bitkom

Resilienz der Telekommunikations-netze stärken

Herausforderungen & Handlungsempfehlungen

Auf einen Blick

Resilienz der Telekommunikationsnetze stärken

Ausgangslage und Bitkom-Bewertung

Telekommunikationsnetze müssen mit einer stetig steigenden Anzahl von schweren Störungen und außergewöhnlichen Angriffen umgehen können und dagegen resilienter werden. Mit der derzeitigen Aufstellung der Telekommunikationsbranche sind auch extreme Fälle von geringen örtlichen Ausdehnungen bereits grundsätzlich gut zu handhaben. Die Telekommunikationsbranche ist sich jedoch einig, dass die Resilienz der Netzinfrastruktur und digitaler Dienste präventiv angepasst und weiter gestärkt wird.

Das Wichtigste

- **Resilienz**

  Resilienz ist die weitestmögliche Widerstandsfähigkeit gegen verschiedenste adverse Einflüsse, von physischen Beschädigungen über Stromversorgungsausfälle bis zu Cyberattacken.

- **Risiken: Die wichtigsten Bedrohungen**

  Es besteht eine erhebliche Anzahl möglicher Vorfälle, die zu Einschränkungen oder dem Ausfall von Telekommunikationsnetzen führen können. Besonders relevante Risiken sind Versorgungsstörungen, Elementarschäden, extreme Temperaturen, immense und netzübergreifende Cyberangriffe sowie vorsätzliche Beschädigung und Sabotage.

- **Voraussetzungen für resiliente TK-Netze und digitale Dienste**

  Eine krisensichere Stromversorgung ist die Grundvoraussetzung für resiliente Telekommunikationsnetze, da diese von der Stromversorgung abhängig sind. Zudem sind sichere und zuverlässige Lieferketten aufgrund der Abhängigkeit von globalen Lieferketten von hoher Bedeutung.

- **Was wir bereits tun**

  Die Branche ist durch Investitionen in Schutzmaßnahmen zum Umgang und zur Abwehr auch außergewöhnlicher Krisensituationen bereits gut für verschiedenste Notfälle gerüstet. Über die Unternehmensgrenzen hinweg zeigen sich die Sicherheitsvorkehrungen auch in der engen Zusammenarbeit zwischen den Unternehmen, Dienstleistern und Lieferanten.

- **Was noch zu tun ist**

  Eine 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 durch die Politik vorgeschrieben werden, muss eine faire Verteilung der Kosten erfolgen.

Inhalt

1 Resilienz

„Resilienz beschreibt die Fähigkeit eines Systems, einer Gemeinschaft oder einer Gesellschaft, sich rechtzeitig und effizient den Auswirkungen einer Gefährdung widersetzen, diese absorbieren, sich an sie anpassen, sie umwandeln 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. Resilienz bedeutet in diesem Zusammenhang die Fähigkeit der Telekommunikationsnetze ein Mindestmaß an Funktionalität auch dann zu gewährleisten, wenn einzelne Teile versagen, angegriffen werden oder andere Störungen auftreten. Dabei ist zwischen digitaler und physischer Resilienz der Netze zu unterscheiden. Darüber hinaus ist noch die Resilienz gegenüber Versorgungsstörungen zu nennen. 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 Beschädigung oder Diebstahl. Beispiele für Versorgungsstörungen umfassen Strommangel und -ausfälle wie auch Verzögerungen und Einschränkungen in der Lieferkette für Netzausrüstung.

2 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

[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.

3 Voraussetzungen für resiliente TK-Netze und digitale Dienste

Krisensichere Stromversorgung: 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. 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 und auch die Erreichbarkeit der Notrufnummern müssen auch in Krisenfällen weiterhin weitestgehend möglich sein.

Hier muss klar sein, dass die Vorsorge in einzelnen Branchen, exemplarisch Telekommunikation, Finanz- oder Gesundheitswesen oder bei Behörden und Organisationen mit Sicherheitsaufgaben (BOS) Defizite im Bereich der Energieversorgung nicht über längere Zeit kompensieren kann. Stromausfälle können nur teilweise mit Batteriespeichern oder Notstromaggregaten überbrückt werden. Zuvorderst muss alles dafür getan werden, einen Stromausfall zu vermeiden. Hierfür ist es erforderlich, die Energieversorgung weiter zu modernisieren 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 die primäre Verantwortung für die Sicherstellung der Versorgung bei den Energieversorgungsunternehmen, zumal nicht nur die TK-Netze versorgt werden müssen, sondern alle Bürgerinnen und Bürger, Unternehmen und Behörden Strom für eine unüberschaubare Anzahl von lebenswichtigen Anlagen benötigen: Eine umfassende Absicherung von Telekommunikationsendgeräten über Licht, Heizungen und Kühlmöglichkeiten bis hin zu Türen und Aufzügen durch Notstromversorgungen ist wirtschaftlich und praktisch nicht möglich.

