pwc

Resilienz – Basiskompetenz für Telekommunikations-unternehmen

In der digitalisierten Welt ist das gesellschaftliche Zusammenleben zunehmend von Informationstechnik und Telekommunikation abhängig. Wirtschaftliche und soziale Entwicklung bauen auf zuverlässige und widerstandsfähige Telekommunikationsnetze und -dienste.

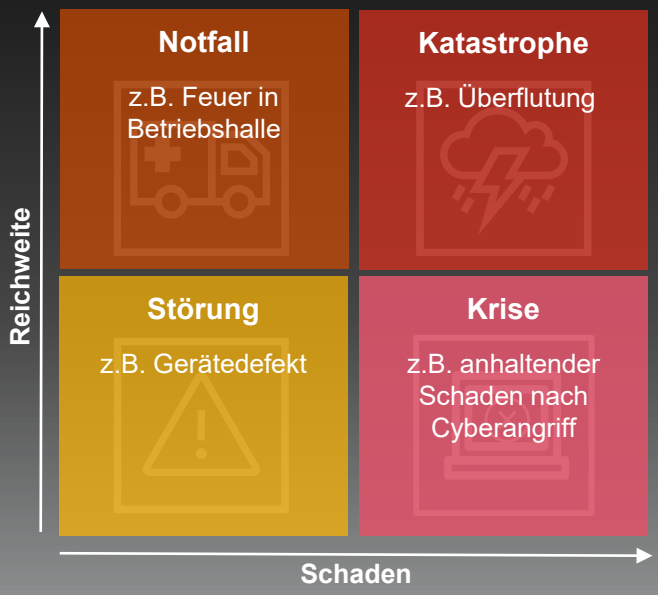
Im Umgang mit Disruptionen und Bedrohungsszenarien der Gegenwart – z.B. die COVID-19-Pandemie, der Angriffskrieg gegen die Ukraine, zunehmende Naturkatastrophen, aber auch Cyberangriffe und mutwillige Zerstörung – wird die hohe Bedeutung digitaler Kommunikationsnetze deutlich.

In der „Global Crisis and Resilience Survey 2023“[1] hat sich PwC mit den aktuellen Bedrohungen sowie den Anstrengungen und Investitionen der Unternehmen zur Steigerung der eigenen Resilienz auseinandergesetzt. Die jüngsten Trends zur Disruption der fast 2.000 im Zuge dieser Survey befragten internationalen Organisationen geben Anlass, sich als Unternehmen eingehend mit der Widerstandsfähigkeit der eigenen Organisation zu beschäftigen.

Resilienz – kontrolliert mit Disruption umgehen können

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].

Reichweite und Schadensausmaß einzelner Gefährdungen werden im deutschen Sprachgebrauch durch unterschiedliche Begriffe definiert.



Lange Zeit als Compliance- und Checklisten-Fingerübung verschmäht, ist Resilienz längst mehr als das Mittel zum Zweck, um potenzielle Verluste zu mindern oder rechtliche Auflagen zu erfüllen - nämlich ein zentraler Wettbewerbsvorteil und eine Voraussetzung für jede erfolgreiche Geschäftsstrategie. Dem stimmten auch die Teilnehmer:innen in unserer Umfrage zu: 89% gaben an, dass Resilienz eine der wichtigsten strategischen Prioritäten ihres Unternehmens ist.

96% (in Deutschland 97%) der Organisationen haben in den letzten zwei Jahren eine Disruption erlebt.

91% (in Deutschland 92%) haben mindestens eine andere Disruption als die globale Pandemie erlebt.

Nur 22% der Resilienz-Programme in deutschen Organisationen werden von den CEOs unterstützt.

[1] PwC (2023): “Global Crisis and Resilience Survey” (https://www.pwc.de/de/managementberatung/forensic-services/global-crisis-survey.html)
[2] United Nations (2016): „Indicators and terminology relating to disaster risk reduction” (https://digitallibrary.un.org/record/852089?ln=en)

Rechtlich-regulatorischer Rahmen

NIS2 –Richtlinie erweitert Anforderungen, Sanktionen und Geltungsbereich

Alle Institutionen, deren Systeme, Netze und Einrichtungen bei einem Ausfall eine erhebliche Auswirkung auf die öffentliche Sicherheit und Wirtschaft haben, unterliegen der europäischen Network and Information Security Directive (NIS). Diese wurde im vergangenen Jahr überarbeitet - die resultierende NIS2 ist seit Januar 2023 in Kraft und muss bis Ende 2024 von den Mitgliedsstaaten umgesetzt werden. NIS2 erweitert die Anforderungen und die Sanktionen, um das Sicherheitsniveau in den Mitgliedstaaten zu erhöhen.

