Resilienz der TK-Netze stärken

Herausforderungen &
Handlungsempfehlungen

bitkom

Auf einen Blick

Resilienz der Telekommunikationsnetze stärken

Ausgangslage und Bitkom-Bewertung

Telekommunikationsnetze sind einer stetig wachsenden Zahl schwerer Störungen und außergewöhnlicher Angriffe ausgesetzt. Der Umgang mit vergangenen Krisen wie der Ahrtalflut, der Energiekrise, Cyberangriffen und nicht zuletzt den Anschlägen auf das Stromnetz in Berlin zeigt, dass die Telekommunikationsinfrastruktur bereits gut aufgestellt ist. Gleichwohl besteht in der Branche Einigkeit, dass die Resilienz der Netzinfrastruktur und digitaler Dienste präventiv angepasst und mit Blick auf die zunehmende Bedrohungslage weiter gestärkt werden muss.

Das Wichtigste

- **Resilienz**
  Für die Definition von Resilienz ist zwischen drei Dimensionen zu unterscheiden: der digitalen Resilienz, der physischen Resilienz und der Resilienz gegenüber Versorgungsstörungen.
- **Risiken: Die wichtigsten Bedrohungen**
  Besonders relevante Risiken sind Elementarschäden, extreme Temperaturen, Versorgungsstörungen, immense und netzübergreifende Cyberangriffe sowie vorsätzliche Beschädigung und Sabotage.
- **Voraussetzungen für resiliente TK-Netze und digitale Dienste**
  Eine krisensichere Stromversorgung ist die zentrale Grundvoraussetzung für den Betrieb von Telekommunikationsnetzen. Zudem sind sichere und zuverlässige Lieferketten von hoher Bedeutung.
- **Was wir bereits tun**
  Die Branche ist durch Investitionen in Schutzmaßnahmen und durch einen energieeffizienten Stromverbrauch bei Energiemangel bereits gut für verschiedenste Notfälle gerüstet. Alle Anbieter prüfen permanent eine Vielzahl von Möglichkeiten, wie die Resilienz von Telekommunikationsnetzen und digitalen Diensten gestärkt werden kann. Dazu sind sie auch fortlaufend im Austausch mit den politischen Institutionen und Behörden.
- **Was noch zu tun ist**
  Die prioritäre Energieversorgung der Netzbetreiber bei Krisen- und Katastrophenfällen ist dringend erforderlich. Vor Implementierung weiterer Schutzmaßnahmen ist unbedingt eine genaue Prüfung bereits vorhandener Notfall- und Sicherheitsvorrichtungen durchzuführen. Sollten zusätzliche kostenintensive Maßnahmen vorgeschrieben werden, müsste nicht nur eine faire Verteilung der Kosten erfolgen, sondern auch weitere Aspekte berücksichtigt werden, wie z. B. Machbarkeit und zeitliche Perspektive. Zudem sind mittel- bis langfristige staatliche Investitionen in Forschung und Entwicklung zur Stärkung der TK-Resilienz notwendig.

Inhalt

1 Allgemeine Einschätzung & Einordnung

Der jüngste Anschlag auf das Berliner Stromnetz Anfang des Jahres hat erneut verdeutlicht, wie eng die Funktionsfähigkeit der Telekommunikationsnetze mit der Stabilität anderer kritischer Infrastrukturen verknüpft ist. Die gezielte Beschädigung an der Energieversorgung führte zu spürbaren Einschränkungen auch beim Mobilfunk. Der Vorfall reiht sich ein in eine Serie von Ereignissen – von vorsätzlicher Sabotage bis hin zu Naturkatastrophen wie der Flut im Ahrtal – die zeigen, dass selbst lokal begrenzte Störungen erhebliche Kaskadeneffekte entfalten können.

Telekommunikationsnetze nehmen dabei eine Schlüsselrolle ein: Sie sind nicht nur selbst von Störungen betroffen, sondern ihre Verfügbarkeit ist zugleich Voraussetzung für die Funktionsfähigkeit nahezu aller anderen kritischen Infrastrukturen – von der Koordination der Krisenbewältigung über die Aufrechterhaltung von Zahlungssystemen bis zur medizinischen Versorgung. Ihre Funktionsfähigkeit steht und fällt jedoch mit einer stabilen Energieversorgung – und genau hier liegt die sektorenübergreifende Verwundbarkeit der gesamten Daseinsvorsorge: Ein Ausfall der Stromversorgung trifft nicht nur die Telekommunikation, sondern gleichzeitig die Lebensmittelversorgung, den Bezug von Kraftstoffen zur Aufrechterhaltung der Mobilität sowie die Wärme- und Wasserversorgung. Darüber hinaus geraten ebenso Einrichtungen der Daseinsfürsorge wie Arztpraxen, Krankenhäuser und Pflegeheime, ohne eine funktionierende Energieversorgung schnell an ihre Grenzen.

