Kritische Infrastrukturen

Resilienz für digitale Infrastrukturen ist eine große Aufgabe

Durch die NIS-2-Richtlinie werden künftig Telekommunikationsunternehmen stärker in die Pflicht genommen, für die Resilienz ihrer Infrastrukturen zu sorgen. Der Beitrag legt einen Schwerpunkt auf die operative Resilienz und zeigt, welchen Beitrag die unbeleuchtete Glasfaser dafür leistet. Von Wolfram Rinner, GasLINE

Telekommunikationsunternehmen spielen eine wichtige Rolle in Wirtschaft und Gesellschaft und gelten daher als Betreiber kritischer Infrastrukturen. Sie unterliegen den gesetzlichen Vorgaben für kritische Infrastrukturen (KRITIS) und sind verpflichtet, Maßnahmen zur Erhöhung der Resilienz zu ergreifen. Im Kern geht es dabei um die Erhöhung der Sicherheit – vor allem vor Netzausfällen. Resilienz ist ein Begriff, der sowohl für Menschen als auch für Unternehmen gilt. Widerstandskraft ist die Qualität, die es zu erreichen gilt. Kurz gesagt ist Resilienz die Fähigkeit einer Organisation oder eines Unternehmens, nach einer Disruption, in der Regel einem Störfall, den normalen Betrieb schnellstmöglich wiederherzustellen. Das Beratungshaus PwC hat in seinem neuen Resilienz-Paper für die Telekommunikationsbranche („Resilienz – Basiskompetenz für Telekommunikationsunternehmen“[1]) die Definition der Vereinten Nationen übernommen: „Resilienz bedeutet die Fähigkeit eines Systems, sich rechtzeitig und effizient den Auswirkungen einer Gefährdung widersetzen, diese absorbieren, sich an sie anpassen, sie umwandeln und sich von ihnen erholen zu können“.[2]
Telekommunikationsnetze gehören zu den KRITIS-Kategorien und damit sind auch deren Betreiber in der Pflicht, für Resilienz der Infrastruktur zu sorgen. Die Betreiber kritischer Infrastrukturen unterliegen regelmäßigen gesetzlich vorgeschriebenen Audits. Auch Bereiche, die Versorgungsaufgaben wahrnehmen, gehören dazu: Energie- und Trinkwasserversorgung, das heißt Stadtwerke und Energieversorger in den Regionen, Logistik, Verkehrswesen und auch die Finanzwirtschaft, wie Banken.

© metamorworks - AdobeStock

Die NIS-2 RL hat Einfluss auf den Telekommunikationssektor

Die am 16.01.2023 in Kraft getretene NIS-2-Richtlinie (EU 2022/2555 Network and Information Security Directive) hat das Ziel, die Netz- und Informationssicherheit für KRITIS-relevante Unternehmen zu gewährleisten. Unter die NIS-2-RL können private und öffentliche Organisationen fallen. Auch kommunale Organisationen und Verwaltungen sind von den Verpflichtungen zur Cybersicherheit und möglichen Sanktionen betroffen. Es werden wesentliche, wichtige und kritische Einrichtungen definiert:

- Anwendungsbereiche der „Sektoren mit hoher Kritikalität“ (Anhang I) sind u.a. Energie, Verkehr, Trink- und Abwasserversorgung, die öffentliche Verwaltung und die digitale Infrastruktur.
- Unter „Sonstige kritische Sektoren“ (Anhang II) fallen z.B. Unternehmen der Abfallbewirtschaftung und Anbieter digitaler Dienste wie Online-Marktplätze und Suchmaschinen.

Als „wesentliche Einrichtungen“ gem. Art. 3 NIS-2-RL sind Einrichtungen aus Anhang I (Sektoren mit hoher Kritikalität) einzustufen, wenn definierte Schwellenwerte für große Unternehmen überschritten werden oder diese von einem EU-Mitgliedsstaat als wesentliche Einrichtung klassifiziert werden:

- Mittlere Unternehmen: < 50 Beschäftigte und ein Jahresumsatz oder eine

1 www.pwc.de/de/branchen-und-markte/oeffentlicher-sektor/pwc-resilienz-basiskompetenz-fuer-telekommunikationsunternehmen.pdf
2 Quelle: https://digitallibrary.un.org/record/852089?ln=en

Bilanzsumme von mindestens 10 bis zu 50 Millionen Euro
- Große Unternehmen: < 250 Beschäftigte und < 50 Millionen Euro Umsatz, respektive eine Jahresbilanzsumme von < 43 Millionen Euro (2003/361/EF)

„Wichtige Einrichtungen" sind laut Definition hingegen Unternehmen mittlerer Größe und solche, die den Sektoren mit hoher Kritikalität oder sonstigen kritischen Sektoren entsprechen, aber aufgrund der Schwellenwerte nicht als wesentliche Einrichtungen gelten.
Unter NIS-2 werden zukünftig mehr Telekommunikationsunternehmen in die Pflicht genommen, die mit dem Schwellenwert als wesentliche, respektive wichtige KRITIS-Unternehmen eingestuft werden.

