Bundesamt
für Sicherheit in der
Informationstechnik

Rückblick auf die gemeldeten IT-Sicherheitsvorfälle der Branche Telekommunikation 2019

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
1.0	15.05.2020	BSI	Finalisierung Bericht und Abstimmung mit BNetzA

Bundesamt für Sicherheit in der Informationstechnik Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582- 0
E-Mail: referat-wg14@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

Abbildungsverzeichnis

1 Einleitung

Der Sektor Informationstechnik und Telekommunikation (IT und TK) stellt durch die Dienstleistung „Sprach- und Datenübertragung“ die technische Basisinfrastruktur zum Austausch von Sprache und Daten für die Allgemeinheit zur Verfügung. Der Sektor IT und TK ist dabei ein Sektor Kritischer Infrastrukturen, die in der „Nationalen Strategie zum Schutz Kritischer Infrastrukturen“ bestimmt wurden. 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. 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 nach § 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 Meldekriterien und -schwellen zutrifft:

- Betroffene Teilnehmerstunden mit dem Grenzwert von 1 Million (Produkt aus der 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 bzw. eine Abschlussmeldung nach Abschluss des Vorfalls zu vervollständigen.

Für diesen Bericht wurden die Meldungen der TKG-verpflichteten Betreiber des Jahres 2019 (1. Januar bis 31. Dezember) analysiert und ausgewertet. Dabei handelt es sich größtenteils um Meldungen der Betreiber Kritischer Infrastrukturen 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 auch deren Meldungen in diesem Bericht berücksichtigt. Auf diese Weise dient der Bericht als Darstellung der IT-Sicherheitslage im Kontext Kritischer Infrastrukturen und soll insbesondere Betreibern Kritischer Infrastrukturen aus allen Sektoren die Möglichkeit geben, die Erkenntnisse aus diesem Bericht in die eigene IT-Sicherheitsbetrachtung mit einfließen zu lassen.

Die im Bericht genannten Daten basieren auf den von den TK-Netzbetreiber und TK-Diensteerbringern über das Meldeformular angegebenen und durch das BSI plausibilisierten Werten. Eine exakte Angabe der

betroffenen Teilnehmer ist den TK-Netzbetreiber und TK-Diensteerbringern oft nicht möglich. Die im Bericht genannten Zahlen dienen daher eher als Richtwert. Die Anzahl der real betroffenen Teilnehmer bei den Vorfällen kann deshalb von der genannten Zahl abweichen. Zur Wahrung der schutzwürdigen Interessen der Meldenden nennt der Bericht keine konkreten Betreiber sowie Gebiete.

.

2 Analyse der Vorfälle

Im Jahr 2019 sind zu 62 Vorfällen Meldungen aus der Telekommunikationsbranche beim BSI und der BNetzA eingegangen. Hiervon wurden 47 nach den oben genannten Kriterien und Schwellen als Pflichtmeldungen (Vorfälle mit beträchtlichen Sicherheitsverletzungen) klassifiziert. Für die Analyse wird jeweils der letzte gemeldete Sachstand des jeweiligen Vorfalls herangezogen. Die TK-Netzbetreiber und TK-Diensteerbringer ordnen die Vorfälle den folgenden Kategorien der IT-Schutzziele zu:

- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Authentizität

Insgesamt gab es durch Vorfälle mit Einschränkungen der Verfügbarkeit eine Ausfallzeit von 153.327.665 Teilnehmerstunden.

Hinzu kamen 75.364.473 Teilnehmerstunden durch einen Vorfall, bei dem die Vertraulichkeit verletzt war. Bei diesem Vorfall handelte es sich um eine einzige Störung, die länger als ein Jahr andauerte. Deshalb wird sie im Folgenden als statistischer Ausreißer behandelt und nicht weiter betrachtet.

2.1 Hauptursachen

Die Vorfälle lassen sich in fünf Hauptkategorien bezüglich der Ursache unterteilen:

- technisches Versagen
- Angriff Dritter
- Ausfall externer Dienste
- menschliches Versagen
- 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, zusammengefasst, aber auch Angriffe auf Hardware, wie beispielsweise Vandalismus.

