Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Rückblick auf die gemeldeten IT-Sicherheitsvorfälle der Branche Telekommunikation 2020

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 228 99 9582-0
E-Mail: referat-wg14@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Erläuterung der Meldepflicht und der Auswertung

Der Sektor Informationstechnik und Telekommunikation (IT und TK) ist ein Sektor Kritischer Infrastrukturen, der in der Nationalen Strategie zum Schutz Kritischer Infrastrukturen bestimmt wurde. Er stellt durch die Dienstleistung „Sprach- und Datenübertragung“ die technische Basisinfrastruktur zum Austausch von Sprache und Daten für die Allgemeinheit zur Verfügung. Durch die Abhängigkeit anderer Sektoren von einer unterbrechungsfreien Sprach- und Datenübertragung können Vorfälle im Sektor IT und TK weitreichende und/oder kaskadierende Auswirkungen auf die Wirtschaft und das gesellschaftliche Leben haben. Ebenso ist bei Vorfällen auch von weiteren Auswirkungen auf die Bevölkerung auszugehen, beispielsweise durch die Erreichbarkeit von Notrufzentralen. Aufgrund dessen zählen Anlagen, wie Zugangs- und Übertragungsnetze, DNS-Resolver und Internetknotenpunkten (IXPs) ab einer bestimmten Größe gem. der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung/BSI-KritisV) i. V. m. § 10 Absatz 1 BSIG als besonders schützenswerte Kritische Infrastrukturen bei der Erbringung der kritischen Dienstleistung „Sprach- und Datenübertragung“. Diese Kritischen Infrastrukturen werden von Betreibern öffentlicher Telekommunikationsnetze und Erbringern öffentlich zugänglicher Telekommunikationsdienste (im Folgenden „TK-Netzbetreiber“ und „TK-Diensteerbringer“) betrieben.

TK-Netzbetreiber und TK-Diensteerbringer haben in Deutschland unabhängig von der Größe der von ihnen betriebenen Anlagen gemäß § 109 Absatz 5 Telekommunikationsgesetz (TKG) die Pflicht, Beeinträchtigungen ihrer Telekommunikationsnetze oder -dienste, welche zu beträchtlichen Sicherheitsverletzungen führen oder führen können, der Bundesnetzagentur (BNetzA) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Beträchtliche Sicherheitsverletzungen sind Einschränkungen der Verfügbarkeit und Verletzungen der Integrität, Authentizität oder Vertraulichkeit, die eine große Auswirkung hinsichtlich der Ausfalldauer, Wirkbreite oder Bedeutung haben. Im Umsetzungskonzept „Mitteilung nach § 109 Absatz 5 TKG“, Version 4.0 vom 10.11.2017 definiert die BNetzA, unter welchen konkreten Bedingungen eine Sicherheitsverletzung als beträchtlich gilt. Dies ist dann der Fall, wenn mindestens eines der folgenden Kriterien zutrifft:

- Betroffene Teilnehmerstunden mit dem Grenzwert von 1 Million (Produkt aus Anzahl der betroffenen Teilnehmer und der Dauer in Stunden)
- Auswirkungen auf internationale Zusammenschaltungen (Interconnection)
- Auswirkung auf Notruflenkung
- Außergewöhnliche IT-Störung

Liegt eine solche Sicherheitsverletzung vor, hat der TK-Netzbetreiber oder TK-Diensteerbringer unverzüglich eine Meldung an das BSI und die BNetzA abzugeben. Dies wurde mittels vereinheitlichter Online-Formulare vereinfacht. Sollte der Vorfall zum Zeitpunkt der Meldung noch andauern, ist der Sachverhalt durch Folgemeldungen zu vervollständigen. Eine Meldung nach Abschluss des Vorfalls ist obligatorisch.

Für diesen Bericht wurden die Meldungen des Jahres 2020 (Meldungseingang zwischen dem 1. Januar und dem 31. Dezember) der gemäß TKG zur Meldung verpflichteten Betreiber analysiert und ausgewertet. Dabei handelt es sich größtenteils um Meldungen von Betreibern aus dem Sektor IT und TK, die dem TKG unter-liegen. Da auch TK-Netzbetreiber und TK-Diensteerbringer, die keinen der in Anhang 4 Teil 3 der BSI-KritisV aufgeführten Schwellenwerte überschreiten, einen Beitrag zur Dienstleistung „Sprach- und Daten-übertragung“ und damit zur Versorgung der Allgemeinheit leisten (wie beispielsweise Zugangsnetze von Stadtwerken), wurden in diesem Bericht auch deren Meldungen berücksichtigt.

Auf diese Weise stellt der vorliegende Bericht die IT-Sicherheitslage im Kontext Kritischer Infrastrukturen im Berichtszeitraum dar. Er soll auch Betreibern Kritischer Infrastrukturen aus anderen Sektoren die Möglichkeit eröffnen, die vorgestellten Erkenntnisse in die eigene IT-Sicherheitsbetrachtung einfließen zu lassen.

Die im Bericht genannten Daten basieren auf von TK-Netzbetreibern und TK-Diensteerbringern mittels Meldeformular angegebenen und durch das BSI plausibilisierten Werten. Eine exakte Angabe der betroffenen Teilnehmer ist den TK-Netzbetreibern und TK-Diensteerbringern in vielen Fällen nicht möglich. Die im Bericht genannten Zahlen dienen daher als Richtwert. Zur Wahrung der schutzwürdigen Interessen der meldenden KRITIS-Betreiber nennt der Bericht nicht deren Namen sowie die betroffenen Gebiete, solange diese nicht öffentlich verfügbar sind (bspw. in Presseartikeln oder Stellungnahmen).

2 Analyse der Vorfälle

Im Jahr 2020 sind Meldungen zu 56 Vorfällen aus der Telekommunikationsbranche beim BSI und der BNetzA eingegangen. Hiervon wurden 42 nach den oben genannten Kriterien und Schwellen als Pflichtmeldungen (Vorfälle mit beträchtlichen Sicherheitsverletzungen) und 14 als freiwillige Meldungen klassifiziert. In Kapitel 2 werden nur die Pflichtmeldungen betrachtet; Kapitel 3 erläutert die freiwilligen Meldungen. Für die Analyse wird jeweils der letzte gemeldete Sachstand des jeweiligen Vorfalls herangezogen. Die TK-Netzbetreiber und TK-Diensteerbringer ordnen die Vorfälle folgenden Kategorien der IT-Schutzziele zu:

- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Authentizität.

