Kommunikation & Recht

Betriebs-Berater für
● Medien ● Telekommunikation ● Multimedia

12
K&R

25. Jahrgang Dezember 2022 Seiten 789 – 876

dfv Mediengruppe · Frankfurt am Main

digitalen Produkten und den damit einhergehenden Pflichten dar. Auch wenn sich die Vorgaben in erster Linie an Hersteller richten, müssen sich auch Importeure und Händler auf einen erheblichen Mehraufwand durch Überprüfungspflichten einstellen. Unternehmen sollten daher frühzeitig prüfen, ob und inwieweit sie vom CRA betroffen sind und rechtzeitig Maßnahmen zur Umsetzung vornehmen. Hierzu gehört insbesondere auch die Implementierung eines geschützten Kanals für Sicherheitsupdates. Updatability kann auch bei der zunehmenden Zahl von Produktwarnungen durch staatliche Stellen, wie dem BSI[33] aber auch den Datenschutzaufsichtsbehörden[34] einen entscheidenden Einwand in Bezug auf die Verhältnismäßigkeit der jeweiligen Warnung darstellen und die Erfolgsaussichten der (gerichtlichen) Überprüfung erhöhen. Darüber hinaus sollten betroffene Unternehmen einen an die Vorgaben des CRA angepassten internen Prozess zum Umgang mit Sicherheitslücken und Produktwarnungen definieren. Dieser sollte unter anderem festlegen, welche Fachabteilung im Ernstfall einzubeziehen ist und welche Behörden ggf. innerhalb welcher Fristen zu informieren sind.

VI. Fazit

Aus Sicht der EU-Kommission stellt der CRA den vorerst letzten Schlussstein der europäischen Produktvorgaben dar. Für eine belastbare Aussage, ob damit sprichwörtlich „das Beste zum Schluss" kommt, ist es in dem aktuellen Entwurfsstadium jedoch noch zu früh. Bereits jetzt ist jedoch festzuhalten, dass der CRA viele gute Ansätze enthält und die EU-Kommission über den weiten Anwendungsbereich erkennbar eine größtmögliche Cybersicherheit von Produkten anstrebt. Gleichzeitig stellt der CRA eine weitere Belastung für – mit Blick auf die vielfältigen und zuletzt umfassend verschärften Vorgaben für Cybersicherheit – ohnehin schon „belasteten" Unternehmen dar. Nunmehr werden sich zunächst das EU-Parlament und der Europäische Rat mit dem Entwurf der EU-Kommission befassen. Nach einer Einigung der Institutionen und der Veröffentlichung im Amtsblatt der EU wird der CRA dann mit Übergangsfristen von 12 bzw. 24 Monaten in Kraft treten. Mit Blick auf die bereits heute bestehenden rechtlichen Risiken bei unzureichender Cybersicherheit von digitalen Produkten sollten Unternehmen dies jedoch nicht zum Anlass nehmen, das Thema auf die lange Bank zu schieben, sondern ein produktbezogenes Cybersecurity Compliance Management aufbauen.

33 Siehe hierzu die Warnung des BSI vor dem Einsatz von Kaspersky-Virenschutzprodukten, abrufbar unter https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html; Vgl. auch OVG NRW, 28. 4. 2022 – 4 B 473/22, K&R 2022, 555 ff. = MMR 2022, 695 ff.; Erst kürzlich warnte das BSI zudem vor dem Einsatz unsicherer Funk-Türschlösser der Marke ABUS, abrufbar unter https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220810_Warnung_ABUS.html.

34 Siehe für einen Überblick *Hessel/Schneider*, K&R 2022, 82 ff.

Stefan Hessel
ist Salary Partner und Head of Digital Business bei reuschlaw Legal Consultants in Saarbrücken.

Christoph Callewaert
ist Associate bei reuschlaw Legal Consultants in Saarbrücken.

RA Dr. Florian Deusch und Prof. Dr. Tobias Eggendorfer*

Update IT-Sicherheitsrecht 2021/2022

Kurz und Knapp

Die Autoren stellen anschließend an ihr Update aus dem Vorjahr in K&R 2021, 689 ff. die Entwicklung des IT-Sicherheitsrechts im Zeitraum 2021/22 anhand ausgewählter Akte der Gesetzgebung und der Rechtsprechung sowie Stellungnahmen aus der Verwaltung dar.

I. Einführung und Gefährdungslage

Durch ausgenutzte („exploits") Sicherheitslücken bzw. Schwachstellen („vulnerabilities") können sich Bedrohungen („threats") als Angriffe („attacks") auf IT-Systeme realisieren, die die Ziele der IT-Sicherheit (insbesondere Verfügbarkeit, Vertraulichkeit, Authentizität und Integrität) beeinträchtigen. Je nach Angriff fallen IT-Systeme teilweise oder vollständig aus, werden von nicht autorisierten Tätern überwacht oder sogar ferngesteuert, exfiltrieren unberechtigt Daten an Dritte oder arbeiten sonstig nicht mehr funktionsgerecht.[1] Die European Cybersecurity Agency (ENISA), das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Polizeibehörden beschreiben im Berichtszeitraum dazu folgende Gefährdungslage:[2]

* Der Beitrag geht auf einen Vortrag der Autoren bei der DSRI-Herbstakademie 2022 zurück, der veröffentlicht wurde im Tagungsband von Heinze (Hrsg.), Daten, Plattformen und KI als Dreiklang unserer Zeit, 2022, S. 803 ff. Er ist überarbeitet und aktualisiert zum Stand Oktober 2022. Alle zitierten Internetquellen wurden zuletzt abgerufen am 11. 10. 2022. Mehr über die Autoren erfahren Sie am Ende des Beitrags.

1 Zum technischen Hintergrund: *Sohr/Kemmerich*, in: Kipker (Hrsg.), Cybersecurity, 2020, Kap. 2 Rn. 1 - 14, 155 - 189; *Deusch/Eggendorfer*, in: Taeger/Pohle (Hrsg.), Computerrechts-Handbuch, 37. Ergänzung, 2022, Kap. 50.1 Rn. 6 - 26, 31 - 169.

2 ENISA, Threat Landscape 2021 (https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 mit den gelisteten Major Incidents im Annex), BSI Lagebericht 2021 (https://www.bmi.bund.de/SharedDocs/

– Spektakuläre Opfer waren kritischen Infrastrukturen (KRITIS) i. S. d. § 2 Abs. 10 BSIG zuzuordnen wie Flughäfen, Universitätskliniken, Regierungs- und Gesundheitsorganisationen (z. B. die Europäische Arzneimittelbehörde EMA in der Zulassungsphase eines COVID-Impfstoffs sowie Angriffe im Zusammenhang mit den Bundes- und Landtagswahlen 2021) sowie Unternehmen der Energieversorgung und Abfallentsorgung, zuletzt im Oktober 2022 die Deutsche Bahn.[3] Auch bei zahlreichen Mittelständlern waren Produktionsausfälle und hohe finanzielle Schäden die Folge. Laut *Schwarz/Marx/Federrath* zeichnen sich IT-Angriffe auf Häfen, Schiffe und Schifffahrtsgesellschaften durch besondere internationale Verflechtungen aus.[4]

– Cryptomining und Ransomware sind vermehrt Schadfunktion von Malware.

– Ransomware-Angriffe haben sich zu einer spezifischen Gefährdung entwickelt. Dabei verschlüsseln Täter die Nutzungsdaten auf den IT-Systemen der Opfer und fordern Lösegeld („Ransom") für die Entschlüsselung oder drohen mit der Preisgabe der erbeuteten Daten, häufig im Rahmen einer Versteigerung. Die Täterschaft nutzt dazu in der Regel Schwachstellen in Software aus. Problematisch sind dabei Sicherheitslücken, die noch nicht publiziert sind[5] und Lücken, für die (noch) kein Patch bereitsteht. Ein Beispiel für Letzteres bietet der Groupware-Server Microsoft Exchange, für den am 8. 2. 2021 eine Sicherheitslücke registriert wurde: Am 2. 3. 2021 erst stellte der Hersteller einen Patch für diese Lücke bereit, obwohl sie bereits vor dem 8. 2. 2021 in „freier Wildbahn" ausgenutzt wurde.[6] Zudem sind die bereitgestellten Updates oft nicht installiert, sei es aufgrund von Kompatibilitätsproblemen oder aus Unkenntnis: daher läuft das kompromittierbare Programm weiter.[7] Ist über einen „Exploit" Zugang zum IT-System des Opfers geschaffen, erforschen die Täter über mehrere Wochen das System, indem sie z. B. Passwörter ausforschen und anhand der gekaperten Daten bewerten, zu welcher Lösegeldzahlung das Opfer mutmaßlich fähig und bereit ist. Sind die Backup-Dateien vom Angriff miterfasst oder aus sonstigem Grund nicht verfügbar, kann das Opfer die verschlüsselten Daten i. d. R. nicht mehr wiederherstellen. Hierzu wird z. T. diskutiert, ob die Zahlung des Lösegelds durch die betroffenen Unternehmen an die Täter strafbar ist als Unterstützung einer kriminellen Vereinigung (§ 129 Abs. 1 S. 2 StGB, § 89c StGB sowie §§ 17, 18 Außenwirtschaftsgesetz). Weiter findet derzeit eine Diskussion zu „silent insurance/silent coverage" statt (Inanspruchnahme von Versicherungsleistungen z. B. in D&O-Versicherungen oder Betriebshaftpflichtversicherungen, die Ransomware-Schäden nicht ausdrücklich ausschließen, aber auch nicht speziell hierfür entwickelt wurden).[8]

– Angriffe aus politischen Motiven verübte die „Anonymous-Gruppe" gegen Russland und Unternehmen, die einen Boykott Russlands nicht unmittelbar unterstützten („Cyberwar").[9] Auch Angriffe staatlicher Akteure gelten als „Cyberwar"; den Autoren ist allerdings kein Fall mit gerichtsfestem Nachweis bekannt, welcher Staat konkret welchen IT-Angriff angeordnet oder verübt hat.[10]

– Insbesondere Ransomware-Angriffe erfolgen gezielter, was auf qualifiziertere Akteure mit entsprechender Ausdauer („Advanced Persistent Threat") schließen lässt. Häufig als Supply Chain Angriffe, die zunächst Schwachpunkte eines Systems attackieren, um sich dann lateral auszubreiten.[11]

– Durch verstärktes Home-Office und Video-Konferenzen, insbesondere durch die Corona-Pandemie, wurde vermehrt Software mit relevanten Sicherheitslücken genutzt, dadurch hat sich die Angriffsfläche vergrößert.[12]

– Unzureichende Datenschutzmaßnahmen nutzen Täter für Erpressungsangriffe durch Daten-Exfiltrationen. Da bei jedem Ransomware-Vorfall die betroffenen Daten kompromittiert sind, folgt damit auch eine Meldepflicht (Art. 33 DSGVO), soweit – wie meist – auch personenbezogene Daten betroffen sind. Auch dies nutzen die Täter als Druckmittel.[13]

---

downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-cybersicherheit-2021.pdf?__blob=publicationFile&v=3), dort insbesondere Seiten 12 ff. zu Ransomware, Polizeiliche Kriminalstatistik 2021 (https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2021/FachlicheBroschueren/IMK-Bericht.pdf?__blob=publicationFile&v=3).