2 Definition Resilienz

»Resilienz beschreibt die Fähigkeit eines Systems, einer Gemeinschaft oder einer Gesellschaft, sich rechtzeitig und effizient den Auswirkungen einer Gefährdung zu widersetzen, diese zu absorbieren, sich an sie anzupassen, sie umzuwandeln und sich von ihnen erholen zu können.« (BMI 2022)[1]

Telekommunikationsnetze müssen mit einer stetig steigenden Anzahl von schweren Störungen und außergewöhnlichen Angriffen umgehen können und dagegen resilienter werden. Dabei ist zwischen drei Dimensionen der Resilienz zu unterscheiden, nämlich der digitalen Resilienz, der physischen Resilienz sowie der

[1] Vgl. Deutsche Strategie zur Stärkung der Resilienz gegenüber Katastrophen, Umsetzung des Sendai Rahmenwerks für Katastrophenvorsorge (2015-2030) – Der Beitrag Deutschlands 2022-2030; Bundesregierung, Bundesministerium des Innern 2022; übersetzt aus: Sendai Framework for Disaster Risk Reduction 2015-2030, United Nations UNDRR 2015.

Resilienz gegenüber Versorgungsstörungen. Digitale Resilienz meint die Widerstandsfähigkeit gegenüber Störungen, die aufgrund digitaler Angriffe oder Ausfälle auftreten. Physische Resilienz bezieht sich hingegen auf Objektschutzmaßnahmen für die Anlagen der Telekommunikationsnetze gegenüber Bedrohungen, wie z. B. Elementarschäden, extreme Temperaturen, vorsätzliche oder versehentliche Beschädigung oder Diebstahl. Beispiele für Versorgungsstörungen umfassen Strommangel und -ausfälle sowie Verzögerungen und Einschränkungen in der Lieferkette für Netzausrüstung.

3 Risiken: Die wichtigsten Bedrohungen

Es besteht eine erhebliche Anzahl möglicher Vorfälle, die zu Einschränkungen oder dem Ausfall von Telekommunikationsnetzen und digitalen Diensten führen können. Die vorliegende Position beschränkt sich auf die relevantesten Risiken, da eine umfassende Würdigung aller Bedrohungen über den Rahmen dieser Publikation hinausgehen würde. Diese sind nach Auffassung des Bitkom:

- Versorgungsstörungen, z. B. Strommangel und -ausfälle oder Einschränkungen in der Lieferkette
- Immense und netzübergreifende Cyberangriffe
- Elementarschäden, extreme Temperaturen
- Vorsätzliche Beschädigung, Sabotage, Vandalismus oder Diebstahl.

4 Voraussetzungen für resiliente TK-Netze und digitale Dienste

Krisensichere Stromversorgung: Die Achillesferse der TK-Branche

Telefone, Internetanschlüsse und Mobilfunknetze sind von der Stromversorgung abhängig. Die Bundesnetzagentur bescheinigt der Stromversorgung in Deutschland grundsätzlich eine sehr gute Zuverlässigkeit und hohe Stabilität. Sollte es im Rahmen

von Extremereignissen zu einem längeren Ausfall der Stromversorgung für Telekommunikationsnetze kommen, so hätte dies jedoch schwerwiegende Folgen für Wirtschaft, Staat und Gesellschaft: Elektronische Zahlungssysteme und Logistikketten würden unterbrochen, Warenlieferungen und die Fernsteuerung von Anlagen wären nicht mehr möglich. Gleichzeitig sind verlässliche Kommunikationsstrukturen entscheidend für eine effiziente Krisenbewältigung: Der Informationsaustausch zwischen Helferinnen und Helfern, Behörden, Bürgerinnen und Bürgern und ihren Angehörigen soll nach Möglichkeit gewährleistet werden und auch die Erreichbarkeit der Notrufnummern muss in Krisenfällen weiterhin weitestgehend möglich sein.

