Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Rückblick auf die gemeldeten IT-Sicherheitsvorfälle der Branche Telekommunikation 2021

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: 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 § 168 Telekommunikationsgesetz (TKG; alt: § 109 Absatz 5 TKG) die Pflicht, Beeinträchtigungen ihrer Telekommunikationsnetze oder -dienste, die 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 Teilnehmerinnen und Teilnehmer sowie 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 2021 (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 unterliegen.

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 Datenübertragung“ 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 Teilnehmerstunden ist den TK-Netzbetreibern und TK-Diensteerbringern in vielen Fällen nicht möglich. Die im Bericht genannten Zahlen dienen daher als Richtwerte. 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 2021 sind 42 Meldungen nach den oben genannten Kriterien und Schwellen als Pflichtmeldungen (Vorfälle mit beträchtlichen Sicherheitsverletzungen) eingegangen. 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-Sicherheitsschutzziele zu:

- Verfügbarkeit,
- Integrität,
- Vertraulichkeit,
- Authentizität.

Überschattendes Ereignis im Jahr 2021 in Deutschland war auch im Bereich Telekommunikation die Flutkatastrophe im Ahrtal. Durch die Zerstörung von wesentlichen Infrastrukturen insbesondere im Bereich von Arbeitsstationen im Mobilfunknetz sowie der „letzten Meile“ im Bereich des Festnetzes, kam es zu erheblichen Ausfallzeiten in Folge des Unwetters. Mehr hierzu in Kapitel 4.

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 subsumiert, 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.

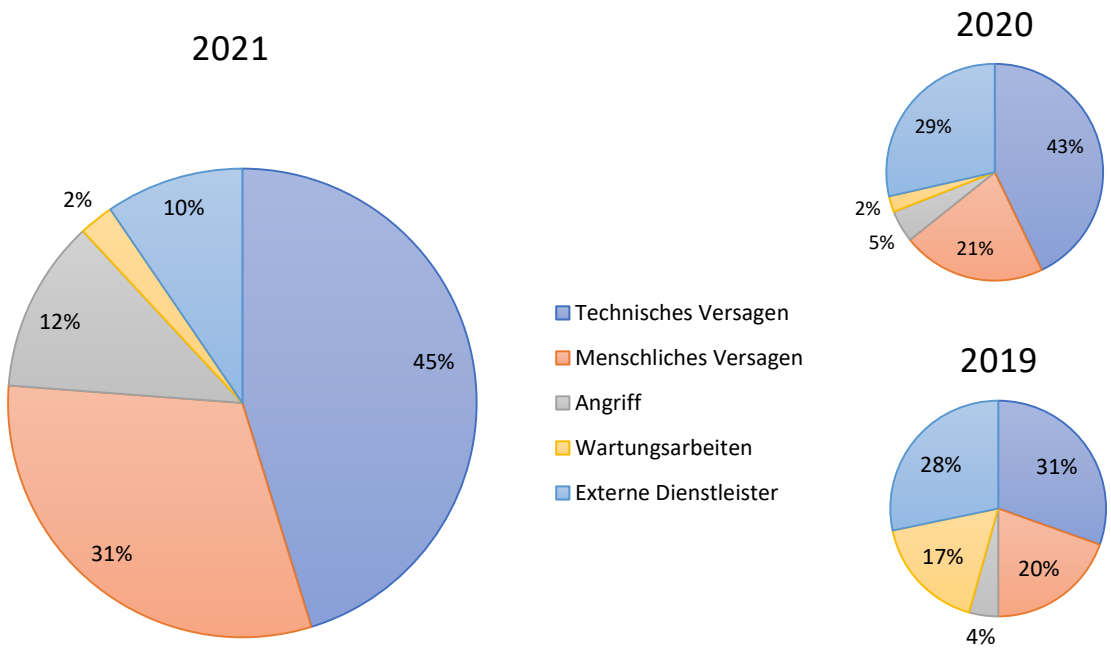

Abbildung 1: Anteile der generischen Ursachen der meldepflichtigen Vorfälle der Jahre 2021, 2020 und 2019

Hinsichtlich der Zuordnung der Vorfälle zu den Hauptursachen bleibt auch im Jahr 2021 das technische Versagen von Systemen die führende Hauptursache für meldepflichtige Vorfälle in der Telekommunikationsbranche. Der Anteil stieg sogar im Vergleich zum Vorjahr etwas an. Insofern zeichnet sich über die vergangenen Jahre ein ansteigender Trend ab.

