Offenlegungspflichten bei Cyberangriffen

Alexander Brüggemeier

I. Einleitung

„Bricht bald der Cyberkrieg los?" titelte vor kurzem die FAZ anlässlich eines Hackerangriffs auf Microsoft.[1] Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) meldet eine stetig steigende Zahl an Cyber-Angriffen mit einem immer größeren Gefahrenpotential für Staat, Wirtschaft und Gesellschaft.[2] Für die Leitung von Unternehmen stellt sich eine Vielzahl an Fragen und Problemen. In der akuten Situation eines Cyberangriffs mögen Offenlegungspflichten vielleicht nicht ganz oben auf der Prioritätenliste der Unternehmensleitung stehen. Aufgrund der nicht unerheblichen Bußgelder, möglicher Schadensersatzansprüche und – in besonders gelagerten Einzelfällen – sogar einer Strafbarkeit bei Nichterfüllung der Offenlegungspflichten sollten diese jedoch in jedem Fall penibel eingehalten und nach Möglichkeit Vorsorge getroffen werden. Dieser Beitrag soll einen Überblick über die in Betracht kommenden Melde- und Veröffentlichungspflichten geben und eine erste Handreichung darstellen. Im Zentrum stehen Melde- und Veröffentlichungspflichten nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), der Datenschutz-Grundverordnung (DSGVO) und der Marktmissbrauchsverordnung (MAR).*

1 *Finsterbusch et al.*, Bricht bald der Cyberkrieg los? 09.03.2021, https://www.faz.net/aktuell/wirtschaft/digitec/chinesischer-hackerangriff-auf-microsoft-die-politische-bedeutung-17235983.html.

2 BT-Drs. 19/26106, S. 1.

* Eine Aufzeichnung des Vortrags, auf dem der Beitrag beruht, ist abrufbar unter https://doi.org/10.17176/20210315-161018-0.

II. BSIG

1. Regelungszweck

Die Offenlegungspflichten nach dem BSIG dienen der Gewährleistung der Cyber- und Informationssicherheit und dem Schutz der Funktionsfähigkeit kritischer Infrastruktur sowie – zukünftig – von Unternehmen von besonderem öffentlichen Interesse und der Verfügbarkeit digitaler Dienste. Das BSI soll die IT-Sicherheitslage in Deutschland einschätzen können und ggf. durch eine schnelle Reaktion einen Übergriff bzw. einen vergleichbaren Vorfall bei anderen Systemen verhindern können.

2. Meldepflichtige Unternehmen

Das BSIG statuiert Meldepflichten für die Betreiber Kritischer Infrastrukturen (§ 8b Abs. 4 BSIG) und die Anbieter digitaler Dienste (§ 8c Abs. 3 BSIG). Nach der nunmehr vom Bundestag verabschiedeten Neuregelung des IT-Sicherheitsgesetzes – die Zustimmung des Bundesrates steht noch aus – werden zukünftig voraussichtlich auch Unternehmen von besonderem öffentlichen Interesse gem. § 8f Abs. 7, 8 BSIG-E einer Offenlegungspflicht unterliegen.[3] Diese Offenlegungspflicht erfasst nach § 2 Abs. 14 BSIG-E neben Unternehmen, die Güter nach § 60 Abs. 1 Nr. 1, 3 AWV herstellen oder entwickeln (Rüstungsindustrie und Hersteller von IT-Produkten für die Verarbeitung staatlicher Verschlusssachen) und bestimmten Unternehmen der Störfall-Verordnung insbesondere auch die Unternehmen, die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind. Welche Unternehmen eine besondere volkswirtschaftliche Bedeutung haben, wird durch eine Rechtsverordnung anhand abstrakt-genereller Kriterien konkretisiert werden, wobei sich die Berechnungsmethodik nach dem Gutachten der Monopolkommission nach § 44 Abs. 1 GWB richten soll.[4]

§ 8b Abs. 4 BSIG verpflichtet Betreiber Kritischer Infrastrukturen bestimmte Störungen unverzüglich über die Kontaktstelle an das Bundesamt

3 BT-Drs. 19/26106, S. 18 f.

4 BT-Drs. 19/26106, S. 31, 58. Die 100 Unternehmen erfassende Liste des Gutachtens der Monopolkommission ist abrufbar unter: https://monopolkommission.de/images/HG23/HGXXIII_Gesamt.pdf, S. 80.

zu melden. Kritische Infrastrukturen sind gem. § 2 Abs. 10 S. 1 BSIG Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören (Nr. 1) und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden (Nr. 2). Nähere Bestimmungen zu dieser Legaldefinition sind in der auf Grundlage von § 2 Abs. 10 S. 2, 10 Abs. 1 BSIG erlassenen BSI-KritisV enthalten. Danach sind die Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation, Gesundheit, das Finanz- und Versicherungswesen sowie Transport und Verkehr erfasst, wobei in den Anhängen der BSI-KritisV die Schwellenwerte festgelegt werden, bei deren Erreichen von einer hohen Bedeutung i.S.v. § 2 Abs. 10 S. 1 Nr. 2 BSIG auszugehen ist. Ausgenommen von der Meldepflicht sind gem. § 8d Abs. 3 BSIG Betreiber Kritischer Infrastrukturen, die auf Grund anderer Rechtsvorschriften Veröffentlichungspflichten unterliegen, die mit § 8b Abs. 4 BSIG vergleichbar oder weitergehend sind, wie beispielsweise gem. § 8d Abs. 3 Nr. 1 Alt. 1 BSIG die Betreiber eines öffentlichen Telekommunikationsnetzes, deren Verpflichtung insoweit aus § 109 Abs. 5 TKG folgt. Zudem sind gem. § 8d Abs. 1 BSIG Kleinstunternehmen i.S.d. der Empfehlung 2003/361/EG der Kommission von der Meldepflicht ausgenommen, sodass Unternehmen, die weniger als zehn Personen beschäftigen und deren Jahresumsatz bzw. Jahresbilanz 2 Millionen Euro nicht überschreitet, nicht zur Meldung an das BSI verpflichtet sind (Art. 2 Abs. 3 des Anhangs zur Empfehlung 2003/361/EG der Kommission).

