Betrachtung möglicher arbeitsrechtlicher Konsequenzen

Dirk Müllmann / Melanie Volkamer

■ Die Pflicht zur Meldung von IT-Sicherheits- und Datenschutzvorfällen in Unternehmen ist eine zentrale organisatorische Maßnahme zum Schutz von deren IT-Infrastruktur und zur Umsetzung von Datenschutzvorgaben. Mitarbeiter offenbaren mit der Meldung des Vorfalls jedoch oftmals eigenes Fehlverhalten. Die Angst vor Konsequenzen kann Arbeitnehmer davon abhalten, der Meldepflicht nachzukommen. Das hat wiederum negative Konsequenzen für das Unternehmen selbst, dem es nicht möglich ist, schnell auf Vorfälle zu reagieren und sie effektiv einzudämmen. Der Beitrag untersucht vor dem Hintergrund der Meldepflichten für Datenschutzverstöße die rechtlichen Grundlagen der Mitteilungspflichten von Mitarbeitern. Er geht ferner auf die Frage der Einschlägigkeit des Selbstbelastungsverbots im Kontext des Arbeitsrechts ein und analysiert die arbeitsrechtlichen Konsequenzen der Offenbarung von Fehlverhalten durch die 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.

Lesedauer: 18 Minuten

■ The obligation to report IT security and data protection cases in companies is a central organizational measure to protect their IT infrastructure and to implement data protection requirements. However, upon notification of an occurrence, employees often disclose their own wrongdoing, which is often used by the employer as a basis for labor law consequences and thus can be used against them. The fear of these consequences can keep employees from fulfilling the notification requirements. This, in turn, has negative consequences for the company itself, which cannot quickly respond to occurrences and effectively curtail them. In view of the obligation of notification regarding data protection violations, this article will investigate the legal bases of the employees' obligation to notify. Furthermore, it will cover the issue of the relevance of the privilege against self-incrimination in the context of labor law and analyzes the labor law consequences of disclosing wrongdoing by fulfilling the obligation to notify. On this basis, it will develop a recommendation on how to improve the reliability of notifications of IT security and data protection occurrences by employees.

Müllmann/Volkamer: Meldepflicht von Mitarbeitenden bei IT-Sicherheits- und Datenschutzvorfällen

I. Einleitung

Ein adäquater Schutz der IT-Infrastruktur vor Cyberangriffen eines jeden Unternehmens ist nur durch eine Kombination aus organisatorischen und technischen Maßnahmen möglich. Organisatorische Maßnahmen beinhalten in der Regel auch Security-Policies[1] und Sensibilisierungsmaßnahmen. Sie legen fest, wie Mitarbeitende Risiken erkennen, sich idealerweise verhalten und an wen Vorfälle zu melden sind. Eine wichtige Komponente der organisatorischen Maßnahme ist das Melden von IT-

Sicherheits- und Datenschutzvorfällen.[2] Eine Pflicht ergibt sich jedoch auch bereits aus dem Pflichtenkanon des Arbeitsverhältnisses selbst.[3]