3 Medienberichten zufolge stand der Bahnverkehr infolge eines mutwillig durchtrennten Kommunikationskabels still (https://www.tagesschau.de/multimedia/video/video-1097903.html). Der Vorfall macht deutlich, dass auch die physische Sicherung der Infrastruktur und Notfallpläne, z. B. für den Stromausfall, Bestandteile der erforderlichen IT-Sicherheit sind, siehe dazu *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Kap. 50.1 Rn. 24, wonach auch der Fall von durchtrennten Erdkabeln unter dem IT-Sicherheitsaspekt der Verfügbarkeit bedacht sein will.

4 *Schwarz/Marx/Federrath*, A Structured Analysis of Information Security Incidents in the Maritime Sector, https://arxiv.org/pdf/2112.06545.pdf.

5 Sicherheitsforscher kontaktieren zunächst den Hersteller im Rahmen eines responsible disclosure. Erst nach dessen Reaktion oder frustranen Fristablauf veröffentlichen sie die Lücke (Zeitpunkt der Publikation), unabhängig von der Einstufung der Schwere und Bereitstellung eines Patches durch den Hersteller.

6 Der 8. 2. 2021 unter http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26855 sagt aus, wann die Entdecker der Lücke sich mit einer abstrakten Beschreibung eine „CVE"-Nummer (Common Vulnerabilities and Exposures) registriert haben. Das Datum ist unabhängig vom Entdeckungsdatum und Informationsdatum des Herstellers (siehe auch Fn. 5). Hier kannten Dritte die Lücke bereits vor dem 8. 2. 2021 und nutzen sie für Angriffe aus, wie u. a. https://www.tenable.com/blog/cve-2021-26855-cve-2021-26857-cve-2021-26858-cve-2021-27065-four-microsoft-exchange-server-zero-day-vulnerabilities meldet. So auch bei anderen Lücken: z. B. zeigten sich für die Heartbleed-Lücke (https://heartbleed.com/) Hinweise in Logfiles, dass sie Angreifer bereits drei Monate vor ihrer (erneuten) Entdeckung durch seriöse Sicherheitsforscher nutzten.

7 So gab es Ende September 2022 erneut Berichte von Angriffen auf die hier geschilderten Sicherheitslücken (https://www.bleepingcomputer.com/news/security/hacking-group-hides-backdoor-malware-inside-windows-logo-image/).

8 *Gelinsky*, „Erst erpresst, dann angeklagt", Frankfurter Allgemeine Zeitung Nr. 109 vom 11. 5. 2022, S. 16; zu „silent insurance/silent coverage" *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Kap. 50.1 Rn. 480.

9 https://twitter.com/YourAnonOne/status/1496965766435926039; https://www.heise.de/news/Cyberkrieg-Schlagabtausch-zwischen-Anonymous-und-Conti-FCC-organisiert-Abwehr-6527023.html; https://nachrichtend.com/ukraine-krieg-anonymous-veroeffentlicht-sensible-daten-von-120-000-russischen-soldaten/; https://www.swr.de/swr2/leben-und-gesellschaft/warum-die-hacker-anonymous-auch-uns-gefaehrlich-werden-koennten-100.html; https://fm4.orf.at/stories/3022280/.

10 Auch *Schwarz/Marx/Federrath*, A Structured Analysis of Information Security Incidents in the Maritime Sector, https://arxiv.org/pdf/2112.06545.pdf weisen auf die schwierige Beweislage hin. Laut Bundeslagebild Cybercrime des BKA (S. 30 ff.; https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.pdf?__blob=publicationFile&v=5) deuten die Ermittlungen in verschiedenen Fällen auf eine staatliche Anordnung bzw. Duldung hin; eindeutige Beweise und Ermittlungen der Täter sind aber von internationaler Zusammenarbeit abhängig, die wiederum im Spannungsfeld politischer Situationen wie z. B. dem Russland-Ukraine-Konflikt steht.

11 Zu rechtlichen Aspekten von Supply-Chain-Angriffen *Hessel/Potel/Beerwald*, K&R 2021, 771 - 776.

12 Es mag der Eindruck entstehen, dass die Corona Pandemie diese Lücken heraufbeschworen hat, tatsächlich aber bestanden sie bereits vorher. Sie sind nur durch den abrupten „Digitalisierungssprung" aufgefallen, und waren nicht mehr durch weitere Maßnahmen, wie z. B. Unternehmensfirewalls, zu kaschieren.

13 S. 13, 17 BSI-Lagebericht 2021 (https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-cybersicherheit-2021.pdf?__blob=publicationFile&v=3) bzw. bei KRITIS-Unternehmen spezialgesetzlich (§§ 8b, 8c BSIG, 11 EnWG oder 168, 169 TKG).

– Unter dem Stichwort „Cybercrime“ erfasst die polizeiliche Kriminalstatistik Straftaten, die sich gegen informationstechnische Systeme richten, insbesondere Fälschung beweiserheblicher Daten, Computersabotage, Ausspähen und Abfangen von Daten und Computerbetrug (§§ 269, 270, 303b, 202a, 202b und 263a StGB), oft durch Malware-Angriffe verwirklicht. Die Aufklärungsquote lag im Jahr 2021 mit 29,3 % deutlich unter der aller Straftaten (58,7 %).[14]

II. IT-Sicherheit in der Gesetzgebung

Die Gefährdungslage und die intensivere IT-Nutzung haben den europäischen und nationalen Gesetzgeber im Berichtszeitraum zu weiteren Rechtsakten motiviert.

1. Geplante und aktuelle Rechtsakte im EU-Recht

a) Vorschläge der EU-Kommission, insbesondere zur Novellierung der NIS-RL und zum Cyber Resilience Act

Die Novellierung der NIS-RL (EU) 2016/1148 in „*NIS 2*“, die IT-Sicherheitspflichten von KRITIS-Unternehmen und Anbietern digitaler Dienste regelt, war im Berichtszeitraum Gegenstand politischer Debatten und erwartet ebenso wie die geplante Richtlinie über die Resilienz kritischer Einrichtungen die erste Lesung im EU-Parlament; ein paralleler Verordnungsvorschlag soll für Organe, Einrichtungen und sonstigen Stellen der EU vergleichbare IT-Sicherheit schaffen.[15]

Am 15. 9. 2022 hat die EU-Kommission den Verordnungsvorschlag zum *Cyber Resilience Act (CRA)* veröffentlicht und dem Europäischen Parlament zugeleitet.[16] Zwei Aspekte stechen aus der geplanten Verordnung heraus:

– Der CRA-Vorschlag definiert IT-Sicherheitsanforderungen, die horizontal für alle Produkte mit digitalen Elementen gelten sollen. Dabei handelt es sich um jegliche Hard- und Software mit einer Verbindung zu einem Gerät („device“) oder einem Netzwerk (Artt. 1 und 2 CRA-Vorschlag). Da die bisherigen legislativen IT-Sicherheitsvorgaben wie etwa die NIS-RL regelmäßig an bestimmte Branchen bzw. Sektoren – vertikal – adressiert waren, ist die Festlegung genereller IT-Sicherheitspflichten horizontal für alle Produkte mit digitalen Elementen ein Novum.[17]
– Die Vorgaben zur IT-Sicherheit sind auch inhaltlich und in ihrem Konkretisierungsgrad im Grundsatz zu begrüßen: Produkte müssen gemäß Art. 5 CRA-Vorschlag i. V. m. Annex I zum CRA nicht nur ein „angemessenes Sicherheitsniveau“ aufweisen. Vielmehr dürfen Produkte nur in Verkehr gebracht werden, wenn sie keine bekannten Schwachstellen („vulnerabilities“) haben. Vorkehrungen gegen den Zugriff durch Unbefugte und zur Vertraulichkeit, Integrität und Verfügbarkeit müssen vorhanden sein. Ein Verfahren zur Offenlegung und Behebung identifizierter Schwachstellen muss gegeben sein.

Unklar bleibt indes, ob es bei „bekannten“ Sicherheitslücken um die Art der Sicherheitslücken geht, z. B. Buffer-Overflows oder SQL-Injections, oder um konkrete Lücken im Produkt. Sinnvoll erscheint ersteres, da die Arten teils seit 50 Jahren bekannt sind und durch einfache Maßnahmen zu verhindern sind.[18]

Die definierten IT-Sicherheitsanforderungen sollen durch bußgeldbewehrte Pflichten der Hersteller, Importeure und Distributoren sichergestellt werden (Kapitel 2, Artt. 10 ff. CRA-Vorschlag). Die Mitgliedstaaten haben Behörden mit entsprechenden Überwachungs- und Eingriffskompetenzen zu benennen (Kapitel V und VII CRA-Vorschlag).

Open Source-Software soll dagegen ausgenommen sein, jedenfalls soweit sie außerhalb kommerzieller Aktivitäten entwickelt oder ergänzt wird (ErwG 10 CRA-Vorschlag). Hier scheint der Verordnungsgeber erkannt zu haben, dass durch die Offenlegung des Quellcodes jederzeit die Qualität des Produktes geprüft werden kann und eben gerade nicht, wie bei Closed-Source vollmundigen Versprechen von Anbietern getraut werden muss. In der Praxis spannend wird die Abgrenzung zwischen „kommerzieller“ und „nicht kommerzieller“ Open Source Entwicklung sein.

Art. 24 CRA-Vorschlag sieht vor, dass die Pflichten 24 Monate nach Inkrafttreten der Verordnung gelten sollen. Allerdings gibt es noch keinen Zeitplan für das Rechtsetzungsverfahren; der zuständige Parlamentsausschuss „Industry, Research and Energy“ hat zum Redaktionsschluss noch keinen Berichterstatter benannt und den Autoren auf Anfrage mitgeteilt, dass im zweiten Quartal 2023 mit weiteren Abstimmungen zu rechnen ist.

b) Vorschläge zur Änderung der eIDAS-Verordnung, Digital Markets Act und Digital Services Act

Die (eIDAS-) VO (EU) Nr. 910/2014 definiert den Rahmen für elektronische Signaturen und Zertifikate in der EU, z. B. für qualifizierte elektronische Signaturen i. S. d. § 126a BGB. Dazu liegt ein Kommissionsvorschlag vor, der sie um eine europäische digitale Identität (eID) und eine persönliche digitale Brieftasche (E-Wallet) ausweiten soll, damit Nutzer sicheren und einfachen Zugang zu öffentlichen und privaten Diensten erhalten und ihre Identitätsangaben nachweisen können, wie Adresse, Alter, Personenstand, Staatsangehörigkeit, Berufsqualifikationen, Genehmigungen und Zahlungsdaten. Sicherheit und Datenschutz würden grenzübergreifend gewährleistet.[19]

---

14 Insbesondere S. 2, 4, 30 ff. Bundeslagebild Cybercrime 2021 des Bundeskriminalamts (s. o. Fn. 10) und S. 23 der polizeilichen Kriminalstatistik (PKS) 2021 – ausgewählte Zahlen im Überblick, S. 10, https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2021/FachlicheBroschueren/IMK-Bericht.pdf?__blob=publicationFile&v=3). Zur Aussagekraft der PKS ist anzumerken, dass sie einerseits nur polizeibekannte, also angezeigte Taten erfasst, und andererseits die Kategorisierung des aufnehmenden Beamten der Taten bei Erfassung für die PKS meist beibehalten wird. Die Kategorien können zudem in den verschiedenen Berichtsjahren abweichen.

