Bundesnetzagentur

Meldekonzept

für die Mitteilung von beträchtlichen Sicherheitsvorfällen nach § 168 TKG

Stand 28.02.2022
Referat 217
Bundesnetzagentur

Inhaltsverzeichnis

1 Regelungsgegenstand 4

2 Pflichtadressat 4

3 Meldegegenstand 4

4 Mitteilungsinhalt 8

5 Verfahrensablauf 8

6 Vertraulichkeit der Mitteilung 11

7 Verschlüsselte Übertragung 11

8 Datennutzung 11

9 Weiterführende Pflichten 12

Einleitung

Mit der Veröffentlichung der Richtlinie (EU) 2018/1972 des Europäischen Parlamentes und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (EKEK)[1] wird der europäische Rechtsrahmen für den Bereich der Telekommunikation von 2009[2] umfangreich überabeitet und an die neuen Bedingungen des Telekommunikationssektors angepasst. Aufgrund der zunehmenden Bedeutung der elektronischen Kommunikation in sämtlichen Bereichen des wirtschaftlichen und gesellschaftlichen Lebens ist auch die Sicherstellung der Sicherheit von Netzen und Diensten wesentliche Zielsetzung des EKEK, vgl. Art. 3 Abs. 2 lit. d EKEK.

Das Gesetz zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation und zur Modernisierung des Telekommunikationsrechts, setzt die europarechtlichen Vorgaben in nationalem Recht um. Das neue TKG ist am 01.12.2021 in Kraft getreten. Mit Umsetzung europarechtlicher Vorschriften wird im TKG der Bereich der öffentlichen Sicherheit aktualisiert und weiterentwickelt. Im Zuge dieser Entwicklungen wird die „Mitteilung- und Informationspflicht“ des bisherigen § 109 Abs. 5 TKG a.F. in § 168 TKG fortgeschrieben, präzisiert und erweitert.

Vor diesem Hintergrund war das bisherige Verfahren für die Mitteilung beträchtlicher Sicherheitsvorfälle zu überarbeiten und anzupassen.

[1] ABl. Nr. L321 v. 17.12.2018, S. 36.

[2] Richtlinie 2009/140/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und –dienste, der Richtlinie 2002/19/EG über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung und der Richtlinie 2002/20/EG über die Genehmigung elektronischer Kommunikationsnetze und –dienste, ABl. Nr. L337 v. 18.12.2009, S. 37.

1 Regelungsgegenstand

Regelungsgegenstand sind Sicherheitsvorfälle nach § 168 TKG. Das Verfahren betrifft anlassbezogene Mitteilungen der pflichtigen Telekommunikationsunternehmen an die national zuständigen Behörden. Rechtsgrundlage des nationalen Meldeverfahrens ist § 168 Abs. 1 bis 4 TKG.

Die aus dem nationalen Meldeverfahren gewonnenen Daten werden im Rahmen des länderübergreifenden Ad-hoc Meldeverfahrens zwischen den national zuständigen Behörden der EU-Mitgliedsstaaten und der Agentur der Europäischen Union für Cybersicherheit (ENISA) ausgetauscht. Die rechtlichen Grundlagen dieses Verfahrens ergeben sich aus § 168 Abs. 5 TKG.

2 Pflichtadressat

Adressaten der Mitteilungspflicht gem. § 168 Abs. 1 TKG sind Betreiber öffentlicher Telekommunikationsnetze und Erbringer öffentlich zugänglicher Telekommunikationsdienste. Wesentlich ist hier, dass sich der Kreis der Pflichtadressaten mit dem TKG um die nummernunabhängigen Dienste erweitert hat. Die Ausdehnung des Pflichtadressaten trägt dem Umstand Rechnung, dass es für den Nutzer unerheblich ist, ob der von ihm genutzte Dienst einen Nummernbezug hat.[3] Im Einzelnen ist dem Telekommunikationsdienst nach § 3 Nr. 61 TKG nunmehr der Erbringer von 1. Internetzugangsdiensten, 2. interpersoneller Telekommunikationsdienst und 3. Diensten zu Signalübertragung zuzuordnen.