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 nicht europäischen 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.

Der Bitkom und seine Mitgliedsunternehmen unterstützen das mit dem europäischen Lieferkettengesetz verfolgte Ziel der EU, die Menschenrechte durch unternehmerische Nachhaltigkeitsprüfung zu stärken und damit einen Beitrag zur Widerstandsfähigkeit und langfristigen Perspektive der Weltwirtschaft zu leisten.

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.

Kompetenz und Vertrauenswürdigkeit der mit Konfiguration und Betrieb betrauten Personen in der TK-Branche sind daher essenziell. Um sich gegen die zukünftigen immensen Cyberangriffe 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.

4 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 hervorragende Sicherheitsorganisationen, Interventionsprozesse und Vorbeugungskonzepte, auch für den Umgang mit außergewöhnlichen Ereignissen und Krisen, wie sie nur in wenigen Unternehmen anzutreffen sind. Beispielsweise hat die Corona-Pandemie gezeigt, dass die Netzinfrastruktur auch mit starken Belastungen gut zurechtkommt und es keinerlei nennenswerte Einschränkungen gibt. Auch die Flutkatastrophe 2021 hat 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 Notstrom- und Netzersatzanlagen, die in Krisenfällen aktiviert werden.

Zudem arbeiten derzeit alle Mobilfunknetzbetreiber in Zusammenarbeit mit der Bundesnetzagentur und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe gemeinschaftlich an der Einführung von Cell Broadcast zum Beginn des neuen Jahres. Cell Broadcast wird als weltweit standardisierte Technologie das Warnsystem für die Bevölkerung weiter verbessern. Diese Einführung sowie dessen Anbindung an das behördliche Modulare Warnsystem (MoWaS) ist ein hervorragendes Beispiel für die Zusammenarbeit zwischen Netzbetreibern und Behörden.

Effizienzmaßnahmen

Insbesondere als Antwort auf Energiemangel ist Energieeffizienz ein Teil der Lösung. Die Anbieter von TK-Netzen beispielsweise optimieren bereits den Stromverbrauch durch Teilabschaltungen in Nebenzeiten mit geringer Nachfrage – etwa nachts, wenn weniger Solarenergie zur Verfügung stehen.

Auch könnte ein „Basisnetzbetrieb“ bei Energiemangellage erfolgen, bei dem beispielsweise ein Teil der Sendeanlage bzw. Frequenzen abgeschaltet und das Angebot verfügbarer Dienste reduziert würde. Allerdings ist hier zu beachten, dass ein solcher Betrieb ebenfalls eine signifikante Vorlaufzeit erfordert. Darüber hinaus muss zuvor analysiert werden, wie die Vor- und Nachteile dieses Ansatzes, vor allem hinsichtlich evtl. reduzierter Kapazität, zu bewerten sind.[2]

Zusammenarbeit

Über die Unternehmensgrenzen hinweg zeigen sich die Sicherheitsvorkehrungen auch in der engen Zusammenarbeit zwischen den Unternehmen, Dienstleistern und

[2] So wird z.B. in der Schweiz eine Ausnahme von der „Kontingentierung“ diskutiert, da die Mobilfunknetze nur rund 1% des Gesamtstrombedarfs verursachen und nur wenig eingespart werden könnte, der (mobilen) Kommunikation jedoch gerade im Krisenfall eine besondere Bedeutung zukommt („Strommangellage – Härtung der Mobilfunknetze“ UVEK/BAKOM 2021).

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.

Bitkom begrüßt, dass die Bundesnetzagentur in ihrem jüngsten Resilienz-Strategiepapier viele bestehende Ansätze aus der Branche für die Erweiterung der Zusammenarbeit übernommen hat, so etwa das gemeinsame Lagezentrum von Netzbetreibern und Behörden. So kann die Kooperation zwischen Akteuren vereinfacht werden und Maßnahmen können zielgerichteter wirken. Zudem unterstützen wir die Intensivierung der Zusammenarbeit durch Übungen. Dabei sollte aber allen Beteiligten klar sein, dass es sich bei den Unternehmen um Wettbewerber handelt und daher der Schutz von Betriebs- und Geschäftsgeheimnissen gewahrt werden muss. Ein solches Lagezentrum sollte deswegen durch unabhängige Instanzen geleitet und koordiniert werden.