Unternehmen und Organisationen müssen sich unter anderem mit den Themen Cyber-Risikomanagement, Kontrolle und Überwachung sowie Umgang mit Zwischenfällen und Geschäftskontinuität befassen. Darüber hinaus erweitert die Richtlinie auch die Zahl der Organisationen, die in den Anwendungsbereich fallen.

Unter NIS2 werden zukünftig voraussichtlich auch Telekommunikationsunternehmen ab 50 Mitarbeitern oder >10Mio EUR Umsatz betroffen sein. Eine frühzeitige Befassung mit NIS2 ist daher auch Telekommunikationsanbietern unterhalb der aktuellen KRITIS Schwellenwerte zu empfehlen.

Das Wichtigste im Überblick

- Am 16.01.2023 ist die NIS2-Richtlinie in Kraft getreten - Umsetzung in nationales Recht bis 2024
- Zur Umsetzung der NIS2-Richtlinie in Deutschland (NIS2UmsuCG) gibt es bereits Referentenentwürfe sowie ein "Diskussionspapier" des Bundesinnenministeriums
- Der Anwendungsbereich der Cyber-Sicherheitsregulierung und damit der Kreis der betroffenen Unternehmen wird auch in Deutschland deutlich ausgeweitet
- Die betroffenen Unternehmen und Organisationen müssen angemessene Maßnahmen in Bereichen wie Cyber-Risikomanagement, Sicherheit in der Lieferkette, Business Continuity Management oder Penetrationstests umsetzen
- Für die Geschäftsleitung der betroffenen Organisationen werden strengere Haftungsregeln diskutiert
- Es bestehen weitere Sonderregelungen für Telekommunikationsanbieter

Frühzeitige Befassung ermöglicht rechtzeitige Weichenstellung und effizientere Umsetzung.

Resilienz im speziellen Kontext der Telekommunikation

Die Fähigkeit eines Unternehmens, mit Bedrohungsszenarien umzugehen, hängt nicht allein an den operativen Prozessen - es zahlen alle Bereiche auf die Resilienz ein. Aber während strategische und finanzielle Resilienz sektorunabhängig den gleichen Prinzipien folgen, zeigen sich im Feld der operativen Resilienz wesentliche Unterschiede.

Strategische Resilienz | **Operative Resilienz** | Finanzielle Resilienz

Hierbei geht es vor allem darum, die für das Unternehmen kritischen Services und Dienstleistungen so widerstandsfähig zu machen, dass diese auch bei großflächigen Störungen gegenüber relevanten Kunden- und Stakeholdergruppen schnell wieder erbracht werden können.

Aus den häufigsten Schadensereignissen lassen sich im Bereich der operativen Resilienz drei zentrale Handlungsfelder für Unternehmen der Telekommunikationsbranche ableiten

Operative Resilienz

Physische Resilienz

- Objekt- und Perimeterschutz
- Geografische Verteilung von Standorten
- Redundante Infrastrukturen

Cyber-Resilienz

- Netzwerk-segmentierung
- Intrusion Detec-tion (IDS) / Prevention Systems (IPS)
- Sicherheitsaudits und Penetrationstests
- Backup-Strategie

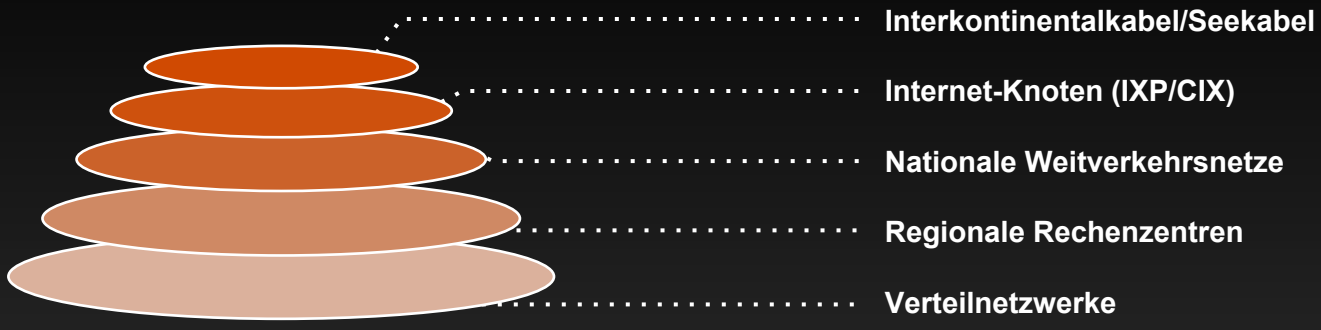
Logistische Resilienz

- Multivendoren-Strategie
- Third Party Risk Management
- Anbindung an das behördliche Modulare Warnsystem (MoWaS)