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

- Versagen durch Softwareprobleme
- Versagen durch Hardwareprobleme

Im Jahr 2021 handelte es sich in sechs der 19 Vorfälle um Softwareprobleme und in 13 Vorfällen um Hardwareprobleme. Im Vergleich mit den Vorjahren wird ersichtlich, dass die Verteilung des technischen Versagens auf Software- und Hardwarefehler jährlich schwankte und sich keine gleichbleibende Mehrheit bei einer der beiden Ursachenarten ableiten lässt. Hieraus wird deutlich, dass sowohl Software- als auch Hardwarefehler zu beträchtlichen Auswirkungen führen können. Das gezielte Betrachten von Produktlebenszyklen, ein ausgereiftes Monitoring bei zentralen Systemen, sowie geeignete Testumgebungen und –verfahren sind wichtige Bausteine bei der Vorbeugung und Erkennung derartiger Vorfälle.

Vorfälle aufgrund von menschlichem Versagen nahmen im Vergleich zu den beiden Vorjahren um circa zehn Prozentpunkte zu und lösten somit externe Dienstleister als zweithäufigste Hauptursache ab. Dieser Wandel könnte verschiedene Ursachen haben:

- Verbesserte Transparenz und Übersicht der verwendeten externen Dienstleister sowie deren Bedeutung für die erbrachten Telekommunikationsdienste
- Striktere und klar definierte Vorgaben in den SLAs samt geregelter Reaktions- und Instandsetzungszeiten sowie Überprüfungen der Einhaltung dieser Vorgaben
- Klar etablierte Kommunikationskanäle zu den Dienstleistern sowie Routineübungen zur Nutzung dieser Kommunikationskanäle
- Zufällige Entwicklung

Der Anteil an erfolgreichen Angriffen, die zu meldepflichtigen Störungen führten, ist ebenfalls leicht gestiegen. Die Hauptursache Angriffe bleibt jedoch, gemessen an der Gesamtzahl der Störungen, weiterhin niedrig. Telekommunikationsanbieter scheinen dementsprechend die Gefährdung durch Angriffe ernst zu nehmen und entsprechende Maßnahmen zur Prävention, Detektion und Reaktion etabliert zu haben, durch die die Anzahl an erfolgreichen Angriffen mit gravierenden Auswirkungen auf die angebotenen Telekommunikationsdienste vergleichbar niedrig gehalten werden kann.

2.2 Vorfälle unterteilt nach Meldekriterien

Die meisten Vorfälle wurden wie in den vergangenen Jahren aufgrund der Überschreitung des Schwellenwertes von einer Million Teilnehmerstunden gemeldet, insbesondere in der Kategorie „mehrere Gründe“ wurden in jedem Fall eine Kombination aus Teilnehmerstunden und einem weiteren Meldekriterium angegeben.

Ähnlich zu den Jahren 2019 und 2020 ist der zweithäufigste Meldegrund die Beeinträchtigung der Notruflenkung. Hier lässt sich unter Berücksichtigung der vergangenen Jahre ein steigender Trend von meldepflichtigen Vorfällen, die einzig durch die Betroffenheit der Notruflenkung gemeldet wurden, ableiten. Gründe hierfür könnten die Abschaltung von ISDN sowie Probleme bei den Übergabepunkten der Notrufe zwischen den Carriern sein.

Betrachtet man die Ausfallzeiten der einzelnen Störungen, ergibt sich, dass im Bereich der Notruflenkung die Störungen relativ schnell (innerhalb von zwölf Stunden) behoben wurden, bzw. es ist ein Routing vorgenommen worden, damit Anrufe verarbeitet werden konnten. Einzige Ausnahme waren die Störungen im Zusammenhang mit dem Flutereignis im Ahrtal.