5 Was noch zu tun ist

Verbesserung der Energieversorgung und Priorisierung der kritischen TK-Unternehmen

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

Es 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 Schaffung von attraktiven Rahmenbedingungen für alle relevanten Marktteilnehmer erfolgen. Die Kompetenzen in mehreren Schlüsselsegmenten der Wertschöpfungskette sollten ausgebaut werden und die gegenseitigen Abhängigkeiten mit internationalen Partnern im Halbleiterwertschöpfungsnetzwerk intensiviert werden. 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.

Weitere Vorkehrungen der TK-Netzbetreiber und der Anbieter digitaler Dienste

Alle Anbieter prüfen derzeit eine Vielzahl von Möglichkeiten, wie die Resilienz von Telekommunikationsnetzen und digitalen Diensten gestärkt werden kann und wie sie ihren gesellschaftlichen Beitrag zur Vorsorge gegen Krisensituationen erhöhen können.

Bei einem länger anhaltenden, großflächigen Stromausfall ist der Ausfall von Kommunikationsmöglichkeiten jedoch nur ein Aspekt. Erforderlich sind dann funktionierende Reaktions- und Hilfsstrukturen für die Bevölkerung und dass die Einsatzfähigkeit der Krisenstäbe und Hilfskräfte sichergestellt bleibt.

Dies kann – wie es die Deutsche Resilienzstrategie und das UN Sendai Rahmenwerk bereits vorsehen – nur über alle Branchen hinweg geschehen. Dafür ist eine Verständigung erforderlich, welche öffentlichen und privaten Dienste trotz überraschenden Eintretens eines Großschadensfalls innerhalb definierter Fristen auf einem einheitlichen Niveau funktionsfähig erhalten werden sollen.

Wahrung der Verhältnismäßigkeit

Die Telekommunikationsbranche ist sich einig, dass die Resilienz der Netzinfrastruktur in Bezug auf extreme Ereignisse, etwa Krisenhandlungen, großflächige Naturkatastrophen und atomare Schadensfälle 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.

Grundsätzlich sollte dabei beachtet bleiben, dass die öffentliche Netzinfrastruktur in erster Linie für den Alltag vorgesehen ist und nicht primär als Kommunikationsmittel für Katastrophenfälle konzipiert werden kann.

Insbesondere ist eine sehr breit angelegte Verpflichtung der TK-Netzbetreiber zur Notstromversorgung vor dem Hintergrund der hohen Zuverlässigkeit der Stromversorgung in Deutschland nicht zielführend. Fraglich ist auch der Mehrwert einer zusätzlichen Notstromversorgung für Telekommunikationsnetze, wenn die Stromversorgung der Bevölkerung nicht zusätzlich gesichert ist und daher der Betrieb von mobilen Endgeräten nach Verbrauch des Akkus nicht mehr möglich ist oder wenn Krisenstäbe, Einsatzleitstellen und Zufluchtsmöglichkeiten für die Bevölkerung nicht zuvor auf gleichem Niveau abgesichert wurden.

Faire Verteilung der Kosten

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 durch die Politik vorgeschrieben werden, muss gleichzeitig eine Regelung zur Kompensation für die daraus resultierenden Aufwände der Telekommunikationsbranche erfolgen (wie bei Cell Broadcast). Wir sprechen uns daher dafür aus, zusätzliche Maßnahmen mit Augenmaß auszuwählen, um die Wirtschaftlichkeit der Telekommunikationsnetze und den damit verbundenen Ausbau moderner Netze nicht zu gefährden.

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), 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 zwar von der Bundesnetzagentur erhoben und verwaltet, sie werden letztlich aber 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. Die Notwendigkeit einer restriktiven Handhabung von Detailinformationen über Infrastrukturen zeigen bspw. auch jüngst vereitelte Anschläge auf Stromtrassen oder die Sabotagen an Erdgaspipelines oder dem Kommunikationsnetz der Deutschen Bahn. Umfassende öffentliche Transparenz kann nicht mehr das (alleinige) Ziel sein, wenn TK-Netze vor Angriffen und Beschädigungen geschützt werden sollen.

Neben einer restriktiven Erfassung sensitiver 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.

Förderung von Forschungsprogrammen

Der Aufbau und Ausbau einer resilienten TK-Infrastruktur sollte ergänzend durch staatliche Forschungsprogramme und Initiativen über alle Schlüsseltechnologien (KI, Cloud-basierend) gefördert werden.

Bitkom vertritt mehr als 2.000 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 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 oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. 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 weltweit führenden Digitalstandort zu machen.

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

Ansprechpartner
Nick Kriegeskotte | Leiter Infrastruktur & Regulierung
T 030 27576-224 | n.kriegeskotte@bitkom.org

Janine Welsch | Referentin für Telekommunikationspolitik
T 030 27576-234| j.welsch@bitkom.org

Verantwortliches Bitkom-Gremium
AK Telekommunikationspolitik

Titelbild
Erik Mclean, Pexels