Die Meldepflicht ist aus einer Reihe von Gründen eine wichtige Komponente der organisatorischen Maßnahmen:[4] So sind Cyberangriffe immer schwerer zu erkennen. Außerdem kann es selbst bei einer idealen Kombination von organisatorischen und technischen Maßnahmen[5] und bei für das Thema Sicherheit und Datenschutz hoch sensibilisierten Mitarbeitenden trotzdem zu IT-Sicherheitsvorfällen kommen.[6] Das zeitnahe Melden von IT-Sicherheitsvorfällen ist zudem 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. Verantwortliche und Experten können so technische und organisatorische Schutzmaßnahmen ergreifen. Im Fall eines Datenschutzvorfalls gibt es zudem gesetzliche Vorgaben, die von den Unternehmen eine Meldung innerhalb vorgegebener Fristen verlangen. So sieht Art. 33 Abs. 1 S. 1 DS-GVO z.B. eine Meldung binnen 72 Stunden an die gem. Art. 55 DS-GVO zuständige Aufsichtsbehörde vor. Eine vergleichbare Pflicht existiert gem. § 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, dass sie wissen, was ein IT-Sicherheits- bzw. Datenschutzvorfall ist und dass es wichtig ist, ihn zu melden, um den Schaden für das Unternehmen so gering wie möglich zu halten.[7] Dennoch wird nicht zwangsläufig jeder IT-Sicherheitsvorfall gemeldet werden, denn Mitarbeitende müssen sich mit dem Melden in der Regel einen Fehler eingestehen und ggf. zugeben, dass sie sich nicht an die Security-Policies gehalten haben. Insbesondere Mitarbeitende, die Angst vor persönlichen oder rechtlichen Konsequenzen haben, werden Vorfälle daher weniger zuverlässig melden. Eine wesentliche Rolle spielt hierbei die allgemeine Fehlerkultur im Unternehmen.[8]

Im Vordergrund der vorliegenden Untersuchung steht die Analyse der persönlichen arbeitsrechtlichen Konsequenzen im Zusammenhang mit der Wahrnehmung von Meldepflichten. Ziel dieses Beitrags ist es, einen Vorschlag zu erarbeiten, wie arbeitsrechtlich mit Vorfällen umgegangen werden könnte, um möglichst wenige Mitarbeitende davon abzuhalten, Vorfälle zu melden, und gleichzeitig Mitarbeiter zu motivieren sich möglichst an die Security-Policies zu halten. Dazu wird zunächst die rechtliche Ausgangslage analysiert.

II. Rechtliche Ausgangslage

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 an Behörden je nach Anwendungsfall und Regelungsgebiet. Die Meldepflicht in der darunterliegenden Ebene, also im 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 von Art. 33 DS-GVO dargestellt werden. Auf die in anderen Bereichen ebenfalls bestehenden unternehmerischen Meldepflichten, wie z.B. bei IT-Sicherheitsverstößen kritischer Infrastrukturen, sei an dieser Stelle jedoch ausdrücklich verwiesen.

1. Gesetzliche Meldepflichten an Aufsichtsbehörden

Um die Informationslage der Aufsichtsbehörden zu verbessern, geeignete Maßnahmen zum Schutz der Betroffenen einzuleiten sowie die Rechtsdurchsetzung und -befolgung datenschutzrechtlicher Normen zu steigern,[9] verlangt die DS-GVO die Meldung der Verletzung des Schutzes von personenbezogenen Daten i.S.d. Art. 4 Nr. 12 DS-GVO an die Aufsichtsbehörde. Art. 33 Abs. 1 S. 1 DS-GVO sieht in diesen Fällen eine Meldung der Verletzung binnen – in der Regel – 72 Stunden an die gem. Art. 55 DS-GVO zuständige Aufsichtsbehörde vor.

Durch diese gesetzliche Verpflichtung sieht sich der Verarbeiter einer Situation ausgesetzt, in der er die Behörden ggf. 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 gem. Art. 83 Abs. 4 lit. a DS-GVO ebenfalls bußgeldbewehrt ist,[10] könnte die Verpflichtung des Verarbeiters, sich in einem Verfahren selbst zu belasten, dennoch im Konflikt mit dem Selbstbezichtigungsverbot des nemo tenetur-Grundsatzes stehen.[11] 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 sie in einem Verfahren nur mit Zustimmung des Verarbeiters verwendet werden dürfen. Die Europarechtskonformität dieser Regelung ist jedoch umstritten.[12] Damit die Unternehmen der Meldepflicht von Schutzverletzungen