15 Zum aktuellen inhaltlichen Stand des NIS 2-Vorschlags der Vermerk des Generalsekretariats des Rates der EU vom 26. 11. 2021 Nr. 14337/21 (https://data.consilium.europa.eu/doc/document/ST-14337-2021-INIT/de/pdf); zum aktuellen Verfahrensstand des NIS 2-Vorschlags: https://eur-lex.europa.eu/legal-content/DE/HIS/?uri=COM:2020:823:FIN und zum Stand des Verordnungsvorschlags zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union COM (2022)122 final https://eur-lex.europa.eu/legal-content/DE/HIS/?uri=COM:2020:823:FIN zur geplanten Richtlinie über die Resilienz kritischer Einrichtungen: https://eur-lex.europa.eu/legal-content/DE/HIS/?uri=COM:2020:823:FIN; zum zugrundeliegenden Soft Law und den Vorschlägen im Übrigen *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Kap. 50.1 Rn. 272 ff., 280a, 337a.

16 COM(2022) 454 final, https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2022/0272(COD)&l=en, dazu ausführlich Hessel/Callewaert, K&R 2022, 789 ff. (in diesem Heft).

17 Zu den sektorenspezifischen IT-Sicherheitsregelungen *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Kap. 50.1 Rn. 281 ff. und Rn. 408 ff. Einzelne horizontale Detailregelungen wie z. B. § 434 Abs. 2 S. 2 BGB (dazu *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Rn. 453) ändern an diesem grundsätzlichen Befund nichts. Der CRA ist in der Cybersicherheitsstrategie 2020 der EU-Kommission angekündigt und nimmt in seiner Begründung (COM(2022) 454 final, Seite 3) Bezug auf das Dokument „Gestaltung der digitalen Zukunft Europas“, dazu siehe *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Rn. 278, 280.

18 *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Rn. 47 ff., Rn. 80 ff.

19 eIDAS = electronic Identification Authentication and Trust Service; zur geltenden eIDAS-Verordnung *Bernhardt/Leeb*, in: Heckmann/Paschke (Hrsg.), Juris-Praxiskommentar Internetrecht, 7. Aufl. 2021, Werksstand

Verweise auf die IT-Sicherheitsanforderungen der DSGVO und der E-Privacy-RL 2002/58/EG enthalten die Kommissionsvorschläge zum Digital Markets Act (wendet sich an Plattformbetreiber) und zum Digital Services Act (der die eCommerce-RL 2000/31/EG ablösen soll). Der Digital Markets Act sieht in Kapitel III Sorgfaltspflichten der Diensteanbieter an ein sicheres Online-Umfeld vor, jedoch ohne technische Vorgaben im engeren Sinn. Zudem werden die Diensteanbieter als Anbieter digitaler Dienste i. S. v. Art. 4 Nr. 6 NIS-RL die IT-Sicherheitsanforderungen der NIS-RL (EU) 2016/1148 zu erfüllen haben.[20]

c) „Chatkontrolle"

Artt. 5, 6 E-Privacy-RL 2002/58/EG schützt die Vertraulichkeit der elektronischen Kommunikation gegen das Mithören, Abhören, Speichern und Abfangen von Nachrichten, sowie die Verkehrsdaten der Nutzer und Kommunikationsteilnehmer. Damit steht fest, dass z. B. Chats in Messengerdiensten oder E-Mails nur die beteiligten Kommunikationspartner etwas angehen; anderen Personen ist der Zugriff hierauf nicht erlaubt, seien es staatliche oder kriminelle Akteure. Um sexuellen Missbrauch von Kindern zu bekämpfen, *ermächtigt* die VO (EU) 2021/1232 – befristet bis zum 3. 8. 2024 – Diensteanbieter dazu, die elektronischen Nachrichten ihrer Nutzer auf verdächtige Inhalte zu prüfen und diese den zuständigen Behörden zu melden. Unter dem Schlagwort „Chatkontrolle" wird der Verordnungsvorschlag COM(2022) 209 final der EU-Kommission vom 11. 5. 2022 diskutiert. Dessen Art. 3 soll Hosting-Provider und Anbieter von E-Mail- und Messengerdiensten *verpflichten*, eine Risikoabschätzung ihrer Dienste zum Kindesmissbrauch vorzunehmen; Art. 4 verlangt davon abgeleitete Maßnahmen zur Risikominimierung. Pflichtverstöße sollen gemäß Art. 35 der geplanten Verordnung mit Bußgeldern bewehrt werden, die sich am Umsatz des verantwortlichen Unternehmens bemessen.[21] Abgesehen von den intensiven politischen Diskussionen ist auch die technische Ausführung dieser Anforderungen noch ungeklärt. Offen ist z. B., ob bereits die Risikoeinschätzung eine Chatkontrolle verlangt, die jedenfalls gemäß Artt. 7, 10 nach einer behördlichen Anordnung erfolgen muss. Dem Wortlaut „Risikoabschätzung" nach geht es um eine a priori Bewertung, die für jeden anonymisierenden Dienst ein pauschales Risiko erwarten lässt. Erfahrungsgemäß wurden und werden entsprechende Materialien aber auch in offenen, nicht anonymisierten Foren getauscht, so dass auch dort ein – wenngleich möglicherweise geringeres – Risiko besteht.

Kritisch zu bemerken ist, dass die Kontrolle der elektronischen Kommunikation auch Ende-zu-Ende-verschlüsselte Nachrichten erfasst. Sie sind – technisch bedingt – nur durch einen Zugriff auf das Endgerät eines Kommunikationspartners oder eine „Hintertüre" der Verschlüsselung zu kontrollieren. In beiden Fällen lässt sich nur über Sicherheitslücken ein Zugang zum Endgerät erhalten oder auf den Kommunikationsvorgang zugreifen. Die Autoren wiederholen ihren kritischen Hinweis, dass es aus technischen Gründen keine Sicherheitslücken gibt, die nur zu einem begrenzten Zweck, z. B. zur Bekämpfung des Kindesmissbrauchs, ausgenutzt werden können. Daher ist zu erwarten, dass staatlich geschaffene Lücken auch Täter oder Geheimdienste entdecken und nutzen, ohne sich an die gesetzlichen Vorgaben zu halten.[22] Ebenso sind andere Überwachungsansätze wie die von Apple in iOS 15 erwogene CSAM-Detection nur sehr eingeschränkt tauglich.[23]

d) Data Governance Act

Der Data Governance Act (VO (EU) 2022/868, gültig ab 24. 9. 2023, Art. 38), regelt in Artt. 3 ff. die Nutzung von Daten im Besitz öffentlicher Stellen, in Artt. 10 ff. die Anforderungen an Datenvermittlungsdienste und in Artt. 16 ff. die altruistische Datenverwendung. Öffentliche Stellen können die Weiterverwendung ihrer Daten durch andere (öffentliche oder private Stellen) von der Einhaltung bestimmter Sicherheitsanforderungen abhängig machen (Art. 5 Abs. 3). Sowohl Datenvermittlungsdienste als auch Organisationen, die Daten zu altruistischen Zwecken zur Verfügung stellen, müssen sich registrieren (Art. 11 bzw. 18). Danach sollen die zuständigen Behörden überwachen, dass die Anbieter angemessene Sicherheitsmaßnahmen für ihre Dienste treffen (Art. 12, 14, 21 und 24). Die Anforderungen für personenbezogene Daten aus Art. 32 DSGVO bleiben neben diesen Regelungen maßgeblich (Art. 1 Abs. 3 S. 2). Offen ist bislang die praktische Umsetzung, insbesondere fehlen einheitliche Standards zur IT-Sicherheit, selbst eine Bezugnahme auf den Stand der Technik wie Art. 32 DSGVO fehlt. Unklar ist auch die Abgrenzung des vage definierten Datenaltruismus von Datenvermittlungsdiensten, z. B. wie festzustellen ist, dass lediglich „Kosten der Bereitstellung" und kein „Entgelt" gefordert wird (Art. 2 Nr. 16). Für die IT-Sicherheit ist diese Abgrenzung relevant, weil die datenaltruistischen Organisationen nur ein „angemessenes Sicherheitsniveau" und Datenvermittlungsdienste „für sensible wettbewerbsrelevante Informationen das höchste Sicherheitsniveau" sicherstellen müssen (Art. 12 lit. l, 21 Abs. 4).[24]

---

13. 6. 2022, Kap. 6 Rn. 109 f., 220 - 258 und *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Kap. 50.1 Rn. 296 ff. und in Rn. 278 zum zugrundeliegenden Soft Law (auch zur geplanten Änderung); der Änderungsvorschlag der Kommission vom 3. 6. 2021 ist unter der Dokumentennummer COM 2021 (281) final veröffentlicht, die Empfehlung 2021/456 der Kommission in ABl. EU Nr. L 210 v. 14. 6. 2021, 51. Relevant ist in dem Kontext auch der Blick auf das EU-Mitglied Estland: Es hat seit vielen Jahren erfolgreich ein eGovernment implementiert, das zudem mittels einer „eResidency" Auswärtigen ermöglicht, an den zahlreichen digitalisierten Alltagsprozessen, von Krankenversicherung bis Immobilienerwerb, teilzunehmen. Die estnische „Information System Authority" (https://www.ria.ee/en.html) nennt verschiedene Portale, zum Beispiel das eID Portal für elektronische und mobile Identitäten, die wie ein Pass genutzt werden können.

20 Der Digital Markets Act (COM/2020/842 final, https://eur-lex.europa.eu/legal-content/en/HIS/?uri=COM:2020:842:FIN) und der Digital Services Act (COM/2020/825 final https://eur-lex.europa.eu/legal-content/en/HIS/?uri=COM:2020:825:FIN) haben im Dezember 2021 bzw. Januar 2022 jeweils die erste Lesung im Europäischen Parlament passiert. Zu den IT-Sicherheitsanforderungen der E-Privacy- und der NIS-Richtlinie *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Kap. 50.1 Rn. 286 ff. und 336 ff.

