Bundesnetzagentur

Meldekonzept

28. Februar 2022

Für die Meldung von erheblichen Sicherheitsvorfällen nach § 168 TKG

1. 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] wurde 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. Mit Umsetzung europarechtlicher Vorschriften wird im TKG der Bereich der öffentlichen Sicherheit aktualisiert und weiterentwickelt.

Dieses Meldekonzept orientiert sich vorrangig an den Vorgaben der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022. Diese Richtlinie legt Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union fest, ändert die Verordnung (EU) Nr. 910/2014 und die Richtlinie (EU) 2018/1972 und hebt zugleich die Richtlinie (EU) 2016/1148 auf. Sie ist allgemein als NIS-2-Richtlinie bekannt.

Darüber hinaus berücksichtigt dieses Meldekonzept die Bestimmungen des auf nationaler Ebene entwickelten Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung.

[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.

Dieses Gesetz dient dabei der nationalen Umsetzung der europarechtlichen Vorschrift NIS-2-Richtlinie.

Im Rahmen des Gesetzes zur Umsetzung der NIS-2-Richtlinie hat sich das Telekommunikationsgesetz (TKG), vor allem im Hinblick auf die Verpflichtungen bezüglich des Meldens von Sicherheitsvorfällen geändert.

2. Regelungsgegenstand

Regelungsgegenstand sind Sicherheitsvorfälle nach § 168 TKG. Das Verfahren betrifft anlassbezogene Meldungen der pflichtigen Telekommunikationsunternehmen an die national zuständigen Behörden. Rechtsgrundlage des nationalen Meldeverfahrens ist § 168 Abs. 1 bis 5 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. 6 TKG.

3. Pflichtadressat

Adressaten der Meldepflicht 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 Telekommunikationsdiensten und 3. Diensten zur Signalübertragung zuzuordnen.

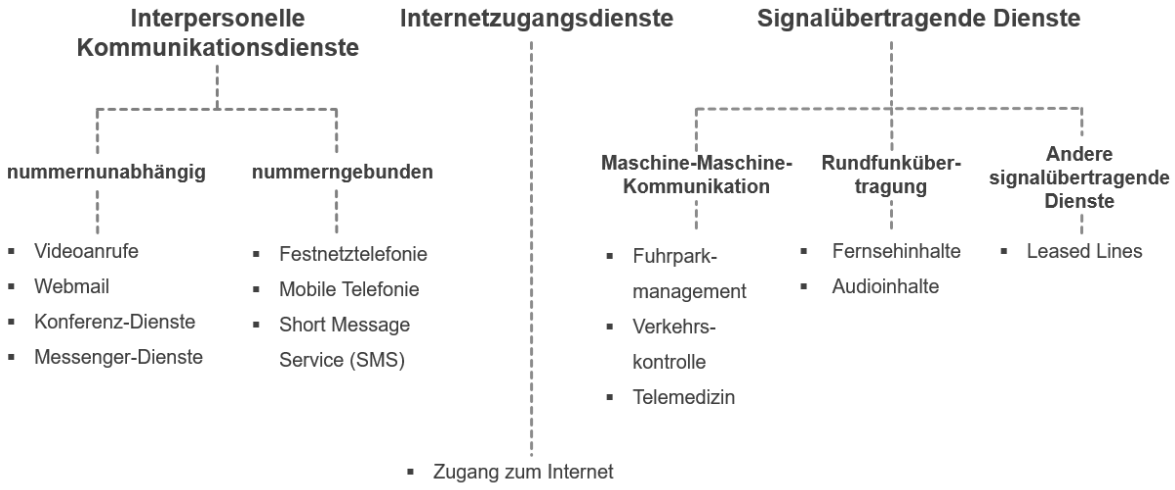

Abbildung 1: ENISA (2021) Technical Guideline on Incident Reporting, S. 11 (übersetzt)

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

4. Meldegegenstand

Der Meldepflicht unterliegen Sicherheitsvorfälle mit erheblichen Auswirkungen auf den Netzbetrieb oder die Diensterbringung.