personenbezogener Daten an die Aufsichtsbehörden nachkommen können, sind sie wiederum dringend auf die Mitwirkung ihrer Mitarbeitenden angewiesen. Hier stellt sich jedoch das o.g. Problem der Offenbarung eigenen Fehlverhaltens gegenüber dem Arbeitgeber. Eine dem Verwertungsverbot in §§ 42 Abs. 4, 43 Abs. 4 BDSG analoge Regelung für Mitarbeitende besteht im BDSG nicht. Es wird zwar i.R.d. Straf- und Bußgeldvorschriften eine analoge Erweiterung des Verwertungsverbots auf Personen, die für andere handeln, i.S.d. §§ 9, 14 OWiG erwogen.[13] Die Konsequenzen einer etwaigen Selbstbelastung von Arbeitnehmern durch die Meldung von Schutzverletzungen werden momentan aber weder in Straf- oder Bußgeldverfahren noch auf zivil- und arbeitsrechtlicher Ebene gesetzlich adressiert.

2. Arbeitsrechtliche Benachrichtigungspflicht

Arbeitnehmer treffen gegenüber ihren Arbeitgebern sowohl Auskunfts-[14] als auch Benachrichtigungspflichten. Beide unterscheiden sich dadurch, dass einem Auskunftsanspruch nur auf Anforderung nachgekommen werden muss,[15] während bei Benachrichtigungspflichten alle erforderlichen Informationen unaufgefordert mitzuteilen sind[16]. Die rechtliche Grundlage zur Herleitung einer nicht explizit vereinbarten arbeitsrechtlichen Benachrichtigungspflicht des Arbeitnehmers gegenüber seinem Arbeitgeber stellen die arbeitsvertraglichen Nebenpflichten dar.[17] Die Informationsbeschaffung des Arbeitgebers ist sowohl auf der Basis einer 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 Datenschutzvorfälle durch Mitarbeitende unaufgefordert wahrgenommen werden. Anders ist das Ziel, schnell auf Vorfälle reagieren zu können, nicht zu errei-

chen. Die Mitteilungspflicht des Arbeitnehmers kann in diesem Fall mit seiner Verantwortung begründet werden, das Integritätsinteresse seines Arbeitgebers zu wahren.[18] Daraus ergibt sich für ihn die Verpflichtung, im Vorfeld einer Schädigung zu handeln und drohende Störungen und Schäden an Betriebsmitteln zur Kenntnis zu bringen.[19] Die Annahme einer Benachrichtigungspflicht stellt in diesen Fällen ferner den einzigen Weg zur Erfüllung der ebenfalls den Arbeitnehmer treffenden Schadensminderungspflicht[20] gegenüber dem Arbeitgeber dar.[21]

3. Arbeitsrechtliche Konsequenzen vor dem Hintergrund der Selbstbelastungsfreiheit

Beispiele für Pflichtverletzungen, die möglicherweise arbeitsrechtliche Konsequenzen nach sich ziehen, können z.B. in der Interaktion mit Phishing-E-Mails, der unbefugten (ggf. zunächst unbewussten) Weitergabe von Daten an Unbefugte, dem (längeren) Unterlassen von Updates oder der Nicht-Nutzung vorgeschriebener Sicherheitsmaßnahmen gesehen werden. Während besonders schwere Verstöße eine ordentliche oder gar fristlose Kündigung[22] zur Folge haben können, wird gerade bei einmaligen oder nur leicht fahrlässig begangenen Sicherheitsverletzungen durch Mitarbeiter aber nur eine Abmahnung in Betracht kommen.[23]

Indem der Arbeitnehmer in diesen Fällen die verschuldete Verletzung meldet, liefert er dem Arbeitgeber zugleich die Grundlage für solche arbeitsrechtlichen Maßnahmen gegen ihn selbst. Dieser Umstand könnte im Widerspruch zur Selbstbelastungsfreiheit gemäß dem nemo tenetur-Grundsatz stehen, der verfassungsrechtlich aus dem Grundrecht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 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.[24] Er ist zudem sowohl in Art. 48 Abs. 2 GRCh als auch in Art. 6 Abs. 3 EMRK als Verteidigungsrecht vorgesehen.[25]