21 *Kiparski*, in: Heinze (Hrsg.), Daten, Plattformen und KI als Dreiklang unserer Zeit, 2022, 845, 849 f., der darauf hinweist, dass Internetzugangsanbieter („Access-Provider") weder eine Risikoabschätzung noch eine Kontrolle der Dateninhalte vornehmen müssen. Sie haben auf behördliche Anforderung jedoch den Zugang zu als kinderpornografisch identifizierten Internetseiten zu sperren (Art. 16 der geplanten Verordnung). Die Sperranforderung erinnert an das Stopp-Schild von der Leyens, das damals wie heute technisch kaum umsetzbar ist (https://www.computerwoche.de/a/rotes-stopp-schild-statt-kinderpornos-im-internet,1884229).

22 Zum Fernmeldegeheimnis in Art. 5 E-Privacy-RL *Deusch/Eggendorfer*, K&R 2017, 93, 94 m. w. N.; zur Verordnung (EU) 2021/1232 und dem Verordnungsvorschlag mit der Kritik am Aufbrechen der Ende-zu-Ende-Verschlüsselung *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Kap. 50.1 Rn. 280, 198, 337, 385; zum Sachstand der politischen Kritik z. B. https://netzpolitik.org/2022/chatkontrolle-bundesregierung-loechert-eu-kommission-mit-kritischen-fragen/#2022-06-10_BuReg_Fragenkatalog.

23 *Eggendorfer/Schmidt-Wudy*, ZD 2021, 674 ff., das Verhältnis zwischen DSGVO und Art. 5 Abs. 3 E-Privacy-RL 2002/58/EG offenlassend.

24 Data Governance Act: Verordnung (EU) 2022/868, ABl. EU Nr. L 152/1 v. 3. 6. 2022; zum Kommissionsentwurf *Spindler*, CR 2021, 98 ff. sowie *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Kap. 50.1 Rn. 280e. Altruistisch ist gemäß Art. 2 Nr. 16 Verordnung (EU) 2022/868 die freiwillige gemeinsame Nutzung von Daten (…), ohne hierfür ein Entgelt zu fordern oder zu erhalten, das über eine Entschädigung für die ihnen durch

e) Durchführungsverordnung zur Funkanlagen-Richtlinie und Verordnungsvorschlag zur Maschinen-Richtlinie

Art. 3 der Funkanlagen-RL 2014/53/EU definiert IT-Sicherheitsvorgaben für Funkanlagen. Hierunter fallen z. B. WLAN-Access Points, Ton- und TV-Empfänger, die ihre Signale per Funk erhalten, GPS-Empfänger, Mobilfunk einschließlich 5G, M2M-Kommunikation und Near-Field-Kommunikation". Die Durchführungsverordnung (EU) 2022/30 (gilt ab 1. 8. 2024) stellt klar, dass diese IT-Sicherheitsanforderungen auch für solche Funkanlagen gelten, die über das Internet kommunizieren, z. B. „smart devices" wie Wearables, Spielzeug und Smart-Home-Anwendungen. Im Anlagenbau wird der Vorschlag der EU-Kommission relevant, die bisherige Maschinenrichtlinie 2006/42/EG zu reformieren und als Verordnung zu fassen. Erwägungsgrund (11) des Verordnungsvorschlags sieht vor, dass die Maschinen auch den Sicherheitsanforderungen der Digitaltechnik und der künstlichen Intelligenz entsprechen sollen. Art. 17 Nr. 5 des Vorschlags vermutet grundlegende Sicherheitsanforderungen als gegeben, wenn ein Zertifikat gemäß dem Cybersecurity Act VO (EU) 2019/881 vorliegt.[25]

2. Neuerungen in der nationalen Gesetzgebung

Im Berichtszeitraum sind Gesetze in Kraft getreten, die bereits Gegenstand des vergangenen Updates waren, darunter die Neufassung des TKG, das TTDSG sowie Novellierungen im BGB mit der Aufnahme von Sicherheitsaspekten im Sachmangelrecht (§ 434 BGB) und Verbraucherrecht (§ 327 ff. BGB), ebenso das IT-Sicherheitsgesetz 2.0 mit seinen Neuerungen im BSIG.[26] Zu § 9c BSIG ist mittlerweile die BSI-IT-Sicherheitskennzeichenverordnung in Kraft getreten. Eine Rechtsverordnung zur Bestimmung von Unternehmen im öffentlichen Interesse gemäß § 8f BSIG fehlt noch immer.[27] Folgende weitere Gesetzesakte sind relevant:

- Bund und Länder verpflichtet das Onlinezugangsgesetz (OZG), Verwaltungsleistungen durch ein einheitliches Onlineportal anzubieten. Die Standards zur IT-Sicherheit sind in § 5 OZG i. V. m. der IT-Sicherheitsverordnung Portalverbund (ITSiV-PV, in Kraft seit 7. 1. 2022) geregelt.[28]
- Die IT-Sicherheit in Arztpraxen und Krankenhäusern regeln die §§ 75b und 75c SGB V nebst zugehöriger IT-Sicherheitsrichtlinie der kassenärztlichen Vereinigung. Die Anlage zu § 307 Abs. 1 S. 3 SGB V enthält eine Datenschutz-Folgenabschätzung zur elektronischen Verarbeitung von Gesundheitsdaten.[29]
- Trotz IT-Sicherheitsbedenken gegen das beA wird die elektronische Kommunikation mit Justiz und Verwaltung nach Maßgabe dieser Strukturen weiter ausgebaut (seit 1. 1. 2022 durch das elektronische Bürger- und Organisationspostfach und ab 1. 1. 2023 das „besondere elektronische Postfach der Steuerberater – beSt").[30]
- Für das Strafrecht relevant: Der Missbrauch von Telekommunikationsanlagen (bis 30.11.2021: §§ 90, 148 TKG a. F.) ist seit 1. 12. 2021 geregelt in den §§ 8, 27 Abs. 1 Nr. 3 TTDSG. Geplant ist zudem ein Tatbestand des digitalen Hausfriedensbruchs gemäß § 202e StGB.[31]

III. Rechtsprechung und Verwaltungspraxis

Folgende gerichtliche und behördliche Entscheidungen im Berichtszeitraum sind für die IT-Sicherheit relevant:

1. Disassemblierung und Dekompilierung, EuGH, C-13/20

Der EuGH hat festgestellt, dass ein Softwarekäufer das erworbene Computerprogramm disassemblieren darf, um eine mangelhafte Funktion zu deaktivieren. Dies gehört zur bestimmungsgemäßen Nutzung gemäß Artt. 5, 6 RL 2009/94/EG (umgesetzt in § 69e UrhG). Da ein Softwaremangel auch in einer Sicherheitslücke bestehen kann, folgt die interessante Anschlussfrage, ob eine Disassemblierung auch zulässig ist, um nach Sicherheitslücken zu suchen. Dies trifft nach Auffassung der Autoren zu, da auch Sicherheitslücken Softwaremängel begründen. Aus technischer Sicht ist anzumerken, dass der EuGH ebenso wie zahlreiche juristische Abhandlungen diese Fragen unter der Überschrift „Dekompilierung" aus Art. 6 RL 2009/94/EG (§ 69e UrhG) diskutiert. Wie der EuGH in Rn. 37 seines Urteils ausführt, ist der Vorgang der Kompilierung (die Übersetzung eines Quellcodes in einen für den Computer ausführbaren Maschinencode mit einem Compiler) nicht umkehrbar. Möglich ist stattdessen eine Disassemblierung: Ein Disassembler übersetzt den Maschinencode in sogenannten Assemblercode. Die weitere Ableitung eines Quellcodes aus diesem Assemblercode ist aufwändig und führt nicht zu dem Quellcode, der der Kompilierung zugrunde lag, sondern allenfalls zu einem „Quasi-Quellcode". Der Begriff „Dekompilierung" in Art. 6 RL 2009/94/EG (§ 69e UrhG) ist daher so zu verstehen, dass alle Bearbeitungen der Software bis hin zum technisch auf-

---

die Bereitstellung ihrer Daten entstandenen Kosten hinausgeht, für Ziele von allgemeinem Interesse gemäß dem nationalen Recht, wie die Gesundheitsversorgung, die Bekämpfung des Klimawandels, die Verbesserung der Mobilität, die einfachere Entwicklung, Erstellung und Verbreitung amtlicher Statistiken, die Verbesserung der Erbringung öffentlicher Dienstleistungen, die staatliche Entscheidungsfindung oder die wissenschaftliche Forschung im allgemeinen Interesse.

25 *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Kap. 50.1 Rn. 295 (Funkanlagen, auch mit der Differenzierung zwischen WLAN-Access-Point und Router), Rn. 280d (Maschinenrichtlinie) und Rn. 232l, 280c zur Künstlichen Intelligenz (KI) und der geplanten KI-Verordnung, die laut Erwägungsgrund 11 des Vorschlags zur Maschinenverordnung zu beachten sein soll.

26 Dazu *Deusch/Eggendorfer*, in: Taeger (Hrsg.), im Fokus der Rechtsentwicklung – Die Digitalisierung der Welt, 2021, S. 321, 326 - 328 und ergänzt in, K&R 2021, 689, 690 - 693 sowie *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Kap. 50.1 Rn. 409 ff. (BSIG), 418 ff. (TTDSG), 424 ff. (TKG), 451 ff. (BGB), jeweils m. w. N. Zur Konkretisierung der IT-Sicherheitspflichten gemäß den §§ 164 ff. TKG haben das BSI und die Bundesnetzagentur zwischenzeitlich weitere Technische Richtlinien veröffentlicht, zum Beispiel zur Zertifizierung von kritischen Komponenten in TK-Infrastrukturen (BSI TR-03163), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/Liste-TR-nach-Aenderungsdatum/traenderungen_node.html. Probleme bei der Adressierung von Bußgeldern nach dem BSIG und der geplanten NIS-2-RL behandeln *Hubert/Schaller*, in: Heinze (Fn. 21), 825 ff.

27 Zur BSI-IT-SiKV: BGBl. I 2021, 4978; die fehlende Rechtsverordnung nach § 8f BSIG ist für 2022 angekündigt, https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Weitere_regulierte_Unternehmen/UBI/FAQ/faq_ubi2_wertschoepfung_allgemein_node.html;jsessionid=C7255F043C67BB6B843E6689A065A436.internet081.

28 *Heckmann*, in: Heckmann/Paschke (Fn. 19), Kap. 5 Rn. 868, 876, 881; *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Kap. 50.1 Rn. 467; zur ITSiV-PV: BGBl. 2022 I S. 18 ff.; eine inhaltliche Auseinandersetzung damit bleibt vorbehalten. Das BMI stellt aktuelle Informationen über die OZG-Umsetzung unter https://www.onlinezugangsgesetz.de/Webs/OZG/DE/startseite/startseite-node.html bereit.

29 Zur IT-Sicherheitsrichtlinie: BSG, 20. 1. 2021 – B 1 KR 7/20 R (juris); die Anlage zu § 307 SGB V ist abgedruckt in BGBl. I 2021, 1350 - 1361.

30 *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Kap. 50.1 Rn. 295; zum eBO https://egvp.justiz.de/buerger_organisationen/220126_sicherer_uebermittlungsweg_buerger_organisationen_v1.pdf zum beStB: https://www.bstbk.de/de/themen/steuerberaterplattform.