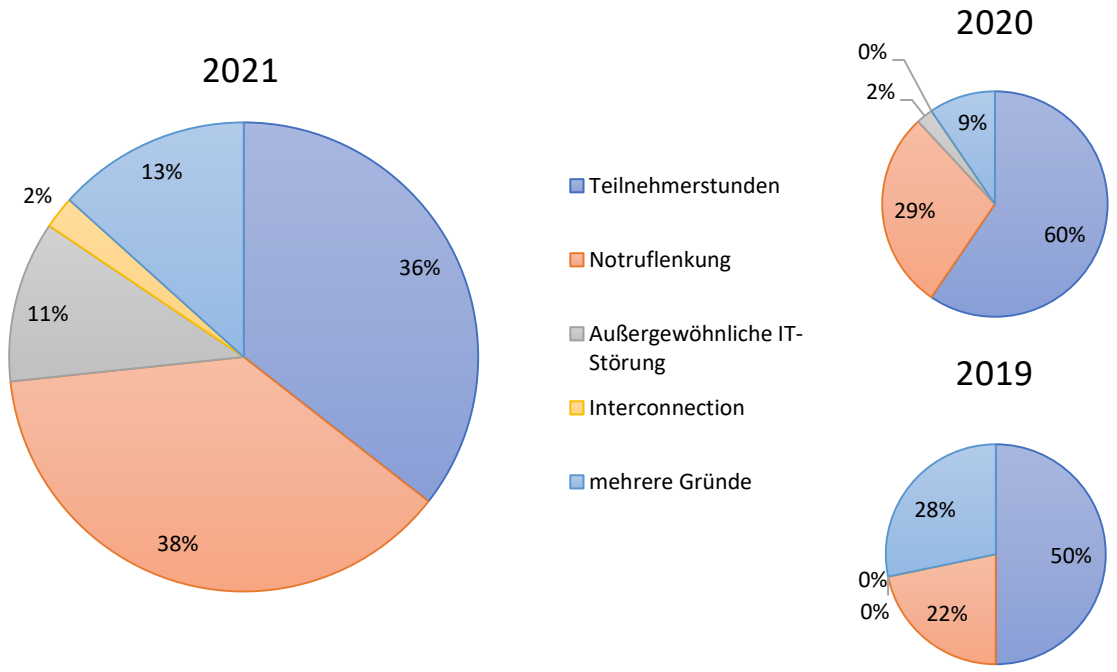

Abbildung 2: Vorfälle nach Meldekriterien sowie Vergleich zu 2020 und 2019

Betroffenheit der Interconnection (Zusammenschaltung zwischen verschiedenen Ländern) wurde ähnlich wie in den letzten Jahren nur sehr selten als Ursache gemeldet. Außergewöhnliche IT-Störungen sind im Vergleich zum Vorjahr von einer auf acht Meldungen angestiegen, spielen jedoch auch weiterhin nur eine untergeordnete Rolle. Auch dieser Aspekt weist auf ein ausgeprägtes Vorfallsmanagement bei den Telekommunikationsanbietern hin.

2.3 Geografische Ausprägung

Zur Ermittlung der geografischen Verteilung von Vorfällen werden diese in die Ausprägungen lokal, regional und bundesweit eingeordnet.

Dabei stellt eine lokale Ausprägung auf eine Betroffenheit einer einzelnen Stadt oder eines Landkreises ab. Typischerweise sind hier nur wenige Teilnehmerinnen und Teilnehmer betroffen. Bezogen auf den Mobilfunk gibt es auf lokaler Ebene nur wenige Sendemasten.

Als regionale Ausprägung werden Störungen verstanden, welche in mehreren Städten bzw. Landkreisen zu Auswirkungen führten. Typischerweise belaufen sich regionale Störungen lediglich auf ein bis zwei Bundesländer.

Vorfälle mit Auswirkungen in mehreren Bundesländern werden der bundesweiten Ausprägung zugeordnet. Störungen dieser Klasse werden oft durch zentrale Komponenten im Kernnetz des Telekommunikationsnetzes verursacht, da Ausfälle dieser Komponenten meist eine große Zahl an Teilnehmerinnen und Teilnehmern im Netz betreffen.

