Veränderungsprozesse durch Recht, Edewecht, 2018. Er ist überarbeitet und aktualisiert zum Stand Oktober 2018. Alle zitierten Internetquellen wurden zuletzt abgerufen am 31. 10. 2018.

1 *Eggendorfer*, Linux-Magazin 10/2015.

2 Siehe zum Beispiel *Conrad*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 34 Rn. 262; *Conrad*, CR 2011, 797 ff.; *Benner*, ZD-aktuell 2017, 05556; *Krügel*, MMR 2017, 795, 796; *Flegel/Raabe/Wacker*, DuD 2009, 735 sowie das Gutachten des Datenschutz-Zentrums Schleswig-Holstein vom 12. 2. 2013 zum Einsatz von „Loss Prevention", becklink 88316.

3 *Gola*, DSGVO, 2017, Art. 33 Rn. 40; *Voigt/von dem Bussche*, EU-Datenschutz-Grundverordnung (DSGVO): Praktikerhandbuch, 2018, Kapitel 3.8.2.2, S. 85.

DSGVO verlangt Maßnahmen, um Datenschutzverstöße „sofort" feststellen und melden zu können.

Folgende Beispiele verdeutlichen die Relevanz von IDS: Der Fahrdienst Uber verlor 2016 Kundendaten an Angreifer, die Daten waren ungesichert auf Amazon-Servern abgelegt. Daraus resultierten umfangreiche Schadenersatzforderungen gegen Uber. Immer noch verfügbar ist ein Tool, das die Standorte aller Uber-Fahrzeuge weltweit auf einer Karte live anzeigt. Bei der Fluggesellschaft British Airways sind Bankdaten von ca. 380 000 Kunden aus dem Zeitraum vom 21. 8. bis 5. 9. 2018 gestohlen worden. Grund war eine Sicherheitslücke bei Onlinebuchungen. Lynda.com, eine Microsoft-Tochter, die die Lernplattform video2brain anbietet, hat vor zwei Wochen Kundendaten über Cloud-Server verloren. Einem französischen Bauunternehmen sind Baupläne von Atomkraftwerken, Gefängnissen und Straßenbahnnetzen durch einen gezielten Angriff entwendet worden.[4]

IDS helfen, solche Datenabflüsse zeitnah zu erkennen, um damit eine Schadensvergrößerung zu verhindern. Dies ist die Voraussetzung zur Erfüllung der Meldepflicht gemäß Art. 33 DSGVO.

II. Funktionsweise von Intrusion Detection Systemen

IDS dienen dazu, sowohl statthabende als auch stattgehabte Angriffe auf IT-Systeme zu erkennen. Sie ermöglichen es, die vom Angreifer gewählten Angriffsvektoren zu erkennen und können zum Beispiel in Kombination mit einer anpassbaren Firewall zur Abwehr von stattfindenden Angriffen genutzt werden, teils sogar automatisiert. Man spricht dann von „Intrusion Prevention Systemen" (IPS). Über diesen Kernzweck hinaus ermöglichen es die IDS je nach Konfiguration, bei Datenexfiltrationen zu erkennen, welche Daten wohin übertragen wurden, sowie die konkreten Tathandlungen und Hinweise auf den Täter forensisch sicher festzustellen.

Im Kern unterscheidet man zwei Typen von IDS (siehe dazu unter 1. und 2.):

– Network Based IDS (NIDS) und
– Host Based IDS (HIDS).

Abzugrenzen sind die IDS im Sinne des vorliegenden Beitrags von anderen Anwendungen, deren datenschutzrechtliche Zulässigkeit unter dem Schlagwort „Data Loss Prevention" diskutiert wird (und ähnliche, siehe dazu unter 3.).

1. Network Based Intrusion Detection

Bei der netzwerkbasierten Erkennung von Angriffen überprüft ein ans Netzwerk angeschlossenes System den Netzwerkverkehr und warnt bei „verdächtigen" Aktivitäten. Um Aktivitäten so einzustufen, gibt es drei grundlegende Ansätze: Signaturbasiert, Anomalie-Erkennung und heuristische Verfahren.

a) Signaturbasierte Verfahren

Signaturbasierte Verfahren kennen die typischen Muster von bekannten Angriffen, die als sogenannte Signaturen ähnlich wie bei Virenscannern in einer Datenbank vorgehalten werden. Diese Systeme vergleichen den Netzwerkverkehr mit den bekannten Signaturen und alarmieren, sobald eine Angriffssignatur erkannt wird.

Solche Systeme[5] sind in der Regel nur in der Lage, bereits bekannte Angriffe zu erkennen, für die bereits Signaturen existieren. Daher gibt es hier regelmäßig Signatur-Updates.

Für die gängigen Standardangriffe und das „Grundrauschen" an Angriffen z. B. durch Script-Kiddies, wie jugendliche Möchte-Gern-Hacker, die automatisierte Angriffstools einsetzen, spöttisch genannt werden, sind diese Systeme gut geeignet, für elaboriertere und insbesondere individuelle Attacken jedoch nicht.

b) Anomalie-Erkennung

In jedem Netzwerk gibt es charakteristischen, üblichen Netzwerkverkehr: In einer Anwaltskanzlei zum Beispiel finden zu den Geschäftszeiten regelmäßig Datenübertragungen zu den Druckern statt, Zugriffe auf Dateien des Fileservers und Aufrufe von Rechtsprechungsdatenbanken. Ändert sich das Verhalten, erfolgen z. B. von einem Rechner plötzlich vermehrt Datenübertragungen zu ungewöhnlichen Zeiten oder ungewöhnlich viele DNS-Zugriffe,[6] kann das ein Anzeichen für einen Angriff sein. NIDS, die eine Anomalie-Erkennung nutzen, melden in solchen Fällen einen Angriffsverdacht.