Hier muss klar sein, dass die Vorsorge in einzelnen Branchen, exemplarisch in der Telekommunikation, im Finanz- oder Gesundheitswesen oder bei Behörden und Organisationen mit Sicherheitsaufgaben (BOS) Defizite im Bereich der Energieversorgung nicht über längere Zeit kompensieren kann. Stromausfälle in den öffentlichen Telekommunikationsnetzen können nur an neuralgischen Punkten und damit nur teilweise und kurzzeitig mit Batteriespeichern und/oder mittelfristig mit Notstromaggregaten (NEAs) überbrückt werden. Vielmehr muss zuvorderst alles dafür getan werden, einen Stromausfall von vornherein zu vermeiden. Hierfür ist es erforderlich, die Energieversorgung weiter zu optimieren, mit belastbaren Redundanzen auszustatten und die Ausbaupotenziale bei erneuerbaren Energien, der Dezentralisierung der Stromproduktion mit Speichermöglichkeiten sowie bei Smart Grids oder Smart Metern zu heben.

Auch für mehr Resilienz von Telekommunikationsnetzen liegt daher eine zentrale Verantwortung für die Sicherstellung der Versorgung bei den Energieversorgungsunternehmen, zumal nicht nur die TK-Netze versorgt werden müssen, sondern alle Bürgerinnen und Bürger, Unternehmen, Einrichtungen und Behörden Strom für eine unüberschaubare Anzahl von lebenswichtigen Anlagen benötigen. Umso wichtiger sind abgestimmte Notfallprotokolle zwischen Energieversorgern, TK-Netzbetreibern und Behörden, die eine priorisierte Wiederherstellung der Stromversorgung für kritische Kommunikationsinfrastrukturen sicherstellen.

Sichere und zuverlässige Lieferketten

Unsere Wirtschaft ist aufgrund globaler Lieferketten von Herstellern und Dienstleistern aus dem Ausland abhängig. Gerade für die Telekommunikationsbranche stellt die Etablierung und Aufrechterhaltung sicherer Lieferketten aufgrund ihrer Komplexität eine Herausforderung dar: Es geht nicht nur um den Ressourcenbedarf für den Aufbau der Infrastrukturnetze, sondern auch um Rohstoffe für die Herstellung von Endgeräten. Dabei ist eine Vielzahl unterschiedlicher Zulieferer und Lieferanten aus dem nichteuropäischen Ausland zu steuern.

Die aktuellen Produktions- und Lieferengpässe bei mikroelektronischen Bauteilen sind ein Anlass, einseitige Abhängigkeiten zu hinterfragen und die Ausgangsposition im globalen Wettbewerb um digitale Technologien zu verbessern. Es ist zudem absehbar, dass die europäische Nachfrage nach Halbleitern und Chips im nächsten Jahrzehnt, angetrieben durch den weiteren Ausbau der digitalen Infrastruktur und die zunehmenden Anforderungen an Rechenleistung und Kommunikation in

verschiedenen Industriezweigen, rasant steigen wird. Investitionen in eine europäische Halbleiterindustrie erscheinen vor diesem Hintergrund besonders dringlich.

Sichere Konfiguration und sicherer Betrieb

Jede Infrastruktur ist nur so sicher wie ihr Betrieb und ihre sichere Herstellung (Security by Design). Mängel in der Konfiguration oder Betriebsführung, unzureichende Redundanz zentraler Systeme, mangelhaftes Notfall-, Krisen- oder Kontinuitäts-Management oder Defizite im Beschaffungsprozess führen zu Risiken, die früher oder später in Schadensfälle münden. Einschlägige regulatorische Rahmenwerke – wie die NIS2-Richtlinie – setzen hier bereits wichtige Leitplanken.

Kompetenz und Vertrauenswürdigkeit der mit Konfiguration und Betrieb betrauten Personen in der TK-Branche sind daher essenziell. Um sich gegen die permanent steigende Zahl von Cyberangriffen auf relevante Einrichtungen zu schützen, ist es erforderlich, dass die IT-Sicherheit von Expertinnen und Experten sichergestellt wird und diese weiterhin in der Lage sind, Angriffen vorzubeugen bzw. diese möglichst in Echtzeit zu erkennen und abzuwehren.

Vergleichbares gilt für die physische Sicherheit, unabhängig davon, ob Extremwetterereignisse, Vandalismus, Sabotage oder Diebstahl vorzubeugen ist.