Resilienz von Telekommunikationsdiensten und -netzen darf nicht auf Cyber-Security verengt werden.

Telekommunikationsnetze – Resilient, wenn alle Netzebenen sicher sind

Um ein Netzwerk widerstandsfähig zu gestalten, ist es erforderlich, dass die Stakeholder der unterschiedlichen Netzebenen (NE) 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.



Redundante Strukturen steigern die Resilienz der Netzebenen wechselseitig – Beispiele aus der Praxis

"Wir achten auf maximale Diversität auf verschiedenen Ebenen: verschiedene Betreiber, verschiedene Unterseekabel, verschiedene Vorprodukte und verschiedene Router, auf denen sie bei uns terminieren. Solche Redundanz bauen wir auch zwischen Rechenzentren innerhalb eines Standortes. Denn es muss nicht immer nur ein Angriff sein, der zu solchen Vorfällen führt, sondern es kann auch z.B. ein Unfall durch Straßenbau sein."
– DE-CIX (NE: Internet-Knoten)

"Operative Resilienz im Störungsfall zu entwickeln, bedeutet für unsere Kunden und deren Enterprise-Kunden auf Alternativen zugreifen zu können, die umgehend zum Einsatz kommen. Ringstrukturen im GasLINE-Backbone, die schnellstmöglich ein Umrouten des IP-Verkehrs über eine andere Leitung oder einen anderen Internetknoten möglich machen, werden im Kundenauftrag und strategisch gezielt im Netz gebaut."
– GasLINE (NE: Nationale Weitverkehrsnetze)

"Mehrere Kontrollinstanzen und ein systemgestützter Zutrittsprozess mit Identitätsabgleich stellen sicher, dass nur angemeldetes und befugtes Personal Zutritt erhält. Zudem sind alle kritischen Versorgungssysteme redundant ausgelegt (Glasfaseranbindung, Stromversorgung, Klimatisierung)."
– Datacenter Leipzig (NE: Regionale Rechenzentren)

"Um die Resilienz des Network Operations Centers (NOC) zu gewährleisten, setzen wir auf eine vollständige Trennung der benötigten Managementnetze vom öffentlichen Internet. Im Krisenfall greift ein Notfallkonzept mit Aufteilung auf geografisch redundante Standorte."
– envia TEL (NE: Verteilnetzwerke)

Ganzheitliche Netzresilienz baut auf Reziprozität und zieht mehrere Ebenen in Betracht.

Resilienz im unternehmerischen Kontext

Telekommunikationsnetze sind das Rückgrat nahezu aller Wertschöpfungsketten und tragen gleichzeitig wesentlich zur Widerstandsfähigkeit von Gesellschaft und Wirtschaft bei. Dieser Bedeutung wird durch ein komplexes regulatorisches Umfeld Rechnung getragen. Nicht zuletzt dadurch verfügt der Telekommunikationssektor bereits heute über den höchsten Anteil vollintegrierter Resilienzkonzepte, verglichen mit anderen Industrien und Sektoren.

Dennoch haben auch die Top 10% im Durchschnitt nur 6,6 verschiedene Resilienzaspekte in ihr Programm integriert – zur Erhöhung von Ausfallsicherheit und Effizienz sind daher weitere Schritte notwendig. Der Telekommunikationssektor plant in den kommenden zwei Jahren wesentliche Investitionen ein:

38%

der Telekommunikations-unternehmen verfügen bereits über einen vollständig integrierten Resilienzansatz. Damit liegt der Telekommunikationssektor deutlich vor allen anderen.