§ 8c Abs. 3 BSIG verpflichtet die Anbieter digitaler Dienste jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Bereitstellung eines von ihnen innerhalb der Europäischen Union erbrachten digitalen Dienstes hat, unverzüglich dem Bundesamt zu melden. Digitale Dienste erfasst gem. § 2 Abs. 11 BSIG Online-Marktplätze (§ 2 Abs. 11 Nr. 1 BSIG), Online-Suchmaschinen (§ 2 Abs. 11 Nr. 2 BSIG) und Cloud-Computing-Dienste (§ 2 Abs. 11 Nr. 3 BSIG), die nicht zum Schutz grundlegender staatlicher Funktionen eingerichtet worden sind oder für diese genutzt werden und Dienste i.S.v. Art. 1 Abs. 1 lit. b der Richtlinie (EU) 2015/1535 darstellen.

3. Auslöser der Meldepflicht

a. § 8b Abs. 4 BSIG

Auslöser der Meldepflicht gem. § 8b Abs. 4 BSIG sind Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben (Nr. 1) bzw. erhebliche Störungen, die zu einem Ausfall oder einer erheblichen Störung führen können (Nr. 2). Der Begriff der Störung ist ausweislich der Begründung zum IT-Sicherheitsgesetz 2015 in Anlehnung an die höchstrichterliche Rechtsprechung zu § 100 TKG funktional zu verstehen.[5] Sie liegt vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken.[6] Dies erfasst beispielsweise Sicherheitslücken, Schadprogramme und erfolgte, versuchte oder erfolgreich abgewehrte Angriffe auf die Sicherheit in der Informationstechnik sowie außergewöhnliche und unerwartete technische Defekte mit IT-Bezug.[7] Hat die Störung bereits zu einem Ausfall oder einer erheblichen Beeinträchtigung geführt, ist eine Erheblichkeit der Störung nicht erforderlich. Ist es hingegen noch nicht zu einem Ausfall oder einer erheblichen Beeinträchtigung gekommen, entsteht eine Meldepflicht nur, wenn es sich um eine erhebliche Störung handelt, die zu einem Ausfall oder einer erheblichen Beeinträchtigung führen kann. Eine erhebliche Störung liegt vor, wenn diese nicht automatisiert oder mit wenig Aufwand behoben werden kann.[8] Eine Beeinträchtigung ist jeweils erheblich, wenn die Infrastruktur nicht mehr in der Lage ist, Versorgungsleistungen wie geplant oder erwartet zu erbringen.[9]

---

5 BT-Drs. 18/4096, S. 27.
6 BT-Drs. 18/4096, S. 27; BGH, Urteil v.03.07.2014 – III ZR 391/13 = NJW 2014, 2500 Rn. 15.
7 BT-Drs. 18/4096, S. 27 f.
8 *Ritter/Schulte*, CR 2019, 617, 619; *Winter*, CR 2020, 576, 578.
9 *Ritter/Schulte*, CR 2019, 617, 619; *Winter*, CR 2020, 576, 578.

b. § 8c Abs. 3 BSIG

Anbieter digitaler Dienste sind verpflichtet, jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Bereitstellung eines von ihnen innerhalb der EU erbrachten digitalen Dienstes zu melden. Ein Sicherheitsvorfall kann in Anlehnung an Art. 4 Nr. 7 der NIS-RL (EU 2016/1148) definiert werden als Ereignis, das tatsächlich negative Auswirkungen auf die Sicherheit von Netz- und Informationssystemen hat. Die Erheblichkeit der Auswirkungen eines Sicherheitsvorfalls bestimmt sich gem. § 8c Abs. 3 S. 2 BSIG i.V.m. Art. 4 der Durchführungsverordnung (EU) 2018/151 auf Grundlage mehrerer Parameter, wie insbesondere der Zahl der betroffenen Nutzer, der Dauer des Sicherheitsvorfalls, dem geographischen Gebiet, dem Ausmaß der Unterbrechung, dem Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten sowie danach, ob der Sicherheitsvorfall zu einem Verlust der Integrität, Authentizität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der entsprechenden Dienste geführt hat, von dem mehr als 100.000 Nutzer betroffen sind, ob eine öffentliche Gefahr oder ein Risiko für die öffentliche Sicherheit entstanden oder Menschen ums Leben gekommen sind, oder der Vorfall zu einem Sachschaden in Höhe von mehr als 1.000.000 Euro geführt hat. Kann der Anbieter die Erforderlichkeit mangels Zugang zu den Informationen über diese Parameter nicht einschätzen, entfällt die Meldepflicht gem. § 8c Abs. 3 S. 3 BSIG.

4. Inhalt der Meldepflicht

§ 8b Abs. 4 BSIG verpflichtet die Betreiber Kritischer Infrastruktur zur unverzüglichen Meldung der Störungen. Der Inhalt der Meldung, für welche das BSI ein Meldeformular zur Verfügung stellt,[10] wird durch § 8 Abs. 4 S. 2 BSIG vorgegeben und umfasst Angaben zu der Störung, zu möglichen grenzübergreifenden Auswirkungen sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur erbrachten kritischen Dienstleistung und zu den Auswirkungen der Störung auf diese Dienstleistung. Eine namentliche Nennung des Betreibers ist gem. § 8b Abs. 4 S. 3 BSIG lediglich erforder-

10 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/Meldeformular_BSIG8b_Muster.pdf?__blob=publicationFile&v=1.

lich, wenn die Störung zu einem Ausfall oder einer Beeinträchtigung führt. Zudem soll das BSI zukünftig gem. § 8b Abs. 4a BSIG-E berechtigt sein, die zur Bewältigung der Störung erforderlichen Daten einschließlich personenbezogener Daten herausverlangen zu können. Die Meldung muss unverzüglich, mithin ohne schuldhaftes Zögern, erfolgen[11] und das BSI geht von dem Grundsatz „Schnelligkeit vor Vollständigkeit" aus.[12] Ein Aufschub bis zur Ausermittlung des Sachverhaltes ist nach Auffassung des BSI nicht zulässig.[13] Stattdessen sind die bislang bekannten Informationen als Erstmeldung zu kennzeichnen und durch spätere Folgemeldungen zu ergänzen.