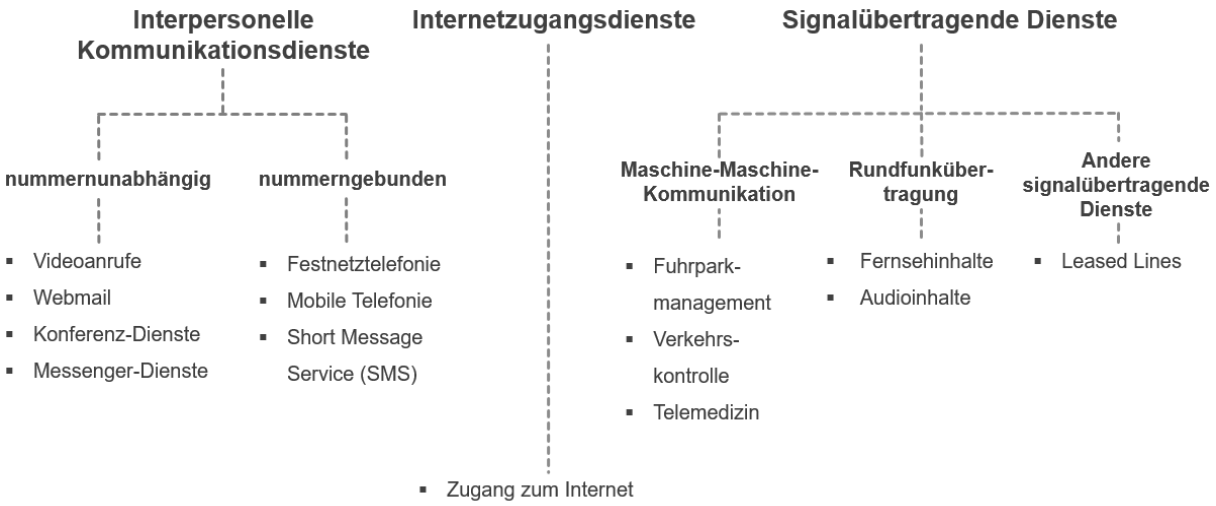

Abbildung 1: ENISA (2021) Technical Guideline on Incident Reporting, S. 11 (übersetzt)

3 Meldegegenstand

Der Mitteilungspflicht unterliegen Sicherheitsvorfälle mit beträchtlichen Auswirkungen auf den Netzbetrieb oder die Diensterbringung.

3.1 Sicherheitsvorfall

Unter einem „Sicherheitsvorfall“ ist ein Ereignis mit nachteiliger Wirkung auf die Sicherheit von Telekommunikationsnetzen oder –diensten (§ 3 Nr. 53 TKG) zu verstehen. Sicherheitsrelevant in diesem Sinn sind Vorfälle, welche die Vertraulichkeit, Authentizität, Integrität und Verfügbarkeit von Netzwerken Diensten beeinträchtigen, sowie über diese zugänglich gemachte Dienste und darüber gespeicherten, übermittelten oder verarbeiteten Daten betreffen.[4]

[3] vgl. EG 15 RL (EU) 2018/1972; BR-Drs. 29/21, S. 267.

[4] vgl. Art. 40 EKEK, ENISA (2021) Technical Guideline on Incident Reporting, S. 11, § 3 Nr. 52 TKG.

3.2 Auswirkungen

Nicht jeder Sicherheitsvorfall ist mitteilungsrelevant. Eine Pflicht zur Mitteilung nach § 168 Abs. 1 TKG entsteht erst ab einer gewissen Beträchtlichkeit. Die europäischen Vorgaben bzw. ihre nationale Umsetzung im TKG haben in dieser Hinsicht mit der Normierung bestimmter Bewertungskriterien nachgebessert.

Die Bewertung der Auswirkungen des Sicherheitsvorfalls hat somit anhand der Kriterien nach § 168 Abs. 2 Nr. 1 bis 5 TKG zu erfolgen, zumindest soweit diese im konkreten Einzelfall verfügbar sind[5]. Die aufgeführten Kriterien sind jedoch nicht abschließend. Die eigenverantwortliche Bewertung des Vorfalls durch den Pflichtadressaten kann weitere Kriterien berücksichtigen, sofern diese zur Einschätzung der Sicherheitsrelevanz im o.a. Sinne geeignet sind. Neben der gesetzlich vorgeschriebenen Mitteilungspflicht wird auch eine Abgabe von freiwilligen Mitteilungen und das damit einhergehende Engagement der mitteilenden Betreiber von Telekommunikationsnetzen oder Erbringer von Telekommunikationsdiensten begrüßt.