4.1 Sicherheitsvorfall

Unter einem „Sicherheitsvorfall“ ist ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden oder zugänglich sind, beeinträchtigt (§ 3 Nr. 53 TKG).

4.2 Auswirkungen

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

Die Bewertung der Erheblichkeit eines Sicherheitsvorfalls erfolgt anhand der Kriterien nach § 168 Abs. 3 TKG. 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 Meldepflicht wird auch eine Abgabe von freiwilligen Meldungen 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. 3 TKG:

4.2.1 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.

4.2.2 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 einschließlich der Ursachenanalyse.

4.2.3 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.[4] Deskriptiv kann das entsprechende Feld des Meldeformulars die Anzahl der betroffenen km² oder Basisstationen aufführen sowie möglichst internationale Zusammenschaltungen benennen. Betroffene Städte, Regionen oder Bundesland/Bundesländer sollen möglichst ausdrücklich benannt werden.

4.2.4 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.[5] Das Meldeformular lässt hierbei die Möglichkeit der Angabe von betroffenen Netzabschnitten und Netzschnittstellen sowie betroffener Festnetz- oder Mobilfunkdienste und weitere Abgrenzungen zu.

4.2.5 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 öffentliche 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.[6]

4.3 Schwellenwerte

Unter Rückgriff auf die bisherige nationale Meldepraxis sollen nachfolgende Schwellenwerte als Anhaltspunkt gelten:

4.3.1 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.

---

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

4.3.2 Ausfalldauer und betroffene Nutzerstunden

Aufgrund des direkten Bezuges bietet es sich an, eine Kumulation der Kriterien aus Anzahl der betroffenen Nutzer und Dauer eines Sicherheitsvorfalls anzunehmen und ein Schwellenwert aus dem Produkt beider Kriterien festzulegen:

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

4.3.3 Internationale Zusammenschaltungen

Zu berücksichtigen sind grundsätzlich die von der ENISA genannten Indikatoren. Eine besondere Bedeutung erlangen jedoch Sicherheitsvorfälle mit grenzüberschreitenden Auswirkungen. Sowohl die europarechtlichen Vorgaben als auch der § 168 Abs. 6 S. 1 TKG beschreiben überdies ein eigenes Meldeverfahren.

Jeglicher Sicherheitsvorfall, welcher eine Grenzüberschreitung kennzeichnet, wird als melderelevant eingestuft. Betrachtet werden exemplarisch Auswirkungen eines Sicherheitsvorfalls auf die internationale Zusammenschaltungen (Interconnection). Unter einer Zusammenschaltung in diesem Sinn wird gem. § 3 Nr. 79 TKG ein Sonderfall des Zugangs verstanden, der zwischen Betreibern öffentlicher Telekommunikationsnetze hergestellt wird; dies mittels der physischen und logischen Verbindung öffentlicher Telekommunikationsnetze, die von demselben oder einem anderen Unternehmen genutzt werden, um Nutzern eines Unternehmens die Kommunikation mit Nutzern desselben oder eines anderen Unternehmens oder den Zugang zu den von einem anderen Unternehmen angebotenen Diensten zu ermöglichen, soweit solche Dienste von den beteiligten Parteien oder von anderen Parteien, die Zugang zum Netz haben, erbracht werden.

> Jeglicher Sicherheitsvorfall zum Kriterium „Zusammenschaltungspunkte mit internationaler Ausprägung" ist erheblich.

4.3.4 Notruflenkung

Eine besondere Bedeutung hat in dieser Hinsicht die Auswirkung auf die Notruflenkung. Entscheidend ist in diesem Zusammenhang 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 erheblich.