31 *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Kap. 50.1 Rn. 465; zu den §§ 90, 148 TKG OLG Köln, 9. 4. 2020 – III-1 RVs 74/20, juris sowie *Deusch/Eggendorfer*, K&R 2017, 93, 97; zum Entwurf des § 202e StGB: BT-Drs. 20/1530 v. 27. 4. 2022; zur Diskussion bereits z. B. *Buermeyer/Golla*, K&R 2017, 14 - 18 sowie *Eisele/Nolte*, CR 2020, 488 - 496.

wändigen Reverse Engineering geregelt sind. Falsch ist dagegen die Vorstellung, die Dekompilierung ermögliche die „Rückübersetzung" des Quellcodes aus dem Maschinen- bzw. Objektcode.[32]

2. IT-Sicherheit als Rechtsgrundlage zur Verarbeitung personenbezogener Daten, Generalanwalt beim EuGH Pikamäe, C-77/21

Zahlreiche IT-Sicherheitsmaßnahmen bringen die Verarbeitung personenbezogener Daten mit sich. Die bislang herrschende Meinung bemisst die Rechtmäßigkeit dieser Verarbeitungen an den berechtigten Interessen des Verantwortlichen (Art. 6 Abs. 1 S. 2 lit. f DSGVO).[33] Der EuGH beantwortete dazu die Frage, ob ein ungarischer TV-Anbieter die Daten seiner Kunden auf einem zusätzlichen internen Datenträger kopieren darf, um eine technische Störung zu überbrücken. Nach Auffassung des Generalanwalts Pikamäe, der der EuGH folgte, kann dies nach Art. 6 Abs. 1 S. 2 lit. b DSGVO zulässig sein, sofern der Verarbeitungszweck „Behebung einer technischen Störung" für die Betroffenen vorhersehbar war. Wenn die Verarbeitung nicht mehr zwingend zur Vertragserfüllung gemäß Art. 6 Abs. 1 S. 2 lit. b DSGVO notwendig war, kann die Rechtfertigung durch Art. 6 Abs. 4 DSGVO begründet sein, sofern der Verantwortliche nachweist, dass die Zwecke der Vertragserfüllung und der Störungsbehebung kompatibel sind. Diese Gedanken lassen sich nach Auffassung der Autoren auf die IT-Sicherheit als Grundlage der Verarbeitung personenbezogener Daten übertragen.[34]

3. Bußgeld Art. 83 DSGVO und § 30 OWiG, EuGH-Vorlage durch KG Berlin, 3 Ws 250/21

Im Vorjahr berichteten die Autoren über die unterschiedlichen Entscheidungen des LG Berlin und des LG Bonn zur Frage, ob § 30 OWiG bei der Festsetzung von Bußgeldern gemäß Art. 83 DSGVO anzuwenden ist. Die Antwort hierauf ist relevant, wenn ein Bußgeld mangels Zuordnung eines Tatbeitrags zu einer bestimmten Person nach § 30 OWiG scheitert. Das KG Berlin hat diese Frage im Berichtszeitraum dem EuGH vorgelegt.[35]

4. IT-Grundrecht mit staatlicher IT-Security-Schutzpflicht; Hackback

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht) hat der IT-Sicherheit Verfassungsrang verschafft, in erster Linie als Abwehrrecht gegen staatliche Eingriffe, insbesondere gegen die Online-Durchsuchung. Im Berichtszeitraum hat das BVerfG auch die nachteiligen Folgen einer Online-Durchsuchung zu Lasten der IT-Sicherheit der davon betroffenen informationstechnische Systeme konstatiert: Die Befugnis zur Online-Durchsuchung schafft beim Staat das Interesse, Sicherheitslücken offenzuhalten, anstatt die Hersteller zur Schließung oder Vermeidung zu veranlassen. Das BVerfG hat den Eingriff in das IT-Grundrecht deshalb aber nicht als unzulässig eingestuft, sondern die Voraussetzungen für den Eingriff entsprechend eng gefasst. Aus Sicht der Autoren bleibt dabei ein Aspekt unberücksichtigt: Schwachstellen in Software lassen sich nicht dergestalt kontrollieren, dass sie nur zu den gesetzlich definierten Zwecken ausgenutzt werden. Kriminelle nichtstaatliche Organisationen oder andere Staaten, die sich nicht an die europäischen und nationalen Verfassungswerte halten, nutzen die Lücken ebenfalls aus. Darüber hinaus hat das BVerfG aus der Wertentscheidung der Verfassung die Pflicht für den Staat abgeleitet, dazu beizutragen, die Integrität und Vertraulichkeit von IT-Systemen zu schützen. Diese grundrechtliche Schutzpflicht hat das BVerfG im Berichtszeitraum in zwei Entscheidungen bestätigt (bayerisches Verfassungsschutzgesetz und hessisches Sicherheits- und Ordnungsgesetz). Beide Verfassungsbeschwerden wurden nur deshalb als unzulässig zurückgewiesen, weil die Beschwerdeführer ihre Beschwerdebefugnis mangels detaillierter Auseinandersetzung mit den angegriffenen Regelungen nicht dargelegt haben.[36]

Vor dem Hintergrund dieser Schutzpflicht stellt sich auch die Frage, ob die politische Idee sogenannter Hackbacks vertretbar bzw. überhaupt umsetzbar ist. Dabei versteht man unter Hackbacks Gegenangriffe. Angreifer sollen so ausgeschaltet werden und/oder deren Angriffe erschwert bis unmöglich gemacht werden. Als Ziel definieren die politischen Ideengeber eine Art digitaler Selbstverteidigung, die das Risiko für Angreifer erhöhen soll. Aus technischer Sicht ist für einen solchen gezielten Gegenangriff zunächst erforderlich, den Täter eindeutig zu identifizieren, und andererseits Sicherheitslücken in seinem System zu finden, um ihm darüber auch im Rahmen der Gegenwehr Schaden zufügen zu können. Erkennbar setzt dies wiederum das Sammeln von IT-Sicherheitslücken durch Akteure voraus, die für einen effektiven Hackback nicht behoben sein sollten. Darüber hinaus ist problematisch, dass IT-Angriffe in der Regel nicht unmittelbar von den Rechnern der Täter verübt werden, sondern häufig über Zwischenstationen zu Tarnzwecken.[37] Diese Zwischenstationen sind also Systeme Dritter. Sie über einen Hackback zu attackieren, wäre ein Stellvertreterkrieg, der erhebliche Kollateralschäden befürchten lässt, aber kaum den tatsächlichen Täter treffen wird. Zudem ist zu erwarten, dass diese

32 EuGH, 6. 10. 2021 – C-13/20, K&R 2021, 785 - 789, Rn. 28 - 53 = GRUR 2021, 1508 - 1511, dazu *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Kap. 50.1 Rn. 232f - 232k, 460.

33 *Taeger*, in: Taeger/Gabel, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 6 DSGVO Rn. 81, 129, 138; *Freund*, in: Schuster/Grützmacher, IT-Recht, Kommentar, 2020, DS-GVO Art. 6 Rn. 42; generell zum Streitstand *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Kap. 50.1 Rn. 328.

34 EuGH, 20. 10. 2022 – C-77/21 (ECLI:EU:C:2022:805) sowie zuvor die Schlussanträge des Generalanwalts beim EuGH Pikamäe v. 31. 3. 2022, Rs. C-77/21, BeckRS 2022, 5909 = CELEX 62021CC0077, insbesondere Rn. 53, 60 und 70; zur IT-Sicherheit als Rechtsgrundlage der Verarbeitung bereits *Deusch/Eggendorfer*, K&R 2018, 753, 757; ähnlich *Piltz*, in: Specht-Riemenschneider et. al., Festschrift *Taeger*, 2020, S. 351, 357, auf Art. 32 als „rechtliche Verpflichtung" i. S. d. Art. 6 Abs. 1 S. 1 lit. c DSGVO abstellend.

35 Zu den Entscheidungen des LG Bonn, 11. 11. 2021 – 29 Owi 1/20, K&R 2021, 133 ff. (laut Pressestelle rechtskräftig) und des LG Berlin 18. 2. 2021 – 526 OWi LG 1/20; *Deusch/Eggendorfer*, in: Taeger (Fn. 26), S. 321, 327 und ergänzt in K&R 2021, 689, 695; zum Vorlagebeschluss an den EuGH, KG Berlin, 6. 12. 2021 – 3 Ws 250/21, K&R 2022, 135.

36 IT-Grundrecht als Abwehrrecht: BVerfG, 27. 2. 2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274 = K&R 2008, 241 (Ls.) = NJW 2008, 822; bestätigt durch BVerfG, 26. 4. 2022 – 1 BvR 1619/17, K&R 2022, 432 (Ls.) = NJW 2022, 1583, 1607, dort Rn. 111, 310, 316 (bayerisches Verfassungsschutzgesetz, in Rn. 316 mit dem Verweis auf die Gefahren der Online-Durchsuchung und auch zur Bestätigung der Schutzpflicht), zur Begründung der Schutzpflicht: BVerfG, 8. 6. 2021, 1 BvR 2771/18, K&R 2021, 571 - 576 = NJW 2021, 3033 (Polizeigesetz Baden-Württemberg); zur Bestätigung der Schutzpflicht BVerfG, 20. 1. 2022 – 1 BvR 1552/19, K&R 2022, 266 ff. – Hessisches Sicherheits- und Ordnungsgesetz (HOSG), K&R 2022, 266 - 268 = NJW 2022, 1310 (nur Ls.); zum Ganzen auch *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Kap. 50.1 Rn. 368 ff. (Grundrecht auf IT-Sicherheit) und 388 ff. (Schutzpflicht zur IT-Sicherheit); kritisch dagegen *Wimmer/Mechler*, in: Gabel/Heinrich/Kiefner/Rechtshandbuch Cyber-Security, 2019, Kap. I Rn. 1 Fn. 6; *Brodowski*, in: Kipker (Fn. 1), Kap. 13 Rn. 4.

37 Der Einsatz von Zwischenstationen ist nicht neu, schon der Pentagon-Hack 1986 durch einen Hamburger lief über mehrere Zwischenstationen, die *Clifford Stoll*, Kuckucksei, 2015, detailliert beschreibt. Fn. 10 deutet an, dass professionelle Angreifer nur schwer, wenn überhaupt, identifizierbar sind.

Maßnahmen professionelle Tätergruppierungen nicht beeindrucken, da sie Vorsorge gegen Hackbacks treffen: Anonymisierungsdienste, gehärtete Systeme, also Systeme mit wenigen Sicherheitslücken und zusätzlichen Erschwernissen gegen Angriffe. Ob derartige Hackbacks unter dem Begriff „aktive Cyberabwehr" in der Cybersicherheitsagenda 2022 des Bundesinnenministeriums gemeint und angestrebt sind, ist Gegenstand einer kleinen Anfrage im Deutschen Bundestag.[38] Im Rahmen einer grundrechtlichen Verhältnismäßigkeitsprüfung ist sowohl die Geeignetheit als auch die Angemessenheit von Hackbacks zu hinterfragen. Aus technischer Sicht ist zu empfehlen, die Bemühungen nicht auf Hackbacks zu verwenden, sondern in sicherere Software und Verfahren zur Prüfung von Software, damit Angriffe einen höheren Aufwand verursachen und deshalb für die Täter unattraktiver werden.