Im Einzelnen zu den ausdrücklich normierten Bewertungskriterien des § 168 Abs. 2 TKG:

3.2.1 Zahl der von dem Sicherheitsvorfall betroffenen Nutzer

Unter Rückgriff auf § 3 Nr. 41 TKG ist unter „Nutzer“ in diesem Sinn jede natürliche oder juristische Person zu verstehen, im Wirkungsbereich der Beeinträchtigung, die einen öffentlich zugänglichen Telekommunikationsdienst für private oder geschäftliche Zwecke in Anspruch nimmt oder beantragt.

3.2.2 Dauer des Sicherheitsvorfalls

Die Zeit, die ein Sicherheitsvorfall andauert, sollte – soweit möglich oder ggf. rekonstruierbar – ab dem tatsächlichen Eintritt eines Sicherheitsvorfalls beginnen. Ansonsten soll der Zeitpunkt der Kenntnisnahme als Beginn des Sicherheitsvorfalls angenommen werden. Das Ende eines Sicherheitsvorfalls soll an dessen vollständige Behebung anknüpfen. Der Sicherheitsvorfall endet somit zeitlich nach Abschluss der letzten Maßnahme.[6]

3.2.3 Geographische Ausdehnung

Zur Beurteilung der geographischen Reichweite eines Sicherheitsvorfalls führt die ENISA bestimmte Indikatoren an. Genannt werden beispielsweise die Grenzüberschreitung eines Sicherheitsvorfalls, die Größe eines betroffenen Gebietes sowie die Frage, ob es sich hierbei um ländliche Gebiete, Inseln oder ganze Hauptstädte handelt. Genannt wird als Indikator auch die Betroffenheit internationaler Zusammenschaltungen.[7] Deskriptiv kann das entsprechende Feld des Mitteilungsformulars die Anzahl der betroffenen km² oder Basisstationen aufführen sowie möglichst internationale Zusammenschaltungen benennen. Betroffenen Städte, Regionen oder Bundesland/Bundesländer sollen möglichst ausdrücklich benannt werden.

3.2.4 Beeinträchtigung des Telekommunikationsnetzes oder des Dienstes

Die Auswirkungen auf Telekommunikationsnetze oder Dienste sollten möglichst anhand der Bedeutung bestimmter Komponenten und Systeme, der Anzahl oder prozentuale Betroffenheit von Telekommunikationsnetzen und –diensten gemessen und möglichst beziffert werden. Auch eine Verminderung der Servicequalität kann als ein Indikator für eine Beeinträchtigung des Telekommunikationsnetzes oder -dienstes herangezogen werden.[8] Das Mitteilungsformular lässt hierbei die Möglichkeit der Angabe von betroffenen Netzabschnitten und Netzschnittstellen sowie betroffener Festnetz- oder Mobilfunkdiensten und weitere Abgrenzungen zu.

---

5 vgl. Art. 40 Abs. 2 EKEK; BR Drs 29/21 S. 429.

6 vgl. ENISA (2016) Security incidents indicators – measuring the impact of incidents affecting electronic communications, S. 25 ff.

7 vgl. ENISA (2021) Technical Guideline on Incident Reporting, S. 21.

8 vgl. ENISA (2016) Security incidents indicators – measuring the impact of incidents affecting electronic communications, S. 42.