Die Selbstbelastungsfreiheit schützt nach h.A. nur vor staatlich veranlasstem Aussagezwang in staatlichen Verfahren, insbesondere Straf- und Ordnungsverfahren.[26] Die vom *BVerfG* aufgestellten Grundsätze zum Schutz gegen Selbstbezichtigung und daraus resultierende strafrechtliche Konsequenzen beschränken sich aber nicht auf diese Verfahren.[27] Sie entfalten nach Ansicht der h.M. jedoch keine Wirkung gegenüber dem Arbeitgeber, da hier kein staatlicher Aussagezwang gegeben sei.[28] Zur Begründung hierfür wird angeführt, dass es dem Arbeitnehmer frei stehe, sich zu äußern, sodass er im Fall einer Äußerung auch mit den Konsequenzen leben müsse.[29] 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 *BVerfG* in der Gemeinschuldnerentscheidung aufgestellten Grundsätze[30] auch auf Äußerungen gegenüber dem Arbeitgeber übertragen werden müssen[31]. Für sie gilt daher ein strafrechtliches Verwertungsverbot.

Auf die im vorliegenden Beitrag untersuchte Mitteilungspflicht gegenüber dem Arbeitgeber und die aus ihr für den Arbeitneh-

mer resultierenden arbeitsrechtlichen Konsequenzen hat das jedoch keinen Einfluss. Da der nemo tenetur-Grundsatz nur in staatlichen Verfahren und gegenüber staatlichen Organen gilt, ist er auf

das privatrechtliche Verhältnis zwischen Arbeitnehmer und -geber nicht direkt anwendbar.[32] 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 nicht selbst belasten zu müssen.[33] Eine Benachrichtigungspflicht im Zusammenhang mit Datenschutz- und IT-Sicherheitsverstößen wird dabei i.E. 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.

Es ist daher davon auszugehen, dass die arbeitsrechtliche Sanktionierung des Fehlverhaltens eines Arbeitnehmers rechtmäßig wäre, selbst wenn das Fehlverhalten nur auf Grund 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.[34] Je nach Schwere eines Verstoßes gegen die Mitteilungspflicht kommen zur Sanktionierung der Nichtmeldung durch den Arbeitnehmer ebenfalls gestufte Maßnahmen von der Abmahnung bis zur fristlosen Kündigung in Betracht.[35] Die Beweislast für den Nachweis eines Fehlverhaltens, dessen Schwere und die Rechtmäßigkeit der darauf basierenden Sanktionen des Arbeitnehmers trifft den Arbeitgeber.[36] In Fällen des Unterlassens der Meldung eines IT-Sicherheitsverstoßes hat er nachzuweisen, dass dem Arbeitnehmer ein meldepflichtiger Vorfall bekannt war oder i.R.e. ordnungsgemäßen Aufgabenerfüllung hätte bekannt sein müssen und er ihn pflichtwidrig nicht mitgeteilt hat.[37] Sofern ein Arbeitnehmer einen IT-Sicherheitsvorfall meldet und der Arbeitgeber ihn deshalb auf Grund 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.

III. Vorschlag für Begrenzung des Verantwortungsmaßstabs

Die drohende Verschleierung eines sicherheitsbezogenen Vorfalls auf Grund etwaiger arbeitsrechtlicher Sanktionen für den Arbeitnehmer führt dazu, dass dieser 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. Es kann aber auch keine Lösung sein, im Fall der Meldung von IT-Sicherheitsvorfällen vollständig auf arbeitsrechtliche Konsequenzen zu verzichten, da sich Mitarbeitende dann an gar keine Security-Policies mehr halten müssten.