5 Was wir bereits tun

Sicherheitsmaßnahmen

Mit der derzeitigen Aufstellung der Telekommunikationsnetzbetreiber, Funkturmanbieter und Betreiber von Rechenzentren sind auch extreme Fälle von geringen örtlichen Ausdehnungen, die in der Praxis schon anzutreffen waren, bereits grundsätzlich gut zu handhaben.

So verfügen diese Unternehmen regelmäßig über umfassende Sicherheitsorganisationen, erprobte Interventionsprozesse und Vorbeugungskonzepte, die auch den Umgang mit außergewöhnlichen Ereignissen und Krisen einschließen. So hat etwa die Corona-Pandemie gezeigt, dass die Netzinfrastruktur auch sprunghafte Anstiege der Nutzungslast – etwa durch flächendeckendes Homeoffice und Videokonferenzen – zuverlässig bewältigen kann. Wenngleich es sich dabei primär um eine Kapazitätsbelastung und nicht um eine physische Bedrohung der Infrastruktur handelte, belegt das Beispiel die grundsätzliche Skalierungsfähigkeit und operative Stabilität der Netze. Auch Ereignisse wie die Flutkatastrophe 2021 im Ahrtal, der Eisregen im Münsterland 2005 sowie die Elbe-Hochwasser 2002, 2006 und 2013 haben unter anderem gezeigt, wie schnell und effektiv die Unternehmen bei solchen Vorfällen reagieren können.

Die Branche ist durch Investitionen in Schutzmaßnahmen zur Abwehr auch außergewöhnlicher Krisensituationen bereits gut für verschiedenste Szenarien gerüstet. Die zahlreichen Vorsorgemaßnahmen und Sicherheitskonzepte werden fortwährend evaluiert und geschärft, um die Resilienz der Telekommunikationsnetze weiter zu stärken. Beispielsweise verfügen Netzbetreiber bereits über ein erprobtes Krisensystem in dem Notstrom- und Netzersatzanlagen in Krisenfällen zeitnah aktiviert werden.

Effizienzmaßnahmen

Insbesondere als Antwort auf Energiemangel ist Energieeffizienz ein Teil der Lösung. Die Anbieter von TK-Netzen optimieren beispielsweise bereits den Stromverbrauch durch ausgeklügelte und bedarfsgerechte Steuerung.

Grundsätzlich könnte auf behördliche Anordnung bei Energiemangellage ein »Basisnetzbetrieb« erfolgen, bei dem ein Teil der Sendeanlage bzw. Frequenzen abgeschaltet und das Angebot verfügbarer Dienste entsprechend reduziert, aber erhalten bleiben würde. Allerdings ist hier zu beachten, dass die rechtlichen und technischen Bedingungen derzeit dafür nicht geklärt sind und dass die Vorbereitungen für einen solchen »Basisnetzbetrieb« eine signifikante Vorlaufzeit erfordern.

Zusammenarbeit

Über die Unternehmensgrenzen hinweg zeigen sich die Sicherheitsvorkehrungen auch in der engen Zusammenarbeit zwischen den Unternehmen, Dienstleistern und Lieferanten. Die Zusammenarbeit in vergangenen Krisen und die aktuelle Energiemangellage zeigen jedoch, wie wichtig eine weitere Vertiefung der Kooperation über verschiedene Branchen und Infrastrukturen hinweg ist. Dies umfasst insbesondere auch die systematische Zusammenarbeit mit Energieversorgern, deren Bedeutung für die Funktionsfähigkeit der TK-Netze in Kapitel 4 dargestellt ist. Bestehende sektorenübergreifende Kooperationsformate bieten hierfür bereits eine Grundlage, die gezielt weiterentwickelt werden können.

Versorgungsmaßnahmen

Alle zentralen Netzknoten und übergeordneten Vermittlungseinrichtungen verfügen in der Regel über Notstrom- und Netzersatzanlagen. Zudem sind viele Mobilfunkstandorte mit einer unterbrechungsfreien Stromversorgung für begrenzte Zeit ausgestattet, da die Stromversorgung in Deutschland eine sehr hohe Verfügbarkeit aufweist und eine flächendeckende Ausstattung wirtschaftlich nicht darstellbar wäre.