Es gibt zwei denkbare Wege, die Normalsituation bzw. die Anomalien zu definieren: Ein Administrator spezifiziert manuell den Normalfall, oder die Systeme nutzen Machine Learning, um unverdächtige Pattern zu erlernen, und können so die Anomalie-Fälle selbstständig identifizieren.

c) Heuristiken

Als „qualifizierte Rateverfahren" dienen Heuristiken. Dabei gibt es Regelsätze, die für „kritisches" und „unkritisches" Netzwerkverhalten sprechen. Das können z. B. Datenmengen je nach Protokoll sein, aber auch Zugriffspattern, die z. B. auf einen Portscan hindeuten oder besondere lange URLs, die z. B. einen Buffer-Overflow auslösen könnten. Wird nun ein kritisches Verhalten entdeckt, wird ein Alarm ausgelöst – ziemlich analog zu den Erfahrungswerten, die z. B. der Zoll nutzt, um Schmuggler an Grenzen zu identifizieren. Solche Heuristiken sind dabei in der Regel vom Hersteller des NIDS vordefiniert und können anschließend bedarfsgerecht angepasst werden.

d) Zusammenfassung

Die NIDS erkennen anhand von Merkmalen des Netzwerkverkehrs ggf. verdächtige Datenpakete. Alle Verfahren haben ein spezifisches Risiko von Fehlalarmen und nicht erkannten Angriffen. Bei den Verfahren werden in unterschiedlichem Umfang personenbezogene und -beziehbare Daten aufgezeichnet. Eine besonders intensive Aufzeichnung erfolgt technisch notwendiger Weise beim automatisierten Erkennen von Anomalien, die nach Definition nur

4 Zu Uber: http://fortune.com/2018/04/12/uber-data-breach-security/, https://github.com/will3942/uber-hack; zu British Airways: http://www.airliners.de/grosses-datenleck-british-airways/46693; zu video2brain: https://www.engadget.com/2018/10/26/uber-breach-linkedin-lynda-indictment/; zu den Atomkraftwerken: https://www.handelsblatt.com/unternehmen/energie/cyber-angriff-hacker-stehlen-von-franzoesischem-bauunternehmen-plaene-von-atomanlagen/23258126.html?ticket=ST-2243861-XgIDAtvxgrmEbEZjvCuU-ap1.

5 Ein verbreitetes Beispiel ist Snort https://snort.org/.

6 Hier könnte z. B. ein Angreifer einen Command und Control-Server kontaktieren, DNS zur Datenexfiltration (https://blogs.akamai.com/2017/09/introduction-to-dns-data-exfiltration.html) nutzen oder sich einen Tunnel (z. B. https://dnstunnel.de/, http://www.linux-magazin.de/ausgaben/2010/04/rettungstunnel/) gebaut haben.

durch die Abweichung vom Normalfall, der dazu bekannt sein muss, erkannt werden können. NIDS können Angriffe sowohl im Versuchsstadium als auch während der Durchführung und im Fall der Anomalie-Erkennung auch deren Folgen erkennen.

2. Host Based Intrusion Detection

Im Gegensatz zu NIDS erkennen HIDS vorrangig die Folgen von erfolgreichen Angriffen. Dazu analysieren die Systeme Rechner (Host) auf spezifische Spuren von Angriffen. Auch hier gibt es verschiedene Möglichkeiten: Vom Malwarescanner (vulgo: Virenscanner), der Schadsoftware sucht, über Rootkit-Scannern, die nach Hinweisen auf eine Übernahme des Rechners durch Angreifer suchen, und Systeme, die Logfiles auf kritische Einträge prüfen, bis hin zu Software, die das Dateisystem auf kritische Änderungen prüft.

a) Malwarescanner

Malwarescanner suchen nach Schadsoftware. Dazu zählen Viren, Würmer, Trojaner und häufig auch Adware oder unerwünschte Anwendungen. Dabei nutzen sie sowohl Signaturen als auch Heuristiken. Typischer Weise scannen die Malwarescanner „on access", d. h. bei jedem Dateizugriff wird anhand aktueller Signaturen geprüft, ob es sich um eine Schadsoftware handelt. „On demand"-Scanner werden stattdessen auf Anforderung des Nutzers oder zeitgesteuert aktiv und überprüfen den gesamten Datenträger.

Neuere Malwarescanner nutzen zudem Cloud-Dienste des jeweiligen Anbieters. Dabei erzeugt das Programm zunächst einen eindeutigen Hash-Wert über die zu prüfende Datei, eine Art Quersumme, die jedoch zahlreichen kryptographischen Anforderungen genügen muss, und überträgt den in die Cloud. Ist die Datei anhand der Quersumme sowie weiterer Parameter als schädlich bzw. unschädlich identifiziert, reagiert die Software entsprechend. Konnte die Cloud keine Rückmeldung geben, wird die gesamte Datei übertragen, was je nach Inhalt der Datei datenschutzrechtlich relevant sein könnte.[7]

b) Rootkit Scanner

Ein Rootkit ist eine Software, die Angreifer auf ein einmal erfolgreich geknacktes System installieren, um sich in Zukunft ohne viel Aufwand wieder Zugriff auf das System verschaffen zu können. Dabei aktiviert das Rootkit meist einen Netzwerkport, sodass ein Zugriff von außen möglich ist, und stellt eine Kommandozeile zur Verfügung. Auf der hat der Angreifer meist „Root"-Rechte. Root ist in Linux-Systemen der Systemadministrator.

Um das Rootkit zu tarnen, erfolgt häufig der Austausch von wichtigen Systemprogrammen, wie z. B. ps, das die Prozesse anzeigt, und so das Rootkit mitlisten würden, oder netstat, das die verwendeten Netzdienste anzeigt. Die modifizierten Programme unterdrücken in ihrer Ausgabe Hinweise auf das Rootkit. Rootkit-Scanner vergleichen nun die Ausgaben verschiedener Systemprogramme sowie interne Systemparameter und warnen bei Abweichungen und Auffälligkeiten.[8]

c) Dateisystemkontrolle

Verbreitetet unter den HIDS, und häufig ausschließlich damit assoziiert, sind Systeme, die auf einem sauberen System unter anderem einen Hash-Wert der wichtigen Systemdateien, deren letzten Änderungsdatum sowie weiterer Parameter in einer besonders gesicherten Datenbank speichern. Diese vergleicht das HIDS periodisch mit dem Ist-Stand und schlägt bei Änderungen Alarm.[9] Dadurch erkennt es insbesondere Manipulationen, die typisch für Rootkits sind.

d) Logfile-Analyse

Zahlreiche Tools analysieren umfangreich die automatisch angelegten Protokolldateien des Systems und prüfen sie auf auffällige Einträge, die auf Angriffe hindeuten können.

e) Fazit HIDS

HIDS erkennen die Spuren, die Angreifer hinterlassen. Dabei arbeiten die Systeme größtenteils lokal auf dem zu schützenden Rechner, einige wenige nutzen einen zentralen, unternehmensweiten Server zur Sammlung der Ergebnisse. Nur einige moderne Malwarescanner nutzen Cloud-Dienste.

