Meldepflicht von IT-Sicherheits- und Datenschutzvorfällen durch Mitarbeitende - Betrachtung möglicher arbeitsrechtlicher Konsequenzen

Dirk Müllmann[1], Melanie Volkamer[2]

Abstract: Die Pflicht zur Meldung von IT-Sicherheits- und Datenschutzvorfällen in Unternehmen ist eine zentrale organisatorische Maßnahme zum Schutz von deren IT-Infrastruktur. Mitarbeiter offenbaren mit der Meldung des Vorfalls jedoch oftmals eigenes Fehlverhalten, das vom Arbeitgeber zur Grundlage arbeitsrechtlicher Konsequenzen gemacht und somit gegen sie verwandt werden kann. Die Angst vor diesen Konsequenzen kann Arbeitnehmer davon abhalten, der Meldepflicht nachzukommen und der Meldemoral im Unternehmen schaden. Das hat wiederum negative Konsequenzen für das Unternehmen selbst, dem es angesichts unterlassener Meldungen nicht möglich ist, schnell auf Vorfälle zu reagieren und sie effektiv einzudämmen. Der Beitrag untersucht vor dem Hintergrund der datenschutzrechtlichen Meldepflichten für Datenschutzverstöße die rechtlichen Grundlagen der arbeitsrechtlichen Mitteilungspflichten von Mitarbeitern. Er geht ferner auf die Frage der Einschlägigkeit des Selbstbelastungsverbots im arbeitsrechtlichen Kontext ein und analysiert die arbeitsrechtlichen Konsequenzen der Offenbarung von eigenem Fehlverhalten durch Arbeitnehmern bei der Erfüllung einer Mitteilungspflicht. Auf dieser Grundlage entwickelt er einen Vorschlag, wie die Verlässlichkeit der Meldung von IT-Sicherheits- oder Datenschutzvorfällen durch Mitarbeiter verbessert werden kann.

Keywords: Meldepflicht; Datenschutzvorfall; IT-Sicherheitsvorfall; Arbeitnehmer; Selbstbelastungsfreiheit; arbeitsrechtliche Konsequenzen

Ein adäquater Schutz der IT-Infrastruktur vor Cyberangriffen eines jeden Unternehmens bzw. einer jeden Organisation ist nur durch eine geeignete Kombination aus organisatorischen und technischen Maßnahmen möglich. Organisatorische Maßnahmen beinhalten in der Regel auch Security Policies[3] und Sensibilisierungsmaßnahmen. Hierbei geht es darum, wie Mitarbeitende Risiken erkennen und sich idealerweise verhalten, um die Risiken zu minimieren. Eine wichtige Komponente der organisatorischen Maßnahme ist das Melden von IT-Sicherheits- und Datenschutzvorfällen[4]. Eine Pflicht zum Melden ergibt sich aus

[1] Karlsruher Institut für Technologie, Kompetenzzentrum für Angewandte Sicherheitstechnologie (KASTEL), Zentrum für Angewandte Rechtswissenschaft (ZAR), Vincenz-Prießnitz-Straße 3, 76131 Karlsruhe, Germany, dirk.muellmann@kit.edu.

[2] Karlsruher Institut für Technologie, Kompetenzzentrum für Angewandte Sicherheitstechnologie (KASTEL), Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB), Kaiserstraße 89, 76133 Karlsruhe, Germany, melanie.volkamer@kit.edu.

[3] *Herath/Rao*, Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness, Decision Support Systems 47 (2009), 154, 157, https://dx.doi.org/10.1016/j.dss.2009.02.005.

[4] *Grispos/Glisson/Bourrie/Storer/Miller*, Security incident recognition and reporting (SIRR): an industrial perspective, 2017, arXiv preprint, https://arxiv.org/abs/1706.06818.

doi:10.18420/inf2020_74

dem Pflichtenkanon des Arbeitsverhältnisses selbst[5]. Dennoch haben viele Unternehmen und Organisationen eine Meldepflicht für IT-Sicherheits- bzw. Datenschutzvorfälle explizit eingeführt, z. B. in Form von Dienstanweisungen. Hier wird festgelegt, welche Vorfälle – in der Regel unmittelbar – an welchen Personenkreis zu melden sind. Die Meldepflicht ist aus einer Reihe von Gründen eine wichtige Komponente der organisatorischen Maßnahmen[6]:

So sind Cyberangriffe immer schwerer zu erkennen. Außerdem liegt es in der Natur der Menschen, dass sie Fehler machen und daher einen Angriff übersehen oder unvorsichtig mit personenbezogenen Daten umgehen. Es kann also auch bei einer idealen Kombination von organisatorischen und technischen Maßnahmen[7] und für das Thema Sicherheit und Datenschutz hoch sensibilisierten Mitarbeitenden nicht davon ausgegangen werden, dass es keine IT-Sicherheitsvorfälle gibt[8]. Das zeitnahe Melden von IT-Sicherheitsvorfällen ist daher wichtig, um die Schäden eines erfolgreichen Cyberangriffs sowie die Kosten der Schadensbehebung, aber auch rechtliche Konsequenzen und den Imageschaden so gering wie möglich zu halten. Durch zeitnahes Melden, können Experten die Situation auch zeitnah nach dem Angriff untersuchen und technische Schutzmaßnahmen ergreifen. Außerdem werden die Verantwortlichen so rechtzeitig informiert und können entsprechende organisatorische Maßnahmen umsetzen. Im Fall eines Datenschutzvorfalls gibt es zudem gesetzliche Vorgaben, die von den Unternehmen bzw. den Organisationen eine Meldung innerhalb vorgegebener Fristen verlangen. So sieht Art. 33 Absatz 1 S. 1 DSGVO zum Beispiel in diesen Fällen eine Meldung binnen 72 Stunden an die gemäß Art. 55 DSGVO zuständige Aufsichtsbehörde vor. Eine vergleichbare Pflicht existiert gemäß § 8b Abs. 4 BSIG auch für Betreiber kritischer Infrastrukturen im Fall von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme.