4.3.5 Außergewöhnliche IT-Störung

Das Kriterium der außergewöhnlichen IT-Störung ist keinem der im Gesetz aufgelisteten Kriterien zuzuordnen. Dennoch kann es bei der Bewertung von erheblichen 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) in der jeweils geltenden Fassung (Anhang 4[7]) fallen, müssen dann eine Meldung abgeben, wenn

- die Ursache der Beeinträchtigung außergewöhnlich oder zum Zeitpunkt der Meldung 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).

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 erheblich.

5. Meldeinhalt

§ 168 Abs. 1 TKG definiert den Mindestinhalt einer Meldung. Hierzu wird von der Bundesnetzagentur (BNetzA) ein entsprechendes Meldeformular bereitgestellt.

Ein weiterer Bestandteil einer Meldung gem. § 168 Abs. 1 Nr. 4 b) 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 Meldeformular 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.

[7] vgl. Anhang 4 der BSI-KritisV (zu § 1 Nummer 4 und 5, § 5 Absatz 4 Nummer 1 und 2) Anlagenkategorien und Schwellenwerte im Sektor Informationstechnik und Telekommunikation

6. Verfahrensablauf

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

6.1 Feststellung eines 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 erheblichen 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. 3 TKG zu bewerten, ob diese tatsächlichen oder möglichen Auswirkungen auf den Betrieb der Netze oder die Erbringung der Dienste erheblich sind oder nicht.

6.2 Unverzügliche Meldung

Die verpflichteten Unternehmen haben den Sicherheitsvorfall der BNetzA und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) unverzüglich zu melden. Die Meldung hat „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 Meldepflichtigen.

Nach § 168 Absatz 1 Nr. 1 ist unverzüglich, spätestens 24 Stunden nach Kenntniserlangung über den Sicherheitsvorfall, durch den Betroffenen eine frühe Erstmeldung abzugeben. Aus dieser Erstmeldung hat hervorzugehen, ob der Verdacht einer rechtswidrigen oder böswilligen Handlung besteht oder ob der Sicherheitsvorfall grenzüberschreitende Auswirkungen haben könnte.

Die Bundesnetzagentur übermittelt nach § 168 Absatz 5 TKG unverzüglich und nach Möglichkeit innerhalb von 24 Stunden eine Bestätigung über den Eingang der Meldung.

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.

Nicht rechtzeitige Meldungen sind gem. § 228 Abs. 1 Nr. 39 TKG bußgeldbewehrt.

6.3 Meldewege

Können im Rahmen dieser unverzüglichen Meldung noch nicht alle erforderlichen Angaben nach § 168 Abs. 1 Nr. 4 TKG zur Beeinträchtigung eines Telekommunikationsnetzes oder -dienstes gemacht werden, ist eine initiale Erstmeldung als Erstmeldung vorzusehen und im Formular entsprechend kenntlich zu machen. Sobald weitere meldungsrelevante Informationen vorliegen, sind diese unter Nutzung des Meldeformulars nachzureichen. Im Zweifelsfall ist eine Meldung nachrangig gegenüber der Eindämmung der akuten Folgen der Beeinträchtigung eines Telekommunikationsnetzes oder -dienstes. Nachfolgend werden die Meldeformen beschrieben.

6.3.1 Initiale Erstmeldung

Die initiale Kurzmitteilung auf Grund eines unvollständigen Informationsstands auf die bereits vorliegenden Informationen zum meldungspflichtigen Sicherheitsvorfall beschränkt werden.

Es sind soweit bekannt folgende Angaben zu machen:

- Kontaktdaten des Meldenden,
- 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 Meldung mit den ausstehenden Angaben ist zu einem späteren Zeitpunkt nachzureichen.

6.3.2 Vollständige Meldung/ Folgemeldung

Schnellstmöglich, spätestens innerhalb von 72 Stunden, ist eine vollständige Meldung abzugeben, in der die vorgenannten Informationen aktualisiert oder bestätigt werden. Im Rahmen der Ausgestaltung des Meldeverfahrens wird in diesem Meldekonzept festgelegt, dass die Meldung nach § 168 Abs. 1 Nr. 2 TKG nicht als „vollständige Meldung", sondern als „Folgemeldung" bezeichnet wird.