In der Kategorie „Ausfall externer Dienste“ werden Vorfälle zusammengefasst, 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

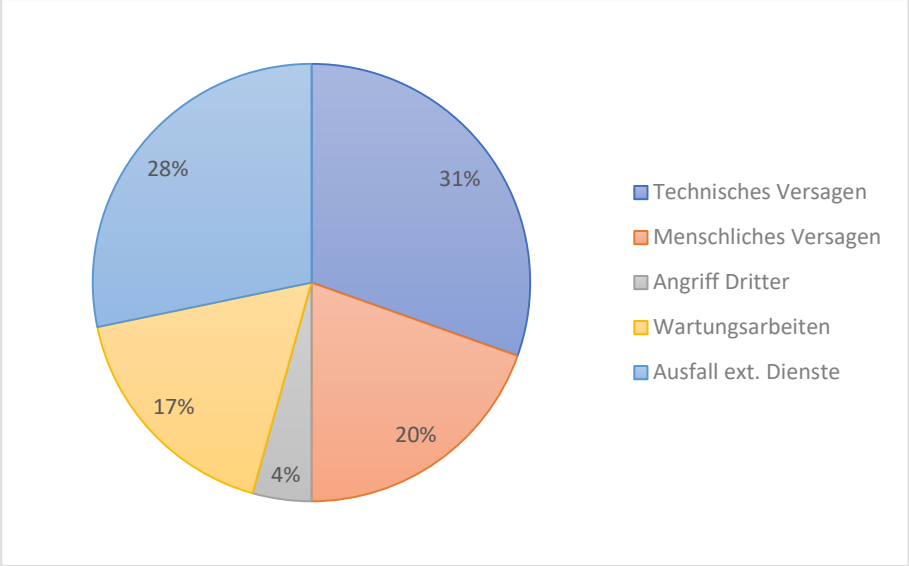

Abbildung 1: prozentuale Darstellung der Ursachen meldepflichtiger Vorfälle

Wie in Abbildung 1 zu sehen ist, lassen sich die meisten Vorfälle im Zeitraum 2019 zu den Kategorien „technisches Versagen“ und „Ausfall externer Dienste“ zuordnen. Zusammen bilden diese beiden Kategorien mit fast 60 % die häufigsten Ausfallursachen. Die Kategorie „Angriffe Dritter“ bildet mit 4 % eine untergeordnete Rolle.

Vorfälle, die sich der Kategorie „Technisches Versagen“ zuordnen lassen, wiesen als Ursache meistens einen Hardware-, Softwaredefekt oder einen Kabelbruch auf.

Vorfälle, die auf Ausfälle externer Dienstleister zurückzuführen sind, wiesen als initiale Ursache technisches Versagen oder einen Stromausfall beim Dienstleister auf.

Bei Vorfällen, bei denen menschliches Versagen ursächlich war, dominierten Fehlkonfigurationen.

Bei der Kategorie „Angriff Dritter“ ist zu berücksichtigen, dass IT-Angriffe durch Sicherheitsmaßnahmen abgeschwächt oder gänzlich abgewehrt werden können und somit erst gar nicht die Meldekriterien erreichen, was die geringe Zahl an Vorfällen erklärt.

2.1.2 Ausfallzeiten im Bezug zu den Ursachen

Im Meldeformular werden die vermutete Anzahl betroffener Teilnehmer sowie die Dauer des Vorfalls angegeben. Aus den genannten Daten wird die Ausfallzeit für jeden Vorfall berechnet. Nachfolgend werden die Ausfallzeiten den Ursachen gegenübergestellt.