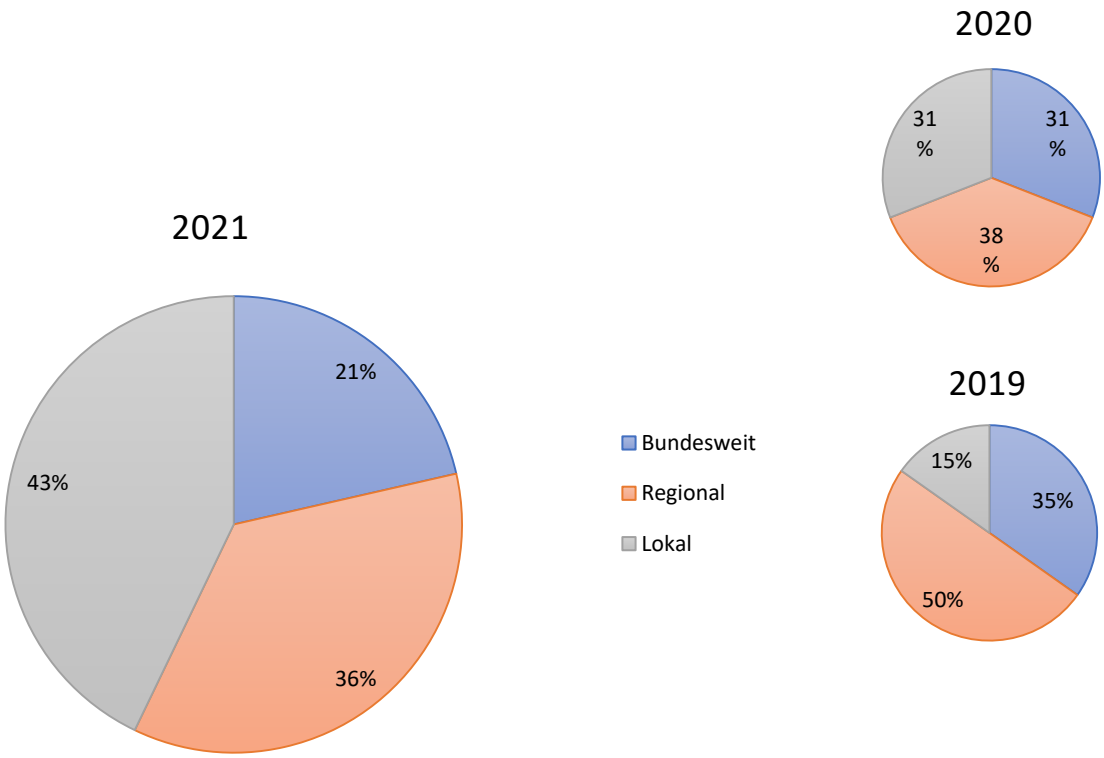

Abbildung 3: Geografische Ausprägung der Vorfälle und Vergleich zu 2020 und 2019

Im Vergleich zu den vorangegangenen Jahren ist in der Verteilung der Störungen ein Anstieg von lokalen Störungen (um circa 30 Prozentpunkte seit 2019) und ein Rückgang an bundesweiten Störungen (um circa 15 Prozentpunkte seit 2019) zu beobachten. Diese Tatsache ist positiv zu werten, da durch weniger bundesweite Störungen typischerweise weniger Teilnehmerinnen und Teilnehmer insgesamt betroffen waren. Sollte sich der Trend auch in den nächsten Jahren fortsetzen, könnte dies ein Indiz dafür sein, dass das Kernnetz der Telekommunikationsnetze robuster geworden ist. Der Anteil an regionalen Störungen hat sich im Vergleich zum Jahr 2020 kaum verändert. Der Anstieg der lokalen Vorfälle korreliert direkt mit der großen Anzahl der gemeldeten Störungen der Notruflenkung.