Insgesamt gab es durch Vorfälle mit Einschränkungen der Verfügbarkeit eine Ausfallzeit von ca. 308 Millionen Teilnehmerstunden. Dies entspricht im Vergleich zum Vorjahr einer Verdopplung der Teilnehmerstunden im Bereich Verfügbarkeit, bei knapp 10 % weniger Meldungen. Dieser Anstieg ist auf eine Meldung zurückzuführen, die alleine über die Hälfte der betroffenen Anzahl an Teilnehmerstunden ausmacht. Eine genauere Beschreibung des Vorfalls wird in Kapitel 2.1.2 vorgenommen.

2.1 Hauptursachen

Die Ursachen der Vorfälle lassen sich in fünf Hauptkategorien unterteilen:

1. Technisches Versagen
2. Angriff Dritter
3. Ausfall externer Dienste
4. Menschliches Versagen
5. Wartungsarbeiten.

In der Kategorie „technisches Versagen“ sind Vorfälle aufgrund von Software- und Hardwarefehlern, Stromausfällen sowie Kabel- und Leitungsdefekten zusammengefasst.

In der Kategorie „Angriff Dritter“ werden sowohl Angriffe auf IT-und TK-Netze, wie DDoS- und Bruteforce-Angriffe, zugeordnet, aber auch Angriffe auf Hardware, wie beispielsweise durch Vandalismus.

In der Kategorie „Ausfall externer Dienste“ werden Meldungen zu Vorfällen gewertet, die aufgrund von Störungen der Verfügbarkeit von Vordienstleistern oder anderen genutzten externen Diensten entstanden sind.

Die Kategorie „menschliches Versagen“ beinhaltet Verfahrensfehler und Fehlkonfigurationen sowie Vorfälle, die durch Bauarbeiten ausgelöst wurden.

In der Kategorie „Wartungsarbeiten“ werden angekündigte (Wartungs-) Arbeiten am eigenen Telekommunikationsnetz durch die Betreiber oder Erbringer zusammengefasst, die zu meldepflichtigen Vorfällen geführt haben.

2.1.1 Zuordnung der Vorfälle zu den Ursachen

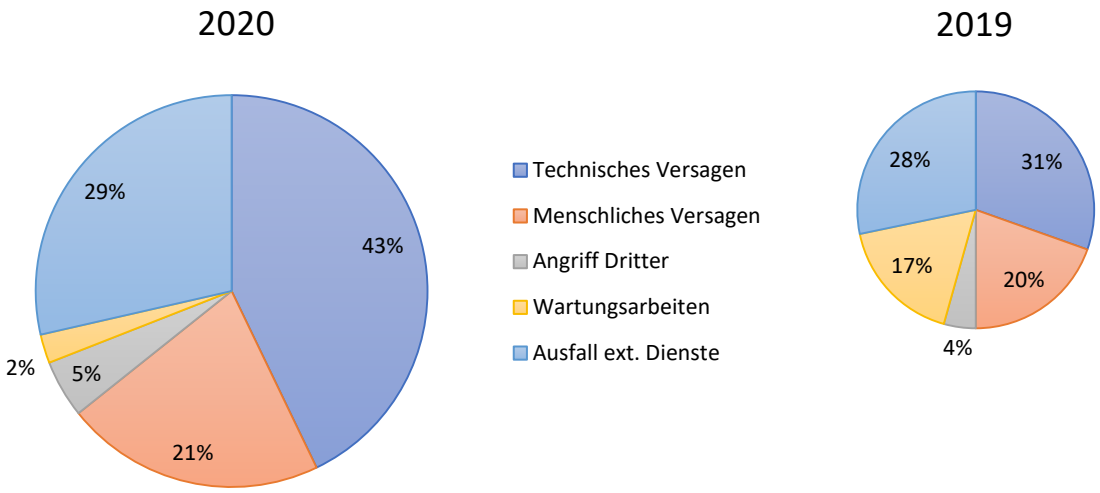

Abbildung 1: Prozentuale Darstellung der generischen Ursachen an den meldepflichtigen Vorfällen

Auch im Jahr 2020 war das technische Versagen von Systemen die Hauptursache für meldepflichtige Vorfälle in der Telekommunikationsbranche. Der Anteil stieg sogar im Vergleich zum Vorjahr etwas an.

Die Ursachen bei technischem Versagen können in zwei Unterkategorien unterteilt werden:

- Versagen durch Softwareprobleme
- Versagen durch Hardwareprobleme

Im Vergleich zum Jahr 2019 kam es zu einer deutlichen Verschiebung. Waren 2019 noch Hardwaredefekte in der Mehrzahl (von 14 Ausfällen bei der Kategorie Technisches Versagen waren 12 auf Hardwarefehler zurückzuführen), änderte sich dies im Jahr 2020. Von 18 Meldungen aufgrund technischen Versagens waren 7 auf Hardwaredefekte und 11 auf Probleme mit der Software zurückzuführen.

Eine deutliche Reduzierung von Meldungen gibt es hingegen bei der Ursachenkategorie Wartungsarbeiten.

Hierfür kommen mehrere Erklärungen in Betracht:

- Netzzusammenschlüsse, die zu einer besseren Redundanz geführt haben,
- bessere Absicherung der Wartungsarbeiten,
- kürzere Wartungsarbeiten, sodass die zugehörigen Vorfälle nicht die Marke von einer Million Teilnehmerstunden überschreiten,
- weniger Wartungsarbeiten aufgrund der Corona-Pandemie bzw. des Lockdowns.

2.1.2 Teilnehmerstunden und Ursachen der Vorfälle

Neben der eigentlichen Ausfallzeit gehören die bei den Vorfällen betroffenen Teilnehmerstunden zu den interessantesten Bezugspunkten, denn diese geben an, wie viele Nutzer über welchen Zeitraum wirklich betroffen waren, also wie groß der Einfluss auf die Bevölkerung war. Sie sind das Hauptmeldekriterium.