Der Inhalt der Meldung nach § 8c Abs. 3 BSIG richtet sich nach § 8b Abs. 4 BSIG.[14] Das BSI stellt wiederum ein Meldeformular zur Verfügung[15] und gibt auf seiner Webseite im Rahmen von FAQ nähere Hinweise.[16] Hiervon gem. § 8c Abs. 3 S. 4 BSIG abweichende Durchführungsakte der Kommission nach Art. 16 Abs. 9 der NIS-RL existieren aktuell nicht.

5. Sanktionen

Die Sanktionen sind bislang insbesondere im Vergleich zu den drohenden Rechtsfolgen eines Verstoßes gegen die Vorschriften der DSGVO und der MAR zahnlos. § 14 Abs. 2 BSIG stellt lediglich ein Bußgeld von bis zu 50.000 Euro in Aussicht. Nach der vom Bundestag verabschiedeten Neuregelung ist in § 14 Abs. 2 Nr. 7, Abs. 5 BSIG-E nunmehr ein Bußgeld von bis zu 500.000 Euro vorgesehen.

---

11 BSI, KRITIS-FAQ, abrufbar unter: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-FAQ/FAQ-zur-Meldepflicht/faq-zur-meldepflicht_node.html; *Buchberger* in: Schenke/Graulich/Ruthig, 2. Aufl. 2019, § 8b BSIG Rn. 6.

12 BSI, KRITIS-FAQ.

13 BSI, KRITIS-FAQ.

14 Der bisherige Verweis auf § 8b Abs. 3 BSIG stellt ein Redaktionsversehen dar und soll durch Art. 1 Ziff. 14 des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme korrigiert werden, BT-Drs. 19/26106, S. 17.

15 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/meldungen_8c3BSIG_vorlage_pdf.pdf?__blob=publicationFile&v=1.

16 BSI, FAQ zur Regulierung von Anbietern digitaler Dienste, abrufbar unter: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Weitere_regulierte_Unternehmen/Anbieter_digitaler_Dienste/FAQ/Meldepflicht/faq_dsp_meldepflicht_node.html.

III. DSGVO

1. Regelungszweck

Die DSGVO enthält mehrere Offenlegungspflichten, die im Falle eines Cyberangriffs einschlägig sein können. Zunächst verpflichtet Art. 33 Abs. 1 DSGVO die Verantwortlichen, eine Verletzung des Schutzes personenbezogener Daten der zuständigen Aufsichtsbehörde zu melden. Zudem ist der Verantwortliche gem. Art. 34 Abs. 1 DSGVO verpflichtet, in bestimmten Fällen die von der Verletzung betroffenen Personen unverzüglich zu benachrichtigen. Schließlich verpflichtet Art. 33 Abs. 2 DSGVO Auftragsverarbeiter, einem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten zu melden. Diese Offenlegungspflichten dienen dem möglichst effektiven Schutz personenbezogener Daten natürlicher Personen durch einen präventiven Anreiz zur Stärkung der Datensicherheit. Zudem stellen sie die Grundlage für Maßnahmen gem. Art. 58 DSGVO dar.[17]

2. Personeller Anwendungsbereich

Die Meldepflicht gegenüber der zuständigen Aufsichtsbehörde gem. Art. 33 Abs. 1 DSGVO und die Benachrichtigungspflicht gem. Art. 34 Abs. 1 DSGVO treffen die Verantwortlichen. Verantwortlicher ist gem. Art. 4 Nr. 7 DSGVO jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Die DSGVO enthält anders als das BSIG keine Einschränkung auf bestimmte Sektoren oder Unternehmen mit besonderer Kritikalität.

Die Pflicht zur Meldung einer Verletzung an den Verantwortlichen trifft Auftragsverarbeiter. Auftragsverarbeiter ist gem. Art. 4 Nr. 8 DSGVO jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

17 *Paal*, ZD 2020, 119.

3. Auslöser der Meldepflicht

a. Art. 33 DSGVO

Auslöser der Meldepflicht gem. Art. 33 Abs. 1 DSGVO ist die Verletzung des Schutzes personenbezogener Daten. Diese liegt gem. Art. 4 Nr. 12 DSGVO bei einer Verletzung der Sicherheit vor, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Es sind vielfältige Cyberangriffe denkbar, die diese Merkmale erfüllen. Beispielhaft kann die Verschlüsselung von Daten durch eine Erpressungssoftware (Verlust) genannt werden. Die Meldepflicht entfällt gem. Art. 33 Abs. 1 Hs. 2 DSGVO, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Es handelt sich um eine Prognoseentscheidung unter Berücksichtigung aller Umstände des Einzelfalls, wobei insbesondere die Eintrittswahrscheinlichkeit und die voraussichtlich betroffenen Rechtsgüter zu berücksichtigen sind.[18] Anders als im Rahmen der Ad-hoc-Publizitätspflicht aus Art. 17 MAR, bei der eine einmal eingetretene Veröffentlichungspflicht nicht wieder entfällt, können Gegenmaßnahmen, die dazu führen, dass das Risiko für die Rechte und Freiheiten der betroffenen Personen nachträglich entfällt, zu einem Entfallen der Meldepflicht führen.[19]

b. Art. 34 DSGVO

Führt die eine Meldepflicht nach Art. 33 DSGVO auslösende Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem hohen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen, sind diese gem. Art. 34 Abs. 1 DSGVO unverzüglich zu benachrichtigen. Anders als bei Art. 33 Abs. 1 Hs. 2 DSGVO ist eine Risikoabwägung bereits zur Begründung der Benachrichtigungspflicht erforderlich. Das Bestehen eines hohen Risikos kann sowohl durch eine hohe Wahrscheinlichkeit eines geringen Schadens als auch durch eine geringe Wahrscheinlichkeit ei-

18 *Paal*, ZD 2020, 119, 121; *Winter*, CR 2021, 576, 579.
19 *Winter*, CR 2021, 576, 579.