Auch eine flächendeckende Ausstattung aller Mobilfunkstandorte ist aus mehreren Gründen nicht realisierbar: Viele Standorte verfügen nicht über die baulichen Voraussetzungen (Platz, Statik, Zugang) und die Aufstellung von Batteriespeichern oder Dieselaggregaten unterliegt strengen Brand- und Immissionsschutzauflagen, die an zahlreichen Standorten – insbesondere in oder auf Gebäuden – nicht ohne weiteres

erfüllt werden können. Dabei sind auch grundsätzlich nur Standorte in entsprechender Höhe geeignet. Der logistische Aufwand für Wartung und regelmäßige Prüfung wäre bei zehntausenden Standorten immens, und die Kosten stünden in keinem Verhältnis zum Nutzen – insbesondere bei abgelegenen Standorten mit geringer Versorgungsrelevanz.

Schließlich ist eine Absicherung der Mobilfunkstandorte gegen Stromausfall über eine längere Zeit ebenfalls aus mehreren Gründen nicht umsetzbar: Wirtschaftlich und angesichts des benötigen Personalaufwands (z. B. Wartung, Akku-Prüfungen) bei über 100.000 Mobilfunkstandorten in Deutschland ist dies nicht zu bewältigen. Ferner stellen häufig Platz- und Gewichtsbegrenzungen, Lüftungs- und Brandschutzanforderungen sowie Einschränkungen durch den Vermieter die wichtigsten limitierenden Faktoren dar.

6 Was noch zu tun ist

Sicherheit und Resilienz vs. Transparenz

Netzbetreiber unterliegen in Deutschland einer Vielzahl von gesetzlichen Transparenzverpflichtungen. Dies betrifft unter anderem die Offenlegung von Netzdaten zu Trassenverläufen (Infrastrukturatlas), Mobilfunkstandorten (EMF-Karte), der Ist-Versorgung von Haushalten und Unternehmen sowohl im Festnetz als auch im Mobilfunk (Breitbandatlas, Mobilfunk-Monitoring) sowie Informationen zum künftigen Netzausbau (u. a. Vorausschau zum Mobilfunknetzausbau). Diese Daten werden von der Bundesnetzagentur erhoben und verwaltet, in Teilen auch im Internet veröffentlicht oder bei nachgewiesenem berechtigtem Interesse zur Verfügung gestellt. Zwar schreibt das TKG der Bundesnetzagentur bzw. der zentralen Informationsstelle des Bundes die Wahrung von Betriebs- und Geschäftsgeheimnissen und teilweise auch die Wahrung der öffentlichen Sicherheit vor, dem stehen aber die gesetzlichen Transparenzvorgaben (Endnutzerinnen und -nutzer, Gebietskörperschaften) gegenüber. Zudem geht der Trend hin zu einer immer stärkeren Verfeinerung der Daten, die bei den Netzbetreibern abgefragt und dann auch veröffentlicht werden.

Dies entspricht nicht mehr der Schutzwürdigkeit der Telekommunikation als kritische Infrastruktur. Resilienz- und Sicherheitsaspekte sollten also auch an dieser Stelle stärker berücksichtigt und als Prüf- und Begründungsmaßstab standardmäßig im Verwaltungshandeln der Bundesnetzagentur verankert werden. Schon bei der Erhebung von Daten bei den Netzbetreibern ist das Prinzip der Datensparsamkeit umzusetzen – erst recht bei jeder Weitergabe und der Veröffentlichung. Der Anschlag auf das Berliner Stromnetz Anfang 2026, bei dem gezielt Stromtrassen beschädigt wurden und ein großflächiger Stromausfall mit unmittelbaren Auswirkungen auf die Mobilfunkversorgung die Folge war, verdeutlicht die Notwendigkeit einer restriktiven

Handhabung von Detailinformationen über kritische Infrastrukturen. Gleiches zeigen die Sabotageakte an Erdgaspipelines, Glasfaser-Unterseekabeln und dem Kommunikationsnetz der Deutschen Bahn. Umfassende öffentliche Transparenz kann nicht mehr das alleinige Ziel sein, wenn TK-Netze vor gezielten Angriffen und Beschädigungen geschützt werden sollen.

Neben einer restriktiven Erfassung sensibler Infrastrukturdaten in behördlichen Datenbanken sollte auch der Zugang zu diesen Daten in geeigneter Weise gesichert werden, beispielsweise durch Ergänzung der bereits bestehenden Notwendigkeit der Begründung des validen Einsichtsbedarfs durch Sicherheitsüberprüfungen und ein Monitoring der Zugriffe auf die Infrastrukturdaten.