Die Gesamtzahl der Ausfallzeiten hat sich im Vergleich zum Jahr 2019 nahezu verdoppelt. Dies liegt insbesondere an einem großen Ausfall, dessen Ursache menschliches Versagen war. Vergleicht man den prozentualen Anteil der Ausfälle an den Teilnehmerstunden ohne diesen Ausreißer, ergibt sich ein ähnliches Bild wie im Jahr 2019.

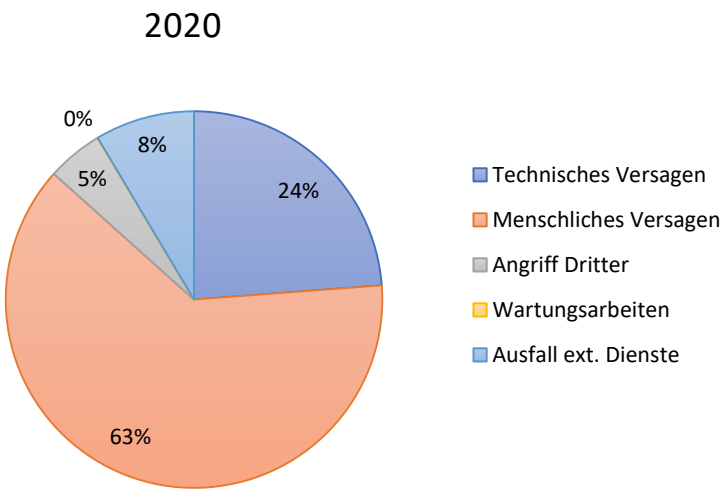

Abbildung 2: Prozentuale Darstellung der betroffenen Teilnehmerstunden je Ursache an der Gesamtausfallzeit der meldepflichtigen Vorfälle

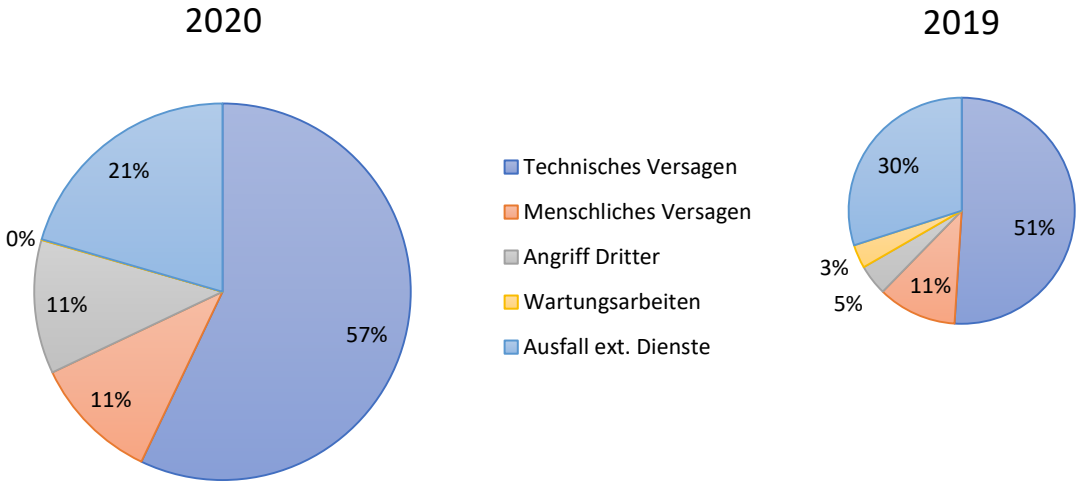

Abbildung 3: Betroffene Teilnehmerstunden je Ursache bereinigt um größten Ausfall und Vergleich 2019

Insbesondere technisches Versagen führt zu großen Ausfallzeiten bei den Teilnehmern. Häufig liegt dies daran, dass erst der Fehler gefunden sowie der Austausch vorgenommen werden muss.

Im Allgemeinen hatte menschliches Versagen im betrachteten Zeitraum keine großen Auswirkungen. Dennoch ereignete sich ein entsprechender Vorfall, der über die Hälfte der betroffenen Teilnehmerstunden bewirkte: Durch einen Konfigurationsfehler entstand eine Störung, die das Mobilfunknetz eines Betreibers bundesweit lahmlegte. Der Ausfall betraf auf diese Weise ca. 25 Mio. Teilnehmer über eine Dauer von fast sieben Stunden, sodass es zu einer Ausfallzeit von insgesamt 175.440.000 Teilnehmerstunden kam. Da sich der Ausfall nachts ereignete, hätte der Einfluss auf die Bevölkerung jedoch noch weitaus schwerwiegender ausfallen können. Damit war der Vorfall, gemessen an Teilnehmerstunden, der größte Ausfall der vergangenen Jahre. Der Vorfall verdeutlicht, wie weitreichend einfache Konfigurationsfehler in Telekommunikationsnetzen sein können und welches Maß an Sorgfältigkeit bei Änderungen an Netzkomponenten angelegt werden muss.

Von Einzelfällen abgesehen, liegen die meisten Vorfälle bei einer Ausfallzeit zwischen einer und fünf Millionen Teilnehmerstunden.

2.2 Vorfälle unterteilt nach Meldekriterien

Bei der Betrachtung der Meldekriterien zeigt sich ein ähnliches Bild wie im letzten Jahr. Die meisten Vorfälle müssen aufgrund der Überschreitung des Schwellenwertes von einer Million Teilnehmerstunden gemeldet werden. Darauf folgt das Kriterium der Beeinträchtigung der Notruflenkung. Betroffenheit der Interconnection (Zusammenschaltung zwischen verschiedenen Ländern) und außergewöhnliche IT- Störungen wurden wie im letzten Jahr nur jeweils einmal als Ursache gemeldet.