3. Begriffsabgrenzung zu Data Loss Prevention

a) Data Loss Prevention und ähnliche Systeme

Teilweise werden IDS gemeinsam mit den Begriffen *Data Loss bzw. Leakage Prevention, Content oder Network Security Monitoring and Filtering und Deep Packet Inspection sowie SIEM* als ein Maßnahmenbündel mit einer Vielzahl von technischen Einzelmaßnahmen dargestellt. Diese beinhalten sowohl NIDS-Komponenten, Content-Filter, aktive Überwachung auf den Clients, Inhaltsanalyse von E-Mail-Nachrichten und weitere Filter. Diese Maßnahmen dienen dabei auch verschiedenen Zwecken, neben dem Erkennen von Angriffen von außen sollen auch Innenangriffe sowie die Nutzung von fremden Datenträgern („USB-Sticks") erkannt werden. Auf dieser Grundlage wird die datenschutzrechtliche Zulässigkeit dieser Maßnahmen vielfach unter die pauschalen Postulate der Verschlüsselung, Pseudonymisierung und Anonymisierung gestellt.[10]

Durch diesen hohen Verquickungsgrad ist es schwierig, für die einzelnen Maßnahmen konkrete Ergebnisse abzuleiten. Vorliegend ist daher das Ziel, die verschiedenen Verfahren individuell zu bewerten, zumal die Datenschutzbehörden „Data Loss Prevention" in die Liste der Verarbeitungen aufgenommen haben, für die gemäß Art. 35 DSGVO eine Datenschutz-Folgenabschätzung erforderlich ist.[11]

Von den vorgenannten Systemen sind die hier behandelten IDS insoweit abzugrenzen, als die *Zielrichtung* von IDS die Überwachung von Datenströmen und Rechner- bzw. Programmaktivitäten ist. Personenbezogene Daten können dabei enthalten sein, indem dabei zum Beispiel IP-Adres-

7 Insbesondere ist hier eine Auftragsverarbeitung anzunehmen, was bei den überwiegend im US-amerikanischen Raum sitzenden Anbietern nicht einfach ist. Dazu kommt jenseits der Problematik des Datenschutzes das Risiko, Betriebs- und Geschäftsgeheimnisse dem Antivirus-Anbieter zu offenbaren.

8 Ein bekanntes Beispiel ist chkrootkit http://www.chkrootkit.org/.

9 Verbreitet sind Tripwire (https://www.tripwire.com/) und AIDE (http://aide.sourceforge.net/).

10 Siehe zum Beispiel *Conrad*, in: Auer-Reinsdorff/Conrad (Fn. 2), § 34 Rn. 262; *Conrad*, CR 2011, 797 ff.; *Benner*, ZD-aktuell 2017, 05556; *Krügel*, MMR 2017, 795, 796; *Flegel/Raabe/Wacker*, DuD 2009, 735, *Haas/Kast*, ZD 2015, 72 ff. sowie das Gutachten des Datenschutz-Zentrums Schleswig-Holstein vom 12. 2. 2013 zum Einsatz von „Loss Prevention", becklink 88316.

11 https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Liste-von-Verarbeitungsvorg%C3 %A4ngen-nach-Art.-35-Abs.-4-DS-GVO-LfDI-BW.pdf, Ziffer 6.

sen sowie Log-in und Log-out-Daten (mit) erfasst werden. Inhalte der Datenströme werden nur relevant, wenn das IDS aufgrund der darin konfigurierten Policies bestimmte Datenpakete als verdächtig einstuft und hieraus auf konkrete Angriffe geschlossen werden muss.

Im Gegensatz dazu geht es bei Data Loss Prevention jedenfalls nach der Lesart der Datenschutzbehörden um die *gezielte Verhaltenskontrolle* und die Erstellung systematischer Profile von *IT-Nutzern* mit der Absicht, unerwünschtes Verhalten zu erkennen.[12]

b) Anonymisierung und Pseudonymisierung bei IDS

Eine häufige Anforderung des Datenschutzes ist die Anonymisierung und Pseudonymisierung von Daten. Ersteres bedeutet, dass eine Zuordnung zur Person nie wieder möglich ist, zweiteres ermöglicht durch eine Rückübersetzung des Pseudonyms die Zuordnung (Art. 4 Nr. 5 DSGVO).[13]

Abweichend von den oben genannten Bewertungen für „Data Loss Prevention Systeme" ist im Fall von Intrusion-Detection-Systemen aus Sicht der IT-Sicherheit eine Anonymisierung unsinnig: Vorfälle müssen zur Aufklärung und zum Ergreifen geeigneter Gegenmaßnahmen Systemen zugeordnet werden. Diese Zuordnung erfolgt in aller Regel über die Netzwerkadresse, also IP- oder MAC-Adresse. Wenn durch Anonymisierung unklar ist, welches System kompromittiert wurde, ist eine angemessene Incident Response unmöglich.[14]

Die Pseudonymisierung würde eine Übersetzung der Netzwerkadresse durch ein Pseudonym erforderlich machen, dieses Pseudonym müsste bei einem Sicherheitsvorfall von der IT-Abteilung aufgelöst werden. Nun ist zunächst fraglich, wer außer der IT-Abteilung, die die Sicherheitsvorfälle bearbeitet, überhaupt eine IP-Adresse einem Arbeitsplatzrechner zuordnen kann. So verstanden wäre bereits die IP-Adresse an sich ein Pseudonym.

Ein Festhalten an dem Postulat der Pseudonymisierung würde jedenfalls für IDS dem Ziel einer effektiven Abwehr von IT-Sicherheitsvorfällen entgegenstehen, insbesondere wenn zur Auflösung der Pseudonyme der Datenschutzbeauftragte und/oder der Betriebsrat hinzuziehen wäre, da nicht alle Personen jederzeit verfügbar sind.