nes hohen Schadens begründet werden.[20] Maßgeblich ist – wie bei Art. 33 DSGVO – ein *probability/magnitude*-Test. In bestimmten Fällen entfällt die Benachrichtigungspflicht gem. Art. 34 Abs. 3 DSGVO, insbesondere, wenn durch nachfolgende Maßnahmen das Bestehen eines hohen Risikos ausgeräumt werden kann. Die Benachrichtigungspflicht entfällt zudem, wenn der Verantwortliche bezüglich der betroffenen Daten – zum Schutz der Rechte und Freiheiten der betroffenen Personen – geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat – auch wenn in diesen Fällen bereits das Bestehen eines hohen Risikos fraglich sein dürfte – oder wenn die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat allerdings eine öffentliche Bekanntmachung oder ähnliche Maßnahme zu erfolgen. Besteht Unsicherheit, ob die Voraussetzungen des Art. 34 Abs. 3 DSGVO vorliegen, bietet es sich an, einen Beschluss nach Art. 34 Abs. 4 DSGVO herbeizuführen, mit welchem festgestellt wird, dass die Voraussetzungen für ein Entfallen der Benachrichtigungspflicht gegeben sind.

4. Verfahren und Inhalt der Meldung

a. Art. 33 DSGVO

Der Verantwortliche hat die Verletzung unverzüglich – mithin ohne schuldhaftes Zögern – und möglichst binnen 72 Stunden, nachdem sie dem Verantwortlichen bekannt wurde, zu melden. Wird diese 72-Stunden-Frist nicht eingehalten, muss die Verzögerung gegenüber der Behörde begründet werden. Insgesamt gilt das Prinzip „Schnelligkeit vor Vollständigkeit", was sich deutlich in der Möglichkeit der Abschichtung der Meldung in Abhängigkeit von den zur Verfügung stehenden Informationen gem. Art. 33 Abs. 4 DSGVO zeigt.

Der Mindestinhalt der Mitteilung ergibt sich aus Art. 33 Abs. 3 DSGVO. Erforderlich sind Informationen über die Art der Verletzung [lit. a)], die Angabe einer Anlaufstelle für weitere Informationen [lit. b)], eine Beschreibung der wahrscheinlichen Folgen [lit. c)] und eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen [lit. d)]. Von den zuständigen Behörden zur Verfügung gestellte Meldeformulare strukturieren

20 *Martini* in: Paal/Pauly, DSGVO/BDSG, 3. Aufl. 2021, Art. 34 Rn. 30. Lediglich auf eine hohe Wahrscheinlichkeit abstellend: *Winter*, CR 2021, 576, 579.

und vereinheitlichen die jeweils zu meldenden Informationen.[21] Benötigt die zuständige Behörde weitere Informationen, kann sie diese jedenfalls auf Grundlage von Art. 58 Abs. 1 DSGVO anfordern.

b. Art. 34 DSGVO

Die unverzügliche Benachrichtigung der betroffenen Personen nach Art. 34 Abs. 2 DSGVO orientiert sich inhaltlich an Art. 33 Abs. 3 DSGVO, reduziert die Verpflichtung aus Art. 33 Abs. 3 lit. a) DSGVO allerdings auf die Art der Verletzung. Die Benachrichtigung hat gem. Art. 34 Abs. 2, 12 Abs. 1, 2 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher, schriftlicher oder anderer, ggf. elektronischer Form in einer klaren und einfachen Sprache zu erfolgen.

5. Sanktionen

Die Erfüllung der Pflichten aus der DSGVO wird mit erheblichen Sanktionen abgesichert. Nach Art. 83 Abs. 4 DSGVO können aufgrund eines Verstoßes gegen Art. 33, 34 DSGVO Bußgelder von bis zu 10 Millionen Euro oder im Fall eines Unternehmens von bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem, welcher der Beträge höher ist. Bei einem Verstoß gegen Art. 58 Abs. 1 DSGVO (ergänzende Informationspflicht) drohen sogar Geldbußen von bis zu 20 Millionen Euro oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist.

21 S. bspw. https://www.ldi.nrw.de/mainmenu_Aktuelles/Formulare-und-Meldungen/Inhalt2/Meldeformular---Verletzung-des-Schutzes-personenbezogener-Daten/formular_art33.pdf.

IV. MAR

1. Regelungszweck

Die Ad-hoc-Publizität ist ein wesentlicher Baustein des europäischen Kapitalmarktrechts zum Schutz der Funktionsfähigkeit der Kapitalmärkte.[22] Sie flankiert das Verbot des Insiderhandels aus Art. 8 MAR,[23] stärkt dadurch das Vertrauen in die Integrität der Kapitalmärkte und fördert die Informationseffizienz und Allokationseffizienz der Kapitalmärkte.[24]

2. Meldepflichtige Unternehmen

Art. 17 MAR erfasst lediglich Emittenten, die für ihre Finanzinstrumente eine Zulassung zum Handel an einem geregelten Markt in einem Mitgliedsstaat beantragt oder erhalten haben, sowie gem. Art. 17 Abs. 1 UAbs. 3 MAR Emittenten, die für ihre Finanzinstrumente eine Zulassung zum Handel auf einem multilateralen (MTF) oder organisierten Handelssystem (OTF) erhalten oder eine Zulassung zum Handel auf einem MTF beantragt haben.[25] Freiverkehrs-Emittenten werden hingegen nicht erfasst.

3. Auslöser der Meldepflicht

a. Insiderinformation gem. Art. 7 Abs. 1 lit. a) MAR

Art. 17 Abs. 1 MAR verpflichtet einen Emittenten, Insiderinformationen, die unmittelbar den Emittenten betreffen, zu veröffentlichen. Der Begriff der Insiderinformation wird definiert durch Art. 7 Abs. 1 lit. a) MAR. Danach sind Insiderinformationen „nicht öffentlich bekannte präzise Infor-

22 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 1.

23 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 1.