Eine offensichtliche Voraussetzung dafür, dass Mitarbeitende IT-Sicherheits- und Datenschutzvorfälle melden, ist das diese durch die verschiedenen organisatorischen Maßnahmen wissen, was ein IT-Sicherheits- bzw. Datenschutzvorfall ist, dass sie diese melden sollen und dass es wichtig ist diese zu melden, um den Schaden für das Unternehmen bzw. die Organisation so gering wie möglich zu halten[9]. Dieses Wissen wird aber nicht zwangsläufig dazu führen, dass jeder IT Sicherheitsvorfall gemeldet wird: Mitarbeitende müssen sich in der Regel mit dem Melden eines IT-Sicherheitsvorfalls einen Fehler eingestehen und gegebenenfalls zumindest indirekt zugeben, dass sie sich nicht an die Security Policies gehalten haben. Dies kann sie vom Melden eines Vorfalls abhalten. Insbesondere Mitarbeitende, die

[5] Vgl. hierzu Kap. 1.2.

[6] *Jaatun/Albrechtsen/Bartnes et al.*, A Study of Information Security Practice in a Critical Infrastructure Application. In: Rong/Jaatun/Sandnes et al. (Hrsg.) Autonomic and Trusted Computing, ATC 2008 Lecture Notes in Computer Science, vol 5060, 527, 527 ff.

[7] *Werlinger/Hawkey/Beznosov*, An integrated view of human, organizational, and technological challenges of IT security management, Information Management & Computer Security, 17 (2009), 4, 4 ff., https://doi.org/10.1108/09685220910944722.

[8] *Dutta/Roy*, Dynamics of organizational information security. System Dynamics Review: The Journal of the System Dynamics Society, 24 (2008), 349, 349 ff., https://onlinelibrary.wiley.com/doi/abs/10.1002/sdr.405.

[9] *Humphrey*, Identifying the critical success factors to improve information security incident reporting, 2017, https://dspace.lib.cranfield.ac.uk/handle/1826/12739.

Angst vor persönlichen Konsequenzen haben, werden Vorfälle weniger zuverlässig melden. Dabei können sie sowohl Angst vor dem eigenen Imageschaden als auch vor rechtlichen Konsequenzen haben. Eine wesentliche Rolle spielt hierbei die allgemeine Fehlerkultur im Unternehmen bzw. der Organisation[10].

Im Vordergrund der vorliegenden Untersuchung steht die Analyse der persönlichen arbeitsrechtlichen Konsequenzen im Zusammenhang mit der Wahrnehmung von Meldepflichten. Aus Sicht der IT-Sicherheit könnte man denken, dass es am besten wäre, die Meldepflicht mit der eindeutigen Aussage zu verknüpfen, dass das Melden eines Vorfalls keine persönlichen rechtlichen Konsequenzen hat, wohl aber dessen Nichtmeldung. Das wäre aber zu kurz gegriffen, weil eine solche Aussage dazu führen würde, dass Mitarbeitenden sich an keine Security Policies mehr halten müssen, solange sie die Vorfälle melden. Das wiederum würde die organisatorischen und gegebenenfalls auch technischen Schutzmaßnahmen aushebeln.

Ziel dieses Beitrags ist es einen Vorschlag zu erarbeiten, wie arbeitsrechtlich mit Vorfällen umgegangen werden könnte, um möglichst wenige Mitarbeitenden davon abzuhalten Vorfälle zu melden, gleichzeitig Mitarbeiter zu motivieren sich möglichst an die Security Policies zu halten. Dazu wird zunächst die rechtliche Ausgangslage analysiert.

1 Rechtliche Ausganslage

Gesetzliche Meldepflichten für den Fall von IT-Sicherheits- oder Datenschutzverstößen existieren für eine Vielzahl unterschiedlicher Situationen. Dabei unterscheiden sich die gesetzlichen Grundlagen und Ausgestaltungen der Meldepflicht von Institutionen oder Unternehmen an Behörden je nach Anwendungsfall und Regelungsgebiet. Die Meldepflicht in der darunterliegenden Ebene, also dem Verhältnis zwischen Arbeitnehmer und Arbeitgeber, beruht hingegen immer auf denselben arbeitsrechtlichen Normen. Angesichts der Fokussierung des Beitrags auf die arbeitsrechtlichen Konsequenzen von Meldepflichten für Mitarbeitende sollen die Meldepflichten von Unternehmen und Institutionen, die ein Auslöser für Meldepflichten von Mitarbeitern sein können, lediglich exemplarisch anhand Art. 33 DSGVO dargestellt werden. Auf die in anderen Bereichen ebenfalls bestehenden unternehmerischen Meldepflichten, wie zum Beispiel bei IT-Sicherheitsverstößen kritischer Infrastrukturen, sei an dieser Stelle jedoch ausdrücklich verwiesen.

1.1 Die Meldepflicht für Datenschutzvorfälle von Unternehmen und Organisationen als Beispiel gesetzlicher Meldepflichten an Aufsichtsbehörden

Um die Informationslage der Aufsichtsbehörden zu verbessern, geeignete Maßnahmen zum Schutz der Betroffenen einzuleiten sowie die Rechtsdurchsetzung und -befolgung

[10] *Werlinger/Hawkey/Beznosov*, An integrated view of human, organizational, and technological challenges of IT security management, Information Management & Computer Security, 17 (2009), 4, 4 ff., https://doi.org/10.1108/09685220910944722.

datenschutzrechtlicher Normen zu steigern,[11] verlangt die Datenschutzgrundverordnung die Meldung der Verletzung des Schutzes von personenbezogenen Daten an die Aufsichtsbehörde. Art. 4 Nr. 12 DSGVO definiert eine solche Schutzverletzung als "*eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenbarung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden*". Art. 33 Absatz 1 S. 1 DSGVO sieht in diesen Fällen eine Meldung der Verletzung binnen, in der Regel, 72 Stunden an die gemäß Art. 55 DSGVO zuständige Aufsichtsbehörde vor.