III. Intrusion Detection und DSGVO

Jede Verarbeitung personenbezogener Daten benötigt gemäß Art. 5 Abs. 1 lit. a und Art. 6 Abs. 1 DSGVO eine Rechtsgrundlage. Als Befugnisnormen für den Einsatz von IDS werden neben der Einwilligung Art. 6 Abs. 1 S. 1 lit. c und f DSGVO diskutiert.[15] Zu prüfen ist, ob und inwieweit diese Befugnisnormen geeignet sind, um IDS in der Praxis effektiv einzusetzen und welche Anforderungen an das „Wie" der Verarbeitung zu stellen sind.

Vorab: Die Einwilligung ist keine geeignete Rechtsgrundlage für den Betrieb von IDS. Sie ist jederzeit widerruflich (Art. 7 Abs. 3 S. 1 DSGVO). Der IDS-Betrieb wäre von der Willkür der betroffenen Personen abhängig.[16]

1. IDS-Betrieb zur Erfüllung einer rechtlichen Verpflichtung?

a) Art. 33 DSGVO als Rechtspflicht

IDS sind als Element zur IT- und Datensicherheit im Sinne der Art. 24, 32 DSGVO anerkannt. Hieraus ergibt sich jedoch noch nicht die Zulässigkeit zum Betrieb eines IDS. Die Rechtfertigung wird bislang ausschließlich an Art. 6 Abs. 1 S. 1 lit. f DSGVO gemessen, wobei die Herstellung der IT-Sicherheit als berechtigtes Interesse des Verantwortlichen angesehen wird.[17]

Der IDS-Betrieb könnte sich aber auch als eine rechtliche Verpflichtung gemäß Art. 6 Abs. 1 S. 1 lit. c DSGVO darstellen. Denn Art. 33 Abs. 1 DSGVO verlangt vom Verantwortlichen, jede Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst innerhalb von 72 Stunden, nachdem ihm die Verletzung bekannt wurde, bei der Behörde zu melden. Eine meldepflichtige Datenschutzverletzung ist gemäß Art. 4 Nr. 12 DSGVO jede *Verletzung der Sicherheit*, die zu einem Verletzungsergebnis führt.[18] Die Meldepflicht gilt zwar erst, wenn die Verletzung dem Verantwortlichen bekannt wurde, hieraus wird jedoch eine Pflicht des Verantwortlichen abgeleitet, Maßnahmen zur zeitnahen Erkennung von Sicherheitsverletzungen zu implementieren.[19] Das Mittel nach dem Stand der Technik, um Verletzungen der Sicherheit festzustellen, ist der Betrieb eines IDS (siehe oben Abschnitt II). Folglich verlangt die Erfüllung der rechtlichen Verpflichtung aus Art. 33 DSGVO, personenbezogene Daten durch IDS zu verarbeiten.

Allerdings ist das bisherige Verständnis von Art. 6 Abs. 1 S. 1 lit. c DSGVO geprägt von zwei Eingrenzungen:

– Die rechtliche Verpflichtung muss *öffentlich-rechtlicher* Natur sein, die Pflichterfüllung darf nicht im eigenen (wirtschaftlichen) Interesse des Verantwortlichen liegen.[20] Die Meldung von Datenschutzverletzungen bezweckt zwar zumindest auch die Vermeidung oder Minderung eines Schadens, was letztlich auch dem Verantwortlichen zugutekommt. Allerdings bezweckt Art. 33 zuvorderst, den Aufsichtsbehörden einen Überblick über Sicherheitslücken und die damit verbundenen Risiken zu verschaffen. Zudem beinhaltet die Norm präventive Wirkung, da die Meldepflicht entfällt, wenn Risiken für die Betroffenen aufgrund ergriffener Schutzmaßnahmen (etwa Verschlüsselung) nicht zu befürchten sind.[21]

Erwägungsgrund 45 zur DSGVO nennt die Gesundheitsvorsorge und die soziale Sicherheit als Beispiele für öffentliche Interessen im Sinne des Art. 6 Abs. 1 S. 1 lit. c

12 https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Liste-von-Verarbeitungsvorg%C3 %A4ngen-nach-Art.-35-Abs.-4-DS-GVO-LfDI-BW.pdf, dort Ziffer 6.

13 *Schantz/Wolff*, Das neue Datenschutzrecht, 2017, Rn. 297.

14 Im Sachverständigengutachten des Breyer-Verfahrens (LG Berlin, 31. 3. 2013 – 57 S 87/08 und EuGH, 19. 10. 2016 – C-582/14, siehe BeckRS 2016, 82520) ist dagegen auf S. 8 dargelegt, dass ein IDS mit Anonymisierung der IP-Adressen jedenfalls für Webseiten durchaus effektiv sei (http://www.daten-speicherung.de/wp-content/uploads/Surfprotokollierung_2011-07-29_Sachverst_an_LG.pdf; abgerufen 10. 10. 2018); laut EuGH kann die Erhebung der IP-Adresse zur Gewährleistung der Funktionsfähigkeit des Web-Auftritts aber sehr wohl nötig sein (EuGH, 19. 10. 2016 – C-582/14, K&R 2016, 811 ff., Rn. 56 und 64).

15 *Krügel*, MMR 2017, 795; *Haas/Kast*, ZD 2015, 72.

16 So bereits *Krügel*, MMR 2017, 975, 798.

17 Zum IDS als Element der IT-Sicherheit: VG Karlsruhe, 27. 5. 2013 – 2 K 3249/12, CR 2013, 428; *Bräutigam/Klindt*, NJW 2015, 1137, 1140; *Heidrich/Wegener*, in: Forgo/Helfrich/Schneider, Betrieblicher Datenschutz, 2. Aufl. 2017, Kapitel 5 Rn. 17; *Manz*, in: Sydow, DSGVO, 2017, Art. 32 Rn. 14; zu Art. 6 Abs. 1 S. 1 lit. f als Maßstab für IDS: *Piltz*, in: Gola, DSGVO (Fn. 3), Art. 32 Rn. 2; deutlich zur damit verbundenen Rechtsunsicherheit: *Krügel*, MMR 2017, 795, 799.