24 *Fleischer/Zimmer* in: dies. Effizienz als Regelungsziel im Handels- und Wirtschaftsrecht, 9, 14 ff.; *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 1; *Klöhn* in: ders., MAR, 1. Aufl. 2018, Art. 17 Rn. 6 ff.

25 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 29 ff.

mationen, die direkt oder indirekt einen oder mehrere Emittenten oder ein oder mehrere Finanzinstrumente betreffen und die, wenn sie öffentlich bekannt würden, geeignet wären, den Kurs dieser Finanzinstrumente oder den Kurs damit verbundener derivativer Finanzinstrumente erheblich zu beeinflussen". Der Emittentenleitfaden der BaFin enthält eine Reihe an Umständen, die potentiell eine Ad-hoc-Pflicht auslösen können. Mögliche Cyberangriffe auf Emittenten werden jedoch nicht diskutiert.[26]

Wann eine Information als präzise anzusehen ist, ergibt sich aus Art. 7 Abs. 2 S. 1 MAR. Erfasst werden sowohl Umstände bzw. Ereignisse, die bereits eingetreten sind, als auch Umstände bzw. Ereignisse, von denen vernünftigerweise erwartet werden kann, dass sie in Zukunft eintreten werden. Eine hinreichende Eintrittswahrscheinlichkeit liegt vor, wenn die Wahrscheinlichkeit, dass der Umstand eintritt, größer als 50 % ist.[27] Die voraussichtlichen Auswirkungen des Ereignisses auf den Börsenkurs sind hingegen nicht bei der Bestimmung der notwendigen Eintrittswahrscheinlichkeit zu berücksichtigen (kein *probability/magnitude*-Test).[28] Zu berücksichtigen ist, dass im Rahmen von gestreckten Sachverhalten sowohl die bereits eingetretenen Zwischenschritte, als auch die zukünftigen Zwischenschritte und das Endereignis mögliche Anknüpfungspunkte darstellen.[29] Selbst wenn ein Cyberangriff also noch nicht zu einem Schaden geführt hat, dieser aber hinreichend wahrscheinlich ist und auch die übrigen Voraussetzungen von Art. 17 MAR vorliegen, kann bereits ein ad-hoc-publizitätspflichtiger Sachverhalt gegeben sein, dessen Nichtveröffentlichung lediglich auf Grundlage eines Aufschubs gem. Art. 17 Abs. 4 MAR möglich ist. Diese Umstände bzw. Ereignisse müssen zudem hinreichend spezifisch sein, um bei der Bildung des Marktpreises berücksichtigt werden zu können.

Die Information darf zudem nicht bereits öffentlich bekannt sein. Dies ist der Fall, wenn sie nicht von einer unbestimmten Anzahl von Perso-

26 BaFin, Emittentenleitfaden, Modul C, Stand: 25.03.2020, S. 22.

27 EuGH, Urteil v. 28.06.2021 – Rs. C-19/11 = NJW 2012, 2787 Rn. 49; BGH, Beschluss v. 23.04.2013 – II ZB 7/09 = NZG 2013, 708 Rn. 29; *Krause* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 6 Rn. 63; *Klöhn* in: ders. MAR, 1. Aufl. 2018, Art. 7 Rn. 97.

28 EuGH, Urteil v. 28.06.2021 – Rs. C-19/11 = NJW 2012, 2787 Rn. 50; *Krause* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 6 Rn. 63 m.w.N.

29 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 73.

nen zur Kenntnis genommen werden kann.[30] Die Kenntnis nur einer Bereichsöffentlichkeit, d.h. der unmittelbaren Marktteilnehmer, ist nicht ausreichend.[31]

Die Information muss außerdem geeignet sein, den Kurs des Finanzinstruments erheblich zu beeinflussen. Dies ist gem. Art. 7 Abs. 4 MAR der Fall, wenn „ein verständiger Anleger [sie] wahrscheinlich als Teil der Grundlage seiner Anlageentscheidung nutzen würde."[32] Dafür ist aus einer objektiven ex-ante-Perspektive festzustellen, ob sich die Information auf den Fundamentalwert des Unternehmens auswirkt.[33] Anders als bei der Prüfung, ob für einen zukünftigen Umstand überhaupt eine hinreichende Eintrittswahrscheinlichkeit besteht, sind im Rahmen der Prüfung der Kursrelevanz die erwartete Auswirkung der Information auf den Kurs sowie die Eintrittswahrscheinlichkeit des Umstandes zu berücksichtigen (*probability/magnitude*-Test).[34] Dass sich ein Cyberangriff auf den Fundamentalwert eines Unternehmens auswirkt, ist in einer Vielzahl von Fällen – bspw. bei einer erheblichen Beeinträchtigung der Produktion oder dem Bekanntwerden von wichtigen Geschäftsgeheimnissen – denkbar, kann aber nicht generell festgestellt werden. Vielmehr ist die Beurteilung auf Grundlage sämtlicher Informationen und Besonderheiten des Einzelfalls vorzunehmen.

b. Unmittelbare Betroffenheit

Zudem muss der Emittent unmittelbar betroffen sein, um eine Ad-hoc-Publizitätspflicht zu begründen. Dies ist in Anlehnung an § 15 Abs. 1 S. 3 WpHG a.F. insbesondere der Fall, wenn die Information im Tätigkeitsbereich des Emittenten selbst eintritt, also bei unternehmensinternen Ereignissen. Allerdings kann auch bei Ereignissen, die von außen stammen, ein hinreichend konkreter Zusammenhang zu dem Emittenten bestehen, sodass ein verständiger Anleger die Veröffentlichung der Information durch

30 BaFin, Emittentenleitfaden, Modul C, S. 10; *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 77.
31 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 77; *Klöhn* in: ders. MAR, 1. Aufl. 2018, Art. 7 Rn. 126 ff.
32 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 78.
33 *Klöhn* in: ders. MAR, 1. Aufl. 2018, Art. 7 Rn. 190 ff.
34 *Klöhn* in: ders. MAR, 1. Aufl. 2018, Art. 7 Rn. 198.

den Emittenten berechtigterweise erwarten darf.[35] Bei Cyberangriffen wird die Information in der Regel im Tätigkeitsbereich des Emittenten selbst eintreten, diesen also unmittelbar betreffen.