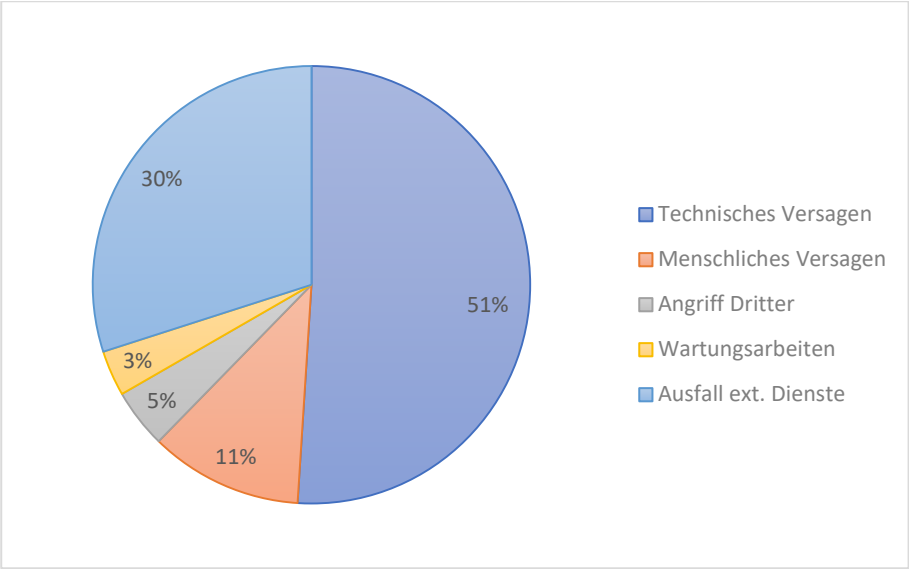

Abbildung 2: prozentuale Darstellung der Ursachen meldepflichtiger Vorfälle an der gesamten Ausfallzeit

Es ist deutlich zu sehen, dass die Kategorie „Technisches Versagen“ bei 31 % Anteil der Vorfälle (vgl. Abbildung 1) mehr als die Hälfte (51 %) der betroffenen Teilnehmerstunden verursacht. Dies ist darauf zurückzuführen, das bei einem technischen Versagen meist eine aufwändige Fehleranalyse und -suche durchgeführt werden muss. Bei menschlichem Versagen lässt sich der Fehler im Allgemeinen schnell finden und beheben. Aus diesem Grund ist die durch Vorfälle der Kategorie „Menschliches Versagen“ entstandene Ausfallzeit geringer.

Bei Ausfällen externer Dienste kann der TK-Netzbetreiber oder TK-Diensteerbringer meist nicht selbst die Ursache beheben. Die vor die Behebung geschaltete Kontaktaufnahme und eventuelle Eskalation bei dem externen Dienstleister wirkt sich negativ auf die Ausfallzeit auf.

2.1.3 Gegenüberstellung der Ursachen und der Dienste

Eine Zuordnung der betroffenen Dienste (Festnetz: Sprache und Internet, Mobilfunk: Sprache und Internet) je Vorfall erfolgt durch den Betreiber oder Erbringer selbst. Dies geschieht durch eine Angabe im eingereichten Meldeformular. Eine Mehrfachnennung von Diensten je Vorfall ist möglich.

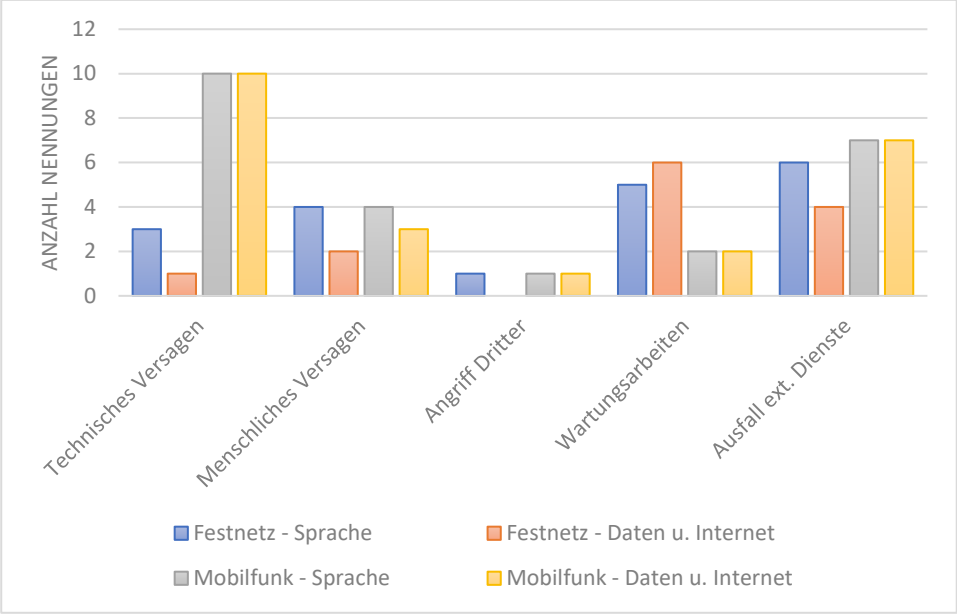

Abbildung 3: Darstellung der betroffenen Dienste je Ursachenkategorie

Beim Ausfall von Mobilfunk-Diensten zeigt sich eine Häufung im Bereich der Kategorie „Technisches Versagen“. Dies ist vor allem auf Hardwaredefekte zurückzuführen. Wartungsarbeiten betreffen hauptsächlich den Festnetzbereich, was daran liegen könnte, dass die gemeldeten Wartungsarbeiten meist an Kabelleitungen durchgeführt wurden.