18 *Schantz/Wolff* (Fn. 13), Rn. 920; *Plath*, BDSG/DSGVO, 3. Aufl. 2018, Art. 33 Rn. 1.

19 *Plath* (Fn. 18), Art. 33 Rn. 3; *Gola* (Fn. 3), Art. 33 Rn. 28 (Ermittlungspflicht) und 40; *Voigt/von dem Bussche* (Fn. 2), Kapitel 3.8.2.2, S. 85.

20 *Assion/Nolte/Veil*, in: Gierschmann, DSGVO, 2018, Art. 6 Rn. 92.

21 *Gierschmann*, in: Gierschmann (Fn. 20), Art. 33 Rn. 1; *Gola*, (Fn. 3), Art. 33 Rn. 2, 3.

DSGVO. Hierbei ist nicht einzusehen, weshalb der IT-Sicherheit ein geringeres Gewicht zukommen sollte.[22]

Somit könnte die Meldung von Datenschutzverletzungen auch als öffentlich-rechtliche Pflicht im Sinne des Art. 6 Abs. 1 S. 1 lit. c DSGVO angesehen werden.

– Die rechtliche Verpflichtung muss sich *unmittelbar auf die Verarbeitung* beziehen. Rechtspflichten, für deren Erfüllung die Verarbeitung personenbezogener Daten nur mittelbar erforderlich sind (etwa weil sie auch auf andere Weise zu erfüllt werden können), sollen nicht unter Art. 6 Abs. 1 S. 1 lit. c zu fassen sein. Hiernach rechtfertigen zum Beispiel § 147 AO und § 257 HGB die Speicherung personenbezogener Daten, da der Gesetzestext ausdrücklich zur „Aufbewahrung" verpflichtet, ebenso die Sozialversicherungs- und Lohnsteuermeldungen des Arbeitgebers an das Finanzamt. Dagegen liege dem Monitoring eines Internet-Providers, um illegale Downloads von Internet-Nutzern zu bekämpfen, keine Rechtspflicht zugrunde, die die Verarbeitung rechtfertige. Dabei wird maßgeblich abgestellt auf das Working Paper 247 der Art. 29-Gruppe zum wortidentischen Art. 7 lit. c der Datenschutzrichtlinie 95/46/EG.[23]

Allerdings stellt die Art. 29-Gruppe nicht darauf ab, dass die Rechtspflicht zwingend die Verarbeitung personenbezogener Daten verlangt, sondern dem Verantwortlichen darf „kein übermäßiges Ermessen bei der Pflichterfüllung" verbleiben (no „undue degree of discretion to comply with the legal obligation").

Für den IDS-Betrieb könnte diese Formulierung greifen. Jedenfalls bei IT-Systemen mit einer gewissen Komplexität gibt es zu IDS keine Alternativen zur Feststellung von Angriffen (zumindest keine datenschutzfreundlicheren), zumal der Erwägungsgrund 87 zur DSGVO Maßnahmen verlangt, um Datenschutzverletzungen „sofort" feststellen und der Behörde melden zu können. Für dieses Verständnis könnte auch sprechen, dass die Verarbeitung personenbezogener Daten beim sogenannten „Terror-Listen-Screening" – insofern vergleichbar mit der Prüfung eines Datenstroms auf Anomalien durch IDS – ebenfalls auf Art. 6 Abs. 1 S. 1 lit. c gestützt wird,[24] obwohl die zugrundeliegenden Normen (VO (EG) Nr. 881/2002 und VO (EG) Nr. 2580/2001) keine unmittelbare Pflicht zur Datenverarbeitung enthalten, sondern lediglich ein Verbot, Wirtschaftsgüter an die gelisteten Terrorverdächtigen zur Verfügung zu stellen nebst einer entsprechenden Meldepflicht.[25]

Somit kann die Verarbeitung personenbezogener Daten durch IDS aufgrund Art. 6 Abs. 1 S. 1 lit. c DSGVO gerechtfertigt sein, jedenfalls dann, wenn sich Verletzungen der Sicherheit aufgrund der Komplexität des IT-Systems nicht anderweitig feststellen lassen.

b) Rechtspflichten aus Art. 32 DSGVO, § 13 TMG Abs. 7 TMG und § 109 ff. TKG

Rechtliche Verpflichtungen zur IT-Sicherheit enthalten auch Art. 32 DSGVO und § 13 Abs. 7 TMG. Gemäß Art. 32 Abs. 1 DSGVO hat der Verantwortliche „unter Berücksichtigung des Stands der Technik,[26] der Implementierungskosten und der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten."[27]

Diese Normen sind *nicht hinreichend konkret*, um eine Verarbeitung personenbezogener Daten als Rechtspflicht gemäß Art. 6 Abs. 1 S. 1 lit. c DSGVO zu rechtfertigen. Sie überlassen dem Verantwortlichen die Einschätzung, welches Sicherheitsniveau erforderlich ist und die Wahl, welche Mittel er hierfür ergreift. Geschuldet ist keine konkrete Handlung (etwa eine Meldung wie bei Art. 33 DSGVO), sondern es sind lediglich Maßnahmen vorzunehmen, mit dem Ziel („… um …"), ein angemessenes Sicherheitsniveau zu erreichen.

Auch die Verpflichtung zur IT-Sicherheit für Telekommunikationsdienstleister gemäß den §§ 109 ff. TKG ist in der Unternehmenspraxis nicht geeignet, als „Rechtspflicht" gemäß Art. 6 Abs. 1 S. 1 lit. c DSGVO die Datenverarbeitung zu rechtfertigen. Abgesehen davon, dass die bisherige Rechtsprechung den Arbeitgeber nicht als Anbieter von Telekommunikationsdiensten einordnet, enthalten auch diese Normen keine konkreten geschuldeten Handlungen, sondern lediglich die Anweisung, „angemessene" Maßnahmen zu treffen.[28]

Die Zulässigkeit aus Art. 6 Abs. 1 S. 1 lit. c DSGVO ergibt sich somit wegen der Rechtspflicht aus Art. 33 DSGVO und nicht aus Art. 32 DSGVO, § 13 TMG oder den §§ 109 ff. TKG.