c. Keine Saldierung

Anders als im Rahmen der Meldepflicht nach Art. 33 DSGVO, bei welcher auch nachträgliche Maßnahmen zu einem Entfall der Veröffentlichungspflicht führen können, wenn dadurch Risiken für die Rechte und die Freiheit natürlicher Personen vermieden werden, kann eine einmal eingetretene Ad-hoc-Pflicht nicht aufgrund nachträglicher Umstände entfallen. Die Veröffentlichungspflicht entfällt nicht, wenn nach dem Entstehen einer veröffentlichungspflichtigen Insiderinformation – bspw. eines erfolgreichen Cyberangriffs, der voraussichtlich zu einem erheblichen Abfluss von Geschäfts- und Betriebsgeheimnissen führt – im Zeitraum eines Aufschubs nach Art. 17 Abs. 4 MAR Maßnahmen getroffen werden können, um diesen Abfluss zu verhindern. Auch können zwei Insiderinformationen, die voraussichtlich einen gegenläufigen Einfluss auf den Kurs haben, nicht saldiert werden.[36]

4. Aufschubbefugnisse gem. Art. 17 Abs. 4 MAR

Von höchster Relevanz sind die Befugnisse des Emittenten, die Veröffentlichung der Insiderinformation aufzuschieben. Ein solcher Aufschub kommt nach Art. 17 Abs. 4 MAR in Betracht, wenn eine unverzügliche Offenlegung geeignet wäre, die berechtigten Interessen des Emittenten zu beeinträchtigen, die Aufschiebung nicht geeignet wäre, die Öffentlichkeit irrezuführen und der Emittent die Geheimhaltung der Information sicherstellen kann. Die Möglichkeit eine Veröffentlichung nach Art. 17 Abs. 4 MAR aufzuschieben, wird konkretisiert durch ein Zusammenspiel der Durchführungsverordnung (EU) 2016/1055, der Leitlinien der ESMA über den Aufschub der Offenlegung von Insiderinformationen und der Verord-

35 BaFin, Emittentenleitfaden, Modul C, Stand: 25.03.2020, S. 33 f.; *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 49 ff.

36 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 79.

nung zur Konkretisierung von Anzeige-, Mitteilungs- und Veröffentlichungspflichten nach dem Wertpapierhandelsgesetz (WpAV).[37]

a. Berechtigte Interessen des Emittenten

Entgegen der Auffassung der ESMA[38] ist der Begriff der berechtigten Interessen tendenziell nicht eng auszulegen.[39] Vielmehr bedarf es eines transparenzrechtlichen Korrektivs zur Ausdehnung des Tatbestands der Insiderinformation zur Vermeidung von Insiderhandel.[40] Nach Art. 6 WpAV liegt ein berechtigtes Interesse vor, wenn die Interessen des Emittenten an der Geheimhaltung der Information die Interessen des Kapitalmarktes an einer vollständigen und zeitnahen Veröffentlichung überwiegen. Diese von § 6 WpAV vorgesehene Abwägung kann dogmatisch am Begriff der *berechtigten* Interessen festgemacht werden.[41] Ein Interesse des Emittenten kann angenommen werden, wenn die Veröffentlichung zu negativen Konsequenzen für den Emittenten, d.h. für dessen Fundamentalwert, führen kann. Allein der Kursverlust, der mit einer negativen Ad-hoc-Mitteilung in der Regel einhergeht, oder ein durch die Veröffentlichung drohender Reputationsverlust stellen allerdings typischerweise kein berücksichtigungsfähiges berechtigtes Interesse des Emittenten dar.[42] Typische Fallgruppen eines berechtigten Interesses, welche auch in einigen Fällen von Cyberangriffen relevant werden können, sind laufende Verhandlungen, deren Ergebnis oder Gang durch eine Veröffentlichung negativ beeinträchtigt würde.[43]

---

37 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 95.

38 ESMA/2016/1130 Rn. 52.

39 *Kumpan/Schmidt* in: Schwark/Zimmer, Kapitalmarktrechts-Kommentar, 5. Aufl. 2020, Art. 17 MAR Rn. 199; *Klöhn* in: ders., MAR, 1. Aufl. 2018, Art. 17 Rn. 173 f.

40 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 96 m.w.N.

41 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 97 m.w.N. Allein die Interessen des Emittenten für maßgeblich erachtend bspw.: *Klöhn* in: ders., MAR, 1. Aufl. 2018, Art. 17 Rn. 167 ff.; *Klöhn*, AG 2016, 423, 430 f.; *Kumpan*, DB 2016. 2039 2043; *Poelzig* NZG 2016, 761, 764.

42 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 99.

43 ESMA/2016/1478 DE Rn. 8 lit. a. S. 4; ESMA/2016/1130 Rn. 55 f.; EW 50 lit. a) MAR; § 6 Nr. 1 WpAV.

b. Keine Irreführung der Öffentlichkeit

Die Aufschiebung der Offenlegung darf gem. Art. 17 Abs. 4 UAbs. 1 lit. b) MAR nicht geeignet sein, die Öffentlichkeit irrezuführen. Eine Eignung zur Irreführung besteht, wenn im Markt, d.h. bei einem breiten Anlegerpublikum, eine Fehlvorstellung über die Information besteht.[44] Das alleinige Bestehen einer Informationsasymmetrie ist allerdings nicht ausreichend, da diese dem Bestehen einer Insiderinformation immanent ist.[45] Drei von der ESMA genannte, nicht abschließende Beispiele[46] lassen sich zu dem Grundsatz verdichten, dass insbesondere eigene Kommunikation eine entsprechende Fehlvorstellung im Markt verursachen kann. Auch hinreichend konkrete Informationen, die nicht auf den Emittenten zurückzuführen sind, können eine entsprechende Fehlvorstellung begründen. Solange im Markt allerdings lediglich Gerüchte kursieren, die nicht auf Kommunikation des Emittenten zurückzuführen sind und die nicht aus anderen Gründen hinreichend konkret sind, ist eine *no comment policy* dringend anzuraten.[47]

c. Sicherstellung der Geheimhaltung

Schließlich muss der Emittent gem. Art. 17 Abs. 4 UAbs. 1 lit. c) MAR die Geheimhaltung der Information sicherstellen.