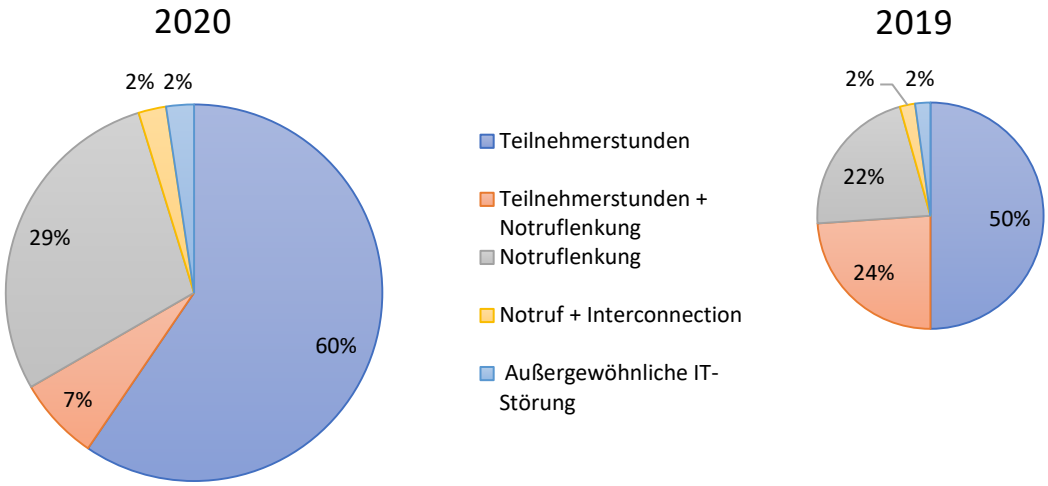

Abbildung 4: Darstellung der Vorfälle nach Meldekriterien sowie Vergleich zu 2019

Betrachtet man die Ausfallzeiten der einzelnen Störungen, ergibt sich, dass im Bereich der Notruflenkung die Störungen relativ schnell (innerhalb von 12 Stunden) behoben wurden, bzw. es ist ein Routing vorgenommen worden, damit Anrufe verarbeitet werden können.

2.3 Geografische Ausprägung

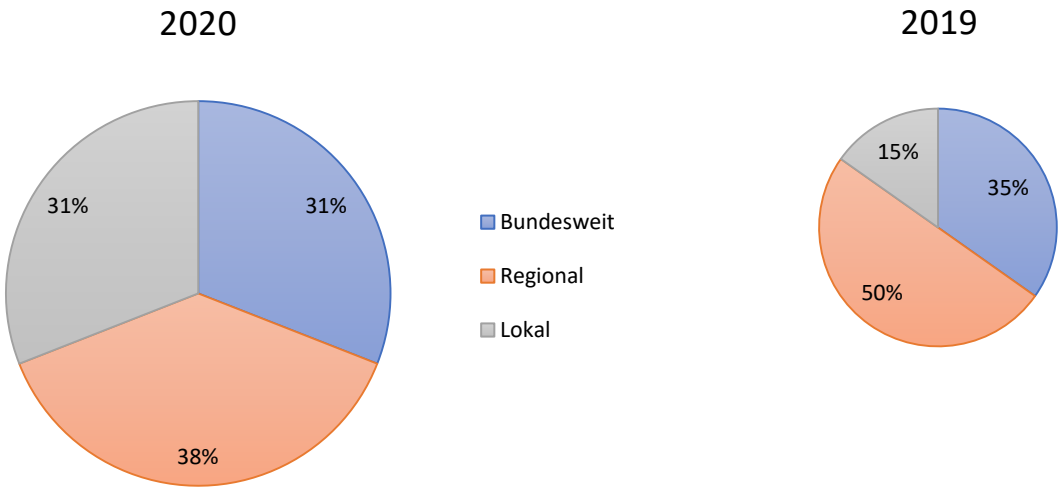

Abbildung 5: Darstellung der geografischen Ausprägung der Vorfälle und Vergleich zu 2019

Bei der geografischen Ausprägung stellen wir eine Verdopplung der lokalen Vorfälle im Vergleich zum vorherigen Jahr fest. Während die regionalen Vorfälle um 12 %-Punkte zurückgegangen sind, ist die Ausprägung auf Bundesebene fast gleichgeblieben.

2.3.1 Ausfalldauer und geografische Ausprägung

Die durchschnittlichen Ausfallzeiten waren im lokalen Bereich erheblich höher als in den anderen Bereichen. Dies lässt sich, wie schon oben im vorherigen Kapitel beschrieben, darauf zurückführen, dass dort Meldungen aufgrund der Überschreitung des Schwellenwertes von einer Million Teilnehmerstunden erheblich länger bestehen müssten, um eine Meldepflicht auszulösen.

Interessanter ist daher die Betrachtung der Einzelmeldungen: Hieraus wird ersichtlich, dass die Behebung bundesweiter Störungen viel schneller erfolgt. Sehr lange Zeit benötigen die Betreiber für die Störungsbehebung bei einzelnen lokalen Vorfällen.