Durch diese gesetzliche Verpflichtung sieht sich der Verarbeiter einer Situation ausgesetzt, in der er die Behörden gegebenenfalls über ein Fehlverhalten seinerseits informieren muss, das in der Folge als sachliche Grundlage für eine Sanktionierung in einem Buß- oder Strafverfahren genutzt werden könnte. Obwohl die Nichtbefolgung der Meldepflicht gemäß Art. 83 Abs. 4 lit. a) DSGVO ebenfalls bußgeldbewehrt ist,[12] könnte die Verpflichtung des Verarbeiters, sich in einem Verfahren selbst zu belasten, daher dennoch im Konflikt mit dem Selbstbezichtigungsverbot des "nemo tentur"-Grundsatzes stehen.[13] Vor diesem Hintergrund hat der deutsche Gesetzgeber in den §§ 42 Abs. 4, 43 Abs. 4 BDSG ein Verwertungsverbot für die Meldungen und Benachrichtigungen von Datenverarbeitern in Ordnungswidrigkeiten- und Strafverfahren vorgesehen, sodass eine Verwendung in einem Verfahren nur mit dessen Zustimmung erfolgen dürfte. Die Europarechtskonformität dieser Regelung ist jedoch umstritten.[14] Damit die Unternehmen der Meldepflicht von Schutzverletzungen personenbezogener Daten an die Aufsichtsbehörden nachkommen können, sind sie dringend auf die Mitwirkung ihrer Mitarbeitenden angewiesen. Durch das Melden eines Datenschutzvorfalls offenbaren sie aber möglicherweise eigenes Fehlverhalten, das zu der Schutzpflichtverletzung geführt hat und arbeitsrechtlich sanktioniert werden könnte. Das könnte sie davon abhalten, Sicherheitsvorfälle, insbesondere solche, die von ihnen verschuldet wurden, zu melden, was wiederum eine frühzeitige Gegenreaktion und Maßnahmen des Arbeitgebers und Datenverarbeiters erschwert. Eine dem Verwertungsverbot in §§ 42 Abs. 4, 43 Abs. 4 BDSG analoge Regelung für Mitarbeitende besteht im BDSG jedoch nicht. Es wird zwar im Rahmen der Straf- und Bußgeldvorschriften eine analoge Erweiterung des Verwertungsverbots auf Personen, die für andere handeln, im Sinne der §§ 9, 14 OWiG erwogen.[15] Die Konsequenzen einer etwaigen Selbstbelastung von Arbeitnehmern

[11] *Martini* in: Paal/Pauly (Hrsg.), DS-GVO / BDSG, 2. Aufl., 2018, Art. 33 DSGVO, Rn. 10; *Dix* in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), DSGVO, 2019, Art. 33, Rn. 1.

[12] *Hladjk* in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2. Aufl., 2018, Art. 33, Rn. 22.

[13] *Spittka*, Si Tacuisses. . . - Nemo Tenetur und die DSGVO, in: Taeger (Hrsg.), Die Macht der Daten und der Algorithmen, 2019, 141, 144; *Reif* in: Gola (Hrsg.), DSGVO, 2. Aufl., 2018, Art. 33, Rn. 44.

[14] *Brink* in: Wolff/Brink (Hrsg.), Beck'scher Onlinekommentar Datenschutzrecht, Art. 33, Rn.15; *Spittka*, Si Tacuisses. . . - Nemo Tenetur und die DSGVO, in: Taeger (Hrsg.), Die Macht der Daten und der Algorithmen, aaO., 141, 150ff.; *Paal*, ZD 2020, 119, 124; *Bergt* in: Kühling/Buchner (Hrsg.), DSGVO / BDSG, 2. Aufl., 2018, § 43 BDSG, Rn. 11 ff.; *Spittka*, RDV 2019, 167, 170 ff.

[15] *Brodowski/Nowak* in: Beck'scher Onlinekommentar Datenschutzrecht, 31. Ed., 2020, § 43 BDSG, Rn. 25, 27; *Boms*, ZD 2019, 536, 539 f.

durch die Meldung von Schutzverletzungen werden momentan aber weder in Straf- oder Bußgeldverfahren noch auf zivil- und arbeitsrechtlicher Ebene gesetzlich adressiert.

1.2 Die arbeitsrechtliche Benachrichtigungspflicht

Arbeitnehmer treffen gegenüber ihren Arbeitgebern sowohl Auskunfts-[16] als auch Benachrichtigungspflichten. Beide unterscheiden sich dadurch, dass einem Auskunftsanspruch nur auf Anforderung nachgekommen werden muss,[17] während bei Benachrichtigungspflichten alle erforderlichen Informationen unaufgefordert mitzuteilen sind[18]. Die rechtliche Grundlage zur Herleitung einer nicht explizit vereinbarten arbeitsrechtlichen Benachrichtigungspflicht des Arbeitnehmers gegenüber seinem Arbeitgeber stellen die arbeitsvertraglichen Nebenpflichten dar.[19] Die Informationsbeschaffung des Arbeitsgebers ist sowohl auf der Basis eines Auskunfts- als auch einer Mitteilungspflicht denkbar. Vorliegend dürfte dem Benachrichtigungsanspruch jedoch größere Bedeutung zukommen. Da es erforderlich ist, von IT-Sicherheits- bzw. Datenschutzvorfällen bereits zu erfahren, wenn sie noch nicht nach außen getreten und für andere sichtbar geworden sind, muss auch die Meldepflicht für IT-Sicherheits- und Datenschutzvorfällen durch Mitarbeitende unaufgefordert wahrgenommen werden. Anders ist das Ziel schnell auf Vorfälle reagieren zu können für Unternehmen und Organisationen nicht zu erreichen. Die Mitteilungspflicht des Arbeitnehmers kann in diesem Fall mit seiner Verantwortung begründet werden, das Integritätsinteresse seines Arbeitgebers zu wahren.[20] Daraus ergibt sich für ihn die Verpflichtung, im Vorfeld einer Schädigung zu handeln und drohende Störungen und Schäden an Betriebsmitteln zur Kenntnis zu bringen.[21] Die Annahme einer Benachrichtigungspflicht stellt in diesen Fällen ferner den einzigen

[16] Die Herleitung eines arbeitsrechtlichen Auskunftsanspruchs ist umstritten. Insbesondere in der Rechtsprechung wird vertreten, dass er als Nebenpflicht zum Arbeitsvertrag § 242 BGB entspringt (so BAG, Urt. v. 07.09.1995, 8 AZR 828/93, BAGE 81, 15; LAG Hamm, Urt. v. 03.03.2009, 14 Sa 1689/08, CCZ 2010, 237, 238; ArbG Saarlouis, Urt. v. 19.10.1983, 1 Ca 493/83, ZIP 1984, 364; wohl auch *Lützler/Müller-Sartori*, CCZ 2011, 19, 19f.), während die Literatur den Anspruch oftmals auf §§ 666, 675 BGB stützt (*Dann/Schmidt*, NJW 2009, 1851, 1852f. Mit Differenzierung, zwischen dem unmittelbaren und mittelbaren Arbeitsbereich des Arbeitnehmers; ebenso *Spehl/Momsen/Grützner*, CCZ 2014, 170, 171).