3.2.5 Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten

Die wirtschaftlichen und gesellschaftlichen Konsequenzen eines Sicherheitsvorfalls können u.a. anhand von Auswirkungen auf die Notruflenkung, internationale Zusammenschaltungen, außergewöhnlicher IT-Störungen oder öffentlicher Warnsysteme gemessen werden. Ferner können entstandene Gefahren für die öffentliche Sicherheit und Ordnung, ein materieller oder immaterieller Verlust (Produktivitätseinbußen, Rufschädigung) oder eine Berichterstattung in den Medien als Indikatoren herangezogen werden. Die Besonderheit einer betroffenen Person (z.B. Politiker) oder eines Unternehmens (z.B. Banken), eines Zeitpunktes (z.B. Wahl), Sektoren oder betroffene Tätigkeiten in/für die Gesellschaft (z.B. Ministerien, staatliche Einrichtung) können ebenfalls von Bedeutung sein.[9]

3.3 Schwellenwerte

Unter Rückgriff auf die bisherige nationale Mitteilungspraxis und in Anlehnung an den „Technical Guideline on Incident Reporting under the EECC“ vom März 2021 der ENISA sollen nachfolgende Schwellenwerte als Anhaltspunkt gelten:

3.3.1 Anzahl betroffener Nutzer

Die Anzahl der betroffenen Nutzer ergibt sich aus der Anzahl aller natürlichen oder juristischen Personen im Wirkbereich des Sicherheitsvorfalls. Nutzer ist jede natürliche oder juristische Person, die einen öffentlichen zugänglichen Telekommunikationsdienst für private oder geschäftliche Zwecke in Anspruch nimmt oder beantragt.

3.3.2 Ausfalldauer und betroffene Nutzerstunden

Aufgrund des direkten Bezuges bietet es sich an eine Kumulation der Kriterien aus § 168 Abs. 2 Nr. 1 TKG (Anzahl der betroffenen Nutzer) und § 168 Abs. 2 Nr. 2 TKG (Dauer eines Sicherheitsvorfalls) anzunehmen und ein Schwellenwert aus dem Produkt beider Kriterien festzulegen:

> Ein Sicherheitsvorfall ist beträchtlich, wenn bei dem Kriterium „Betroffene Nutzerstunden“ der Schwellwert von 1 Million Nutzerstunden überschritten wird.

[9] vgl. ENISA (2021) Technical Guideline on Incident Reporting, S.21 f.

3.3.3 Internationale Zusammenschaltungen

Zu berücksichtigen sind grundsätzlich die von der ENISA genannten Indikatoren (s.o.). Eine besondere Bedeutung erlangen jedoch Sicherheitsvorfälle mit grenzüberschreitenden Auswirkungen. Sowohl die europarechtlichen Vorgaben als auch der § 168 Abs. 5 S. 1 TKG beschreiben überdies ein eigenes Meldeverfahren. Der Technical Guideline on Incident Reporting der ENISA konkretisiert Sicherheitsvorfälle mit länderübergreifenden Auswirkungen.
Jeglicher Sicherheitsvorfall, welchen eine Grenzüberschreitung kennzeichnet, wird als melderelevant eingestuft.[10] Betrachtet werden exemplarisch Auswirkungen eines Sicherheitsvorfalls auf die internationalen Zusammenschaltungen (Interconnection). Unter einer Zusammenschaltung in diesem Sinn wird gem. § 3 Nr. 79 TKG der Zugang verstanden, der die physische und logische Verbindung öffentlicher Telekommunikationsnetze herstellt, um Teilnehmern eines Unternehmens die Kommunikation mit Teilnehmern desselben oder eines anderen Unternehmens oder die Inanspruchnahme von Telekommunikationsdiensten eines anderen Unternehmens zu ermöglichen. Der hier betrachtete Zugang beschränkt sich auf Zusammenschaltungspunkte mit internationaler Ausprägung.

Jeglicher Sicherheitsvorfall zum Kriterium „Zusammenschaltungspunkte mit internationaler Ausprägung“ ist beträchtlich.

3.3.4 Notruflenkung

Eine besondere Bedeutung hat in dieser Hinsicht die Auswirkung auf die Notruflenkung. Entscheidend ist in dieser Hinsicht nicht die Funktionalität eines Telekommunikations- und Datenverarbeitungssystems der Nutzer, sondern die Hard- und/oder Software, die dediziert zur Notruflenkung benötigt wird. Erfasst ist auch der Anschluss einer Notrufabfragestelle an ein Telekommunikationsnetz, der je nach technischer Ausgestaltung ausschließlich für die Entgegennahme von Notrufverbindungen genutzt wird einschließlich der zugehörigen Daten oder der den Notruf begleitenden Daten.