Höchste Investitionen	In den vergangenen zwei Jahren		In den nächsten zwei Jahren	
1	Cyber-Resilienz	**52%**	Cyber-Resilienz	**56%**
2	Krisenmanagement	**48%**	Notfallmanagement	**45%**
3	Threat Monitoring	**45%**	Krisenmanagement	**43%**

Um die einzelnen Resilienzaspekte effizient miteinander zu verbinden, bedarf es eines klaren Zielbilds. So können Insellösungen vermieden und Risikofaktoren ganzheitlich bewertet werden. Zum Beispiel können nicht nur Cyberangriffe oder Lieferkettenstörungen Auswirkungen auf den Netzbetrieb haben – sondern auch Ausfälle von Schlüsselpersonal, nicht abgestimmte Reaktionspläne oder nicht identifizierte kritische Abhängigkeiten in Geschäftsprozessen.

Die Identifikation und Mitigation dieser Risiken sowie die Schaffung einer effizienten Governance-Struktur verbinden die Handlungsfelder physische, Cyber- und logistische Resilienz zu **operativer Resilienz**.

Der Schlüssel zu mehr Effizienz liegt in der gezielten Steuerung von Resilienzmaßnahmen entlang klar definierter, strategischer Ziele.

Wie Sie sich vorbereiten können

Betroffenheit ermitteln
Die Behörden teilen Ihnen nicht mit, ob Richtlinien wie NIS2 auf Sie zutreffen. Ihr Unternehmen oder Ihre Institution muss sich selbst anhand der Kriterien beurteilen, die sowohl Branchenelemente als auch Größenüberlegungen beinhalten.

Verantwortlichkeit klären
Die Führungskräfte in Ihrem Unternehmen sollten mit den Anforderungen der Richtlinien und den Maßnahmen zum Risikomanagement vertraut sein. Sie sind direkt dafür verantwortlich, dass Risiken erkannt und angegangen werden und dass die Anforderungen erfüllt werden.

Aufgabenbereich abstecken
Die erhöhten Anforderungen an das Risikomanagement und die Widerstandsfähigkeit bedeuten, dass Ihre Organisation mit Risiken umgehen können muss und sowohl Maßnahmen zur Schadensvermeidung als auch zur Schadensminimierung umsetzen muss, um Risiken und Auswirkungen zu verringern.

Geschäftskontinuität absichern
Ihr Unternehmen sollte sich Gedanken darüber machen, wie die Geschäftskontinuität sichergestellt werden kann, wenn Sie von einem größeren Cybervorfall betroffen sind.

Meldeverfahren einrichten
Organisationen müssen über Verfahren verfügen, die eine ordnungsgemäße Meldung an die Behörden gewährleisten. Unter anderem ist es zwingend erforderlich, dass größere Vorfälle innerhalb von 24 Stunden gemeldet werden.

Aus unserer Erfahrung in der Zusammenarbeit mit Organisationen in der gesamten EU empfehlen wir die folgenden Schritte

- Ermitteln Sie den Status-Quo der Resilienz in Ihrem Unternehmen;
- Etablieren Sie einen Sponsor aus der Geschäftsleitung;
- Identifizieren Sie Lücken in Bezug auf die Anforderungen von Richtlinien wie der NIS2, insbesondere mit Blick auf Verpflichtungen des Managements;
- Entwickeln Sie eine starke operative Resilienzstrategie, die organisatorische und technische Maßnahmen umfasst;
- Entwickeln und implementieren Sie Überwachungsmechanismen zur kontinuierlichen Überprüfung der Wirksamkeit Ihrer Maßnahmen.

Resilienzprozesse unterliegen einem ständigen Wandel und müssen kontinuierlich weiterentwickelt werden.

[3] BMI (2022): „Deutsche Strategie zur Stärkung der Resilienz gegenüber Katastrophen"

Ihre Ansprechpartner

Ansprechpartner Resilienzkonzepte

Christian Muth
Partner
Resilienz, Forensik und Krisenmanagement
+49 151 6199 7530
christian.muth@pwc.com

Jakob Großehagenbrock
Manager
Operative Resilienz und Krisenmanagement
+49 160 6755 782
jakob.grossehagenbrock@pwc.com

Ansprechpartner Cyber Security & Privacy

André Glenzer
Partner
Cyber Security & Privacy
+49 160 9447 0376
andre.glenzer@pwc.com

Florian Gibala
Senior Manager
Cyber Security & Privacy
+49 170 3858 057
florian.gibala@pwc.com

Ansprechpartner Digitale Infrastruktur

Caspar von Preysing
Partner
Digital Infrastructure
+49 175 2902 184
caspar.preysing@pwc.com

Daniel Kleid
Manager
Digital Infrastructure
+49 151 6734 5808
daniel.kleid@pwc.com