5. Nachweis und Disponibilität der TOM; Verantwortlichkeit

Das Update der Autoren im Vorjahr berichtete über eine Entscheidung des OLG Stuttgart, wonach ein ISO 27001-Zertifikat ausreichende TOM gemäß Art. 32 DSGVO bescheinigen kann. Die Revision ist noch beim BGH anhängig. Im Fall eines DSGVO-Verstoßes hat das LG München angenommen, dass die Datenschutzverletzung bei der Einhaltung adäquater Sicherheitsmaßstäbe vermieden worden wäre. Zwischenzeitlich hat die Deutsche Datenschutzkonferenz beschlossen, dass es eine objektive Rechtspflicht des Verantwortlichen ist, angemessene IT-Sicherheitsmaßnahmen gemäß Art. 32 DSGVO zu ergreifen; dies steht nicht zur Disposition der Betroffenen. Weiter haben sich die Datenschutzbehörden zu den Sicherheitsanforderungen in der E-Mail- und Telefax-Kommunikation positioniert.[39]

Das OLG Dresden hat im Berichtszeitraum geurteilt, dass auch ein Geschäftsführer persönlich für Datenschutzverstöße der von ihm geführten Gesellschaft verantwortlich sein kann. Denn der Geschäftsführer bestimmt über die Zwecke und Mittel der Verarbeitung personenbezogener Daten (§ 4 Nr. 7 DSGVO).[40]

6. Keine Klarnamenpflicht wegen IT-Sicherheit, BGH, III ZR 4/21

Der Hinweis auf die „Sicherheit" eines Nutzerkontos ist für den BGH nicht ausreichend gewesen, um eine Klarnamenpflicht zur Nutzung der Facebook-Plattform zu begründen.[41]

7. Landesinformationsrecht und IT-Sicherheit

Das VG Wiesbaden hat eine Klage auf Herausgabe des Quellcodes einer Schulsoftware nach Maßgabe des hessischen Landesinformationsgesetzes abgelehnt, weil die Preisgabe des Quellcodes die IT-Sicherheit gefährde. Dies kann bezweifelt werden: Es ist die Pflicht des Staates, Sicherheitslücken zu beseitigen, statt sie zu verdecken (siehe oben Ziffer 4). Richtig ist indes, dass der Quellcode einer Schulsoftware keine amtliche Information ist, die unter die Auskunftsrechte der Landesinformationsfreiheitsgesetze fällt.[42]

8. BSI-Warnung: Kaspersky Antivirus, OVG Münster, 4 B 473/22

Gemäß § 7 Abs. 1 Nr. 1a BSIG kann das Bundesamt für Sicherheit in der Informationstechnik (BSI) Warnungen vor Sicherheitslücken in informationstechnischen Systemen an die Öffentlichkeit richten. § 7 Abs. 2 S. 1 BSIG setzt für die Warnung unter Nennung des Herstellers und des Produkts zudem Anhaltspunkte dafür voraus, dass durch die Lücke Gefahren für die Sicherheit in der Informationstechnik ausgehen.[43]

Sich auf darauf berufend hat das BSI davor gewarnt, Virenscanner der russischen[44] Unternehmensgruppe Kaspersky einzusetzen. Nach Ansicht des BSI könne die Antivirensoftware weitreichend in das System des Nutzers eingreifen, möglicherweise auch Daten exfiltrieren. Da insbesondere mit Blick auf den Ukraine-Krieg eine relevante Gefahr von Cyberangriffen staatlicher russischer Akteure ausgehe, erfolge die Warnung. Das OVG Münster lehnte die Anträge von Kaspersky im einstweiligen Rechtsschutz auf Unterlassung und Widerruf der Warnung ab und folgte der Begründung des BSI: Die Warnung rechtfertige § 7 Abs. 1 Nr. 1a, Abs. 2 S. 1 BSIG. Umstritten ist dabei das Tatbestandsmerkmal der Sicherheitslücke (legaldefiniert in § 2 Abs. 6 BSIG). Für das OVG Münster weisen Virenscanner per se eine Sicherheitslücke auf (Hinweis: Die Autoren sind anderer Auffassung). Dritte könnten aus Sicht des Gerichts diese weitreichenden Zugriffsrechte des Virenscanners ausnutzen, um sich gegen den Willen des Berechtigten Zugang zu dessen Systemen zu verschaffen oder deren Funktionen zu beeinflussen. Da Kaspersky aus Russland geleitet werde und es enge Verbindungen mit den russischen Behörden gebe, hält das Gericht eine Einflussnahme der russischen Regierung für möglich. Insbesondere wegen des Russland-Ukraine-Konflikts habe das BSI ausreichende Anhaltspunkte für eine hierdurch begründete Gefahr für die Sicherheit in der

38 Zur Cybersicherheitsagenda 2022 https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2022/07/cybersicherheitsagenda.html; zur parlamentarischen Anfrage nach Hackbacks BT-Drs. 20/3308.

39 Zu OLG Stuttgart, 31. 3. 2021 – 9 U 34/21, K&R 2021, 748 ff. = ZD 2021, 375 mit der Vermutung zur Erfüllung der TOM (Revision beim BGH: VI ZR 111/21) siehe *Deusch/Eggendorfer*, in: Taeger (Fn. 26), S. 321, 327 und ergänzt in, K&R 2021, 689, 695; LG München I, 9. 12. 2021 – 31 O 16606/20, ZD 2022, 242 - 243, Rn. 39; generell zum Sach- und Streitstand beim Nachweis der TOM *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1) Kap. 50.1 Rn. 309 (Beweislastumkehr LAG Baden-Württemberg, 25. 2. 2021 – 17 Sa 37/20, ZD 2021, 436, dort Rn. 61 (Revision beim BAG: 8 AZR 209/21, gemäß Sitzungsergebnis des BAG vom 22. 9. 2022 an den EuGH vorgelegt, allerdings mit Fragen zu Art. 88 DSGVO – Anforderungen an Kollektivvereinbarungen – und 82 DSGVO) – Voraussetzungen immateriellen Schadensersatzes, https://www.bundesarbeitsgericht.de/sitzungsergebnis/8-azr-209-21/); zum DSK-Beschl. v. 24. 11. 2021 (Verzicht auf TOM): https://www.datenschutzkonferenz-online.de/media/dskb/20211124_TOP_7_Beschluss_Verzicht_auf_TOMs.pdf, dazu *John/Schaller*, CR 2022, 156; zu den DSK-Empfehlungen für E-Mail und Fax: DSK-Orientierungshilfe zu E-Mails: https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf; die hessische Datenschutzbehörde zu Telefax und Art. 32 DSGVO: https://datenschutz.hessen.de/datenschutz/it-und-datenschutz/zur-%C3%BCbermittlung-personenbezogener-daten-per-fax.

40 OLG Dresden, 30. 11. 2021 – 4 U 1158/21, NJW-RR 2022, 589; kritisch dazu *Müller-Peltzer/Selz*, PinG, 2022, 76, 77 sowie *Reichert/Groh*, NZG 2022, 307 - 308.

41 BGH, 27. 1. 2022 – III ZR 4/21, K&R 2022, 268 ff. = WRP 2022, 468 - 472 = NJW-RR 2022, 621 - 624.

42 VG Wiesbaden, 7. 1. 2022 – 6 K 784 21.WI, kritisch dazu *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Kap. 50.1 Rn. 467a.

43 *Schulte*, in: Ritter, Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2021, § 7 BSIG Rn. 307, 317 - 320.

44 Die Unternehmensgruppe gehört einer in Großbritannien registrierten Holding, Niederlassungen und Unternehmen sind weltweit zu finden. Kaspersky entstand ursprünglich in Russland, die drei Gesellschafter der britischen Holding, darunter der Unternehmensgründer Jewgeni Kaspersky, sind russische Staatsbürger. Die Leitung des Konzerns sowie wesentliche Entwicklungsleistungen werden in den Räumen der russischen Tochtergesellschaft in Moskau erbracht. Das Unternehmen arbeitet nach eigenen Angaben mit dem russischen Geheimdienst FSB zusammen (Rn. 107 - 114 des Beschlusses). Hieraus leitet das BSI die Gefahr der Unzuverlässigkeit des Herstellers ab.

Informationstechnik vorgetragen. Zumindest bestehe eine erhöhte Gefahrenlage für Kollateralschäden für Kaspersky-Nutzer.[45]

Aus technischer Sicht ist zunächst richtig, dass Virenscanner umfassenden Systemzugriff benötigen, um Malware zu erkennen: Funktionsbedingt sollten sie jeden Zugriff auf Datenträger abfangen, um die gelesenen Daten zu prüfen. Weiterhin müssen sie mindestens bei ihrem Start den Arbeitsspeicher und kritische Bereiche der Festplatte auf Malware scannen. Dabei erhalten Antivirenprogramme generell einen umfassenden Einblick in alle auf dem System verarbeiten Daten. Dies ist der Aufgabe geschuldet und keine Besonderheit von Produkten eines bestimmten Herstellers, wie Kaspersky.

Die polizei- und ordnungsrechtliche Gefahr, die die Warnung gemäß § 7 Abs. 2 S. 1 BSIG zusätzlich zur Sicherheitslücke voraussetzt, liest das Gericht in das Tatbestandsmerkmal „Sicherheitslücke" aus § 7 Abs. 1 Nr. 1 lit. a BSIG hinein. Gemäß Rn. 70 des Beschlusses seien für den sicheren Einsatz der beschriebenen Software „die Zuverlässigkeit, der Eigennutz und die authentische Handlungsfähigkeit des Herstellers" entscheidend. Die Autoren verstehen die Formulierungen des OVG so, dass die bestimmungsgemäße Funktion einer Software zur Sicherheitslücke werden soll, wenn der Hersteller nicht (mehr) zuverlässig ist. Eine solche Gesetzesauslegung löst den Begriff der Sicherheitslücke vom technischen Sachverhalt los und macht sie von einer polizeirechtlichen Gefahr und der Beurteilung des Herstellers abhängig. Das Gesetz definiert die konkrete Gefahr im Sinne des Polizeirechts aber nicht als Tatbestandsmerkmal der Sicherheitslücke, sondern als weitere Voraussetzung einer Warnung gemäß § 7 Abs. 2 S. 1 BSIG.[46] Weshalb BSI und Gericht nicht geprüft haben, ob die vorhandenen Erkenntnisse ausreichen, um die Gefahr eines unerlaubten Zugriffs auf die Daten der Nutzer gemäß § 7 Abs. 1 Nr. 1c BSIG anzunehmen, ist den Autoren unklar. Zudem hätte das BSI seine Mitteilung auch aufgrund von § 7 Abs. 1 Nr. 1d BSIG verbreiten können. In beiden Fällen wäre es nicht notwendig gewesen, den technisch besetzten Begriff der Sicherheitslücke zu „verbrennen", indem nichttechnische Sachverhalte wie die politische Gefahrenlage in das Tatbestandsmerkmal hineingelesen werden.[47]