[17] *Fischer* in: Bamberger/Roth/Hau/Poseck (Hrsg.), Beck'scher Onlinekommentar BGB, 53. Ed., 2020, §666, Rn.5; BGH, Urt. v. 16.6.2016, III ZR 282/14, Rn. 37, NJW-RR 2016, 1391, 1394.

[18] *Fischer* in: Bamberger/Roth/Hau/Poseck (Hrsg.), Beck'scher Onlinekommentar BGB, 53. Ed., 2020, §666, Rn.3; *Schäfer* in: Münchener Kommentar zum BGB, 8. Aufl., 2020, §666, Rn. 22.

[19] *Preis* in: Erfurter Kommentar zum Arbeitsrecht, 20. Aufl., 2020, § 611a BGB, Rn. 736; *Spinner* in: Münchener Kommentar zum BGB, 8. Aufl., 2020, §611a, Rn. 993, 1030; *Joussen* in: Beck'scher Onlinekommentar Arbeitsrecht, 54. Ed., 2019, §611a BGB, Rn.446; *Reichold* in: Münchener Handbuch zum Arbeitsrecht, Band I, 4. Aufl., 2018, §55, Rn. 4, 8.

[20] *Joussen* in: Beck'scher Onlinekommentar Arbeitsrecht, 54. Ed., 2019, §611a BGB, Rn.446.

[21] *Joussen* in: Beck'scher Onlinekommentar Arbeitsrecht, 54. Ed., 2019, §611a BGB, Rn.446; *Preis* in: Erfurter Kommentar zum Arbeitsrecht, 20. Aufl., 2020, § 611a BGB, Rn. 742.

Weg zur Erfüllung der ebenfalls den Arbeitnehmer treffenden Schadensminderungspflicht[22] gegenüber dem Arbeitgeber dar.[23]

1.3 Arbeitsrechtliche Konsequenzen der Meldung von IT-Sicherheits- und Datenschutzvorfällen vor dem Hintergrund der Selbstbelastungsfreiheit

Sofern ein IT-Sicherheitsvorfall auf eine Pflichtverletzung, z.B. die Nicht-Einhaltung einer Security Policy, durch einen Arbeitnehmer zurückgeht, kann ihm ein Fehlverhalten vorgeworfen werden, das arbeitsrechtliche Konsequenzen nach sich ziehen kann. Beispiele hierfür können z.B. in der Interaktion mit Phishing-E-Mails, der unbefugten (ggf. zunächst unbewussten) Weitergabe von Daten an Unbefugte, dem (längerem) Unterlassen von Updates oder der Nicht-Nutzung vorgeschriebener Sicherheitsmaßnahmen gesehen werden. Während besonders schwere Verstöße eine ordentliche oder gar fristlose Kündigung[24] zur Folge haben können, wird gerade bei einmaligen oder nur leicht fahrlässig begangenen Sicherheitsverletzungen durch Mitarbeiter aber nur eine Abmahnung in Betracht kommen.[25]

Indem der Arbeitnehmer in diesen Fällen die verschuldete Verletzung meldet, liefert er dem Arbeitgeber zugleich die Grundlage für arbeitsrechtliche Maßnahmen gegen ihn selbst. Dieser Umstand könnte im Widerspruch zur Selbstbelastungsfreiheit gemäß dem nemotentur-Grundsatz stehen, der verfassungsrechtlich aus dem Grundrecht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG oder ergänzend aus dem Recht auf ein faires und rechtsstaatliches Verfahren nach Art. 20 Abs. 3 GG bzw. Art. 6 Abs. 1 EMRK abgeleitet wird.[26] Er ist zudem sowohl in Art. 48 Abs. 2 der Charta der Grundrechte der Europäischen Union als auch in Art. 6 Abs. 3 EMRK als Verteidigungsrecht vorgesehen.[27]

Die Selbstbelastungsfreiheit schützt nach herrschender Ansicht nur vor staatlich veranlasstem Aussagezwang in staatlichen Verfahren, insbesondere Straf- und Ordnungsverfahren.[28] Die vom Bundesverfassungsgericht aufgestellten Grundsätze zum Schutz gegen Selbstbezichtigung und daraus resultierende strafrechtliche Konsequenzen beschränken sich aber

[22] *Preis* in: Erfurter Kommentar zum Arbeitsrecht, 20. Aufl., 2020, § 611a BGB, Rn. 744ff.; *Spinner* in Münchener Kommentar zum BGB, 8. Aufl., 2020, §611a, Rn. 1001; BAG, Urt.v. 01.06.1995, 6 AZR 912/94, NZA 1996, 135, 136.

[23] Vgl. auch *Joussen* in: Beck'scher Onlinekommentar Arbeitsrecht, 54. Ed., 2019, §611a BGB, Rn.446; *Reichold* in: Münchener Handbuch zum Arbeitsrecht, Band I, 4. Aufl., 2018, §55, Rn. 8.

[24] Vgl. nur ArbG Siegburg, Urt. v. 15.01.2020, 3 Ca 1793/19.

[25] *Fuhlrott*, NZA 2019, 649, 650, 652f.; *Niemann* in: Erfurter Kommentar, 20. Aufl, 2020, §626 BGB, Rn. 29f.

[26] BVerfG, Beschl. v. 13.01.1981, 1 BvR 116/77, Rn. 18, NJW 1981, 1431, 1432; BVerfGE 38, 105, 113; BGHSt 14, 358, 264, BGH, NJW 1989, 1228, 1229; EGMR, NJW 2002, 499, 501.

[27] EuGH, Urt. v. 07.01.2004, C-204/00 (Alborg), Slg. 2004,I-123, Rn.64f.; Urt.v.25.10.2001, Slg. 2002, I-8275, Rn. 273f.;*Jarass*, Charta der Grundrechte der EU, 3. Aufl., 2016, Art. 48, Rn. 31; EGMR, Urt. v. 08.04.2004, 38544/97, Rn. 46, JR 2005, 423.