Um eine verbesserte 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.[38] Die Mitarbeiter müssten der Anonymität eines solchen Meldesystems 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 in jedem Fall 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 offenbart. Dieselbe Bagatellhandlung, wie ein Klick auf den Anhang einer Mail eines unbekannten Absenders, kann entweder vom Virenschutzprogramm aufgehalten werden oder die Systeme eines ganzen Betriebs 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 innerbe-

trieblichen 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.[39] Dies gilt i.Ü. auch für Schäden, die dem Arbeitgeber oder Dritten durch IT-Sicherheitsvorfälle entstehen, die ein Arbeitnehmer schuldhaft verursacht hat. Diesem Grundgedanken des Schadensausgleichs folgend 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 wäre die Begründung dafür nicht die Kontrolle der innerbetrieblichen Anstrengungen zur Schadensprävention durch den Arbeitgeber.[40] Vielmehr würde er von der Verlässlichkeit rechtzeitiger Meldungen von IT-Sicherheitsverstößen durch Mitarbeiter und den damit einhergehenden Schadensminimierungen profitieren. Außerdem würden der Datenschutz und die IT-Sicherheit wesentlich gestärkt. Die pflichtgemäße Meldung eines Vorfalls erführe ferner gegenüber einer Nichtmeldung eine Privilegierung, da ein Unter-

lassen 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, was die Sanktionierung des Arbeitnehmers somit häufig mit der rechtlichen Unsicherheit einer gerichtsfesten Beweisbarkeit behaftet und angreifbar macht. Ein Sanktionsverzicht bewirkt ferner nicht den Ausschluss einer arbeitsrechtlichen Sanktionierung bei wiederholtem oder gleichgelagertem Fehlverhalten. Vielmehr kann nämlich bei Zugrundelegen eines objektiven zivilrechtlichen Sorgfaltsmaßstabs[41] der Vorwurf grober Fahrlässigkeit auf eine subjektive, das normale Maß übersteigende Vorwerfbarkeit des Fehlers gestützt werden,[42] die sich gerade aus der Wiederholung schon begangener Pflichtverletzungen ergeben kann.

IV. 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 auf Grund eines zusammen mit einer Meldung offengelegten eigenen Fehlverhaltens können der bereitwilligen Wahrnehmung dieser Pflicht entgegenstehen. Mitarbeiter, die der Meldepflicht dennoch nachkommen, erfahren aber auf arbeitsrechtlicher Ebene keinen Schutz, z.B. durch die Anwendung der Selbstbelastungsfreiheit. Sie erwartet vielmehr 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 ggf. 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. Der Vorschlag bietet dabei den Vorteil, dass er am Verschulden und damit der objektiven Vorwerfbarkeit des Fehlverhaltens des Arbeitnehmers anknüpft. Er relativiert die Angst der Arbeitnehmer vor arbeitsrechtlichen Konsequenzen, ohne sie dabei aber 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. 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 steigt. Ebenso muss weiter untersucht werden, wie der Arbeitgeber die Arbeitnehmer ausreichend aufklären und ihnen dadurch ein ausreichendes Bewusstsein für entsprechendes Fehlverhalten ermöglichen kann.

Schnell gelesen ...

- Die Meldung von IT-Sicherheits- oder Datenschutzvorfällen durch Mitarbeitende ist ein wesentli-

cher Baustein von Informationssicherheitsmaßnahmen und Maßnahmen zur Umsetzung von Datenschutzvorgaben in Unternehmen.

■ Kommen Mitarbeitende der Meldepflicht nach und offenbaren so ein eigenes Fehlverhalten gegenüber ihrem Arbeitgeber, werden sie zwar straf-, nicht aber arbeitsrechtlich privilegiert, sodass ihnen Abmahnungen oder Kündigungen drohen können.

■ Die Angst vor arbeitsrechtlichen Konsequenzen kann sich negativ auf die „Meldemoral" im Unternehmen auswirken, was das IT-Sicherheits- und Datenschutzniveau herabsetzt.

■ Um Mitarbeitende zur umfassenden Meldung von Sicherheitsvorfällen zu ermutigen, sollten die Grundsätze des innerbetrieblichen Schadensausgleichs auf die arbeitsrechtlichen Sanktionen übertragen und (leicht) fahrlässige Verstöße nicht sanktioniert werden.