Neben den stets zu berücksichtigenden Grundsätzen für die Sicherstellung der Geheimhaltung ist im Falle von Cyberangriffen insbesondere das Zusammenspiel mit den im Einzelfall parallel eingreifenden Publizitätspflichten nach dem BSIG und der DSGVO zu berücksichtigen. Aus Art. 4 Abs. 1 lit. c) i) DurchführungsVO (EU) 2016/1055 ergibt sich, dass Emittenten sicherstellen müssen, dass lediglich Personen, denen gegenüber eine Offenlegung der Insiderinformation nach Art. 10 MAR erfolgen darf, Zugang zu der Information haben. Nach Art. 10 MAR ist eine Offenlegung insbesondere erlaubt, wenn die Offenlegung im Zuge der normalen Ausübung einer Beschäftigung oder eines Berufs oder der normalen Erfül-

44 *Klöhn* in: ders., MAR, 1. Aufl. 2018, Art. 17 Rn. 251.
45 *Kumpan* in: Baumbach/Hopt, HGB, Art. 17 MAR Rn. 18.
46 ESMA/2016/1130 Annex V Nr. 3.2.5 Rn. 80.
47 ESMA, Questions and Answers on the Market Abuse Regulation (MAR), Version 14, 29. März 2019, ESMA70–145–111, S. 13; *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 129; *Klöhn* in: ders., MAR, 1. Aufl. 2018, Art. 17 Rn. 259.

lung von Aufgaben geschieht. Dies erfasst insbesondere die Erfüllung anderer gesetzlicher Publizitätspflichten. Auch wenn grundsätzlich zu prüfen ist, ob auch die jeweilige Informationspflicht Vorrang gegenüber dem insiderrechtlichen Weitergabeverbot genießt,[48] kann jedenfalls für die Pflichten nach dem BSIG und der DSGVO festgehalten werden, dass diese zur Weitergabe berechtigen. Zwar dient die Benachrichtigungspflicht nach Art. 34 DSGVO nicht der normalen Ausübung einer Beschäftigung oder eines Berufes, allerdings verfolgt Art. 34 DSGVO mit dem Schutz der persönlichen Rechte und Freiheiten von natürlichen Personen ein wichtiges Regelungsziel. Der Schutz der Funktionsfähigkeit des Kapitalmarktes muss in diesem Fall über die unverzügliche Veröffentlichung der Insiderinformation gewährleistet werden. Auch die weiteren Veröffentlichungspflichten nach dem BSIG und DSGVO berechtigen zur Weitergabe an die jeweils zuständige Behörde. Die Pflichten enthalten – anders als bspw. das Informationsrecht des Aktionärs gem. § 131 Abs. 1, 3 Nr. 5 AktG – keinen Vorbehalt hinsichtlich etwaiger entgegenstehender Pflichten. Zudem erfüllen auch sie mit dem Schutz der Funktionsfähigkeit kritischer Infrastruktur und dem Schutz personenbezogener Daten wichtige Regelungszwecke, die im Rahmen einer Abwägung Vorrang vor dem insiderrechtlichen Weitergabeverbot haben. Eine Veröffentlichungspflicht gem. Art. 17 Abs. 8 MAR wegen nach Art. 10 Abs. 1 MAR erfolgter Offenlegung greift allerdings in der Regel wegen § 67 BBG, § 30 VwVfG und den landesspezifischen Äquivalenten nicht ein.

Während die Erfüllung der Benachrichtigungspflicht nach Art. 34 DSGVO deshalb im Ergebnis zum Entfallen der Aufschubbefugnis führt, da die Geheimhaltung nicht mehr sichergestellt werden kann, führen die Pflichten nach dem BSIG und nach Art. 33 DSGVO in der Regel nicht zu einem Entfallen der Aufschubbefugnis. Allerdings ist auch das BSI nach § 7 Abs. 1 S. 1 Nr. 1 BSIG berechtigt, Warnungen an die Öffentlichkeit oder an die betroffenen Kreise zu richten. Enthält eine solche Warnung keinen konkreten Bezug zum IT-Sicherheitsvorfall des Emittenten, besteht keine Gefahr, dass die Geheimhaltung nicht sichergestellt werden kann. Insbesondere wenn die Warnung allerdings gem. § 7 Abs. 1 S. 1 Nr. 1 lit. c) BSIG über den Verlust von oder den unerlaubten Zugriff auf Daten informiert und insoweit ein erkennbarer Zusammenhang zu der aufgeschobenen Insiderinformation besteht, kann die Sicherstellung der Geheimhaltung im Einzelfall gefährdet sein.

48 *Klöhn* in: ders., MAR, 1. Aufl. 2018, Art. 10 Rn. 98.

Schließlich können erfolgreiche Cyberangriffe auch Auswirkungen auf die Pflicht zur Veröffentlichung anderer Insiderinformationen haben, wenn deren Veröffentlichung gem. Art. 17 Abs. 4 MAR bislang aufgeschoben wurde, der Cyberangriff allerdings zu einem Abfluss von Daten geführt hat und nicht ausgeschlossen werden kann, dass auch die Insiderinformation hiervon betroffen ist. In diesem Fall ist die Information unverzüglich zu veröffentlichen.