[28] BVerfG,Beschl. v. 13.01.1981, 1 BvR 116/77, Rn. 18f., NJW 1981, 1431, 1432; *Wessing* in: Hauschka/Moosmeyer/Lösler, Corporate Compliance, 3. Aufl., 2016, §46, Rn. 50; *Schaefer*, NJW-Spezial, 2010, 120.

nicht auf diese Verfahren.[29] Sie entfalten nach Ansicht der herrschenden Meinung jedoch keine Wirkung gegenüber dem Arbeitgeber, da hier kein staatlicher Aussagezwang gegeben sei.[30] Zur Begründung hierfür wird angeführt, dass es dem Arbeitnehmer frei stehe, sich zu äußern, sodass er im Fall einer Äußerung auch mit deren Konsequenzen leben müsse.[31] Dieser Argumentation ist vor dem Hintergrund der Annahme einer arbeitsvertraglichen Benachrichtigungspflicht jedoch nicht zuzustimmen. Wenn eine solche Pflicht besteht und sanktioniert werden kann, steht dem Arbeitnehmer eine Äußerung gerade nicht frei. In Bezug auf etwaige strafrechtliche Konsequenzen einer Mitteilung an den Arbeitgeber ist daher der in der Literatur vertreten Ansicht zuzustimmen, dass die vom Verfassungsgericht in der Gemeinschuldnerentscheidung aufgestellten Grundsätze[32] auch auf Äußerungen gegenüber dem Arbeitgeber übertragen werden müssen[33]. Für sie gilt daher ein strafrechtliches Verwertungsverbot.

Auf die im vorliegenden Beitrag untersuchte Mitteilungspflicht gegenüber dem Arbeitgeber und die aus ihr für den Arbeitnehmer resultierenden arbeitsrechtlichen Konsequenzen hat das jedoch keinen Einfluss. Da der nemo-tenetur-Grundsatz nur in staatlichen Verfahren und gegenüber staatlichen Organen, insbesondere mit Bezug zum Strafrecht gilt, ist er auf das privatrechtliche Verhältnis zwischen Arbeitnehmer und -geber nicht direkt anwendbar.[34] In der Situation muss zwar eine Abwägung zwischen einem berechtigten, billigens- und schützenswerten Interesse des Arbeitgebers auf Information und dem Interesse des Arbeitnehmers vorgenommen werden, ein Fehlverhalten nicht zuzugeben und sich nichts selbst belasten zu müssen.[35] Eine Benachrichtigungspflicht im Zusammenhang mit Datenschutz- und IT-Sicherheitsverstößen wird dabei im Ergebnis jedoch regelmäßig zu bejahen sein. Für sie streiten sowohl die Schäden, die dem Arbeitgeber ohne die Erfüllung der Informationspflicht drohen, als auch die datenschutzrechtliche Pflicht zur Meldung von Sicherheitsverstößen, mit der auch die Interessen der Datenobjekte gewahrt werden. Auch die meist schuldhafte Verursachung eines Verstoßes durch den Arbeitnehmer spricht eher für die Annahme einer Mitteilungspflicht. Gegen sie können lediglich die im Vergleich dazu weniger gravierenden arbeitsrechtlichen Konsequenzen für den Arbeitnehmer ins Feld geführt werden.

[29] BVerfG, Beschl. v. 13.01.1981, 1 BvR 116/77, Rn. 19, NJW 1981, 1431; *Wessing* in: Hauschka/Moosmeyer/Lösler, Corporate Compliance, 3. Aufl., 2016, §46, Rn. 50.

[30] OLG Karlsruhe, Beschl. v. 06.09.1988, 1 Ss 68/88, NStZ 1989, 287, 288; *Wessing* in: Hauschka/Moosmeyer/Lösler, Corporate Compliance, 3. Aufl., 2016, §46, Rn. 50; *Bittmann/Molkenbur*, wistra 2009, 68.

[31] OLG Karlsruhe, Beschl. v. 06.09.1988, 1 Ss 68/88, NStZ 1989, 287, 288. Anders im Fall des Gemeinschuldners, der nach der zum Zeitpunkt der Gemeinschuldnerentscheidung des Verfassungsgerichts geltenden Rechtslage gemäß § 100 KO zur Auskunft verpflichtet war: BVerfG, Beschl. v. 13.01.1981, 1 BvR 116/77, Rn. 26 f., NJW 1981, 1431.

[32] BVerfG, Beschl. v. 13.01.1981, 1 BvR 116/77, Rn. 26 f., NJW 1981, 1431, 1432.

[33] *Wessing* in: Hauschka/Moosmeyer/Lösler, Corporate Compliance, 3. Aufl., 2016, §46, Rn. 50, 56; *Schrader/Thoms/Mahler*, NZA 2018, 965, 969; *Dann/Schmidt*, NJW 2009, 1851; 1855; LAG Hamm, Urt. v. 03.03.2009, 14 Sa 1689/08, CCZ 2010, 237.

[34] *Spehl/Momsen/Grützner*, CCZ 2014, 170, 171; *Dann/Schmidt*, NJW 2009, 1851, 1855; *Lützeler/Müller-Satori*, CCz 2001, 19, 20.

[35] Vgl. *Dann/Schmidt*, NJW 2009, 1851, 1853; *Spehl/Momsen/Grützner*, CCZ 2014, 170, 171.

Nach aktueller Rechtslage ist daher davon auszugehen, dass die arbeitsrechtliche Sanktionierung des Fehlverhaltens eines Arbeitnehmers rechtmäßig wäre, selbst wenn das Fehlverhalten nur aufgrund seiner selbstbelastenden Mitteilung vom Arbeitgeber erkannt werden konnte. Nur einer strafrechtlichen Verwertung der Meldung steht ein von der Rechtsprechung entwickeltes Verbot entgegen. Darüber hinaus kann angesichts des Bestehens der arbeitsrechtlichen Nebenpflicht zur Benachrichtigung und Schadensabwendung auch das Unterlassen der Meldung eines Verstoßes durch den Arbeitnehmer vom Arbeitgeber arbeitsrechtlich sanktioniert werden.[36] Je nach Schwere eines solchen Verstoßes gegen die Mitteilungspflicht kommen zur Sanktionierung der Nichtmeldung durch den Arbeitnehmer ebenfalls gestufte Maßnahmen von der Abmahnung bis zur fristlosen Kündigung in Betracht.[37] Die Beweislast für den Nachweis eines Fehlverhaltens, dessen Schwere und die Rechtmäßigkeit der darauf basierenden Sanktionen des Arbeitnehmers trifft den Arbeitgeber.[38] In Fällen des Unterlassens der Meldung eines IT-Sicherheitsverstoßes hat er nachzuweisen, dass dem Arbeitnehmer ein meldepflichtiger Vorfall bekannt war oder im Rahmen einer ordnungsgemäßen Aufgabenerfüllung hätte bekannt sein müssen und er ihn pflichtwidrig nicht mitgeteilt hat.[39] Sofern ein Arbeitnehmer einen IT-Sicherheitsvorfall meldet und der Arbeitgeber ihn deshalb aufgrund eines vermuteten Fehlverhaltens sanktionieren möchte, muss er demnach aber auch nachweisen können, dass der IT-Sicherheitsvorfall tatsächlich auf einem Fehlverhalten des Arbeitnehmers, z.B. in Bezug auf die Security Policies, beruht. Das Erfüllen dieser Beweispflicht ist angesichts der vielfältigen Quellen für diese Verstöße und der damit uneindeutigen Beweislage nicht immer einfach oder überhaupt möglich. Dies zeigen auch die folgenden Beispiele.