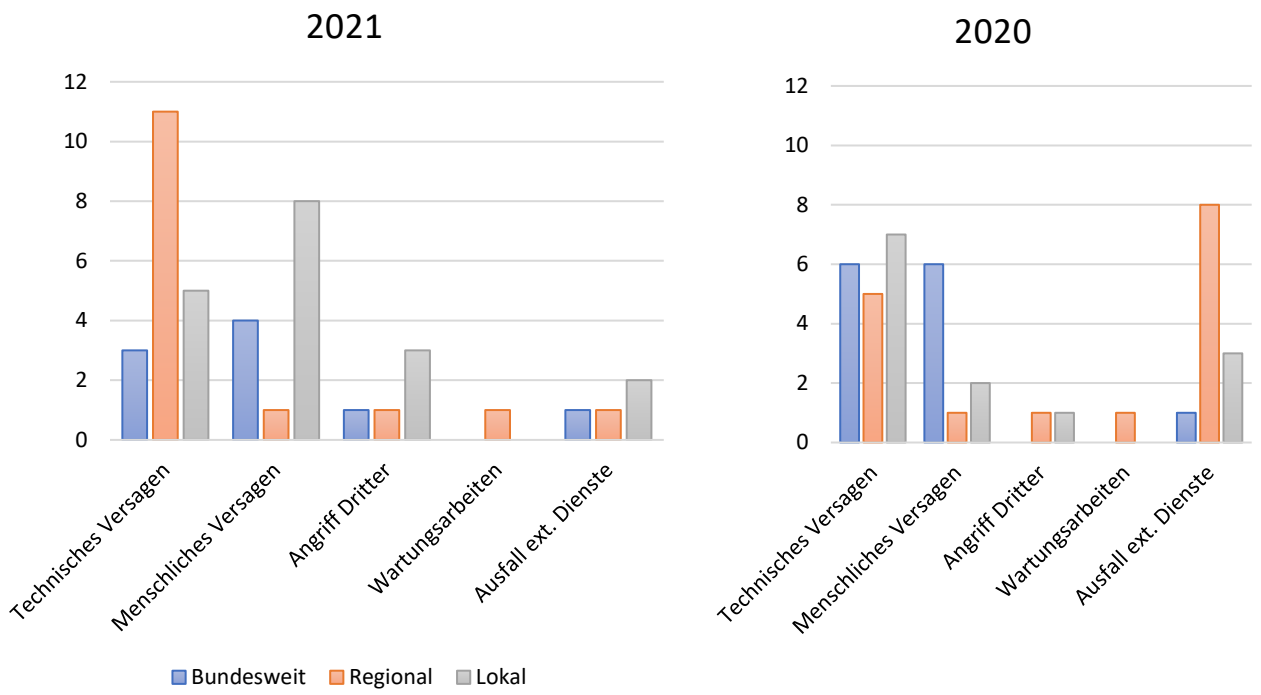

Abbildung 4: Generische Ausfallursachen, aufgeschlüsselt nach der geografischen Ausprägung

Bei der Gegenüberstellung von Hauptursachen und der geografischen Ausprägung, wird im Jahr 2021 ein Anstieg von Vorfällen im lokalen Bereich aufgrund von menschlichem Versagen im Vergleich zum Jahr 2020 deutlich. Die häufigste Ursache waren hier Fehlkonfigurationen. Diese traten öfter bei Störungen auf, die die Notruflenkung beeinträchtigten.

Wie in Kapitel 2.1 beschrieben, gingen die Vorfälle aufgrund von Ausfällen externer Dienstleister im Jahr 2021 erheblich zurück. Damit verschwand auch die Auffälligkeit aus dem Jahr 2020, dass Ausfälle externer Dienste hauptsächlich Störungen auf regionaler und lokaler Ebene bewirkten.

Die bundesweiten Vorfälle entstanden, wie im vorangegangenen Jahr, 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. Bereits einzelne Fehlkonfigurationen oder fehlerhafte Updates im Backbone können 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 aufwändigere Fehleranalysen sowie Anfahrtswege erforderlich sind. Insgesamt wird deutlich, dass Redundanzen auf allen Ebenen eine wichtige Rolle spielen.

Im Jahr 2021 ist auch ein leichter Anstieg von Angriffen zu sehen, die zu erheblichen Beeinträchtigungen auf lokaler Ebene führten. Bei zwei von drei Angriffen, die Auswirkungen auf lokaler Ebene hatten, handelte es sich um physische Angriffe. Bei einem weiteren um einen DDoS-Angriff.

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 die Endkundinnen und Endkunden sich einwählen 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 ist.

Bei 22 der 42 Vorfälle waren die Mobilfunkdienste betroffen und in 28 Fällen die Festnetzdienste (Mehrfachnennung möglich). Im Vergleich zu den vorangegangenen Jahren 2019 und 2020 traten Störungen mit Auswirkungen auf Festnetzdienste erstmals häufiger auf als Auswirkungen auf Mobilfunkdienste.