---

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

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

3 Vgl. hierzu unter II.2.

4 *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 ff.

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

6 *Dutta/Roy*, Dynamics of organizational information security. System Dynamics Review: The Journal of the System Dynamics Society, 24, 2008, 349 ff., abrufbar unter: https://onlinelibrary.wiley.com/doi/abs/10.1002/sdr.405.

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

8 *Werlinger/Hawkey/Beznosov* (o. Fußn. 5).

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

10 *Hladjk*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 33 Rn. 22.
11 *Spittka*, in: Taeger (Hrsg.), Die Macht der Daten und der Algorithmen, 2019, S. 141 (144); *Reif*, in: Gola (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 33 Rn. 44.
12 *Brink*, in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Art. 33 Rn. 15; *Spittka* (o. Fußn. 11), S. 141 (150 ff.); *Paal*, ZD 2020, 119 (124); *Bergt*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, § 43 BDSG Rn. 11 ff.; *Spittka*, RDV 2019, 167 (170 ff.).
13 *Brodowski/Nowak*, in: BeckOK Datenschutzrecht, 31. Ed. 2020, § 43 BDSG Rn. 25, 27; *Boms*, ZD 2019, 536 (539 f.).
14 Die Herleitung eines arbeitsrechtlichen Auskunftsanspruchs ist umstritten. Insb. in der Rspr. wird vertreten, dass er als Nebenpflicht zum Arbeitsvertrag gem. § 242 BGB entspringt (so *BAG* U. v. 7.9.1995 – 8 AZR 828/93; *LAG Hamm* U. v. 3.3.2009 – 14 Sa 1689/08; *ArbG Saarlouis* U. v. 19.10.1983 – 1 Ca 493/83; wohl auch *Lützler/Müller-Sartori*, CCZ 2011, 19 f.), während die Lit. den Anspruch oftmals auf §§ 666, 675 BGB stützt (*Dann/Schmidt*, NJW 2009, 1851 (1852 f.) mit Differenzierung, zwischen dem unmittelbaren und mittelbaren Arbeitsbereich des Arbeitnehmers; ebenso *Spehl/Momsen/Grützner*, CCZ 2014, 170 (171)).
15 *Fischer*, in: Bamberger/Roth/Hau/Poseck (Hrsg.), BeckOK BGB, 53. Ed. 2020, § 666 Rn. 5; *BGH* MMR 2016, 674, Rn. 37.
16 *Fischer* (o. Fußn. 15), Rn. 3; *Schäfer*, in: MüKoBGB, 8. Aufl. 2020, § 666 Rn. 22.
17 *Preis*, in: Erfurter Kommentar zum Arbeitsrecht, 20. Aufl. 2020, § 611a BGB Rn. 736; *Spinner*, in: MüKoBGB (o. Fußn. 16), § 611a Rn. 993, 1030; *Joussen*, in: BeckOK Arbeitsrecht, 54. Ed. 2019, § 611a BGB Rn. 446; *Reichold*, in: Münchener Hdb. zum Arbeitsrecht, Bd. I, 4. Aufl. 2018, § 55 Rn. 4, 8.
18 *Joussen* (o. Fußn. 17).
19 *Joussen* (o. Fußn. 17); *Preis* (o. Fußn. 17), Rn. 742.
20 *Preis* (o. Fußn. 17), Rn. 744 ff.; *Spinner* (o. Fußn. 17), Rn. 1001; *BAG* U. v. 1.6.1995 – 6 AZR 912/94.