2.2 Vorfälle unterteilt nach Meldekriterien

Je nach Ausprägung des Vorfalls können von den Betreibern oder Erbringern entweder ein oder mehrere Meldekriterien gleichzeitig ausgewählt werden. Die nachfolgende Darstellung würdigt die jeweils bei Vorfällen angegebenen Meldekriterien getrennt voneinander.

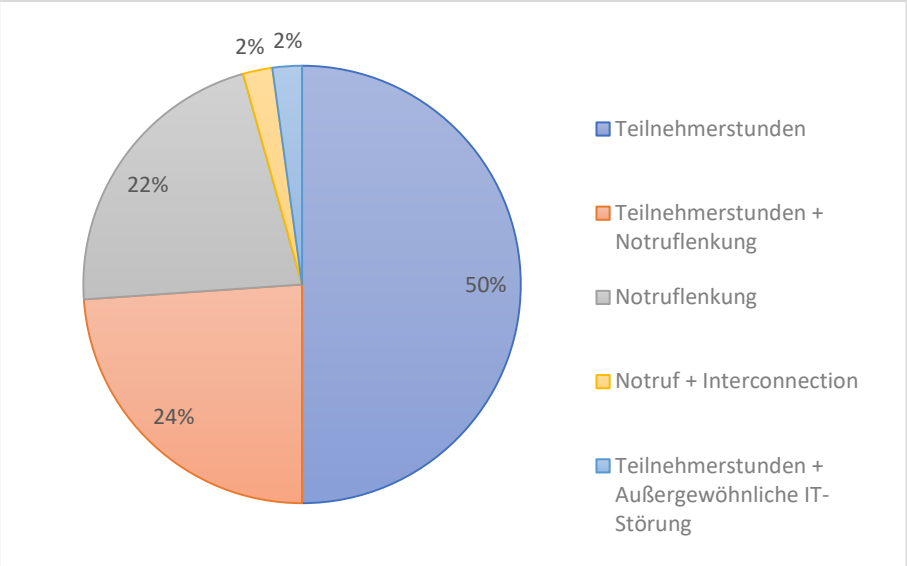

Abbildung 4: prozentuale Darstellung der Vorfälle je Meldekategorie

Die meisten Vorfälle erfolgen aufgrund der Überschreitung des Meldekriteriums von einer Million Teilnehmerstunden und/oder der Betroffenheit der Notruflenkung. Außergewöhnliche IT-Störungen sowie Internationale Zusammenschaltungen sind nur äußerst seltene Meldegründe.

2.3 Geografische Ausprägung

Im Meldeformular ist die geografische Ausprägung vom meldenden TK-Netzbetreiber oder TK-Dienste-erbringer anzugeben. Im Regelfall werden hierbei Postleitzahlen oder sonstige Bezeichnungen, wie Vorwahlen, verwendet. Zur Aufbereitung einer statistischen Auswertung, werden diese Angaben der geografischen Ausprägung von den angegebenen Bezeichnungen auf die Kategorien

- lokal (max. eine Stadt/Landkreis betroffen)
- regional (max. ein Bundesland betroffen) und
- bundesweit (mindestens zwei Bundesländer betroffen)

übertragen.