2.4.1 Ursachen und betroffene Dienste

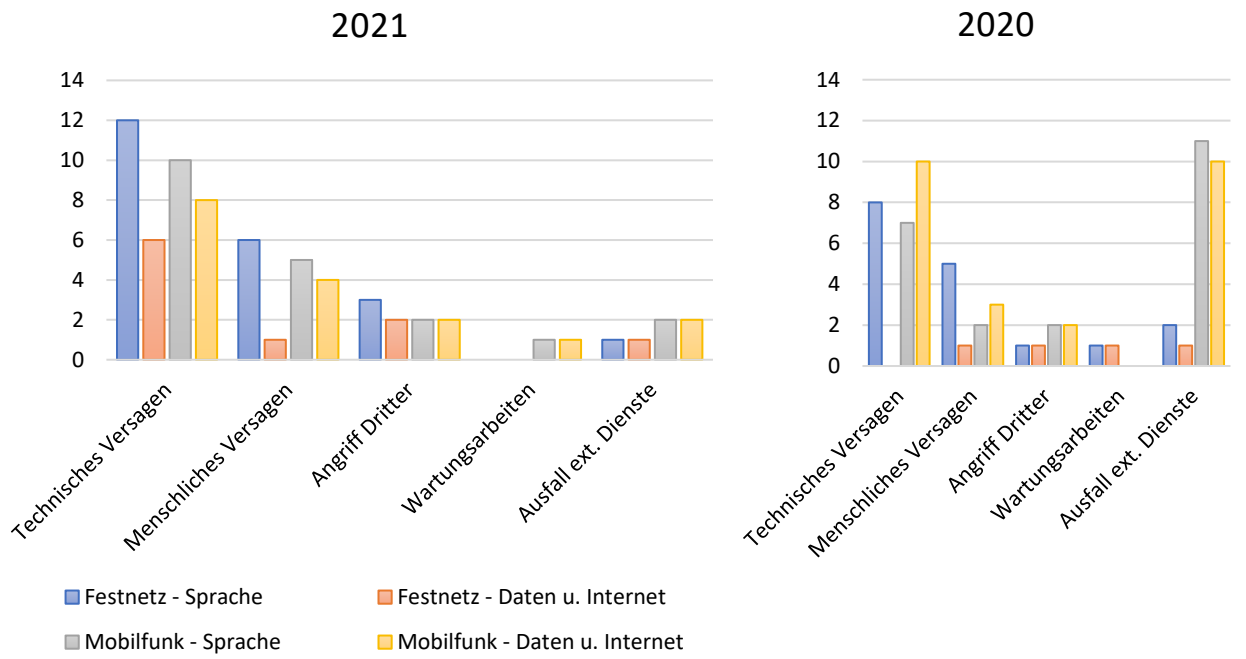

Abbildung 5: Generische Ausfallursachen, aufgeschlüsselt nach betroffenen Diensten

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 beträchtlichen Sicherheitsverletzung. Dies schlägt sich auch in den Meldungen nieder. So war bei 16 von 22 Vorfällen, bei denen der Festnetz-Sprachdienst betroffen war, auch die Notruflenkung tangiert. Dieser Sachverhalt deckt sich auch mit der Verteilung aus 2020.

Der im Jahr 2020 auffällig hohe Anteil an Ausfällen von externen Dienstleistern bei Mobilfunkdiensten ist im Jahr 2021 erheblich zurückgegangen. Das Dienstleister-Management scheint demnach erfolgreich weiterentwickelt worden zu sein.

Ähnlich zum Jahr 2020 war auch 2021 bei der Betroffenheit des Festnetzes und Mobilfunks das technische Versagen die häufigste Ursache. Auffällig ist jedoch in diesem Kontext, dass Vorfälle aufgrund technischen Versagens im Bereich der Festnetz-Datendienste im Jahr 2021 erheblich zunahmen. Im Jahr 2020 gab es keine derartigen Vorfälle; im Jahr 2021 nahm die Zahl der Vorfälle dieser Vorfallsart um sechs zu. Drei dieser sechs Vorfälle sind allerdings dem Flutereignis im Ahrtal zuzurechnen.