Jeglicher Sicherheitsvorfall zum Kriterium „Notruflenkung“ ist beträchtlich.

3.3.5 Außergewöhnliche IT-Störung

Das Kriterium der außergewöhnlichen IT-Störung ist keinem, der im Gesetz aufgelisteten Kriterien, zuzuordnen. Dennoch kann es bei der Bewertung von beträchtlichen Auswirkungen auf den Betrieb der Netze oder die Erbringung der Dienste als Indikator und Schwellenwert herangezogen werden. Betreiber öffentlicher Telekommunikationsnetze oder Erbringer öffentlich zugänglicher Telekommunikationsdienste, welche unter die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSIG) vom 21.06.2017 (Anhang 4) fallen, müssen dann eine Mitteilung abgeben, wenn

- die Ursache der Beeinträchtigung außergewöhnlich oder zum Zeitpunkt der Mitteilung nicht nachvollziehbar ist und
- die Beeinträchtigung nicht mehr im Rahmen des Tagesgeschäfts durch übliche Maßnahmen bewältigt werden kann (es müssen ggf. zusätzliche deutlich erhöhte Ressourcen eingesetzt werden).

[10] vgl. ENISA (2021) Technical Guideline on Incident Reporting, S. 17.

Eine Ursache ist außergewöhnlich, wenn sie

- (z. B. als Folge von Softwareupdates oder Systemfehlern) zu einer unerwarteten Beeinträchtigung führt oder
- auf einen nicht alltäglichen technischen Angriff zurückzuführen ist (z.B. ungewöhnlicher (D)DoS-Angriff aufgrund der Bandbreite bzw. Vorgehensweise oder Ausnutzung einer neuen, bisher nicht veröffentlichten Sicherheitslücke).

Jeglicher Sicherheitsvorfall zum Kriterium „außergewöhnliche IT-Störung“ ist beträchtlich.

4 Mitteilungsinhalt

§ 168 Abs. 3 TKG präzisiert den Inhalt einer Mitteilung. Demnach muss eine Mitteilung nach Abs. 1 mindestens folgende Angaben enthalten:

1. Angaben zu dem Sicherheitsvorfall,
2. Angaben zu den Kriterien nach Abs. 2,
3. Angaben zu den betroffenen Systemen sowie
4. Angaben zu der vermuteten oder tatsächlichen Ursache.

Hierzu wird von der Bundesnetzagentur (BNetzA) ein entsprechendes Mitteilungsformular vorgehalten.

§ 168 Abs. 3 Nr. 1 TKG beschreibt in erster Linie allgemeine Informationen eines Sicherheitsvorfalls, z.B. Angaben des mitteilenden Unternehmens, Datum und Uhrzeit und ob es sich um eine initiale Kurzmitteilung oder eine vollständige Mitteilung handelt. Entsprechende Angaben können im Mitteilungsformular der BNetzA ausgeführt werden. Das genannte Mitteilungsformular enthält ferner weitere Felder, welche der Beschreibung der Auswirkungen zu den Kriterien nach Abs. 2 sowie Angaben zu betroffenen Systemen erheben sollen.

Ein weiterer Bestandteil einer Mitteilung ist gem. § 168 Abs. 3 Nr. 4 TKG ist die Angabe der vermuteten oder tatsächlichen Ursache. Aufgrund der Vielzahl von theoretisch möglichen Ursachen ist es jedoch praktisch unmöglich, diese in einer allumfassenden Tabelle abzubilden. Dennoch ist es für die Analyse, die Bewertung und zur Behebung der mitteilungspflichtigen Beeinträchtigung unerlässlich, die festgestellte oder vermutete Ursache möglichst zu identifizieren und entsprechend darzulegen.

Zudem bietet das Mitteilungsformular die Möglichkeit, bereits Angaben zu ergriffenen Abhilfemaßnahmen zu erläutern. Die BNetzA kann gem. § 168 Abs. 4 S. 2 TKG einen detaillierten Bericht über den Sicherheitsvorfall und die ergriffenen Abhilfemaßnahmen verlangen.