© Sashkin - AdobeStock

Die Auswirkung von Disruption im Kontext KRITIS

Disruptionen und Bedrohungsszenarien haben existenzbedrohenden Charakter, wenn Unternehmen und Institutionen nicht entsprechend vorbereitet sind und die Krise und die Störung nicht schnell meistern. Cyberangriffe und andere bedrohliche Maßnahmen Dritter oder unbeabsichtigte Störungen durch menschliche Fehler führen zu Disruptionen. Das wirkt sich auf einzelne betroffene Unternehmen, die Wirtschaft oder sogar Teile der Bevölkerung aus, in Abhängigkeit von dem Schaden. Es geht nicht mehr um das Antizipieren der Eintrittswahrscheinlichkeit von Vorfällen mit disruptivem Charakter, sondern um die Fragestellung, wie damit umzugehen ist.
PwC hat sich in der „Global Crisis and Resilience Survey 2023"[3] mit Bedrohungen und den damit einhergehenden Anstrengungen, Maßnahmen und Investitionen der befragten internationalen Unternehmen (2.000) auseinandergesetzt. 96 Prozent, in Deutschland 97 Prozent, der befragten Organisationen haben in den letzten zwei Jahren Disruptionen erlebt. In Resilienz muss investiert werden und das langfristig. Gemäß der Studie verteilten sich die Investitionen der einbezogenen Unternehmen in den letzten zwei Jahren folgendermaßen: Cyber-Resilienz 52 Prozent, Krisenmanagement 48 Prozent und 45 Prozent investierten in Threat Monitoring. In den nächsten zwei Jahren sollen die Investitionen für Cyber-Resilienz auf 56 Prozent erhöht werden, während sie für die beiden anderen Bereiche leicht rückläufig geplant werden.

Die Aufgabe der Resilienz in der TK-Branche

PwC stellte fest, dass 38 Prozent der Telekommunikationsunternehmen bereits über einen vollständig integrierten Resilienzansatz verfügen. Im Vergleich zu anderen Sektoren sei das ein guter Ist-Zustand. Ergänzend zur globalen Studie hat PwC ein Resilienz-Paper für die Telekommunikationsbranche mit dem Titel „Resilienz – Basiskompetenz für Telekommunikationsunternehmen"[4] veröffentlicht. GasLINE war als Weitverkehrsnetzbetreiber und Infrastrukturanbieter mit seiner Praxissicht und den Maßnahmen für Resilienz beteiligt. PwC definiert Resilienz als „kontrolliert mit Disruption umgehen zu können".
Um dies zu erreichen, müssen umfassende Sicherheitsmaßnahmen, -mechanismen und Prozesse eingesetzt werden. Anhand der häufigsten Schadensereignisse definiert PwC drei Kernbereiche:
- Strategische Resilienz
- Operative Resilienz
- Finanzielle Resilienz

In diesem Beitrag steht die operative Resilienz aus der Sicht eines Infrastrukturanbieters und Netzbetreibers im Fokus. Diese ist für Infrastrukturanbieter von Glasfasernetzen, Netzbetreiber und Betreiber der Internetaustauschknoten mit Konnektivität relevant. Sie umfasst drei Felder:
- Physische Resilienz (Objekt- und Perimeterschutz, geografische Verteilung von Standorten, redundante Infrastrukturen und auch Feuer- und Wasserschutzsysteme)
- Cyber-Resilienz (Netzwerksegmentierung, Intrusion Detection/Prevention Systems, Sicherheitsaudits, Penetrationstests, Entwicklung eines Incident-Response-Plans, und Back-up-Strategien)
- Logistische Resilienz (Multivendor-Strategien, Third Party Risk Management, Ressourcen-Diversifikation)

Diese Auflistung umfasst typische Maßnahmen, die teilweise bereits im Risiko-Management von den Telekommunikationsunternehmen eingesetzt wurden, zusammen. Sie ist nicht vollständig. Darüber hinaus werden Unternehmen auch individuelle Vorsorgemaßnahmen ergreifen. Der Schutz vor Cybercrime wird immer eine Abwehrfunktion bleiben, das zeigen leider die Ereignisse der letzten Jahre. Die technischen Möglichkeiten werden sich weiter entwickeln und Resilienz fördern.
Für GasLINE geht es bei der operativen Resilienz um Störungen auf der untersten Netzebene Layer-Null, das heißt