2.4.2 Betroffene Dienste und geografische Ausbreitung

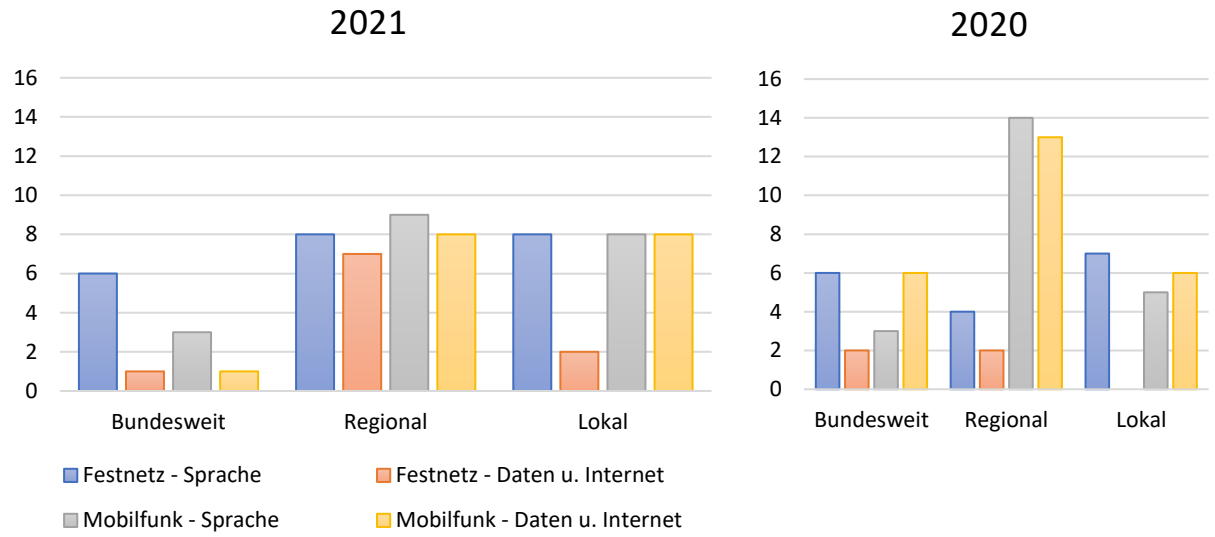

Abbildung 6: Geografische Ausbreitung, aufgeschlüsselt nach betroffenen Diensten

Hinsichtlich der lokalen Ausfälle sind weiterhin Festnetz-Datendienste am seltensten betroffen. Bei den ausgefallenen lokalen Festnetz-Sprachdiensten ist der Meldegrund bis auf eine Meldung die hiermit zusammenhängende Störung der Notruflenkung.

Im Vergleich zum Jahr 2020 ist eine Dominanz der Mobilfunkdienste bei regionalen Ausfällen nicht mehr zu sehen. Vielmehr hat sich bei den regionalen Ausfällen beinahe eine Gleichverteilung zwischen allen Diensten hergestellt.

Bei Störungen mit bundesweiten Auswirkungen waren am häufigsten Festnetz-Sprachdienste betroffen. In drei der sechs Vorfälle führten Fehlkonfigurationen an zentralen Netzelementen zu den Auswirkungen. Die restlichen Dienste spielen eine untergeordnete Rolle.

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, die hiermit einen Beitrag zur Bewertung der Cyber-Sicherheitslage und damit zur Verbesserung der Cyber-Sicherheit in Deutschland leisten. Im Folgenden werden die Erkenntnisse aus den Pflichtmeldungen um die aus den freiwilligen Meldungen ergänzt, um ein detaillierteres Lagebild zu erhalten.

Die Gesamtzahl der Meldungen, die als „nicht erhebliche Sicherheitsverletzung (freiwillig)“ eingestuft wurden, ist im Vergleich zu den Jahren 2019 und 2020 in etwa 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 Umfang des Vorfalls noch nicht vollständig absehbar war, wurden in diesen Fällen die Behörden vorsorglich ins Bild gesetzt.

Die größte Häufung belief sich bei den freiwilligen Meldungen auf die Hauptursache Angriffe. Dabei handelte es sich um

- DDoS-Angriffe,
- Verwundbarkeiten im Kontext mit Microsoft Exchange-Schwachstellen, zu denen das BSI im Rahmen mehrerer Warnmeldungen informiert und verwundbare Betreiber zudem telefonisch direkt gewarnt hatte,
- unberechtigte Login-Versuche am Kundenportal sowie
- Rufumleitungen ins Ausland.

4 Flutkatastrophe im Ahrtal

Das Flutereignis im Ahrtal im Sommer 2021 sorgte auch in der Telekommunikationsbranche für eine erhöhte Zahl von meldepflichtigen Vorfällen mit beträchtlichen und lang anhaltendenden Auswirkungen aufgrund von Naturkatastrophen.

Als direkte Auswirkung nach der Flut war die Beeinträchtigung bis hin zur Nichterreichbarkeit des Mobilfunknetzes aller vier großen Mobilfunknetzbetreiber zu spüren.[1] Durch die Überflutung von Basisstationen sowie die Zerstörung der Glasfaserinfrastruktur kam es zu Ausfällen im gesamten Bereich der Ahr. Neben dem Mobilfunknetz waren aufgrund der infrastrukturellen Schäden auch Festnetzdienste betroffen.

Durch mobile Notfallsendemasten inkl. Notstromaggregate konnte der Netzbetrieb innerhalb weniger Tage rudimentär wieder etabliert werden. Die betroffenen Telekommunikationsanbieter haben dahingehend sehr schnell reagiert und auf existierende Notfallprozesse zurückgegriffen. Dennoch sorgte insbesondere die Aufstellung und Belieferung der entsprechenden Anlagen für Hürden. So fielen beispielsweise einige Sendemasten aus, obwohl sie nicht von dem Unwetter beschädigt waren, die jedoch aufgrund des nicht funktionierenden Stromnetzes nicht mehr mit Strom versorgt wurden. Da die Sendemasten aufgrund der infrastrukturellen Schäden, u. a. an Straßen, nicht mit Betriebsstoffen für die Notstromaggregate beliefert werden konnten, waren diese Sendemasten ebenfalls aufgrund der fehlenden Stromversorgung nach kurzer Zeit funktionslos.