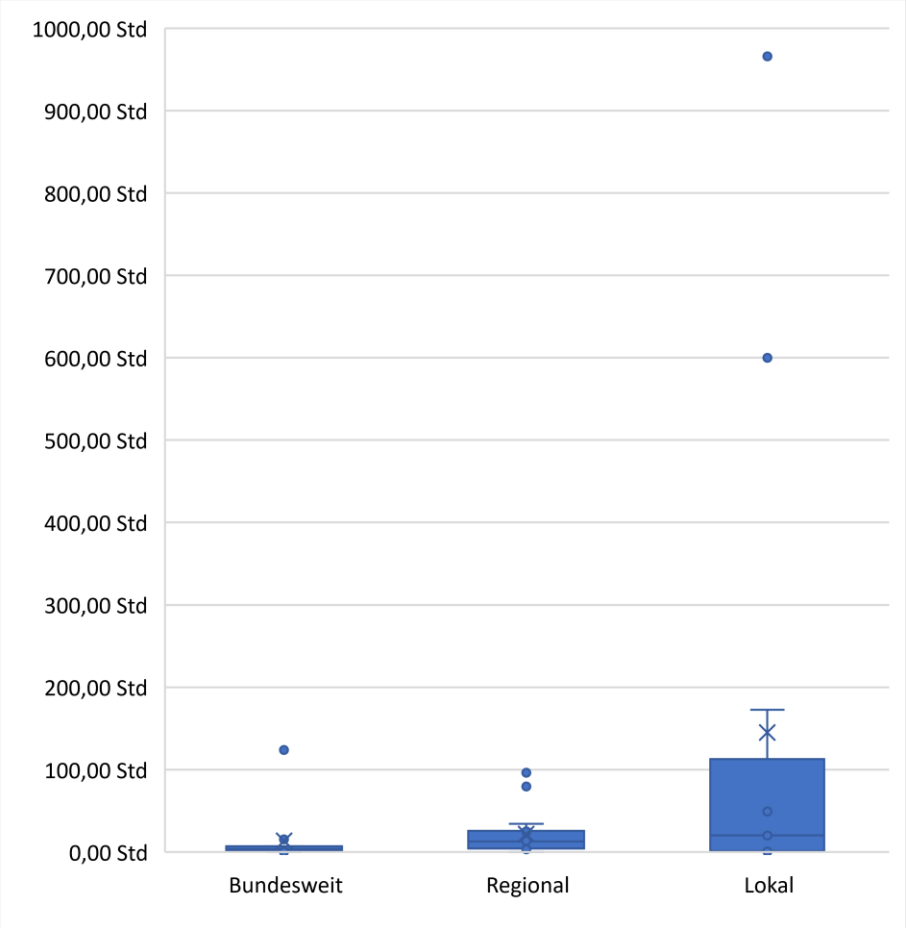

Abbildung 6: Darstellung der Ausfallzeiten nach der geografischen Ausprägung

Der Anstieg der durchschnittlichen Behebungszeit im Vergleich zum letzten Jahr im Bereich der lokalen Ausfälle könnte sich eventuell durch die Corona-Situation erklären lassen. Durch diese sind ggf. Anfahrten zu den Standorten länger bzw. es gibt Verzögerungen bei der Entdeckung.

Aber auch die Lokalisierung der Ursache kann auf lokaler Ebene länger dauern als im Kernnetz, welches typischerweise einem intensiven Monitoring unterliegt.

2.3.2 Gegenüberstellung von Ursachen und geografischer Ausprägung

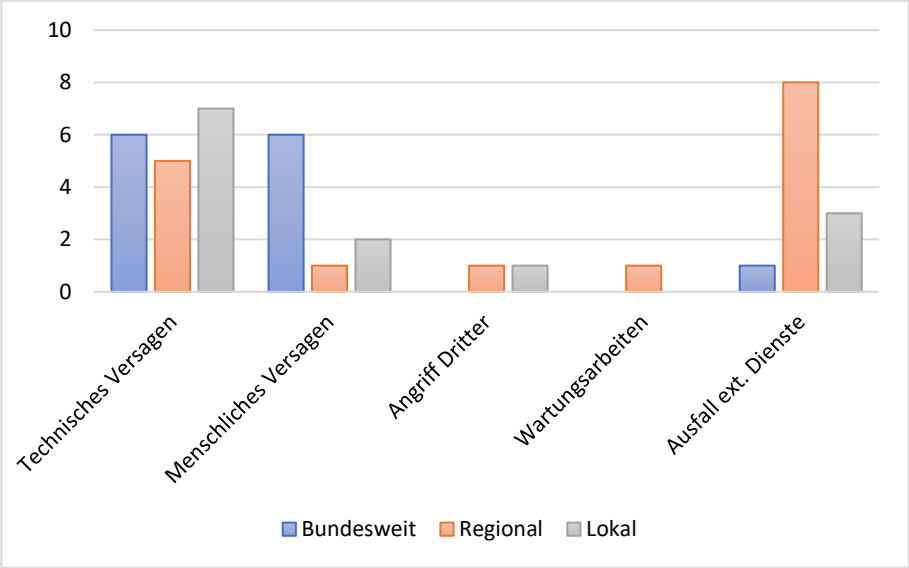

Abbildung 7: Darstellung der generischen Ausfallursachen aufgeschlüsselt nach der geografischen Ausprägung

Im lokalen Bereich traten häufig Störungen auf, die die Notruflenkung beeinträchtigten. Dabei handelte es sich meist um technisches Versagen. Bei menschlichem Versagen ging es meistens um Kabelbruch auf Baustellen.

Auffällig ist, dass Ausfälle externer Dienste hauptsächlich Störungen auf regionaler und lokaler Ebene bewirkten. Das kann damit zusammenhängen, dass das Backbone in der Regel in Betreiberhand liegt, im Rahmen der Zugangsnetze aber oft Vordienstleister einbezogen werden.

Die bundesweiten Vorfälle entstanden überwiegend durch technisches oder menschliches Versagen. Dies macht erneut deutlich, wie wichtig gut strukturierte und definierte Prozesse des Asset- und Change-Managements sowie die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter sind. So können bereits einzelne Fehlkonfigurationen oder fehlerhafte Updates im Backbone zu bundesweiten Störungen führen.

Technisches Versagen stellt in allen geografischen Bereichen eine zentrale Ursache dar. Typischerweise kommt auf regionaler und lokaler Ebene hinzu, dass häufig eine aufwändigere Fehleranalyse sowie Anfahrtswege erforderlich sind. Insgesamt wird deutlich, dass Redundanzen auf allen Ebenen eine wichtige Rolle spielen.

2.4 Betroffene Dienste

Bei TK-Netzbetreibern und TK-Diensteerbringern können verschiedene Arten von Diensten betroffen sein. Grob lassen sich diese in Festnetzdienste und Mobilfunkdienste unterteilen. Hierbei ist immer das Medium gemeint, über das der Endkunde sich einwählt und wo eine Betroffenheit vorliegt.

Für jeden der Dienste wird zusätzlich unterschieden, ob die Sprachfunktionalität und/oder auch die Datenverbindung bspw. für E-Mail, Internet oder OTT (Over-The-Top) -Dienste betroffen sind.

Bei 27 der 42 Vorfälle waren die Mobilfunkdienste betroffen und in 16 Fällen die Festnetzdienste, bei einem Vorfall gab es keine Nennung der betroffenen Dienste (Mehrfachnennung möglich). Im Vergleich zu 2019 ging damit der Anteil an Festnetzstörungen zurück (25 Mobilfunkdienste und 23 Festnetzdienste).