2 Beispielhafte IT-Sicherheits- bzw. Datenschutzvorfälle und die Problematik der Beweislage

Es gibt Datenschutz- und IT-Sicherheitsrechtsvorfälle, die sich eindeutig einem konkreten Verhalten des Arbeitnehmers zuordnen lassen, und andere bei denen das weniger einfach möglich ist. Hier beispielhafte Fälle:

Fall 1: Ein Arbeitnehmer meldet, dass das Passwort seines Accounts für das Unternehmen bzw. die Institution in einer veröffentlichten Datenbank, wie der des Hasso-Plattner-Instituts[40], enthalten ist. Dies kann viele Ursachen haben. So ist die Passwortspeicherung

[36] Vgl. nur *Preis* in: Erfurter Kommentar, 20. Aufl., 2020, §611a, Rn. 748.

[37] *Preis* in: Erfurter Kommentar, 20. Aufl., 2020, §611a, Rn. 748.

[38] BAG, Urt. v. 11.03.1987, 5 AZR 739/85, NZA 1987, 452; Urt. v. 13.03.1987, 7 AZR 601/85, NZA 1987, 518, LAG M-V., Urt. v. 11.02.2020, 2 Sa 133/19, Rn. 36 ff.; LAG Köln, Urt. v. 17.01.2007, 7 Sa 526/06, I. 2. e) bb) aaa); *Schmidt* in: Küttner (Hrsg.), Personalbuch 2020, 27. Aufl., 2020, Stichwort Abmahnung, Rn. 42; *Weizenegger* in: Bredemeier/Neffke, TVöD/TV-L, 5. Aufl., 2017, Vorb. §34 TVöD, Rn. 641f.; *Niemann* in: Erfurter Kommentar, 20. Aufl., 2020, §626, Rn. 234.

[39] Vgl. *Joussen* in: Beck'scher Onlinekommentar Arbeitsrecht, 54. Ed., 2019, §611a BGB, Rn. 446; *Preis* in: Erfurter Kommentar, 20. Aufl., 2020, §611a, Rn. 736.

[40] https://sec.hpi.de/ilc/search?lang=de.

beim Arbeitgeber möglicherweise nicht sicher erfolgt oder der Arbeitnehmer das hat das gleiche Passwort auch für andere Accounts genutzt, bei denen es nicht sicher gespeichert wurde. Auch ist es möglich, dass der Arbeitnehmer auf eine Phishing-Nachricht, die unterschiedlich einfach oder schwer zu erkennen ist, reingefallen ist oder ihm jemand bei der Eingabe des Passworts am Laptop in der Bahn über die Schulter geschaut hat.

Fall 2: Ein Arbeitnehmer meldet, dass ein USB-Stick, auf dem personenbezogene Daten unverschlüsselt gespeichert werden, verloren gegangen ist. Auch hier kommen verschiedene Ursachen in Betracht. Der USB-Stick kann zum Beispiel gestohlen worden sein, während man in ein Gespräch verwickelt wurde (Teil eines Social Engineering Angriffs und dadurch schwer zu verhindern), oder er wurde im Café auf dem Weg zum Vorgesetzen, der um diese Daten gebeten hat, vergessen.

In diesem Zusammenhang ist ebenfalls darauf hinzuweisen, dass einige Ursachen zwar theoretisch als Fehlverhalten des Arbeitnehmers interpretiert werden könnten, sich im Einzelfall aber die Frage stellt, ob der Arbeitgeber seine Arbeitnehmer für das entsprechende Fehlverhalten ausreichend sensibilisiert hat. Hätte der Arbeitnehmer es also besser wissen können und standen ihm die erforderlichen Tools zur Verfügung? Oftmals reicht zum Beispiel die bloße Aufforderung zur Löschung von Phishing-E-Mails nicht aus, da nicht verlangt werden kann, jede dieser Mails zu erkennen (insbesondere wenn entsprechende Schulung nicht angeboten werden). Außerdem kann in der Regel nicht erwartet werden, dass alle Arbeitnehmer in der Lage sind, sich selbst mit einer Verschlüsselungssoftware vertraut zu machen, um Daten auf dem USB-Stick verschlüsselt zu speichern.

3 Vorschlag für Begrenzung des Verantwortungsmaßstabs zur Stärkung der IT-Sicherheit und des Datenschutzes

Die drohenden arbeitsrechtlichen Konsequenzen der Meldung eines IT-Sicherheitsverstoßes können dazu führen, dass der Arbeitnehmer entgegen seiner Verpflichtung einen solchen Vorfall nicht meldet, versucht, ihn zu verschleiern, oder so weit aufzuschieben, dass er seinem Fehlverhalten nicht mehr zugeordnet werden kann. Dies gilt umso mehr als auch die Nichtmeldung eines Vorfalls einen sanktionsfähigen Verstoß gegen seine arbeitsrechtlichen Pflichten darstellt. Die praktische Folge dieses Vorgehens des Arbeitnehmers ist, dass der Sicherheitsvorfall nicht in seinen Anfängen bekämpft und eingegrenzt werden kann und sich immer weiter ausbreitet. Dem Arbeitgeber und dem Datenschutz ist damit nicht geholfen - im Gegenteil. Auch, wenn er den Mitarbeiter bei so einem Fehlverhalten strenger sanktionieren kann, eine Verhinderung oder zumindest Verminderung des Schadens wäre für ihn wünschenswerter.