An die Bewohner des Ahrtals wurden in Folge der Ereignisse Mobiltelefone und Powerbanks ausgegeben.

Wesentlich schwieriger war die Instandsetzung der zerstörten Festnetzinfrastruktur. Durch die extremen Zerstörungen der Ortschaften dauerten die Maßnahmen zur Beseitigung der meisten Schäden bis ins Jahr 2022 an. Diese lange Behebungszeit war damit verbunden, dass die Telekommunikationsanbieter oft keine Einflussmöglichkeiten auf die infrastrukturellen Wiederherstellungsarbeiten hatten.

Der Vorfall macht deutlich, dass das Mobilfunknetz trotz erheblicher infrastruktureller Schäden schnell wiederhergestellt werden kann, solange zentrale Systeme im Mobilfunknetz weiterhin verfügbar sind. Eine lückenlose Abdeckung der betroffenen Gebiete ist jedoch in einer derartigen Notsituation schwierig zu erreichen. Nationales Roaming könnte sich in derartigen Vorfällen positiv auswirken, da die Telekommunikationsanbieter gemeinsam eine höhere und zuverlässigere Abdeckung der betroffenen Gebiete erreichen können und sich Lasten an einzelnen Sendemasten gegebenenfalls besser verteilen lassen. Um im Krisen- oder Ereignisfall eine schnelle Umsetzung von Nationalem Roaming zu ermöglichen sollten Telekommunikationsanbieter bereits heute die notwendigen Vorbereitungen und Absprachen untereinander anstoßen.

Der Wiederaufbau des Festnetzes inklusive Glasfaseranbindungen nimmt bei derartigen infrastrukturellen Schäden sehr viel Zeit in Anspruch, in der die Festnetzdienste den Kunden nicht zur Verfügung stehen. Diese Tatsache unterstreicht die herausgehobene Bedeutung von Mobilfunk, die insbesondere in Verbindung mit der stärkeren Vernetzung durch 5G umso mehr an Relevanz gewinnt.

[1] https://www.spiegel.de/netzwelt/netzpolitik/hochwasser-gebiete-provider-stellen-mobilfunknetz-wieder-her-a-40805f59-a610-4557-a123-9f3013ddf5ec

5 Fazit

Wie in den vergangenen Jahren zeichnet sich durch das Meldegeschehen ein hohes Absicherungsniveau im Bereich der IT-Sicherheit in der Branche Telekommunikation ab. Abgesehen von sehr außergewöhnlichen externen Ereignissen, zu der die Flutkatastrophe im Ahrtal zu rechnen ist, tragen im Berichtszeitraum externe Faktoren kaum zu Vorfällen bei. Besonders erfreulich ist, dass die Anzahl an Vorfällen durch Ausfälle externer Dienstleister stark zurückging.

Durch die Vorfälle aufgrund menschlichen und technischen Versagens wird ersichtlich, wie schnell bereits einzelne Fehlhandlungen oder eine zu ungenaue Übersicht über die im Netz verbauten Komponenten zu erheblichen Auswirkungen führen können. Insbesondere ein 4- bzw. 6-Augen-Prinzip bei Konfigurationsänderungen im Backbone-Netz sowie ein detailliertes Nachhalten und Überwachen des Lebenszeitendes („end of life“) der verbauten Komponenten und ein damit einhergehendes Patch- und Update-Management sind daher ungemein wichtig.

Obwohl Angriffe in den gemeldeten Vorfällen eine untergeordnete Rolle gespielt haben, ist die Branche Ziel von Angriffen. Das BSI bewertet das Risiko von Cyber-Angriffen als sehr hoch. Hinzu kommt das ebenso ernstzunehmende Risiko von sonstigen Angriffen, beispielsweise von Sabotageakten. Dieser Sachverhalt spiegelt sich auch in der gestiegenen Anzahl an meldepflichtigen Vorfällen, die aufgrund von Angriffen verursacht wurden, sowie in der Tatsache, dass die Hauptursache bei den freiwillig gemeldeten Vorfällen Angriffe waren, wider. 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 insbesondere auch am Fall des Flutereignisses im Ahrtal deutlich. Dort waren die Vorfälle mit einer geografischen Betroffenheit und einer infrastrukturellen Zerstörung verbunden, wodurch die Versorgung der Bevölkerung über Wochen hinweg nicht wie gewohnt erbracht werden konnte.

Abschließend ist festzustellen, dass das im BSI gebildete und hiermit veröffentlichte Lagebild stark vom Detailierungsgrad 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