Kaspersky wendete ein, das BSI müsse auch vor den Virenscannern anderer Hersteller warnen, wenn jeder eine Sicherheitslücke schaffe. Dazu hat das OVG Münster in Rn. 160 geprüft, ob es willkürlich war, nur vor Kaspersky zu warnen und nicht auch z. B. vor chinesischen oder US-Herstellern. Einen solchen willkürbedingten Ermessensfehler will das Gericht aber nicht gelten lassen. Anders als Russland habe weder China noch die USA Deutschland zum unfreundlichen Staat erklärt. Diese Argumentation ist inkonsistent: Einerseits empfiehlt der BSI-Grundschutz den Einsatz von Virenscannern, andererseits soll damit eine Sicherheitslücke verbunden sein. Zu hinterfragen ist auch, ob die Lücke in einem russischen Produkt tatsächlich gefährlicher ist als in chinesischen oder US-Produkten. Schließlich reglementiert § 9b BSIG („lex Huawei") aus Misstrauen gegen China den Softwareeinsatz in KRITIS-Bereichen. Auch für US-Produkte haben die „Snowden-Enthüllungen" geheimdienstliche Datenzugriffe offenbart.[48] Im Nachgang des einstweiligen-Rechtsschutz-Verfahrens haben journalistische Recherchen weitere Umstände zum Zustandekommen der BSI-Warnung herausgearbeitet, die dafür sprechen könnten, dass es sich weniger um eine wissenschaftlich-technische, als vielmehr um eine politische Entscheidung der Behörde gehandelt haben könnte.[49] Ob und wie sich diese Erkenntnisse in etwaigen Hauptsacheverfahren auswirken, bleibt abzuwarten.

9. Vermieter als Telekommunikationsanbieter, BGH, I ZR 106/20

Der BGH hat (gewerblich tätige) Vermieter, die ihren Mietern einen Kabel-TV-Anschluss als Vermietungsleistung gegen Kostenumlage zur Verfügung stellen, als Anbieter eines öffentlichen Telekommunikationsdienstes i. S. d. § 43b TKG a. F. angesehen (kurz: TK-Anbieter). Streitpunkt im Verfahren war die Abmahnung eines Verbraucherverbands, weil der Vermieter die Mieter an seine TV-Leistung über den gesamten Zeitraum des Mietvertrags bindet, obwohl § 43b TKG a. F. eine Bindungsdauer von maximal 24 Monaten zulässt.[50] Das Urteil wirft indes interessante Folgefragen auf: Ein solcher Vermieter müsste sich konsequenterweise auch als TK-Anbieter gemäß § 5 TKG bei der Bundesnetzagentur registrieren und die Sicherheitsanforderungen der § 165 ff. TKG erfüllen. Auch die Frage, ob Arbeitgeber TK-Anbieter sind, wenn sie ihren Beschäftigten die private Nutzung von Internet oder E-Mail erlauben, wird neu befeuert. Denn für die Eigenschaft als TK-Anbieter (von der LAG-Rechtsprechung für den Arbeitgeber mehrheitlich abgelehnt) war für den BGH entscheidend, dass mehr als 100 000 Mieter das TV-Angebot nutzten. Sind künftig Arbeitgeber mit mehr als 100 000 Beschäftigten TK-Anbieter?[51]

10. Elektronische Kommunikation im Kontext von § 2 Nr. 1b GeschGehG und § 3a VwVfG

Gemäß § 2 Nr. 1b GeschGehG kann eine Information nur dann ein Geschäftsgeheimnis sein, wenn sie Gegenstand

45 OVG Münster, 28. 4. 2022 – 4 B 473/22, K&R 2022, 555 - 561 = NJW 2022, 1547 ff. (Rn. 48 ff.). Die Verfassungsbeschwerde hiergegen hat das BVerfG nicht zur Entscheidung angenommen, weil die Einwendungen des Beschwerdeführers Argumente betreffen, die im Hauptsacheverfahren zu prüfen sind, BVerfG, Nichtannahmebeschluss vom 2. 6. 2022 – 1 BvR 1071/22 – juris = NJW 2022, 2250 - 2251.

46 *Schulte*, in: Ritter (Fn. 43), § 7 BSIG Rn. 319.

47 *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Kap. 50.1 Rn. 410; kritisch auch *Kipker*, Replik zum Beschluss des OVG NRW zur Warnung vor Kaspersky, https://intrapol.org/2022/04/28/replik-zum-beschluss-des-ovg-nrw-zur-warnung-vor-kaspersky-eine-katastrophale-entscheidung/.

48 BSI-Empfehlung zu Virenscannern: Baustein OPS 1.1.1.4.A3; zum „lex Huawei" *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Kap. 50.1 Rn. 413 m. w. N.; zu US-Produkten: *Yang/West/Thiruvathukal/Klingensmith/Fawaz*, Are You really muted (https://wiscprivacy.com/papers/vca_mute.pdf) haben jedenfalls für Video-Konferenztools den Beweis dafür erbracht, dass die Anbieter sich nicht immer an die Einstellungen der Nutzer halten, sondern z. T. anderweitige oder sogar gegenteilige Funktionen ausführen. https://www.splunk.com/en_us/product-security/announcements/svd-2022-0608.html zeigt, dass Sicherheitssysteme zu Sicherheitslücken werden können, hier ein Netzwerkmonitor, der durch einen Programmierfehler das Einschleusen von Code auf allen Sensoren im Netz ermöglicht. Das ist aus Sicherheitssicht Lücken in Virenscannern ähnlich.

49 https://www.tagesschau.de/investigativ/br-recherche/software-kaspersky-sicherheit-warnungen-101.html, pikant in dem Kontext sind die vom Recherchenetzwerk „Policy Networks Analytics" mit Jan Böhmermann veröffentlichten mutmaßlichen Verbindungen des BSI-Präsidenten Arne Schönbohm bzw. des von ihm (mit) gegründeten Vereins „Cybersicherheitsrat Deutschland e. V." mit russischen Anbietern im Bereich der IT-Sicherheit, insbesondere soll den Berichten zufolge der IT-Sicherheitsanbieter „Protelion", der mit dem Monitoring kritischer Infrastrukturen in Deutschland beauftragt sei, im Mehrheitsbesitz von russischen Gesellschaftern sein https://www.zdf.de/comedy/zdf-magazin-royale/zdf-magazin-royale-vom-7-oktober-2022-100.html, https://www.channelpartner.de/a/schwere-vorwuerfe-gegen-bsi-praesident-schoenbohm,3615737. Eine BSI-Warnung vor Protelion – vergleichbar zur Kaspersky-Warnung – hat soweit ersichtlich bislang nicht stattgefunden.

50 BGH, 18. 11. 2021 – I ZR 106/20, K&R 2022, 198 - 202 = CR 2022, 124 m. Anm. *Kiparski*; § 43b TKG ist seit 1. 12. 2021 abgelöst worden durch § 56 TKG.

51 *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Kap. 50.1 Rn. 419.

angemessener Geheimhaltungsmaßnahmen ist. Angemessene Geheimhaltung verlangt technische und organisatorische Maßnahmen (TOM) zum Schutz der Information. Die Rechtsprechung hat im Berichtszeitraum dazu weitere Kriterien herausgearbeitet, wenngleich im Einzelnen vieles streitig bleibt. Fest steht danach lediglich: (i) Die geheimzuhaltende Information darf nur solchen Personen anvertraut werden, die sie zur Durchführung ihrer Aufgabe benötigen (Need-to-Know-Prinzip). (ii) Art und Umfang der Schutzmaßnahmen sind abhängig vom Grad der Schutzbedürftigkeit der Information. Entscheidend hierfür sind der Wert des Geschäftsgeheimnisses und dessen Entwicklungskosten, die Natur der Information, deren Bedeutung für das Unternehmen, die Größe des Unternehmens, die üblichen Geheimhaltungsmaßnahmen in dem Unternehmen, die Art der Kennzeichnung der Informationen sowie vereinbarte vertragliche Regelungen mit Arbeitnehmern und Geschäftspartnern. Der Schutz als Geschäftsgeheimnis wurde z. B. versagt,

- wenn die betreffende Information vom IT-System des Unternehmens auf einen privaten Datenträger kopiert werden konnte,
- wenn keine Schutzmaßnahmen gegen den Zugriff Unbefugter auf Papierdokumente ergriffen sind,
- lediglich auf „generelle Schutzmaßnahmen zur Etablierung einer angemessenen IT-Sicherheit" verwiesen wird, ohne konkrete Maßnahmen zu benennen, die auf den Schutz spezifischer Information abzielen.
- Verschwiegenheitsvereinbarungen sind eine geeignete Schutzmaßnahme, wenn sie die betreffende Information hinreichend definieren (keine „Catch-All-Klauseln", allerdings ist eine Geheimhaltungsvereinbarung bei hinreichender Beschreibung auch formularvertraglich möglich, LAG Stuttgart, Urt. v. 18. 8. 2021 – 4 SaGa 1/21).[52]

Das OLG Schleswig-Holstein hat für eine unternehmerische Preiskalkulation „übliche Schutzmaßnahmen wie Passwörter und Firewalls" nebst einer „TLS-Verschlüsselung in der E-Mail-Kommunikation" als ausreichend erachtet. Insbesondere die TLS-Verschlüsselung sei ein „gängiges Verschlüsselungsprogramm" und im konkreten ausreichend. Diese Entscheidung wirft aus technischer Sicht Zweifel auf: TLS ist kein Verschlüsselungsprogramm, sondern ein Protokoll, also eine Vorschrift für den Datenaustausch. TLS kommt z. B. für HTTPS zum Einsatz. Ziel des Protokolls ist dabei, den Datenaustausch zwischen zwei Rechnern unabhängig vom Anwendungsprotokoll zu schützen. Zu den Hauptanwendungszwecken zählten daher die Übertragung von Login-Daten oder von Kreditkartendaten, etwa beim Online-Einkauf. Um möglichst interoperabel und abwärtskompatibel zu sein, können zwei Systeme, die TLS verwenden, neben der konkreten TLS-Version (aktuell ist TLS 1.3) auch die verwendeten Verschlüsselungsalgorithmen und weitere Parameter aushandeln. Bei E-Mail diente TLS zunächst dem Schutz der Login-Daten beim Abrufen der Mails, später erlangte es Popularität als Option beim E-Mailversand. Dabei ist i. d. R. TLS für den Versand nicht verpflichtend, sondern fakultativ: Wenn der empfangende Rechner das TLS-Protokoll nicht akzeptiert, entscheidet der versendende Mailserver, ob er die Nachricht unverschlüsselt überträgt oder ob er den Versand unterlässt. Selbst wenn die TLS-Verschlüsselung erfolgt, entschlüsselt der empfangende Mailserver die Nachricht. Der übliche Vergleich, dass eine E-Mail aus Sicherheitssicht einer Postkarte gleiche, also offen für jedermann zu lesen ist, lässt sich mit TLS ergänzen: Zwischen zwei Postverteilzentren (Mailservern) kann (!) die Post die Karte zum Schutz in einen Umschlag stecken. Damit wäre sie auf dem Transport zwischen diesen zwei Zentren geschützt, aber schon im Verteilzentrum folgte das Öffnen des Briefkuverts, wobei alle dort beschäftigten Personen den Brief lesen und dessen Inhalt weitergeben könnten. Das TLS-Verschlüsselungsprotokoll erwirkt damit aus technischer Sicht keinen besonderen Schutz für die Kommunikation und ist nach Auffassung der Autoren kein Kriterium, das eine Information als Geschäftsgeheimnis i. S. d. § 2 Nr. 1b GeschGehG qualifiziert.[53]