3 www.pwc.de/de/forensic-services/global-crisis-survey.html
4 www.pwc.de/de/branchen-und-markte/oeffentlicher-sektor/pwc-resilienz-basiskompetenz-fuer-telekommunikationsunternehmen.pdf

der unbeleuchteten Glasfaser, die an die Kunden vermietet wird. Ein Netz kann für eine unbeabsichtigte Beschädigung anfällig sein, z. B. durch einen Bagger, der bei Bauarbeiten das Kabelschutzrohr beschädigt. Um eine hohe Sicherheit für das große bundesweite Glasfasernetz von GasLINE zu gewährleisten, werden die Kabel außerhalb geschlossener Ortschaften grundsätzlich einen Meter unter der Erdoberfläche verlegt. Ein Großteil der Infrastruktur wurde in den Schutzstreifen der Gasleitungen der Gesellschafterunternehmen verlegt. Dies bietet aufgrund der Zugangsrestriktion einen hohen Schutzfaktor. Im Backbone werden Ringschlüsse und Vermaschungen kontinuierlich ausgebaut, damit Kunden aus dem Carrier-Bereich die Resilienz ihres eigenen Netzes erhöhen können.
Netzbetreiber und Telekommunikationsanbieter haben eine große Mit-Verantwortung für die Enterprise-Resilienz ihrer Kunden. Es gilt Ausfälle zu minimieren und Entstörung schnell zu gewährleisten. Für Redundanz müssen mindestens zwei alternative Routen im Netz, Back-up-Rechenzentren und redundante Systeme im Netzbetrieb bereitgestellt werden.

Enterprise-Resilienz funktioniert nur im Zusammenspiel

Für das PwC Resilienz-Paper wurde in dem Briefing-Gespräch gemeinsam mit GasLINE die fünfstufige Netzstruktur entwickelt: Verteilnetzwerke, Regionale Rechenzentren, nationale Weitverkehrsnetze, Internetknoten (IX) und Interkontinental- und Seekabel.
Ganzheitliche Netzresilienz ist auf Reziprozität aufgebaut und bezieht mehrere Ebenen ein. „Um ein Netzwerk widerstandsfähig zu gestalten, ist es erforderlich, dass die Stakeholder der unterschiedlichen Netzebenen das Prinzip der Wechselseitigkeit (Reziprozität) beachten. Sie sind verantwortlich für die Robustheit ihrer eigenen Angebote und Dienste, müssen jedoch gleichzeitig auf die Resilienz der nachfolgenden Ebenen vertrauen können“, heißt es in dem Resilienz-Paper.

Der Resilienz-Ansatz bei GasLINE

Operative Resilienz im Störfall zu entwickeln, bedeutet für die Kunden der GasLINE im Hinblick auf die Enterprise-Resilienz von deren Kunden, auf Alternativen zugreifen zu können, die umgehend zum Einsatz kommen. Im Kundenauftrag werden daher Ringstrukturen im GasLINE-Backbone gebaut, die schnellstmöglich ein Umrouten im IP-Verkehr über eine andere Leitung oder einen anderen Internetknoten möglich machen.
Redundanz durch Ringe und einen hohen Vermaschungsgrad ist auf der physischen Netzebene der beste Schutz, um Ausfallzeiten zu minimieren. Das bedeutet jedoch auch, dass die Kunden der GasLINE im Carrier-Markt redundante Netze errichten müssen. Das ist auf jeden Fall für kritische, also wichtige Netzverbindungen dringend zu empfehlen. Unternehmen, Institutionen, Kommunen und auch Stadtwerke, die unter KRITIS fallen, sind in der Pflicht, auf ihrer Seite redundante Infrastruktur für eine durchgängige Resilienz zu implementieren. Diese sogenannte Enterprise-Resilienz ist für die Unternehmen im Geschäftskunden-Segment relevant. Es geht um eine verteilte Verantwortung, die von der physischen Glasfaser über den Netzbetrieb bis zur Bereitstellung von Cloud-Lösungen und Diensten reicht. Ähnlich wie bei einem Zahnrad greifen die verschiedenen Ebenen der Widerstandsfähigkeit ineinander. Eine Schwachstelle auf einer Ebene wirkt sich negativ auf den Schutz-Level der anderen, darüber liegenden Ebenen aus.
Das KRITIS-Dachgesetz, das die nationale Umsetzung der EU-Richtlinien zum Schutz kritischer Einrichtungen regelt, soll spätestens am 01.01.2026 in Kraft treten. Dies wird Auswirkungen auf das Geschäft von GasLINE haben, da die Carrier-Kunden die erforderlichen Vorkehrungen für die Sicherheit ihrer Netzinfrastruktur treffen und mehr Glasfasern anmieten müssen. GasLINE ist dafür offen, mit anderen Akteuren der Telekommunikationsbranche zusammenzuarbeiten, um für die Sicherung von Resilienz gemeinsam Synergien zu schaffen und zukünftig zu nutzen. Hier gilt es, verantwortungsbewusst über das eigene Unternehmen hinaus zu denken, um insbesondere für Enterprise-Resilienz gemeinsam neue Lösungen zu finden. ■

© GasLINE

Wolfram Rinner – Geschäftsführer GasLINE GmbH & Co KG