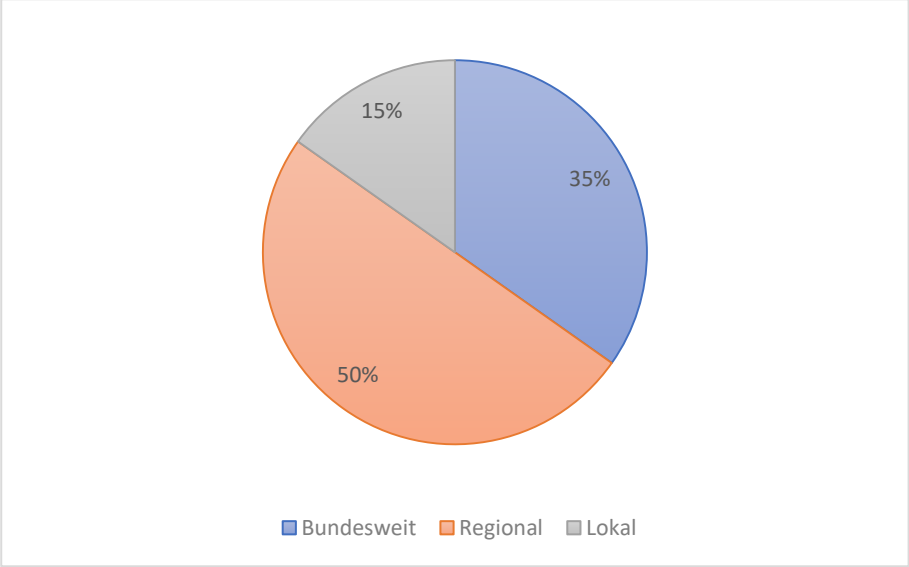

Abbildung 5: prozentuale Darstellung der geografischen Ausprägung der Meldungen

In Abbildung 5 ist erkennbar, dass regionale Ausfälle die Hälfte der Vorfälle ausmachen. Dies lässt sich dadurch erklären, dass lokale Ausfälle nur selten die Meldeschwelle erreichen, bundesweite Vorfälle wiederum meist durch Redundanzen aufgefangen werden können, und es so zu weniger beträchtlichen Vorfällen kommt.

Es ist davon auszugehen, dass eine große Anzahl von lokalen Vorfällen unterhalb der Meldeschwellen existieren.

2.3.1 Korrelation betroffener Dienste und der geografischen Ausprägung

Beim Vergleich der Dienste (Festnetz: Sprache und Internet, Mobilfunk: Sprache und Internet) mit den geografischen Ausprägungen ergibt sich das in Abbildung 6 dargestellte Bild. Es können je Vorfall mehrere Dienste betroffen sein.

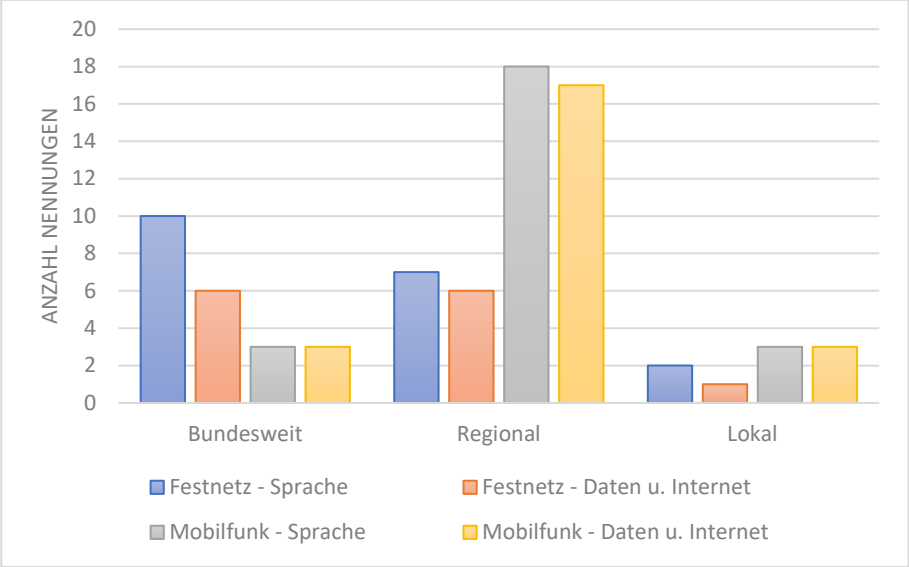

Abbildung 6: Darstellung der betroffenen Dienste zur geografischen Ausprägung

Bei den bundesweiten Ausfällen dominieren die Festnetzdienste, wohingegen bei regionalen und lokalen Vorfällen die Mobilfunkdienste stärker betroffen sind. Die bundesweiten Vorfälle betrafen meistens das Kernnetz des jeweiligen Betreibers oder Erbringers, wohingegen die lokalen und regionalen Ausfälle hauptsächlich im Zugangsnetz stattfanden, wodurch sich dort auch die starke Betroffenheit des Mobilfunks erklären lässt.