Bei dem TK-Änderungsgesetz ist es daher entscheidend, das Gigabit-Grundbuch zu fokussieren und die richtige Balance zwischen Sicherheit und Transparenz zu finden. Es besteht die Gefahr, dass Datenlieferungspflichten für TK-Unternehmen erhebliche neue und unkalkulierbare bürokratische Belastungen bedeuten. Wir begrüßen, dass der Grundsatz der Datensparsamkeit gesetzlich zu verankern und die Sicherheitsstandards für den Umgang mit Infrastrukturdaten kontinuierlich auf dem neuesten Stand der Technik zu halten sind. Konkret sollte dies umfassen: eine restriktive Erhebungspraxis, differenzierte Zugangsstufen je nach Schutzwürdigkeit der Daten sowie ein durchgängiges Monitoring der Zugriffe. Umfassende Daten und Veröffentlichungen haben dazu geführt, dass Versorgungsstrukturen teilweise im Internet für jedwede Person einsehbar sind.

Auch der Koalitionsausschuss sieht die Notwendigkeit einer Neuausrichtung von Transparenz im Kontext gestiegener Resilienzbedürfnisse. Transparenz- und Informationspflichten verfolgen zwar grundsätzlich berechtigte Anliegen. Angesichts der ernsten Bedrohungslage müsse jedoch stärker berücksichtigt werden, dass transparente Informationen zur Vorbereitung von Angriffen auf kritische Infrastrukturen missbraucht werden könnten. Der Sicherheit kritischer Infrastrukturen und dem Schutz der Bevölkerung sei deshalb Vorrang einzuräumen.

Ebenso hat der Gesetzgeber in seiner Sitzung vom 29. Januar 2026 entschieden, dass die Bundesregierung eine Strategie zur Verbesserung der Resilienz kritischer Infrastrukturen verabschieden soll (§ 1 KRITIS-Dachgesetz). Für den Umgang mit Transparenzpflichten hat er dabei bereits die Richtung vorgegeben: Angesichts der ernsten Bedrohungslage sollen diese Pflichten überprüft und, wo nötig, angepasst oder begrenzt werden, um einen Missbrauch sensibler Informationen zu verhindern.

Digitalisierung Energieversorgung und Priorisierung kritischer TK-Anlagen

Die Informationstechnik und Telekommunikation (ITK) sind unverzichtbare Dienste für Staat, Wirtschaft und Gesellschaft. Die Netzinfrastrukturbetreiber erbringen sogenannte kritische Dienstleistungen: Die ITK umfassen die Sprach- und Datenübertragung sowie die Datenspeicherung und Datenverarbeitung. Der Ausfall dieser Dienstleistungen würde zu erheblichen Versorgungsengpässen und zur Gefährdung der öffentlichen Sicherheit führen, da weite Teile der Wirtschaft und der

öffentlichen Verwaltung, aber auch der Bildungs- und Gesundheitssektor auf funktionierende Kommunikationsnetze angewiesen sind. Zudem basieren auch unsere private Kommunikation und Versorgung mit Informationen auf diesen Technologien. Eine prioritäre Energieversorgung der Telekommunikationsnetzbetreiber bei Krisen- und Katastrophenfällen ist dringend erforderlich.

Hierfür ist es erforderlich, die Digitalisierung der Energieversorgung über die Umsetzung von Smart Grids in Verbindung mit dem Rollout von Smart Meter Gateways (SMGW) mit entsprechenden Steuerboxen zu beschleunigen. Dadurch wird zum einen die Resilienz der Energieversorgung erheblich erhöht und der Strombezug von bspw. kritischen Infrastrukturen wie Mobilfunkanlagen können prioritär gegenüber anderen Verbrauchern gesichert werden, wobei Endkunden immer eine Basisversorgung zur Verfügung stehen wird, allerdings bspw. das Laden eines Elektromobils nur eingeschränkt erfolgen kann.

Auch ist wichtig, dass zunächst der Anteil erneuerbarer Energien kontinuierlich ausgebaut wird. Bitkom befürwortet eine Beschleunigung der Nutzung regenerativer Energien wie Wind oder Solar nicht nur aus der Umweltschutz- und Nachhaltigkeitsperspektive, sondern weil dies durch die Reduktion der Abhängigkeit von ausländischen Energielieferanten auch für die Resilienz durch Versorgungssicherheit wie auch für geringere Energiepreise förderlich ist.