Um dieses Ziels mittels einer verbesserten Meldemoral von Sicherheitsvorfällen erreichen zu können, erscheinen verschiedene Maßnahmen denkbar. Zunächst könnte in Unternehmen ein Meldesystem etabliert werden, dass eine pseudonymisierte oder anonymisierte Meldung von Schutzverletzungen erlaubt. Arbeitnehmer könnten den zuständigen Stellen im Betrieb

Vorfälle auf diese Weise zur Kenntnis bringen, ohne sich namentlich dazu bekennen zu müssen und direkte arbeitsrechtliche Konsequenzen befürchten zu müssen. Ein solches Meldesystem wird inzwischen auch in vielen Unternehmen zum Schutz von Whistleblowern bei der Bekämpfung von firmeninternen Missständen angewandt.[41] Die Mitarbeiter müssten der Anonymität eines solchen Meldesystem jedoch unbedingt vertrauen, da sie bei Bekanntwerden ihrer Identität auch weiterhin mit arbeitsrechtlichen Konsequenzen rechnen müssten. Insofern wäre eine anonyme Meldung auch nur bei Verstößen sinnvoll, die nicht von ohnehin einer Person zugeordnet werden können. Für ein pseudonymes Meldesystem gelten diese Einschränkungen umso mehr, als dort die Daten des Arbeitnehmers, wenn auch nicht direkt, weiterhin zuordenbar wären. Darüber hinaus erscheint fraglich, ob es überhaupt wünschenswert ist, einen Arbeitnehmer vollständig von der Pflicht zu entbinden, sich zu einem Fehlverhalten bekennen zu müssen. Sofern ein Verstoß, z.B. gegen Security Policies, keine Konsequenzen für ihn hat, weil er ihm nicht zugeordnet werden kann, existiert auch kein Anreiz, sich an die bestehenden Regelungen zu halten. Für das Ziel einer Verbesserung des Datenschutzes und der IT-Sicherheit wäre das sogar kontraproduktiv.

Dasselbe Argument ließe sich auch für die Einführung einer Bagatellgrenze bei Sicherheitsverstößen anführen. Sofern man kleine Verstöße gegen die Schutzvorschriften generell nicht ahnden würde, bestünde kein Anreiz, ein solches Fehlverhalten zu vermeiden. Es kommt in diesem Zusammenhang hinzu, dass die Schwere der Auswirkungen eines Verstoßes gegen IT-Sicherheits- oder Datenschutzregeln sich oftmals erst im Nachhinein offenbaren. Dieselbe Bagatellhandlung, wie ein Klick auf den Anhang einer Mail eines unbekannten Absenders, kann entweder vom Virenschutzprogramm aufgehalten werden oder die Systeme eines ganzen Betriebes lahmlegen. Ob eine Sanktionierung erfolgen würde, wäre beim Vorliegen einer Bagatellgrenze damit vom Zufall abhängig.

Zur besseren Durchsetzung der Meldepflicht, der effektiveren und effizienteren Bekämpfung von Sicherheitsvorfällen sowie zur Stärkung des Datenschutzes und der IT-Sicherheit sollte daher eine teilweise Abkehr vom Gedanken der arbeitsrechtlichen Sanktion erwogen werden. Ein Ansatzpunkt wäre hierbei die Übertragung der Grundsätze der Arbeitnehmerhaftung auf die arbeitsrechtlichen Sanktionen eines vom Arbeitnehmer verursachten und gemeldeten Sicherheitsverstoßes.

Nach den von der Rechtsprechung entwickelten Grundsätzen des innerbetrieblichen Schadensausgleichs haftet der Arbeitnehmer bei betrieblich veranlassten Schäden nur bei Vorsatz und grober Fahrlässigkeit in vollem Umfang, bei mittlerer Fahrlässigkeit nur anteilig und bei leichtester Fahrlässigkeit gar nicht.[42] Dies gilt im Übrigen auch für Schäden, die dem Arbeitgeber oder Dritten durch IT-Sicherheitsvorfälle entstehen, die ein Arbeitnehmer schuldhaft verursacht hat.

Dem Grundgedanken des Schadensausgleichs folgenden sollte in Fällen, in denen Verstöße auf fahrlässiges oder leicht fahrlässiges Verhalten des Arbeitnehmers zurückzuführen sind, auf arbeitsrechtliche Sanktionen gegenüber dem verursachenden Arbeitnehmer in Form von Abmahnungen oder Kündigungen verzichtet werden. Anders als bei der Haftungsverteilung

[41] Vgl. nur: *Steffen/Stöhr*, RdA 2017, 43, 48.

[42] *Koch* in: Schaub/Koch, Arbeitsrecht von A-Z, 24. Auflage, 2020, Stichwort Haftung des Arbeitnehmers; *Wagner*, Münchener Kommentar zum BGB, 7. Aufl., 2017, § 823, Rn. 128.

wäre die Begründung dafür nicht die Kontrolle der innerbetrieblichen Anstrengungen zur Schadensprävention durch den Arbeitgeber.[43] Vielmehr würde er von der Verlässlichkeit rechtzeitiger Meldungen von IT-Sicherheitsverstößen durch Mitarbeiter und die damit einhergehenden Schadensminimierungen profitieren. Außerdem würde der Datenschutz und die IT-Sicherheit insgesamt wesentlich gestärkt, da der teilweise Verzicht auf Sanktionen die „Meldemoral" verbessern würde. Die Meldung würde dann nämlich nicht mehr durch Bedenken vor arbeitsrechtlichen Konsequenzen behindert. Zudem erführe die pflichtgemäße Meldung eines Vorfalls gegenüber einer Nichtmeldung eine Privilegierung, da ein Unterlassen der Meldung von Verstößen fast immer strengere Sanktionen nach sich ziehen würde als eine ordnungsgemäße Erfüllung der Meldepflicht.