5 Verfahrensablauf

Nachfolgend werden bezüglich einer Mitteilung nach § 168 TKG der Verfahrensablauf, insbesondere der Zeitpunkt der Mitteilung, die Mitteilungsformen sowie die Vertraulichkeit und der Umgang mit einer Mitteilung, beschrieben.

5.1 Feststellung des Sicherheitsvorfalls

Die Feststellung eines Sicherheitsvorfalls nach § 168 Abs. 1 TKG hat der Verpflichtete in geeigneter Weise sicherzustellen. Werden Dritte für die Sicherstellung der Feststellung in Anspruch genommen, so bleibt der Verpflichtete nach wie vor primär verantwortlich. Werden Anhaltspunkte für einen Sicherheitsvorfall mit beträchtlichen Auswirkungen auf den Betrieb der Netze oder die Erbringung der Dienste festgestellt, so hat der Verpflichtete zunächst in eigener Verantwortung und unter Berücksichtigung insbesondere der Kriterien nach § 168 Abs. 2 TKG zu bewerten, ob diese tatsächlichen oder möglichen Auswirkungen auf den Betrieb der Netze oder die Erbringung der Dienste beträchtlich sind oder nicht.

5.2 Unverzügliche Mitteilung

Die pflichtigen Unternehmen haben den jeweiligen Sicherheitsvorfall der Bundesnetzagentur und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) unverzüglich mitzuteilen. Die Mitteilung hat daher „ohne schuldhaftes Zögern“ (§ 121 BGB) zu erfolgen. Angezeigt ist eine Übermittlung nach diesen Maßstäben grundsätzlich dann, wenn eine entsprechende Kenntnislage vorliegt und weiteres Zuwarten nach den Umständen des Einzelfalles nicht geboten ist. Führen Mängel in der Organisation zu einer Verzögerung, so gehen diese Umstände zu Lasten des Mitteilungspflichtigen.

Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste mit erhöhtem Gefährdungspotenzial (§ 167 Abs. 1 Nr. 3 TKG) stellen sicher, dass der BNetzA und dem BSI unverzüglich, in jedem Fall aber innerhalb von 3 Stunden nach Kenntnisnahme des Sicherheitsvorfalls, eine erste Meldung als Frühwarnung, zukommt. In dieser Frühwarnmeldung ist anzugeben, ob der Sicherheitsvorfall vermutlich auf rechtswidrige oder böswillige Handlungen zurückzuführen ist.
Kann nur eine erste Meldung als Frühwarnmeldung abgegeben werden, so soll in der Folge ein Zwischenbericht über relevante Statusaktualisierungen abgegeben werden. Der Zwischenbericht hat mindestens folgenden Inhalt:

- eine Aktualisierung der Beschreibung des Sicherheitsvorfalls;
- Erkenntnisse zu seinem Schweregrad und seinen möglichen Auswirkungen;
- Erkenntnisse zur Art der Bedrohung bzw. zugrundeliegenden Ursache, die den Sicherheitsvorfall wahrscheinlich ausgelöst hat;
- Angaben zu den getroffenen und laufenden Abhilfemaßnahmen.

Unverzüglich nach der vollständigen Behebung des Sicherheitsvorfalls, spätestens jedoch drei Tage nach der vollständigen Behebung des Sicherheitsvorfalles, ist ein Abschlussbericht vorzulegen. Der Abschlussbericht hat mindestens folgenden Inhalt:

- eine ausführliche Beschreibung des Sicherheitsvorfalls, seines Schweregrads und seiner Auswirkungen;
- Angaben zur Art der Bedrohung bzw. zugrundeliegenden Ursache, die den Sicherheitsvorfall wahrscheinlich ausgelöst hat;
- Angaben zu den getroffenen und laufenden Abhilfemaßnahmen.

Im Einvernehmen mit der BNetzA und dem BSI kann im Einzelfall von den festgelegten Fristen abgewichen werden. Ein Abweichen kann insbesondere gerechtfertigt sein, wenn der Vorfall noch andauert und vorhandene Ressourcen zur Schadensbehebung benötigt werden.