2. IDS-Betrieb zur Wahrnehmung berechtigter Interessen

Auf Erwägungsgrund 49 zur DSGVO abstellend, sieht die wohl herrschende Meinung Art. 6 Abs. 1 S. 1 lit. f DSGVO als Rechtsgrundlage an für die Verarbeitung personenbezogener Daten durch IT-Sicherheitsmaßnahmen (Wahrnehmung berechtigter Interessen). Hierbei wird aber die Rechtsunsicherheit beklagt, die sich zu Lasten des Verantwortlichen aus dem (Bußgeld-) Risiko einer fehlerhaften Abwägung seiner Sicherheitsbelange gegen die Interessen der Betroffenen ergebe (sofern man Art. 83 DSGVO trotz rechtsstaatlicher Bedenken für wirksam hält).[29]

Der Rechtsunsicherheit könnte mit einer präzisen Erfassung des technischen Sachverhalts begegnet werden. Eine undifferenzierte Betrachtung von IDS, Deep Packet Inspection und SIEM kann keine verlässliche Interessenabwägung herbeiführen.[30] Dagegen kommt die BAG-Entscheidung „Keylogger" zu verlässlicheren Beurteilungen,

22 Jedenfalls sind IT-Sicherheitsmaßnahmen häufig nicht nur durch Art. 6 Abs. 1 S. 1 lit. f, sondern such gemäß lit. c gerechtfertigt, siehe hierzu *Assion/Nolte/Veil*, in: Gierschmann (Fn. 20), Art. 6 Rn. 92.

23 *Schantz/Wolff* (Fn. 13), Rn. 595 referenzieren auf das „Working-Paper" der Art. 29-Gruppe vom 9. 4. 2014, dort S. 17, 24 (http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf).

24 *Gola* (Fn. 3), Art. 6 Rn. 42.

25 Vgl. das BAFA-Merkblatt Terrorismusbekämpfung unter http://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_embargomassnahmen_terrorismusbek%C3 %A4mpfung.html.

26 Siehe dazu *Deusch/Eggendorfer*, K&R 2018, 223, 226.

27 Ähnlich § 13 Abs. 7 TMG: „(…) soweit dies technisch möglich und wirtschaftlich zumutbar ist (…)".

28 Zur Eigenschaft des Arbeitgebers als (kein) Diensteanbieter: LAG Berlin-Brandenburg, 14. 1. 2016 – 5 Sa 657/15, K&R 2016, 293; LAG Niedersachsen, 31. 5. 2010 – 12 Sa 875/09, K&R 2010, 613; VGH Hessen, 19. 5. 2009 – 6 A 2672/08.Z, K&R 2009, 748; zur fehlenden Konkretheit der TK-Normen: *Krügel*, MMR 2017, 797.

29 *Schantz/Wolff* (Fn. 13), Rn. 667, *Plath* (Fn. 18), Art. 6 Rn. 56; *Assion/Nolte/Veil*, in: Gierschmann (Fn. 20), Art. 6 Rn. 134; ebenso EuGH, 19. 10. 2016 – C-582/14 – Breyer, Ls. 2, K&R 2016, 811 ff.; die Rechtsunsicherheit des Abwägungsrisikos kritisierend *Krügel*, MMR 2017, 795, 799.

30 Zum Beispiel *Krügel*, MMR 2017, 795, 799.

weil darin differenziert wird: Der Einsatz von Keyloggern zur gezielten Erfassung von Tastatureingaben von Beschäftigten – insofern vergleichbar mit der Zielrichtung eines Data Loss Prevention Systems – ist nur aufgrund eines hinreichend konkreten Anfangsverdachts einer Straftat oder schweren Pflichtverletzung zulässig. Jedoch ist es bereits aufgrund einer abstrakten Gefahr zulässig, die Verlaufsdaten von Internetbrowsern vorübergehend zu speichern und nach abstrakt definierten Kriterien zu prüfen, ohne dass ein oder mehrere konkrete Mitarbeiter verdächtigt werden.[31] Die abstrakte Kontrolle von Browserdaten ist insofern vergleichbar mit der Prüfung des Datenstroms innerhalb eines Netzwerks durch ein IDS anhand zuvor definierter Signaturen, Anomalien oder Heurisiken.

Größere Probleme als bei der Interessenabwägung könnten sich ergeben, weil jeder Betroffene das Recht hat, der Verarbeitung seiner Daten gemäß Art. 21 Abs. 1 S. 1 DSGVO zu widersprechen. Hierüber ist er gemäß Art. 21 Abs. 4 DSGVO aufzuklären. Zwar dürfte der Widerspruch des Betroffenen in der Regel an Art. 21 Abs. 1 S. 2 DSGVO scheitern, weil die Interessen des Verantwortlichen an der IT-Sicherheit überwiegen bzw. die Verarbeitung zur Ausübung von Rechtsansprüchen dient (siehe dazu unter 3. a); dies muss der Verantwortliche dem Betroffenen jedoch gemäß Art. 12 Abs. 3 S. 1 DSGVO unverzüglich, längstens innerhalb eines Monats nachweisen.[32]

Den Verantwortlichen ist somit zu empfehlen, für derartige Nachweise einen standardisierten Prozess zu definieren für den Fall, dass Art. 6 Abs. 1 S. 1 lit. c DSGVO nicht greift.

3. Datenschutz-Anforderungen an den IDS-Betrieb

Unabhängig von der Rechtsgrundlage des IDS-Betriebs stellen sich die Fragen nach der Information der Betroffenen und einer datenschutzfreundlichen Gestaltung des IDS-Betriebs.

a) Information gemäß Art. 13 DSGVO

Der Verantwortliche muss die Betroffenen gemäß Art. 13 DSGVO informieren. Dabei steht es dem Sicherheitsinteresse entgegen, den Betroffenen den Zweck der Datenerhebung gemäß Art. 13 Abs. 1 lit. c bzw. d DSGVO mitzuteilen und damit die eigenen Sicherheitsvorkehrungen preiszugeben, zumal nicht nur die internen Nutzer des IT-Systems zu informieren wären, sondern auch alle, die über Schnittstellen mit externen Netzwerken (etwa aus dem Internet) mit dem IT-System kommunizieren.