2.3.2 Korrelation Ursachen und geografische Ausprägung

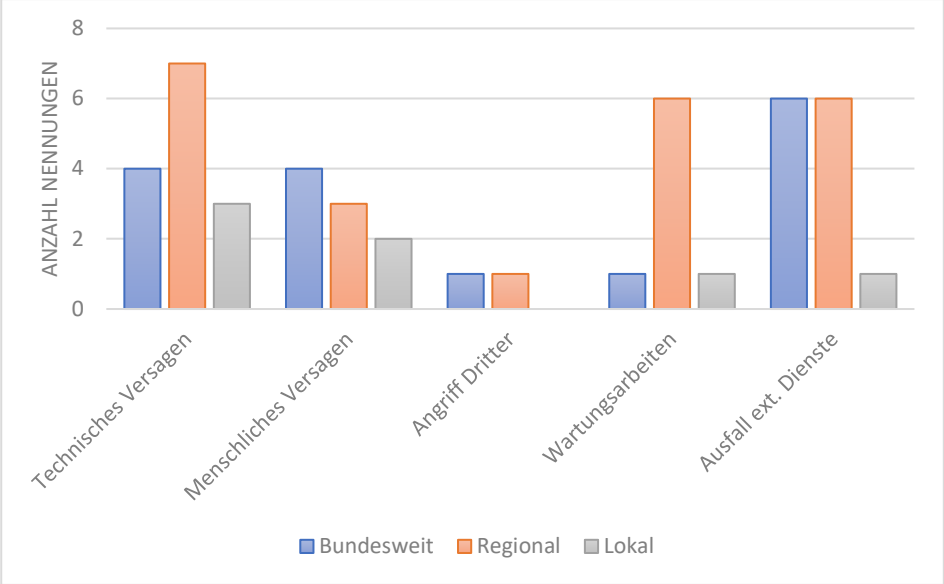

Abbildung 7: Darstellung der geografischen Ausprägung zu den Ursachen

Die Vorfälle aus der Kategorie „Technisches Versagen“, die gleichzeitiger bundesweite Auswirkungen hatten, sind hauptsächlich auf Softwarefehler als Ursache zurückzuführen. Hingegen liegen bei den regionalen Vorfällen aus dieser Kategorie hauptsächlich Kabeldefekte als Ursache zugrunde.

Bei Wartungsarbeiten sind primär regionale Vorfälle gemeldet worden. Dies könnte daran liegen, dass bei Wartungsarbeiten für bundesweite Bereiche entsprechende Redundanzen vorhanden und somit keine Ausfälle zu erwarten sind.

Bei den restlichen Kategorien lässt sich keine Häufung einzelner Ursachen erkennen, die eine Aussage ermöglichen würden.

3 Freiwillige Meldungen

Das BSI und die BNetzA erreichen nicht nur Pflichtmeldungen aus der Telekommunikationsbranche. So kann jedes Unternehmen 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 Cybersicherheitslage und damit zur Verbesserung der Cybersicherheit in Deutschland zu leisten, sehr. Im Folgenden werden die Pflichtmeldungen um die Erkenntnisse aus den freiwilligen Meldungen ergänzt, um so einen detaillierteren Datensatz zu erzeugen.

Zusätzlich zu den 47 Pflichtmeldungen wurden 15 Vorfälle auf freiwilliger Basis gemeldet. Die freiwilligen Meldungen veränderten die bereits bei den Pflichtmeldungen dargestellte Verteilung der Ursachenkategorien nicht grundlegend. Einzig bei der Kategorie „Angriff Dritter“ lässt sich ein größerer Anstieg verzeichnen. So wurden acht Vorfälle, die sich dieser Kategorie zuordnen lassen, gemeldet. Prozentual wächst dadurch der Anteil der Vorfälle, die sich der Kategorie „Angriff Dritter“ zuordnen lassen, auf 16 %. Die Hauptursache waren hierbei DDoS- und Bruteforce-Angriffe.

Wie bereits erwähnt lässt sich daraus schließen, dass die TK-Netzbetreiber und TK-Diensteerbringer durchaus solchen Angriffen ausgesetzt sind, diese aber – aufgrund von teilweiser oder erfolgreicher Mitigation - nur in seltenen Fällen eine so große Auswirkung haben, dass sich daraus eine außergewöhnliche IT-Störung oder eine Betroffenheit von eine Million Nutzerstunden ergibt, die dann zu einer Meldung verpflichten würde.