5. Verfahren und Inhalt der Mitteilung

Die Ad-hoc-Mitteilung muss gem. Art. 17 Abs. 1 UAbs. 1 MAR unverzüglich, d.h. ohne schuldhaftes Zögern,[49] erfolgen. Dies erfordert, dass der Emittent alle erforderlichen und zumutbaren Vorkehrungen trifft, um die Information zu erkennen, ggf. den Sachverhalt weiter aufzuklären und die Information weiterzuleiten sowie zu analysieren und zu veröffentlichen.[50] Die Berücksichtigung einer Frist auch für die weitere Aufklärung der Information ist nicht gleichzusetzen mit der Möglichkeit, den Sachverhalt zunächst „auszuermitteln". Denn der Emittent muss auch das Interesse des Marktes an einer zügigen Veröffentlichung berücksichtigen. Er muss abwägen, ob der Nutzen, den er von der weiteren Ermittlung für den Kapitalmarkt erwartet, das Interesse des Marktes an der Veröffentlichung der Information in der aktuellen Form überwiegt.[51]

Der Inhalt der Mitteilung ergibt sich aus Art. 17 Abs. 1 UAbs. 2 MAR i.V.m. Art. 2 Abs. 1 lit. b) VO (EU) 2016/1055 und § 26 Abs. 4 WpHG i.V.m. § 4 WpAV. Erforderlich sind sowohl Angaben zum Emittenten als auch zur Insiderinformation. Weitere Erläuterungen finden sich im Modul C des Emittentenleitfaden der BaFin.[52] Die Information muss gem. Art. 2, 3 VO (EU) 2016/1055 über öffentlich zugängliche Medien verbreitet werden. Sind die Wertpapiere zum Handel an einem geregelten Markt zugelassen, ist die Information in einem amtlich bestellten System zu veröffentlichen.

---

49 *Klöhn* in: ders., MAR, 1. Aufl. 2018, Art. 17 Rn. 116. Für ein objektives, nicht an § 121 BGB angelehntes Verständnis: *Kumpan/Schmidt* in: Schwark/Zimmer, Kapitalmarktrechts-Kommentar, 5. Aufl. 2020, Art. 17 MAR Rn. 72.

50 ESMA/2016/162 Rn. 64, 67; *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 129; *Klöhn* in: ders., MAR, 1. Aufl. 2018, Art. 17 Rn. 116 ff.

51 *Klöhn* in: ders., MAR, 1. Aufl. 2018, Art. 17 Rn. 125.

52 Emittentenleitfaden, Modul C, Stand: 25.03.2020, S. 43 ff.

Nach der Veröffentlichung ist der Emittent nicht verpflichtet, die Ad-hoc-Mitteilung zu aktualisieren, es sei denn, der neu eingetretene Umstand erfüllt für sich genommen den Tatbestand einer Insiderinformation.[53] Ist die Information hingegen so unvollständig oder fehlerhaft veröffentlicht worden, dass die Bewertung der Information durch den Kapitalmarkt beeinträchtigt wird, besteht eine Pflicht des Emittenten, die Ad-hoc-Mitteilung nach Maßgabe von § 4 Abs. 3 WpAV zu korrigieren.[54]

6. Sanktionen

Die in Betracht kommenden Sanktionen bei Verstößen gegen die Pflicht zur Veröffentlichung von Insiderinformationen sind mannigfaltig. Eine Strafbarkeit kommt grundsätzlich nur bei gleichzeitigem Verstoß gegen das Verbot der Marktmanipulation in Betracht (§ 119 Abs. 1 WpHG).[55] Allerdings können nach § 120 Abs. 15 Nr. 6–11, Abs. 18 WpHG Bußgelder[56] von bis zu einer Million Euro, gegenüber juristischen Personen dem höheren der Beträge von bis zu zweieinhalb Millionen Euro oder bis zu 2 Prozent des Gesamtumsatzes verhängt werden. Zudem kann der Verstoß nach § 120 Abs. 18 S. 3, 4 WpHG mit dem dreifachen des geschätzten gezogenen wirtschaftlichen Vorteils geahndet werden.[57] Die Bußgeldandrohung richtet sich sowohl an die Leitung des Emittenten als auch an den Emittenten selbst. Schließlich ist auch auf die Bekanntmachung von Sanktionen (sog. *naming and shaming*) und auf die zivilrechtliche Haftung des Emittenten aus §§ 97, 98 WpHG und aus § 826 BGB hinzuweisen.[58]

---

53 Emittentenleitfaden, Modul C, Stand: 25.03.2020, S. 46; *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 179.

54 Emittentenleitfaden, Modul C, Stand: 25.03.2020, S. 46; *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 182.

55 *Rönnau/Wegner* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 28.

56 *Rönnau/Wegner* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 29.

57 S. auch BaFin, WpHG, Bußgeldleitlinien II, Stand: Februar 2017.

58 *Wolf/Wink* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 30.

V. Schlussfolgerungen

Cyberangriffe können diverse Offenlegungspflichten auslösen. Diese sind inhaltlich nicht deckungsgleich, da sie unterschiedliche Regelungszwecke verfolgen, haben aber eine gemeinsame Schnittmenge. Insbesondere nach Zustimmung des Bundesrates zum geänderten IT-Sicherheitsgesetz steigt die Wahrscheinlichkeit für ein börsennotiertes Unternehmen, sowohl einer Publizitätspflicht nach Art. 17 MAR als auch nach § 8f BSIG zu unterliegen, deutlich. Sind von dem Ereignis personenbezogene Daten betroffen, greifen zudem die Vorgaben der DSGVO.

Jedenfalls aus kapitalmarktrechtlicher Perspektive besteht keine aufsichtsrechtliche Pflicht, eine Compliance-Organisation zu etablieren, um die Ad-hoc-Publizitätspflicht zu erfüllen.[59] Allerdings lässt sich jedenfalls aus gesellschaftsrechtlicher Perspektive für alle der diskutierten Offenlegungspflichten aus der Legalitätspflicht der Geschäftsleitung die Pflicht ableiten, Vorkehrungen zu treffen, potentiell offenlegungspflichtige Informationen zu erkennen, zu bewerten und entsprechend der jeweiligen Offenlegungspflicht zu veröffentlichen.[60] Zu diesem Zweck bietet es sich an, die für die Erfüllung aller Offenlegungspflichten erforderlichen Informationen zentral zusammenzustellen und den jeweils für die Erfüllung der Offenlegungspflichten zuständigen Personen regelbasiert zur Verfügung zu stellen.

59 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 25.

60 *Veil/Brüggemeier* in: Meyer/Veil/Rönnau, Hdb. Marktmissbrauchsrecht, 1. Aufl. 2018, § 10 Rn. 26.