Einen Ausweg aus diesem Dilemma könnte § 32 Abs. 1 Nr. 4 BDSG liefern. Hiernach besteht keine Informationspflicht gemäß Art. 13 DSGVO, wenn eine Information über die Weiterverarbeitung der Daten die Ausübung rechtlicher Anspruche beeinträchtigen würde und die Interessen des Verantwortlichen die Interessen des Betroffenen überwiegen. Diese Ausnahme ist gegeben, wenn von dem Betroffenen nach seiner Informierung Handlungen zu erwarten sind, die die Ausübung der rechtlichen Ansprüche erschweren würden, zum Beispiel Vermögensverschiebungen oder Beweisvereitelungen.[33]

Der IDS-Betrieb ist mit diesen Konstellationen vergleichbar. Durch das IDS übt der Verantwortliche seinen Anspruch auf Unterlassung von Angriffen auf sein IT-System gemäß §§ 823, 1004 BGB, 202 a und 202 b StGB aus. Die Verarbeitung durch das IDS ist eine Weiterverarbeitung im Sinne des Art. 6 Abs. 4 DSGVO, da die Daten der Betroffenen nicht zum Zweck des IDS, sondern zum Austausch von Daten erhoben werden. Die Information aller Betroffenen würde auch die Angreifer erfassen und somit die Gefahr von Umgehung der IDS begründen.

Falls hiervon abweichend § 32 BDSG nicht angewendet wird, bleibt dem Verantwortlichen lediglich, seine Information gemäß Art. 13 DSGVO so transparent wie nötig zu gestalten, ohne zu viel Informationen über seine Sicherheitsmaßnahmen preiszugeben.

b) Datenschutzfreundlichkeit

Da Verschlüsselung, Anonymisierung und Pseudonymisierung nicht mit dem Zweck eines IDS vereinbar sind,[34] sind die Anforderungen der Art. 5, 25 und 32 DSGVO durch andere organisatorische Vorkehrungen zu erfüllen, insbesondere durch folgende:

– Festlegung des Zwecks der Verarbeitung durch IDS, zum Beispiel im Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DSGVO.

Ob die Zweckfestlegung auch in einer Betriebsvereinbarung gemäß Art. 88 Abs. 1 DSGVO i.V.m. § 26 Abs. 4 BDSG und §§ 77, 87 BetrVG[35] erfolgen kann, ist fraglich. Dies scheitert jedenfalls dann, wenn der Arbeitgeber zum IDS-Betrieb verpflichtet ist. Denn ein Mitbestimmungsrecht gemäß § 87 BetrVG scheidet aus, wenn der Arbeitgeber keinen Entscheidungsspielraum hat.[36] Dies trifft in allen Fällen zu, in denen das IT-System des Arbeitgebers derart komplex ist, dass zu IDS keine technischen Alternativen bestehen, um Verletzungen der Sicherheit im Sinne des Art. 4 Nr. 12 DSGVO überhaupt zu erkennen.

Raum für Betriebsvereinbarungen besteht dagegen, wenn man zur Rechtfertigung des IDS-Betriebs auf Art. 6 Abs. 1 S. 1 lit. f DSGVO abstellt, da der Arbeitgeber in diesem Fall Entscheidungsspielräume hat (siehe oben unter 1.).

- Beschränkung der Zugriffsrechte auf die IT-Abteilung.
- Beschränkung der Zugriffswege auf und Schnittstellen zu den IDS-Daten.
- Begrenzter Speicherzeitraum.
- Keine geeignete Maßnahme dürfte es dagegen sein, auf ein „Zweischlüssel-Prinzip“ oder gar ein Treuhand-Modell abzustellen, bei dem Zugriff auf die IDS-Daten nur gestattet wird, wenn der Betriebsrat als Treuhänder im Einzelfall zustimmt.[37] Art. 33 DSGVO verlangt eine „unverzügliche Meldung“ an die Aufsichtsbehörden,

31 BAG, 27. 7. 2017 – 2 AZR 681/16, K&R 2017, 745, Rn. 24, 31.
32 *Gola* (Fn. 3), Art. 21 Rn. 14.
33 *Schantz/Wolff* (Fn. 13), Rn. 1166; *Schaffland/Holthaus*, in: Schaffland/Wiltfang, DSGVO/BDSG, 2018, § 32 BDSG Rn. 10.
34 Siehe oben Abschnitt II Ziffer 3 lit. b.
35 Einschlägig dürfte § 87 Abs. 1 Nr. 1 BetrVG sein; ob daneben § 87 Abs. 1 Nr. 6 BetrVG greift, hängt davon ab, ob man das IDS als Einrichtung versteht, die dazu bestimmt ist, das Verhalten von Arbeitnehmern zu überwachen. Zwar reicht hierfür eine lediglich objektive Eignung aus (*Kania*, in: Müller-Glöge/Preis/Schmidt, Erfurter Kommentar zum Arbeitsrecht, 18. Aufl. 2019, § 87 BetrVG Rn. 55). Ob diese objektive Eignung bei IDS jedoch vorliegt, obwohl die IDS-Daten aufgrund ihrer Abstraktheit nicht ohne weiteres „auf Knopfdruck“ für eine Verhaltenskontrolle genutzt werden können, bleibt einer vertiefenden Auseinandersetzung vorbehalten.
36 BAG, 11. 12. 2012 – 1 ABR 78/11, BB 2013, 1075.
37 So aber ein Ansatz im Rahmen des Forschungsprojekts DREI zur datenschutzkonformen Erkennung von Innentätern durch Softwaresysteme, ZD-Aktuell 2017, 05556; da zu dieser Studie bislang keine Ergebnisse veröffentlicht wurden, kann an dieser Stelle leider keine weitergehende Auseinandersetzung erfolgen. Kritisch zur praktischen Anwendung von „Zweischlüssel-Systemen“ (selbst bei Videoüberwachungen): *Lachenmann*, in: Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, 2. Aufl. 2018, Kapitel H, III, Anm. 18, S. 872.