4 Fazit

Aus den erhobenen Daten wird ersichtlich, dass Störungen unabhängig von ihrer Ursache gleichermaßen zu Auswirkungen für die Nutzer in Deutschland führen können. Für einen Bürger oder ein angeschlossenes Unternehmen ist es unerheblich, was zu einem Ausfall der Telekommunikationsdienstleistung geführt hat. Statistisch gesehen war jeder Nutzer in Deutschland circa 2 Stunden im Jahr 2019 von Auswirkungen beträchtlicher (meldepflichtiger) Vorfälle betroffen. Hinzu kommen Auswirkungen von Störungen, hauptsächlich im lokalen Bereich, die nicht meldepflichtig sind.

2019 führten nur wenige IT-Angriffe zu Vorfällen mit beträchtlichen Beeinträchtigungen. Dies darf allerdings nicht zu dem Fehlschluss führen, dass die Telekommunikationsbranche nicht Ziel von IT-Angriffen ist. So äußerten verschiedene TK-Netzbetreiber in Gesprächen mit dem BSI, dass sie eine Großzahl von IT-Angriffen (wie beispielsweise DDoS, Malware, Phishing) im Rahmen des Tagesgeschäfts in ihren Netzen sehen. Bei TK-Netzbetreibern und TK-Diensteerbringern ist nach eigenen Aussagen von einem hohen Sicherheitsniveau auszugehen, durch welches eine Großzahl von Angriffen detektiert und abgewehrt werden können, bevor sich diese zu einer meldepflichtigen Beeinträchtigung entwickeln. Das BSI hat derzeit keinen Anlass, an dieser Einschätzung zu zweifeln. Einerseits spricht die geringe Zahl an Meldungen von Vorfällen aufgrund von IT-Angriffen dafür, dass diese mit den bestehenden Sicherheitsmechanismen abgewehrt werden können. Andererseits legen TK-Netzbetreiber und TK-Diensteerbringer der BNetzA im Rahmen von § 109 Absatz 4 TKG ihr Sicherheitskonzept vor, sodass davon auszugehen ist, dass eventuelle Sicherheitsmängel zeitnah behoben werden. Grundsätzlich kann allerdings nicht ausgeschlossen werden, dass organisierte, aufwändigere Angriffe zu massiven Schäden führen könnten.

Aufgrund dessen und vor dem Hintergrund der sich ständig ändernden Bedrohungslage sollten TK-Netzbetreiber und TK-Diensteerbringer auch weiterhin die Umsetzung des Standes der Technik in ihrem Unternehmen vorantreiben sowie eine Reduktion der Ausfallzeiten anstreben. Im Hinblick auf die im Jahr 2019 aufgeführten Ursachen, die zu meldepflichtigen Vorfällen geführt haben, können unter anderem folgende Maßnahmen eine Orientierung bieten:

- Nutzung des 4-Augen-Prinzips
- Abgleich der eingesetzten Hardware mit der erwarteten Produktlebenszeit sowie rechtzeitiger Austausch alter Hardware
- Identifizierung der Abhängigkeiten von Dienstleistern
- Reaktionszeiten von Dienstleistern vertraglich festlegen
- Etablierung von Kommunikationskanälen zu den Dienstleistern, Aufbau von Eskalationsprozessen unter Einbeziehung der zuständigen Mitarbeiter kommunizieren sowie Beübung
- detaillierte Beschreibung der Schnittstellen zwischen Netzbereichen
- weiterer Ausbau von Redundanzen.

Sind Nutzer der Telekommunikationsnetze bzw. -dienste aufgrund erhöhter Anforderungen auf das Funktionieren der Telekommunikationsdienstleistung angewiesen, wäre es ratsam, die Verfügbarkeit durch zusätzliche Telekommunikationsanschlüsse anderer TK-Netzbetreiber und TK-Diensteerbringer oder 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.

Abschließend ist anzumerken, dass ein solches Lagebild stark vom Detailgrad der eingereichten Meldungen abhängig ist. Je detaillierter und nachvollziehbarer die einzelnen Meldungen hinsichtlich der Ursachen, dem Hergang und der Auswirkungen sind, desto vollständiger und genauer kann auch ein Lagebild erstellt werden.

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