2.4.1 Gegenüberstellung der Ursachen und der betroffenen Dienste

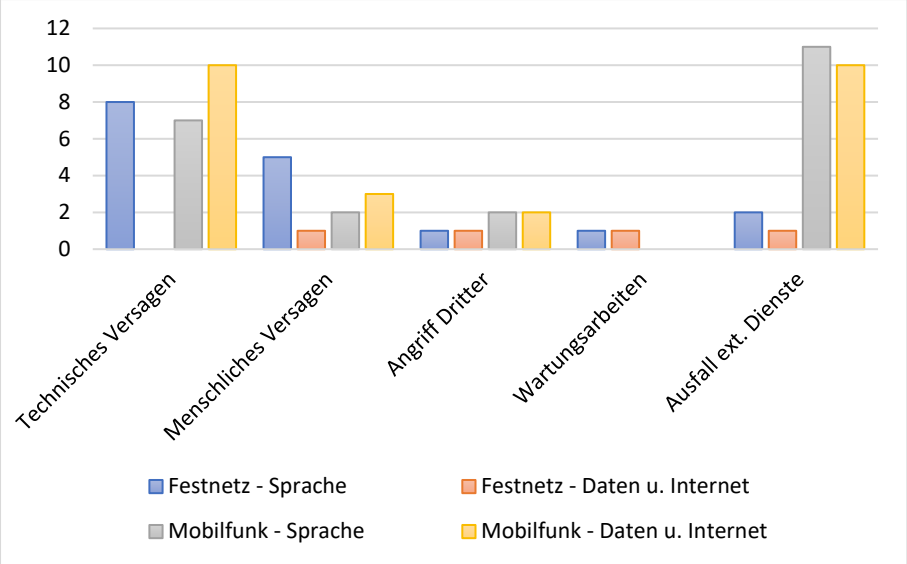

Abbildung 8: Darstellung der generischen Ausfallursachen aufgeschlüsselt nach betroffenen Diensten

Auffällig bei den betroffenen Diensten ist insbesondere der hohe Anteil an Ausfällen von externen Dienstleistern bei Mobilfunkdiensten. Dies liegt insbesondere daran, dass hier häufig auf bestimmten Strecken Carrier eingesetzt werden. Fällt bei diesen eine Leitung aus, verlängert sich die Bearbeitung entsprechend, da der Carrier erst über diesen Ausfall informiert werden muss und die Behebung selbst vornimmt.

Bei Festnetzdiensten waren hauptsächlich die Sprachdienste betroffen. Ein möglicher Grund hierfür ist, dass die Anbindung an die Notruflenkung hierunter fällt. Ist diese gestört, ergibt sich sofort ein Vorfall mit einer schwerwiegenden Sicherheitsverletzung. Dies schlägt sich auch in den Meldungen nieder. So war bei 13 von 17 Vorfällen, bei denen der Festnetz-Sprachdienst betroffen war, auch die Notruflenkung tangiert. Großflächige Ausfälle im Bereich des Festnetzes, bei denen sowohl Daten als auch Internet betroffen sind, existieren anscheinend seltener oder erreichen die Meldeschwelle nicht.

2.4.2 Gegenüberstellung betroffener Dienste und geografischer Ausprägung

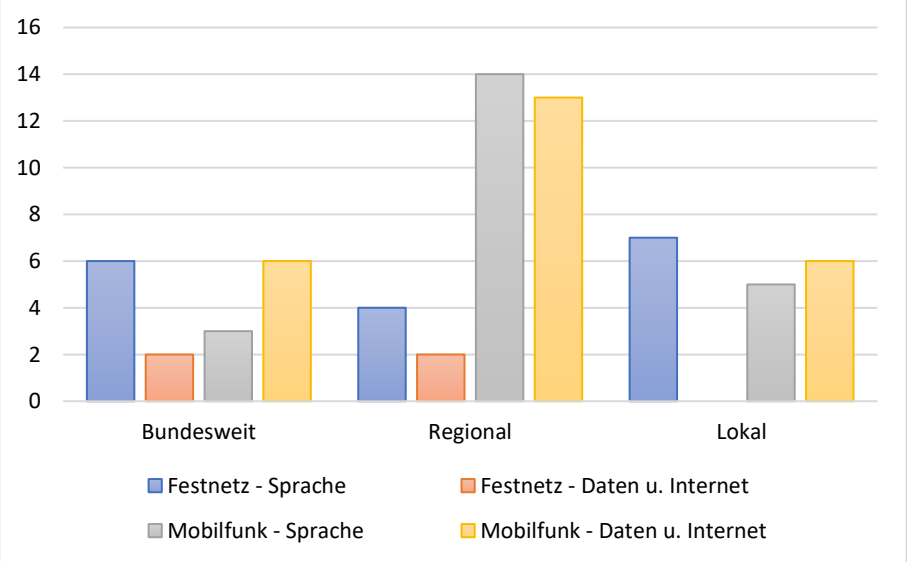

Abbildung 9: Darstellung der geografischen Ausbreitung aufgeschlüsselt nach betroffenen Diensten

Bei regionalen Ausfällen dominieren die Mobilfunkdienste, während es bei bundesweiten und lokalen Ausfällen eher ausgeglichen ist. Auch hier lassen sich die in Kapitel 2.4.1 genannten Gründe anführen. Die Korrelation zwischen regionaler Ausprägung und Ausfall externer Dienste wurde bereits in Kapitel 2.3.2. betrachtet. Ausfälle der Festnetzdatendienste im lokalen Bereich erreichten nach den Angaben der Betreiber nicht die Meldeschwelle. Bei den ausgefallenen lokalen Festnetzsprachdiensten ist der Meldegrund bei allen Meldungen die hiermit zusammenhängende Störung der Notruflenkung.

3 Freiwillige Meldungen

Das BSI und die BNetzA erreichen nicht nur Pflichtmeldungen aus der Telekommunikationsbranche. Jedes Unternehmen kann auf freiwilliger Basis Meldungen zu Vorfällen abgeben, die die Meldeschwellen nicht überschreiten. Das BSI begrüßt diese freiwilligen Meldungen und das damit einhergehende Engagement der meldenden Betreiber oder Erbringer, einen Beitrag zur Bewertung der Cyber-Sicherheitslage und damit zur Verbesserung der Cyber-Sicherheit in Deutschland zu leisten. Im Folgenden werden die Erkenntnisse aus den Pflichtmeldungen um die aus den freiwilligen Meldungen ergänzt, um ein detaillierteres Lagebild zu erhalten.

Im Vergleich zum Jahr 2019 mit 15 Meldungen ist mit 14 im Jahr 2020 die Anzahl der als „nicht erhebliche Sicherheitsverletzung (freiwillig)“ eingestuften Meldungen ungefähr gleichgeblieben.