„möglichst innerhalb von 72 Stunden." Erwägungsgrund 87 DSGVO geht sogar von einer „sofortigen" Meldung aus. Dieses enge gesetzliche Zeitfenster lässt keinen Raum für betriebsverfassungsrechtliche Auseinandersetzungen (unabhängig davon, dass der „Treuhänder" an sieben Tagen in der Woche von 0.00 Uhr bis 24.00 Uhr erreichbar sein müsste). Darüber hinaus dürfte ein effektiver IT-Sicherheitsschutz bereits vor Ablauf der 72 Stunden sofortige Gegenmaßnahmen verlangen, etwa wenn ein noch laufender Angriff erkannt wird (siehe oben Abschnitt II 3. b). Überdies ist fraglich, ob dem gesetzlichen Mandat des Betriebsrats ein derartiger Treuhand-Auftrag entnommen werden kann, welche Treuhand-Auflagen gelten sollen und wie die Haftung des Treuhänders gestaltet ist.

IV. Fazit

Bei der Beurteilung von IDS ist der technische Sachverhalt präzise zu erheben, insbesondere, um IDS abzugrenzen von der zielgerichteten Mitarbeiterüberwachung durch Data Loss Prevetion Systeme.

Der Betrieb eines IDS-Systems zur Kontrolle des Datenstroms eines IT-Systems mit dem Ziel, Angriffe zu erkennen und abzuwehren sowie Datenschutzverletzungen gemäß Art. 33 DSGVO zu melden, ist zulässig gemäß Art. 6 Abs. 1 S. 1 lit. c bzw. f DSGVO.

Die Information der Betroffenen kann den Sicherheitsbelangen entgegenstehen und gemäß § 32 BDSG entbehrlich sein.

Die Anforderungen der Art. 5, 25, 32 DSGVO sind durch organisatorische Vorkehrungen zu erfüllen.

Prof. Dr. Hubertus Gersdorf, Leipzig*

Informationsauftrag des öffentlich-rechtlichen Rundfunks

Ist eine gesetzliche Präzisierung des Angebotsauftrags verfassungsrechtlich möglich – und wie weit darf sie gehen?

Die Rundfunkpolitik überlegt derzeit, das Auftragsprofil des öffentlich-rechtlichen Rundfunks dergestalt zu präzisieren, dass der Schwerpunkt des Auftrags im Bereich Kultur, Information und Bildung liegen muss. Der vorliegende Beitrag zeigt, dass der Gesetzgeber zu einer solchen Angebotskonkretisierung zugunsten des Informationsauftrags des öffentlich-rechtlichen Rundfunks berechtigt ist. Dies gilt auch in Bezug auf die Hauptprogramme von ARD und ZDF. Darüber hinaus sind zur Verwirklichung des Informationsauftrags der Sendeanstalten weitere Regelungen (sendezeitbezogene Vorgaben und genrebezogene Budgetierungen) erforderlich bzw. sinnvoll. Sie sind mit der Angebotsautonomie der Anstalten vereinbar und verfassungsrechtlich zulässig.

I. Gegenstand der Untersuchung

Für den einen ist die (Schlüssel-)Frage ein alter Hut, für den anderen ein Evergreen: die Konkretisierung des Funktionsauftrags des öffentlich-rechtlichen Rundfunks. Auch aktuell steht diese Frage (wiederum) auf der Agenda der Medienpolitik. Da die von den 16 Bundesländern im März 2016 eingesetzte Arbeitsgruppe „Auftrag und Strukturoptimierung der Rundfunkanstalten" bis zum Frühjahr 2018 keine verwertbaren Ergebnisse erzielt hat, haben 7 Bundesländer (Bayern, Baden-Württemberg, Schleswig-Holstein, Hamburg, Sachsen, Thüringen und Brandenburg) eine eigene „AG Auftrag" ins Leben gerufen. Diese Bundesländer haben sich – aufbauend auf dem von Schleswig-Holstein entwickelten sogenannten ABC-Modell (Auftrag, Budgetierung und Controlling)[1] – auf eine medienrechtliche Neukonzeption verständigt, die eine Flexibilisierung des Angebotsauftrags des öffentlich-rechtlichen Rundfunks und eine Indexierung des Rundfunkbeitrags vorsieht.[2] Das Steuerungsmittel der gesetzlichen Beauftragung im Bereich des linearen Rundfunks soll begrenzt und durch die anstaltsinterne Angebotskonkretisierung im Wege des Drei-Stufen-Verfahrens, das bislang nur für den nichtlinearen Bereich galt, ersetzt werden. Wird die Gestaltungsfreiheit der öffentlich-rechtlichen Rundfunkanstalten durch den Reformplan wesentlich gestärkt, enthält die Konzeption gleichwohl eine Konkretisierung des Angebotsauftrags, die der Autonomie der Anstalten Grenzen setzt. Danach soll das Auftragsprofil der öffentlich-rechtlichen Rundfunkanstalten dergestalt präzisiert werden, dass der Schwerpunkt des Auftrags im Bereich Kultur, Information und Bildung liegen muss. Der Bereich Unterhaltung (einschließlich Sport) soll (selbstredend) weiterhin zum Angebotsauftrag gehören, aber nicht den Schwerpunkt bilden.

Im Folgenden wird untersucht, ob der Gesetzgeber berechtigt ist, eine solche Angebotskonkretisierung zugunsten des Informationsauftrags des öffentlich-rechtlichen Rundfunks zu regeln. Weiter stellt sich die Frage, ob es zur Verwirklichung des Informationsauftrags der Sendeanstalten weiterer Regelungen (sendezeitbezogene Vorgaben und

* Mehr über den Autor erfahren Sie auf S. VIII. Der Beitrag ist die gekürzte Fassung eines Rechtsgutachtens, das der Verfasser im Auftrag der Arbeitsgemeinschaft Dokumentarfilm (AG DOK) erstellt hat. Das vollständige Gutachten findet sich im K&R Online-Archiv unter www.kommunikationundrecht.de bei Eingabe der Volltext-ID KuRL2018-759 und auf der Internetseite der AG DOK.

1 *Knothe*, Medienkorrespondenz 11–12/2017, 3 ff.

2 Vgl. im Einzelnen *Nünning*, Medienkorrespondenz 12/2018, 3 ff.; *Roethe*, epd medien, 19/2018, 3 ff.