Um die Abhängigkeit von fossilen Energierohstoffen zu minimieren, wollen auch die Netzbetreiber, Betreiber von Funkturmstandorten und Rechenzentren in Zukunft verstärkt auf den Einsatz von erneuerbaren Energien für Technikstandorte setzen. Hier besteht jedoch Bedarf, die regulatorischen Rahmenbedingungen zu verbessern.

Digitale Autonomie und resiliente Lieferketten

Die Mobilisierung von Investitionen zur Stärkung des Wertschöpfungsnetzwerks im breiteren Sinne sollte vor allem durch die Schaffung von attraktiven Rahmenbedingungen für alle relevanten Marktteilnehmer erfolgen. Die Kompetenzen in mehreren Schlüsselsegmenten der Wertschöpfungskette sollten ausgebaut werden und die strategische Zusammenarbeit mit verlässlichen internationalen Partnern, beispielsweise Halbleiterherstellern, gezielt vertieft werden, um einseitige Abhängigkeiten durch diversifizierte Kooperationsstrukturen zu ersetzen. Die Anwenderunternehmen der Digitalwirtschaft sollten frühzeitig in die Konzeption der jeweiligen Fördermaßnahmen einbezogen werden; ein strukturierter Dialog mit Anwender- und Anbieterindustrien in Europa über strategische qualitative Bedarfe und zukünftige Anforderungen in Europa sollte etabliert werden.

Wir begrüßen den Schutz von Lieferketten. Durch bilaterale Investitions- und Handelsabkommen können die deutschen Wirtschaftsbeteiligten länderspezifische Risiken in ihrer Beschaffung diversifizieren, die Lieferketten resilienter machen und neue Märkte erschließen. Somit kann eine gesicherte Produktion realisiert werden.

Wahrung der Verhältnismäßigkeit

Die Telekommunikationsbranche ist sich einig, dass die Resilienz der Netzinfrastruktur in Bezug auf extreme Ereignisse, etwa großflächige Naturkatastrophen und Sachbeschädigungen, präventiv gestärkt werden sollte. Dabei ist jedoch eine Überregulierung zu vermeiden. Vor Implementierung weiterer Maßnahmen ist unbedingt eine genaue Prüfung bereits vorhandener Notfall- und Sicherheitsvorrichtungen durchzuführen, um die Eignung, Erforderlichkeit und Verhältnismäßigkeit zusätzlicher Vorsorgemaßnahmen zu bewerten.

Insbesondere ist eine sehr breit angelegte Verpflichtung der TK-Netzbetreiber zur Notstromversorgung vor dem Hintergrund der hohen Zuverlässigkeit der Stromversorgung in Deutschland nicht zielführend. Neben der Absicherung der Stromversorgung müssen auch Krisenstäbe, Einsatzleitstellen und Zufluchtsmöglichkeiten für die Bevölkerung auf gleichem Niveau abgesichert werden.

Extremereignisse mit größten Auswirkungen liegen außerhalb des Verantwortungsbereichs der Netzbetreiber und erfordern Maßnahmen, die mit erheblichen Kosten verbunden sind. Diese können vor dem Hintergrund des Verursacherprinzips nicht allein durch die Netzbetreiber getragen werden, sondern müssen als Teil der staatlichen Daseinsvorsorge betrachtet werden.

Sollten zusätzliche kostenintensive Maßnahmen vorgeschrieben werden, muss gleichzeitig eine Regelung zur Kompensation für die daraus resultierenden Aufwände der Telekommunikationsbranche erfolgen (wie bei Cell Broadcast). Darüber hinaus müssen zusätzliche Aspekte in geeigneter Weise berücksichtigt werden, beispielsweise die Machbarkeit und die zeitliche Perspektive. Wir sprechen uns daher dafür aus, zusätzliche Maßnahmen mit Augenmaß und unter Wahrung der Verhältnismäßigkeit auszuwählen, um die Wirtschaftlichkeit der Telekommunikationsnetze und den damit verbundenen Ausbau moderner Netze nicht zu gefährden.

Bitkom vertritt mehr als 2.300 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 700 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner
Nick Petersen | Referent für digitale Infrastrukturen
M +49 151 14824830 | n.petersen@bitkom.org

Verantwortliches Bitkom-Gremium
AK Telekommunikationspolitik