21 Vgl. auch *Joussen* (o. Fußn. 17); *Reichold* (o. Fußn. 17), Rn. 8.
22 Vgl. nur *ArbG Siegburg* U. v. 15.1.2020 – 3 Ca 1793/19.
23 *Fuhlrott*, NZA 2019, 649 (650) (652 f.); *Niemann*, in: Erfurter Kommentar zum Arbeitsrecht (o. Fußn. 17), § 626 BGB Rn. 29 f.
24 *BVerfG* B. v. 13.1.1981 – 1 BvR 116/77, Rn. 18; BVerfGE 38, 105 (113); BGHSt 14, 358 (364); *BGH* NJW 1989, 1228 (1229); *EGMR* NJW 2002, 499 (501).
25 *EuGH* U. v. 7.1.2004 – C-204/00, Rn. 64 f. – Alborg; U. v. 25.10.2001, Slg. 2002, I-8275, Rn. 273 f.; *Jarass*, GRCh, 3. Aufl. 2016, Art. 48 Rn. 31; *EGMR* U. v. 8.4.2004 – 38544/97, Rn. 46.
26 *BVerfG* B. v. 13.1.1981 – 1 BvR 116/77, Rn. 18 f.; *Wessing*, in: Hauschka/Moosmeyer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 46 Rn. 50; *Schaefer*, NJW-Spezial, 2010, 120.
27 *BVerfG* NJW 1981, 1431; *Wessing* (o. Fußn. 26).
28 *OLG Karlsruhe* NStZ 1989, 287 (288); *Wessing* (o. Fußn. 26); *Bittmann/Molkenbur*, wistra 2009, 68.
29 *OLG Karlsruhe* NStZ 1989, 287 (288); anders im Fall des Gemeinschuldners, der nach der zum Zeitpunkt der Gemeinschuldnerentscheidung des *BVerfG* geltenden Rechtslage gem. § 100 KO zur Auskunft verpflichtet war: *BVerfG* NJW 1981, 1431.
30 *BVerfG* NJW 1981, 1431 (1432).
31 *Wessing* (o. Fußn. 26), Rn. 50, 56; *Schrader/Thoms/Mahler*, NZA 2018, 965 (969); *Dann/Schmidt*, NJW 2009, 1851 (1855); *LAG Hamm* CCZ 2010, 237.
32 *Spehl/Momsen/Grützner*, CCZ 2014, 170 (171); *Dann/Schmidt*, NJW 2009, 1851 (1855); *Lützeler/Müller-Satori*, CCZ 2001, 19 (20).
33 Vgl. *Dann/Schmidt*, NJW 2009, 1851 (1853); *Spehl/Momsen/Grützner*, CCZ 2014, 170 (171).
34 Vgl. nur *Preis* (o. Fußn. 17), Rn. 748.
35 *Preis* (o. Fußn. 17), Rn. 748.
36 *BAG* NZA 1987, 452; *BAG* NZA 1987, 518; *LAG Mecklenburg-Vorpommern* U. v. 11.2.2020 – 2 Sa 133/19, Rn. 36 ff.; *LAG Köln* U. v. 17.1.2007 – 7 Sa 526/06, dort unter 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. 641 f.; *Niemann*, in: Erfurter Kommentar zum Arbeitsrecht (o. Fußn. 17), § 626 Rn. 234.

37 Vgl. *Joussen* (o. Fußn. 17); *Preis* (o. Fußn. 17).

38 Vgl. nur *Steffen/Stöhr*, RdA 2017, 43 (48).

39 *Koch*, in: Schaub/Koch, Arbeitsrecht von A-Z, 24. Aufl. 2020, Stichwort Haftung des Arbeitnehmers; *Wagner*, in: MüKoBGB, 7. Aufl. 2017, § 823 Rn. 128.

40 *Wagner* (o. Fußn. 39).

41 Vgl. nur *BVerfG* NJW-RR 1996, 980; *BGH* NJW 1981, 1603 (1604); *BGH* NJW 2001, 1786 (1787); *Lorenz*, in: BeckOK BGB (o. Fußn. 15), § 276 BGB Rn. 20; *Grundmann*, in: MüKoBGB (o. Fußn. 16), § 276 Rn. 55 f.; *Schulze*, in: NK-BGB, 10. Aufl. 2019, § 276 Rn. 13.

42 *BGH* NJW 1953, 1139; *BGH* NJW 1992, 2418; *Grundmann*, (o. Fußn. 41).