Mehrere Meldungen wurden vom BSI gemeinsam mit der BNetzA nach Erhalt der Abschlussmeldung als nicht erhebliche Sicherheitsverletzung zurückgestuft. Dies zeugt von einem guten und engagierten Verhalten der Meldenden. Obwohl der komplette Umfang des Vorfalls noch nicht absehbar war, wurden hier die Behörden vorsorglich ins Bild gesetzt.

Im Vergleich zum letzten Jahr gab es weniger Meldungen auf Grundlage von DDoS-Angriffen. Ob dies einem Rückgang entspricht oder lediglich weniger Vorfälle gemeldet wurden, lässt sich aus den vorhandenen Daten nicht ermitteln.

4 Presseschau

Im Jahr 2020 wurde viel über Ausfälle in den Netzen, insbesondere in den mobilen Netzen, in der Presse berichtet.

4.1 DDoS-Angriffe auch gegen Telekommunikationsunternehmen

Im Jahr 2020 kam es wieder zu DDoS-Angriffen gegen Telekommunikationsunternehmen. Über einige dieser Angriffe wurde in der Presse berichtet, da sie zu Ausfällen führten, die für die Kunden spürbar waren. Dies war beispielsweise im Juni 2020 der Fall:[1] Ein Angriff über ein Bot-Netz führte zu mehrtägigen Störungen bei einem Betreiber in Kassel und in der Region. Später konnte der Angriff mit einer Reihe von Angriffen in Verbindung gebracht werden, Tatverdächtige wurden festgenommen.

Auch bei den beträchtlichen Sicherheitsverletzungen kam es zu Meldungen aufgrund von DDoS-Angriffen. Diese hatten zwar aufgrund von bestehenden DDoS-Mitigationsmaßnahmen in der Regel keine Auswirkungen auf Kunden, jedoch sind auch die Telekommunikationsunternehmen nicht von dieser Art Angriffen ausgenommen. Beim BSI ist im Bereich Telekommunikation im Jahr 2020 insbesondere die Gruppe "Armada Collective" aufgefallen. Die DDoS-Angriffe begannen in der Regel mit einem Erpresserschreiben und einem kleineren DDoS-Angriff zur Demonstration. Diese Angriffe erfolgten typischerweise in der Größenordnung von 100 Gbit/s. Im Erpresserschreiben wurde dann mit DDoS-Angriffen einer erheblich größeren Bandbreite gedroht, sofern ein gefordertes Lösegeld nicht gezahlt werde. Ähnliche DDoS-Angriffe auf Telekommunikationsbetreiber konnten im EU-Ausland beobachtet werden. Obwohl in vielen Fällen der angedrohte DDoS-Angriff ausgeblieben ist, kann nicht ausgeschlossen werden, dass ein angekündigter Angriff doch erfolgt. Dem BSI ist in diesem Kontext ein Fall bekannt, in dem zwar der angekündigte DDoS-Angriff ausblieb, bei dem die Angreifer jedoch mehrere Monate nach dem ersten Erpresserschreiben einen weiteren Erpressungsversuch starteten. Das neue Erpresserschreiben bezog sich in dem Fall auf das erste Schreiben.

Das BSI empfiehlt, nicht auf die Forderungen der Erpresser einzugehen, da nicht ausgeschlossen werden kann, dass diese oder eine andere Gruppe in Zukunft erneut einen Angriffsversuch unternimmt. In diesem Kontext verweist das BSI auf die BSI-Veröffentlichung „Prävention von DDoS-Angriffen“ [2]. Für den Fall eines akuten DDoS-Angriffs kann die BSI-Veröffentlichung „Abwehr von DDoS-Angriffen“ [3] hilfreich sein. Darüber hinaus kann sowohl bei der Prävention als auch nach einem akuten Sicherheitsvorfall die Einbindung eines qualifizierten Dienstleisters sinnvoll sein. Das BSI hat eine Liste mit qualifizierten DDoS-Mitigation-Dienstleistern zusammengestellt[4].

4.2 Zerstörung von Funkmasten

Generell tauchen Vorfälle, die auf Zerstörung von Funkmasten zurückzuführen sind, eher selten in den Meldungen auf. Oft können kleinere Defekte schnell repariert werden und führen daher gar nicht erst zu einem meldepflichtigen Vorfall. Meldeschwellen werden in der Regel erst erreicht, wenn es in Folge von polizeilichen Ermittlungen, zu Verzögerungen bei der Reparatur der Funkmasten kommt.

[1] https://www.hna.de/lokales/kreis-kassel/kassel-internet-probleme-ausfall-anbieter-aco-connect-13801149.html

[2] https://www.allianz-fuer-cybersicherheit.de/dok/454112
[3] https://www.allianz-fuer-cybersicherheit.de/dok/454114
[4] https://www.allianz-fuer-cybersicherheit.de/dok/518574

In Großbritannien sowie im EU-Ausland, unter anderem in den Niederlanden, Belgien und Zypern, führten Aufrufe von Verschwörungstheoretikern, die einen Zusammenhang zwischen 5G und der Corona-Pandemie sahen, vermehrt zu gezielten Angriffen auf Mobilfunkmasten[5,6]. Auch in Deutschland kam es über die ganze Bundesrepublik verteilt[7], insbesondere nach der Versteigerung der 5G-Frequenzen sowie im Rahmen des immer weiter fortschreitenden Ausbaus der 5G-Funkmasten, zu mehreren Brandanschlägen auf Mobilfunkmasten[8]. In München und Bonn gab es wiederholt Brände an und in Mobilfunkmasten. Ein ggf. notwendiger Austausch der Technik kann in solchen Fällen zu Ausfällen führen. Da die genaue Motivation der Täter jedoch in der Regel im Unklaren blieb, kann ein Zusammenhang der Brandanschläge mit dem 5G-Ausbau nicht mit Sicherheit hergestellt werden.

4.3 Corona-Pandemie

Im Zusammenhang mit der verstärkten Nutzung von Home-Office-Möglichkeiten und der daraus resultierenden Verlagerung der Nutzung von Telekommunikationsdiensten wurde durch den erhöhten Bedarf an Bandbreite (beispielsweise durch Videokonferenzen oder Remote-Arbeiten) eine Einschränkung in der Verfügbarkeit der Telekommunikationsnetze befürchtet.