Nicht rechtzeitige Mitteilungen sind gem. § 228 Abs. 1 Nr. 39 TKG bußgeldbewehrt. Zur Entgegennahme von Sicherheitsvorfällen nach § 168 TKG wurde bereits bei der BNetzA ein ständiger Bereitschaftsdienst eingerichtet. Dieser Dienst zur Entgegennahme und Bearbeitung der Mitteilungen wird auch nach Modifizierung der Meldepflicht fortgeführt.[11]

[11] vgl. BT-Drs. 17/5707, S. 83.

5.3 Mitteilungswege

Können im Rahmen dieser unverzüglichen Mitteilung noch nicht alle erforderlichen Angaben nach § 168 Abs. 3 TKG zur Beeinträchtigung eines Telekommunikationsnetzes oder -dienstes gemacht werden, ist eine initiale Kurzmitteilung als Erstmeldung vorzusehen und im Formular entsprechend kenntlich zu machen. Sobald weitere mitteilungsrelevante Informationen vorliegen, sind diese unter Nutzung des Mitteilungsformulars nachzureichen. Im Zweifelsfall ist eine Mitteilung nachrangig gegenüber der Eindämmung der akuten Folgen der Beeinträchtigung eines Telekommunikationsnetzes oder -dienstes. Nachfolgend werden die Mitteilungsformen beschrieben.

5.3.1 Initiale Kurzmitteilung

Die initiale Kurzmitteilung kann aus Zeitmangel oder auf Grund eines unvollständigen Informationsstands auf die bereits vorliegenden Informationen zum mitteilungspflichtigen Sicherheitsvorfall beschränkt werden.

Es sind soweit bekannt folgende Angaben zu machen:

- Kontaktdaten des Mitteilenden,
- Information darüber, was nach ersten Erkenntnissen vorgefallen ist,
- Eintritt der Beeinträchtigung(en) von Telekommunikationsnetzen und -diensten gem. § 168 TKG (Datum und Zeit),
- erste Einschätzung der Auswirkungen unter Überschrift 2 sowie den Schwellenwerten unter Überschrift 3 sowie
- mögliche Ursache(n).

Die vollständige Mitteilung mit den ausstehenden Angaben ist zu einem späteren Zeitpunkt nachzureichen.

5.3.2 Vollständige Mitteilung

Sollten bereits sämtliche, für den Sicherheitsvorfall relevanten Informationen vorliegen, ist unverzüglich eine vollständige Mitteilung des Sicherheitsvorfalls vorzunehmen.

5.3.3 Detaillierter Bericht

Die BNetzA kann über die o.a. Mitteilung hinaus einen detaillierten Bericht über den Sicherheitsvorfall und die ergriffenen Abhilfemaßnahmen verlangen, sofern dies im Einzelfall erforderlich sein sollte.

5.3.4 Mitteilungsmodalität und –adresse

Zur strukturierten Erhebung mitteilungsrelevanter Informationen wird ein Mitteilungsformular von der BNetzA bereitgestellt. Dieses ist

per E-Mail an	die BNetzA und sicherheitsvorfall.tkg@bnetza.de	das BSI Meldungen-tkg@bsi.bund.de
	oder alternativ	
per Telefax an	(0681) 9330 775 und	(0228) 9910 9582 6171

zu übersenden.

Die Eilbedürftigkeit der Mitteilung gebietet grundsätzlich die Wahl der vorstehenden Übermittlungswege. Können Gründe der Eilbedürftigkeit ausgeräumt werden, so ist grundsätzlich auch ein Versand per Post an die nachstehend genannte Anschrift möglich:

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
Referat 217
An der Trift 40
66123 Saarbrücken.

6 Vertraulichkeit der Mitteilung

Nach § 168 Abs. 6 S. 2 TKG ist im Rahmen des Meldeverfahrens § 8e BSIG entsprechend anzuwenden. Die Vorschrift regelt das Auskunftsrecht Dritter, nicht am Meldeverfahren Beteiligter oder nichtöffentlicher Institutionen zu mitteilungspflichtigen Informationen.