Es kommt hinzu, dass dem Arbeitgeber der Nachweis eines Fehlverhaltens des Arbeitnehmers gerade in Fällen nur schwer möglich sein wird, in denen ein Verstoß auf nur leicht fahrlässigem oder fahrlässigem Verhalten beruht. Die Sanktionierung des Arbeitnehmers ist in diesen Situationen somit häufig mit der rechtlichen Unsicherheit einer gerichtsfesten Beweisbarkeit behaftet und somit angreifbar. Das Interesse des Arbeitgebers an einer solchen unsicheren Sanktionierung ist daher auch gering. Zugleich bestünde durch den Sanktionsverzicht in Fällen von leichter und normaler Fahrlässigkeit nicht die Gefahr, dass eine arbeitsrechtliche Sanktionierung von insbesondere wiederholtem oder gleichgelagertem Fehlverhalten ausgeschlossen würde. Auch bei Zugrundelegen eines objektiven zivilrechtlichen Sorgfaltsmaßstabs[44] erfordert der Vorwurf grober Fahrlässigkeit regelmäßig eine subjektive, das normale Maß übersteigende Vorwerfbarkeit des Fehlers.[45] Dies kann gerade bei der Wiederholung einer schon begangenen Pflichtverletzung regelmäßig angenommen werden. Zuletzt spricht auch die Existenz des Verwertungsverbots in den §§ 42 Abs. 4, 43 Abs. 4 BDSG für Meldungen und Benachrichtigungen von Datenverarbeitern in Ordnungswidrigkeiten- und Strafverfahren für eine Bevorzugung von Arbeitnehmern, die Datenschutz- und IT-Sicherheitsverstöße in Betrieben an ihre Arbeitgeber melden. Durch die vorgeschlagene Privilegierung werden nämlich die Folgen der Unanwendbarkeit des Selbstbelastungsverbots auf arbeitsrechtliche Mitteilungspflichten abgemildert. Außerdem käme es zu einer Angleichung der Sanktionen für Arbeitnehmer und Unternehmen. Denn ebenso wie Unternehmen aufgrund des Verwertungsverbots im BDSG keine strafrechtlichen Konsequenzen drohen, wenn sie der ihnen auferlegten Meldepflicht nachkommen, müsste Arbeitnehmer bei Einhaltung der Meldepflicht in Fällen mit geringem Verschuldensvorwurf dann keine arbeitsrechtlichen Folgen befürchten.

Gegenüber den zuvor erwogenen Alternativen eines anonymisierten Meldesystems oder einer Bagatellgrenze bietet der teilweise Sanktionsverzicht einerseits den Vorteil, dass am Verschulden und damit der objektiven Vorwerfbarkeit eines Fehlverhaltens angeknüpft wird. Andererseits setzt er am Grundproblem der Arbeitnehmer an, nämlich deren Angst vor

[43] *Wagner*, Münchener Kommentar zum BGB, 7. Aufl., 2017, § 823, Rn. 128.

[44] Vgl. nur: BVerfG, Beschl. v. 07.05. 1996, 1 BvQ 4/96, NJW-RR 1996, 980; BGH, Urt.v.17.03.1981, VI ZR 191/79, NJW 1981, 1603, 1604; BGH, Urt. v. 13.02.2001, VI ZR 34/00, NJW 2001, 1786,1787; *Lorenz* in: Beck'scher Onlinekommentar BGB, 53. Ed., 2020, §276 BGB, Rn. 20; *Grundmann*, Münchener Kommentar zum BGB, 8. Aufl., 2019, § 276, Rn. 55f.; *Schulze* in: NK-BGB, 10. Aufl., 2019, §276, Rn. 13.

[45] BGH, Urt.v. 11.05.1953, IV ZR 170/52, NJW 1953, 1139; BGH, Urt. v. 17.06.1992, XII ZR 119/91, NJW 1992, 2418; *Grundmann*, Münchener Kommentar zum BGB, 8. Aufl., 2019, § 276, Rn. 55f.

arbeitsrechtlichen Konsequenzen, ohne sie aus ihrer grundsätzlichen Verantwortung für die Einhaltung der Sicherheitsregeln zu entlassen. Insoweit löst der Vorschlag das Problem auf der Basis einer Abwägung zwischen den Interessen und betrieblichen Anforderungen der Arbeitgeberseite, den problemauslösenden Bedenken der Arbeitnehmer und dem Ziel einer Verbesserung des Datenschutzes und der IT-Sicherheit.

4 Fazit

Die Meldepflicht von IT-Sicherheits- oder Datenschutzverstößen ist eine der zentralen organisatorischen Institutionen zum Schutz der IT-Infrastruktur von Unternehmen. Die auf ihr basierenden Maßnahmen, insbesondere in Form früher und effektiver Reaktionen auf Angriffe, können ihre Wirkung jedoch nur entfalten, wenn die Meldepflicht eine hohe Akzeptanz innerhalb eines Unternehmens genießt und in der Praxis auch tatsächlich umgesetzt wird. Drohende arbeitsrechtliche Sanktionen aufgrund eines zusammen mit einer Meldung offengelegten eigenen Fehlverhaltens können der bereitwilligen Wahrnehmung dieser Pflicht entgegenstehen. Mitarbeiter, die der Meldepflicht dennoch nachkommen, erfahren dabei keinen Schutz durch ein Verwertungsverbot oder die Anwendung der Selbstbelastungsfreiheit. Sie erwartet in Form einer Abmahnung oder Kündigung vielmehr theoretisch dieselbe arbeitsrechtliche Sanktion wie ihre Kollegen, die eine Meldung unterlassen.
Zur Stärkung der Durchsetzung einer Meldepflicht und damit einhergehend des Datenschutzes und der IT-Sicherheit in Unternehmen sollte erwogen werden, arbeitsrechtliche Sanktionen gegen Mitarbeiter auszusetzen, die mit einer Meldung gegebenenfalls eigenes leicht fahrlässiges oder fahrlässiges Verhalten offenbaren. Hierdurch könnten Arbeitnehmer die Meldepflicht ohne Sorge vor persönlichen Konsequenzen wahrnehmen, was sich positiv auf die Akzeptanz der Maßnahme auswirken würde und das Unternehmen vor schwerwiegenden Konsequenzen bewahrt, die aus unentdeckten Angriffen auf ihre IT-Infrastruktur entstehen können. Für zukünftige Arbeiten bleibt an dieser Stelle jedoch offen, wie den Arbeitnehmern die Unterscheidung zwischen (leicht) fahrlässigem und grob fahrlässigem Verhalten erklärt werden kann, damit die Akzeptanz und Ausübung der Meldepflicht tatsächlich steigen. Ebenso muss weiter untersucht werden, wie der Arbeitgeber die Arbeitnehmer ausreichend aufklären und ihnen dadurch ein ausreichendes Bewusstsein für entsprechenden Fehlverhaltens ermöglichen kann.