Der DE-CIX als einer der größten Internetknoten weltweit verzeichnete bereits in den vergangenen Jahren auf Grund der Digitalisierung eine stetige Zunahme des Datenverkehrs. Während der Corona-Pandemie wurden bereits im März 2020 9 Tbit/s Datenverkehr gemessen. Dieser Rekordwert wäre wahrscheinlich unter normalen Entwicklungen erst wesentlich später im Jahr erreicht worden. Im November 2020 kam es dann zu einem weiteren Rekordwert von 10 Tbit/s, als die Lockdown-Maßnahmen erneut intensiviert wurden.[9]

Auch die Agentur der Europäischen Union für Cyber-Sicherheit (ENISA) untersuchte diesen Sachverhalt, bezogen auf die Telekommunikationsnetze der EU.[10] Das Ergebnis der Untersuchung war, dass sich die Telekommunikationsnetze in der EU während der Corona-Pandemie gegenüber dem erhöhten Bandbreitenbedarf resilient zeigten. Dieses Bild zeichnete sich auch in den Telekommunikationsnetzen in Deutschland ab.[11] So sah der DE-CIX seine Ressourcen trotz des gestiegenen Datenverkehrs als ausreichend an. Auch die großen Betreiber von Telekommunikationsnetzen waren laut eigener Aussage entsprechend gut aufgestellt.

[5] https://www.handelsblatt.com/politik/deutschland/coronavirus-verschwoerungstheorien-motivieren-zu-anschlaegen-auf-5g-masten/25770420.html
[6] https://www.daserste.de/information/politik-weltgeschehen/weltspiegel/grossbritannien-172.html
[7] https://www.tagesschau.de/faktenfinder/5g-corona-mobilfunk-101.html
[8] https://ga.de/bonn/stadt-bonn/gibt-es-in-bonn-eine-brandanschlagserie-auf-funkmasten_aid-50251185
[9] https://www.de-cix.net/en/about-de-cix/media/press-releases/number-of-the-year-2020-32-exabytes-of-data-traffic-at-de-cix-internet-exchanges-worldwide-1
[10] https://www.enisa.europa.eu/publications/telecom-security-during-a-pandemic
[11] https://www.chip.de/news/Deutschland-ist-zuhause-Haelt-das-Netz-von-Telekom-Vodafone-und-Co.-das-aus_182552718.html

5 Fazit

Auch in diesem Jahr lässt sich sagen, dass die Branche der Telekommunikation im Bereich der IT-Sicherheit prinzipiell gut aufgestellt ist. Vor allem externe Faktoren tragen kaum zu Vorfällen bei. Jedoch muss bei internen Faktoren noch sorgfältiger gearbeitet werden. Insbesondere ein 4- bzw. 6-Augen-Prinzip bei Konfigurationsänderungen im Backbone-Netz sowie ein detailliertes Nachhalten und Überwachen des End-of-Life der verbauten Komponenten und ein damit einhergehendes Patch- und Update-Management ist unersetzlich. Ebenso zeigten die Vorfälle, die aufgrund von Ausfällen externer Dienste entstanden sind, die Notwendigkeit von klar definierten Service Level Agreements auf, in denen die Reaktions- und bestenfalls Vorort-Zeiten festgelegt sind. Kommunikationskanäle zu den Dienstleistern sollten etabliert und regelmäßig getestet werden.

Der erhöhte Bedarf an Kapazitäten, der auf den vermehrten Einsatz von Home-Office in der Corona-Pandemie zurückging, konnte von den Internet Service Providern ohne Probleme abgedeckt werden. Größere meldepflichtige Ausfälle in diesem Zusammenhang wurden im Jahr 2020 nicht festgestellt.

Obwohl Angriffe in den gemeldeten Vorfällen eine untergeordnete Rolle gespielt haben, wäre die Schlussfolgerung falsch, dass die Branche nicht das Ziel von Angriffen sei. Das BSI bewertet das Risiko von Cyber-Angriffen als sehr hoch. Hinzu kommt das ebenso ernstzunehmende Risiko von sonstigen Angriffen, beispielsweise von Sabotageakten. Die Meldungen zeigen ein hohes Sicherheitsniveau bei den TK-Netzbetreibern und TK-Diensteerbringern, durch das eine Vielzahl von Angriffen detektiert und abgewehrt werden kann, bevor diese sich zu einer meldepflichtigen Beeinträchtigung entwickeln. Grundsätzlich bleibt jedoch das Risiko, dass wohlorganisierte, aufwändigere Angriffe zu massiven Schäden führen können.

Sind Nutzer der Telekommunikationsnetze bzw. -dienste aufgrund erhöhter Anforderungen auf das Funktionieren der Telekommunikationsdienstleistung angewiesen, ist es ratsam, die Verfügbarkeit durch zusätzliche Telekommunikationsanschlüsse anderer TK-Netzbetreiber und TK-Diensteerbringer oder durch alternative Kommunikationskanäle (wie beispielsweise Satellitentelefone) zu erhöhen. Hierbei ist allerdings anzumerken, dass eine absolute Ausfallsicherheit nie erreicht werden kann und daher auch Notfallprozesse existieren sollten, die den Betrieb der eigenen Institution bei einem Ausfall der Telekommunikationsdienstleistung zumindest zeitweise sicherstellen können.

Dies wurde auch in jüngsten Vorfällen aus dem Jahr 2021 deutlich, die mit einer geographischen Betroffenheit und infrastrukturellen Zerstörung verbunden waren, wodurch die Versorgung der Bevölkerung über mehrere Tage bzw. Wochen hinweg nicht erbracht werden konnte.

Abschließend ist festzustellen, dass das im BSI gebildete und hiermit veröffentlichte Lagebild stark vom Detailgrad der eingereichten Meldungen abhängt. Je detaillierter und nachvollziehbarer die Meldungen hinsichtlich der Ursachen, des Hergangs und der Auswirkungen sind, desto vollständiger und genauer kann ein solches Lagebild erstellt und zur Verfügung gestellt werden.

Das BSI beobachtet in diesem Zusammenhang auch weiterhin gemeinschaftlich mit der BNetzA die IT-Sicherheitslage in der Telekommunikationsbranche, um ggf. in Zusammenarbeit mit den TK-Netzbetreibern und TK-Diensteerbringern schnell auf eine geänderte Bedrohungslage reagieren zu können.

6 Abbildungsverzeichnis