Der Zugang zu Informationen ist demnach zu verneinen, sofern schutzwürdige Interessen der mitteilungspflichtigen Unternehmen an einer vertraulichen Behandlung sowie die Verletzung wesentlicher Sicherheitsinteressen anzunehmen sind. Die Zuordnung eines Betreibers zu einem Sicherheitsvorfall stellt ein schutzwürdiges wirtschaftliches Interesse in diesem Sinn dar. Ein Zugang zu personenbezogenen Daten wird ebenfalls grundsätzlich abgelehnt.[12]

7 Verschlüsselte Übertragung

Bei Übermittlung einer Mitteilung per E-Mail durch den Verpflichteten an die oben angegebene Adresse wird von der BNetzA empfohlen, ein sicheres Übermittlungsverfahren anzuwenden. Das von der BNetzA hierzu bereitgestellte Verfahren ist auf der Internetseite der BNetzA unter folgendem Link ersichtlich:

https://www.bundesnetzagentur.de/sicherheitsvorfall

Zur elektronischen Übermittlung von Sicherheitsvorfällen stellt die BNetzA und das BSI einen öffentlichen PGP-Schlüssel zur Verfügung, um die Nachricht als E-Mail verschlüsselt zu übertragen.

Der öffentliche PGP-Schlüssel der BNetzA wird unter folgendem Link als Textdatei zum Download bereitgestellt:

https://www.bundesnetzagentur.de/sicherheitsvorfall

Der öffentliche PGP-Schlüssel des BSI wird unter folgendem Link als Textdatei zum Download bereitgestellt:

https://bsi.bund.de/FAQ-Meldepflicht-IT-SiG

8 Datennutzung

Die mitgeteilten Daten fließen in eine Datenbank und sind Grundlage für die europäischen Meldeverfahren.[13] Auf Grundlage der eingegangenen Mitteilung bewertet die BNetzA diese und behält sich vor, falls erforderlich, weitere Auskünfte in einem detaillierten Bericht gem. §168 Abs. 4 S. 2 TKG einzuholen und in eigenem Ermessen eine Einstufung nach § 168 TKG vorzunehmen. Das betroffene Unternehmen wird darüber in Kenntnis gesetzt.

Das Melden eines Sicherheitsvorfalls mit grenzüberschreitendem Charakter an die nationalen Regulierungsbehörden der anderen Mitgliedstaaten der Europäischen Union und die ENISA im Rahmen des länderübergreifendes Ad-hoc Meldeverfahrens erfolgt im Ermessen der BNetzA. Dies umfasst sowohl die Entscheidung der Meldung selbst, als auch eine Beurteilung der Relevanz bestimmter Informationen.[14]

[12] vgl. BT-Drs. 18/4096, S. 30.
[13] vgl. unter Regelungsgegenstand die Verfahren der lfd. Nr. 2 und 3.
[14] vgl. ENISA (2021) Technical Guideline on Incident Reporting, S. 17.

Gelangt die BNetzA zu dem Ergebnis, dass eine Bekanntgabe des Sicherheitsvorfalls im öffentlichen Interesse liegt, so kann sie selbst die Öffentlichkeit informieren oder den Verpflichteten nach Abs. 1 zur Unterrichtung verpflichten gem. § 168 Abs. 5 S. 2 TKG.
Der Jahresbericht gem. § 168 Abs. 7 TKG über die eingegangenen Mitteilungen und die ergriffenen Abhilfemaßnahmen wird von der BNetzA in anonymisierter Form an die Europäische Kommission, die ENISA und dem BSI versendet.
Die Pflicht zur Erteilung von Auskünften gegenüber der BNetzA nach § 190 Abs. 1 S. 2 TKG bleibt hiervon unberührt.

9 Weiterführende Pflichten

Unberührt von der vorliegenden Mitteilungspflicht ist die mit dem § 168 Abs. 6 TKG neu eingeführte Informationspflicht gegenüber dem Nutzer. Im Falle einer besonderen und erheblichen Gefahr eines Sicherheitsvorfalls informieren die verpflichteten Unternehmen die von einer Gefahr potenziell betroffenen Nutzer über alle möglichen Schutz- oder Abhilfemaßnahmen, die von ihnen ergriffen werden können. Gegebenenfalls ist auch über die Gefahr selbst zu informieren