Den identischen Problemkreis von „Transportverschlüsselung" und Ende-zu-Ende-Verschlüsselung betrifft der Beschluss des VG Frankfurt vom 15. 7. 2022 im einstweiligen Rechtsschutz. Zugrunde lag die Praxis des Bundesamts für Wirtschaft und Ausfuhrkontrolle, die Kommunikation mit Waffenhändlern über gesetzlich vorgegebene Meldungen zum Kriegswaffenbuch gemäß § 3a VwVfG per E-Mail zu führen. Auch in diesem Fall hat das Gericht eine elektronische Kommunikation per Transportverschlüsselung als „ausreichend" sicher bewertet. Der hiervon betroffene Waffenhändler könne keine Ende-zu-Ende-Verschlüsselungen für diese Kommunikationen verlangen. Dies sei – so das Gericht – weder mit Blick auf die DSGVO gefordert, noch habe der Antragsteller glaubhaft gemacht, dass die Kommunikation aufgrund von Interessen krimineller und ressourcenreicher Dritter besonders zu schützen sei.[54] Für diesen Beschluss lassen sich die Bedenken gegen die Entscheidung des OLG Schleswig-Holstein übertragen: Aus technischer Sicht führt die sogenannte „Transportverschlüsselung" nicht zu einer erhöhten Sicherheit. Die Entscheidung ist daher abzulehnen.

11. Sicherheit von Online-Meetings (Webex), LAG Köln, 9 TaBV 7/21

§ 129 BetrVG hat die Online-Versammlung von Betriebsräten bis zum 19. 3. 2022 zugelassen, wenn sichergestellt ist, dass nur teilnahmeberechtigte Personen Kenntnis von dem Inhalt der Versammlung nehmen können. Seit 19. 3. 2022 gilt dies gemäß § 30 Abs. 2 Nr. 3 BetrVG. Das LAG Köln hat dazu in einem Beschluss die Auffassung vertreten, die „heutigen marktgängigen Konferenzsysteme" (namentlich CiscoWebex) böten „durchweg die Möglichkeit einer hinreichend sicheren und verschlüsselten Kommunikation". Demgegenüber ist festzustellen: technische Untersuchungen haben das Gegenteil erwiesen. Kamera und Mikrofon waren aktiviert, obwohl der Nutzer sie nicht aktiviert hatte. Darüber hinaus dürfen US-amerikanische Dienste wie Webex nur unter den Voraussetzungen der Artt. 44 ff. DSGVO genutzt werden. Dies hat das LAG

52 OLG Stuttgart, 19. 11. 2020 – 2 U 575/19 – juris, Rn. 259 f. = WRP 2021, 242 - 258 (Kopiermöglichkeit auf private Datenträger); ArbG Aachen, 13. 1. 2022 – 8 Ca 1229/20, Rn. 85 f., NJW-RR 2022, 178 (kein substantiiert vorgetragenes Schutzkonzept und keine spezifische Geheimhaltungsvereinbarung); LAG Stuttgart, 18. 8. 2021 – 4 SaGa 1/21, MMR 2022, 79 (formularvertragliche Geheimhaltungspflicht durch Untersagung, unternehmensinterne Datenbestände außer Haus zu bringen).

53 OLG Schleswig-Holstein, 28. 4. 2022 – 6 U 39/21, K&R 2022, 628 - 631, in Rn. 112 ff. (K&R 2022, 630) vornehmlich abstellend auf „TLS-Verschlüsselung", kritisch dagegen *Deusch/Eggendorfer*, K&R 2022, 577 - 581 sowie in Taeger/Pohle, (Fn. 1), Kap. 50.1 Rn. 189 f., 196 (technischer Sachverhalt zur TLS-Verschlüsselung) und Rn. 423 (Kritik am Urteil des OLG Schleswig-Holstein); generell zu Schutzmaßnahmen auch *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Kap. C Rn. 147 und zu TLS *Deusch/Eggendorfer*, K&R 2022, 404, 406.

54 VG Frankfurt a. M., 15. 7. 2022 – 5 L 1281/22.F, https://www.rv.hessenrecht.hessen.de/bshe/document/LARE220003171.

Köln erkannt, aber in seiner Entscheidung für die Wirksamkeit des virtuellen Betriebsratsbeschlusses für unwesentlich gehalten. US-Dienstleister dürfen jedoch ohne die Voraussetzungen der Art. 28, 44 ff. DSGVO keine Kenntnis von den Inhalten der virtuellen Sitzungen nehmen. Mit Blick auf den technischen Sachverhalt ist dies aber gerade nicht gegeben. Die Autoren halten die Entscheidung des LAG Köln deshalb für falsch.[55]

12. Kryptohandys, BGH, 5 StR 457/21

Der BGH hat sich in der Diskussion um den Straftatverdacht aufgrund der Verwendung sogenannter Kryptohandys positioniert. Er hält es für zulässig, die Beweise aus einer Online-Durchsuchung der Kryptohandys zu verwerten, da allein die Nutzung des Handys vom Hersteller „Encrochat" einen hinreichenden Straftatverdacht liefere. Die Kriterien, die der BGH für einen solchen Straftatverdacht herausgearbeitet hat, sind aber aus Sicht der Autoren nicht geeignet, um Tatverdächtige von Unschuldigen abzugrenzen. Die Frage liegt aktuell dem EuGH und dem BVerfG vor; auch der französische Kassationshof hat seine Bedenken formuliert.[56]

IV. Fazit und Blick in die Zukunft

Rechtsprechung und Gesetzgebung haben auch im letzten Jahr zur IT-Sicherheit viele neue Impulse gesetzt. Während einige begrüßenswert sind, leiden andere an einem fehlenden Wissenstransfer zwischen Informatik und Jurisprudenz. Auch politische Ideen und Vorstellungen, wie Verschlüsselungen, die nur für Behörden zu knacken sind, Chatkontrolle oder Hackback unterstreichen, dass ein Wissenstransfer von Seiten der Informatik dringend erforderlich ist, um fundierte rechtliche Beurteilungen und legislative Gestaltungen auf der Grundlage des korrekten Sachverhalts treffen zu können.

55 LAG Köln, 25. 6. 2021 – 9 TaBV 7/21 (Rn. 31), AnwBl 2021, 621 = MMR 2021, 926 - 927, dazu *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Kap. 50.1 Rn. 508; zur Überwachung durch das amerikanische WebEx s. o. Fn. 48. Dabei hält sich Cisco in seinen zahllosen „Privacy"-Dokumenten bedeckt, welche Daten konkret wohin übertragen werden, u. a. https://trustportal.cisco.com/c/r/ctp/trust-portal.html#/1552559092865171.

56 Zum bisherigen Meinungsstreit *Deusch/Eggendorfer*, in: Taeger (Fn. 26), S. 321, 326 - 331 f. und ergänzt in, K&R 2021, 689, 695; nunmehr BGH, 2. 3. 2022 – 5 StR 457/21, K&R 2022, 433, kritisch dazu *Deusch/Eggendorfer*, K&R 2022, 404 ff., Aktenzeichen beim BVerfG: 2 BvR 684/22; zur EuGH-Vorlage der Beschluss des LG Berlin, 19. 10. 2022 – (525 KLs) 279 Js 30/22 (8/22), abgerufen https://openjur.de/u/2453066.html, Beschluss des cour de cassation, Strafkammer, No M 21-85.148 F-D v. 11. 10. 2022.

Florian Deusch
ist als Rechtsanwalt und Fachanwalt für Informationstechnologierecht in der Anwaltskanzlei Dr. Gretter tätig und Lehrbeauftragter an der Hochschule Ravensburg-Weingarten. Er ist zudem als Datenschutzbeauftragter tätig.

Tobias Eggendorfer
ist Professor für IT-Sicherheit und aktuell an der Agentur für Innovation für Cybersicherheit des Bundes als Abteilungsleiter für „Sichere Systeme" für die Weiterentwicklung der Forschung im Bereich der IT-Sicherheit zuständig. Er ist zudem als IT- und Datenschutzbeauftragter und Lehrbeauftragter tätig.

Dipl.-Jur. Alexander Erdelt*

Erhalt der Vertragsmäßigkeit des digitalen Produkts beim Verbraucher durch Aktualisierungen (§ 327f BGB)

Kurz und Knapp

§ 327f BGB normiert seit dem 1. 1. 2022 die Updatepflicht für digitale Produkte. Diese Norm des BGB stellt eine Umsetzung des Art. 8 Abs. 2 und 4 DI-RL dar. Wesentlich ist hierbei die Aktualisierungspflicht zum Erhalt der Vertragsmäßigkeit des digitalen Produktes als Ausfluss des Verbraucherrechts. Der Autor beschäftigt sich kritisch mit der Umsetzung der Updatepflicht und geht auf die wesentlichen Probleme ein.

I. Die Aktualisierungspflicht als eigenständige Pflicht – Ausfluss der Digitale-Inhalte-Richtlinie

1. Digitale-Inhalte-Richtlinie, Umsetzungsgesetz

Mit der Umsetzung der Digitale-Inhalte-Richtlinie (DI-RL)[1] durch das Umsetzungsgesetz vom 25. 6. 2021,[2] welches am 1. 1. 2022 Gültigkeit erlangt hat, wurden zahlreiche Neuerungen ins allgemeine Schuldrecht des BGB implementiert.

Vorangegangen war neben einem Referentenentwurf auch ein Regierungsentwurf, welcher nur wenige Änderungen beinhaltete. Verbraucherschutzaspekte sowie das Verlangen nach mehr Cybersicherheit, z. B. durch Sicherheitsaktualisierungen, waren Gründe, die den Gesetzgeber zur Einführung bewogen hatten.[3]

Aufgrund rascher technischer, kurzzyklischer (Weiter-)Entwicklung ist es nicht ohne Weiteres selbstverständlich, dass die bereitgestellten digitalen Inhalte oder digita-

* Mehr über den Autor erfahren Sie am Ende des Beitrags.

1 RL (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. 5. 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (ABl. 2019 L 136, 1).

2 Gesetz vom 25. 6. 2021 zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, BGBl. I 2021, 2123.

3 *Hessel/Potel*, RDi 2022, 25.