Zudem ist eine erste Einschätzung/Bewertung des Sicherheitsvorfalls, einschließlich seines Schweregrades und seiner Auswirkungen sowie ggf. Kompromittierungsindikatoren[8] anzugeben.

6.3.3 Abschlussmeldung

Spätestens nach einem Monat der Übermittlung des Sicherheitsvorfalls ist eine Abschlussmeldung gemäß § 168 Absatz 1 Nr. 4 TKG zu übermitteln. Diese enthält:

a) Eine ausführliche Beschreibung des erheblichen Sicherheitsvorfalls einschließlich seines Schweregrades und seiner Auswirkungen
b) Angaben zur Art der Bedrohung bzw. zugrundeliegende(n) Ursache(n), die (wahrscheinlich) den Sicherheitsvorfall ausgelöst hat
c) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen
d) Gegebenenfalls die grenzüberschreitenden Auswirkungen des erheblichen Sicherheitsvorfalls

[8] Kompromittierungsindikatoren sind digitale Spuren und Hinweise, dass ein Sicherheitsvorfall stattgefunden hat, wie bspw. ungewöhnlich hohe Netzauslastung, die nicht erklärbar ist oder Anmeldung des gleichen Nutzers in zwei völlig verschiedenen Städten zur gleichen Zeit.

6.3.4 Detaillierter Bericht

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

6.3.5. Meldungsmodalität und –adresse

Zur strukturierten Erhebung meldungsrelevanter Informationen wird ein Meldeformular von der Bundesnetzagentur bereitgestellt. Dieses ist

per E-Mail an

- die BNetzA: sicherheitsvorfall.tkg@bnetza.de
  und
- das BSI: Meldungen-tkg@bsi.bund.de

oder alternativ per Telefax an (0681) 9330 775
zu übersenden.

Die Eilbedürftigkeit der Meldung 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
Tulpenfeld 4
53113 Bonn

7. Vertraulichkeit der Meldung

Nach § 168 Abs. 7 TKG informiert der Verpflichtete, im Falle einer besonderen und erheblichen Gefahr eines Sicherheitsvorfalls die von der Gefahr potenziell betroffenen Nutzer über alle möglichen Schutz- oder Abhilfemaßnahmen, die von den Nutzern ergriffen werden können sowie gegebenenfalls auch über die Gefahr selbst. § 42 des BSI-Gesetzes gilt entsprechend.

8. Verschlüsselte Übertragung

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

https://www.bundesnetzagentur.de/sicherheitsvorfall

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

Der öffentliche PGP-Schlüssel der Bundesnetzagentur 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

9. Datennutzung

Die mitgeteilten Daten fließen in eine Datenbank und sind Grundlage für die europäischen Meldeverfahren.[9] Auf Grundlage der eingegangenen Meldung 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.

Gelangt die BNetzA zu dem Ergebnis, dass eine Bekanntgabe des Sicherheitsvorfalls im öffentlichen Interesse liegt, so kann sie selbst nach Anhörung der nach § 168 Abs. 1 TKG Verpflichteten die Öffentlichkeit informieren oder den Verpflichteten zur Unterrichtung verpflichten, vgl. § 168 Abs. 6 TKG.

Der Jahresbericht gem. § 168 Abs. 8 TKG über die eingegangenen Meldungen und die ergriffenen Abhilfemaßnahmen wird von der BNetzA in anonymisierter Form an die Europäische Kommission, die ENISA und das BSI versendet.

Die Pflicht zur Erteilung von Auskünften gegenüber der BNetzA nach § 183 Abs. 1 S. 2 TKG bleibt hiervon unberührt.

[9] vgl. unter Regelungsgegenstand die Verfahren der lfd. Nr. 2 und 3.

10. Weiterführende Pflichten

Unberührt von der vorliegenden Meldepflicht ist die mit dem nach § 168 Abs. 7 TKG bestehende 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.