Cybersicherheits-Risikoanalyse in der DACH-Region

Quantum Fort AG
George Astakhov, Statistiker
Gregoire Devauchelle, CTO
September 26, 2025

Einführung

Quantum Fort AG ist ein Schweizer Unternehmen mit Spezialisierung auf Cybersicherheit und mehr als zehn Jahren Erfahrung in der Entwicklung und Umsetzung umfassender Lösungen im gesamten Cyberrisikoumfeld. Unser Leistungsspektrum umfasst technische Beratung sowie das Scannen und Bewerten von Cybersecurity-Infrastrukturen (inkl. der angebundenen Drittanbieter), Unterstützung bei regulatorischen Anforderungen bis hin zur Beratung und Empfehlung von Cyber-Versicherungen. Zu unseren Kunden zählen unter anderem führende Institutionen wie die City of London Police sowie namhafte Unternehmen, die wir bei der Stärkung ihrer digitalen Resilienz begleiten. Unser interdisziplinäres Team vereint Fachwissen aus den Bereichen Cybersicherheit, Data Science, Risikobewertung und Softwareentwicklung, um massgeschneiderte Sicherheitsstrategien für unterschiedlichste Organisationen zu entwickeln.

Der vorliegende Bericht beleuchtet die aktuelle Cybersicherheitslandschaft in der DACH-Region. Dabei werden interne Daten mit proprietären Informationen kombiniert, um wesentliche Bedrohungen und Trends in verschiedenen Branchen zu identifizieren. Ziel ist es, ein faktenbasiertes Verständnis der regionalen Cyberrisikoposition zu vermitteln und praxisnahe Empfehlungen für Unternehmen und Institutionen in Deutschland, Österreich und der Schweiz zu formulieren. Durch die Analyse von Angriffsmustern, Compliance-Herausforderungen und neuen Risikofeldern unterstützt **Quantum Fort AG** Organisationen sowohl im öffentlichen als auch im privaten Sektor bei der Stärkung ihrer Sicherheitsarchitektur.

Allgemeine Insights zu Cyber-Breaches in der DACH-Region

Die Analyse basiert auf **>1'100 Datenpunkten** zu Sicherheitsvorfällen in Deutschland, Österreich und der Schweiz. Dabei ist zu beachten, dass **ein einzelner Breach mehrere Ursachen haben kann**, sodass die Summe der erfassten Kategorien die Gesamtzahl der Vorfälle übersteigt.

Zudem muss die Qualität und Repräsentativität des Datensatzes kritisch betrachtet werden. Insbesondere kleinere und mittelständische Unternehmen (KMU) sind im DACH-Datensatz unterrepräsentiert, da sie im Gegensatz zu den USA nicht verpflichtet sind, Sicherheitsvorfälle öffentlich zu melden. Die amerikanischen Unternehmen sind aufgrund des Freedom of Information Act (FOIA) verpflichtet, die Fälle öffentlich zu melden. Dies führt zu einer Verzerrung hin zu größeren und etablierten Organisationen. Diese Einschränkung gilt nicht nur für die hier dargestellten allgemeinen Insights, sondern betrifft auch die weiteren Abschnitte dieses Reports. **Die Ergebnisse sollten daher stets im Lichte dieser Datenlage interpretiert werden.**

Die häufigsten Ursachen entfallen auf die Kategorie **Cyberangriffe** (1148 Fälle). Dazu gehören unter anderem *Datendiebstahl, Ransomware, DDoS-Attacken, Malware, Credential Stuffing oder Identitätsdiebstahl.* Diese Ergeb-

nisse unterstreichen, dass klassische Angriffsformen wie Schadsoftware und Erpressungstrojaner weiterhin die grösste Bedrohung darstellen.

An zweiter Stelle stehen **Schwachstellen in Infrastruktur und Technik** (561 Fälle), die beispielsweise durch *Sicherheitslücken, Konfigurationsfehler, Supply-Chain-Probleme oder technische Ausfälle* verursacht wurden.

Die Kategorie **Datenvorfälle und Informationsabfluss** (395 Fälle) umfasst unter anderem *Datenlecks, Datenverluste oder bekannte Vorfälle wie MOVEit und GoAnywhere*. Diese zeigen, wie stark externe Software-Schwachstellen und fehlerhafte Handhabung sensibler Daten Unternehmen gefährden können.

Darüber hinaus finden sich **Betrug, Manipulation und Social Engineering** (104 Fälle), darunter *Phishing, Erpressung, Deepfakes, Fake News oder Spionage*. Solche Angriffe setzen gezielt auf die Ausnutzung menschlichen Vertrauens und sind oft schwer zu erkennen.

Seltener, aber dennoch relevant, sind **Insider-Bedrohungen und menschliche Faktoren** (19 Fälle), zum Beispiel durch *Innentaeter, Sabotage oder menschliches Versagen*. Schließlich treten **weitere und neue Risiken** (13 Fälle) wie *Blockchain- sowie kryptobezogene Vorfälle* auf.

Ein Blick auf die regionale Verteilung zeigt, dass die meisten gefundene Breaches in **Deutschland (921 Fälle)** auftraten, gefolgt von der **Schweiz (175 Fälle)** und **Österreich (83 Fälle)**.

Zudem zeigt sich, dass in **über 68 % der Fälle private Organisationen betroffen** sind. **Staatliche Institutionen wie Universitäten, Behörden oder andere öffentliche Einrichtungen** stellen hingegen den kleineren Anteil dar. Dies verdeutlicht, dass Unternehmen in der DACH-Region nach wie vor ein zentrales Angriffsziel für Cyberkriminelle sind.

Einfluss des Unternehmensalters auf die Wahrscheinlichkeit von Cyber-Breaches

Unsere Analyse zeigt einen deutlichen Zusammenhang zwischen dem Alter eines Unternehmens und der Wahrscheinlichkeit, von einem Cyber-Breach betroffen zu sein. Ähnlich wie im Texas Report beobachten wir, dass ältere Unternehmen signifikant häufiger angegriffen werden als jüngere. In der DACH-Region ist eine vergleichbare Situation festzustellen, wobei der Unterschied statistisch signifikant ist ($p < 0.05$).

Ein wesentlicher Grund dafür liegt in der gewachsenen **Komplexität älterer IT-Landschaften**: Mit der Zeit entstehen umfangreiche digitale Infrastrukturen und Legacy-Systeme, die schwer abzusichern sind. Gleichzeitig steigt die Menge sensibler Daten, was Unternehmen zu attraktiveren Zielen für Bedrohungsakteure macht.

Darüber hinaus zeigt sich eine unterschiedliche Dynamik zwischen Unternehmensgrößen. Während größere Organisationen mit zunehmendem Alter in der Regel auch ihre Investitionen in IT-Sicherheit ausweiten können, fehlt kleineren und mittleren Unternehmen häufig die finanzielle und organisatorische Flexibilität, um mit dieser Komplexität Schritt zu halten. **Nur für ältere KMU**, wie auf der Abbildung 1 ersichtlich, wurde ein besonders deutlicher und **statistisch-signifikanter** Effekt gemessen. Hier entstehen über die Jahre technische Schulden und Sicherheitslücken, die das Risiko für Breaches erheblich erhöhen.

Diese Ergebnisse verdeutlichen, dass gerade langjährig bestehende Unternehmen, insbesondere KMUs, kontinuierlich in die Modernisierung ihrer Cybersecurity-Strategien investieren müssen, um ihre wachsende Angriffsfläche zu reduzieren und den steigenden Bedrohungen wirksam zu begegnen.

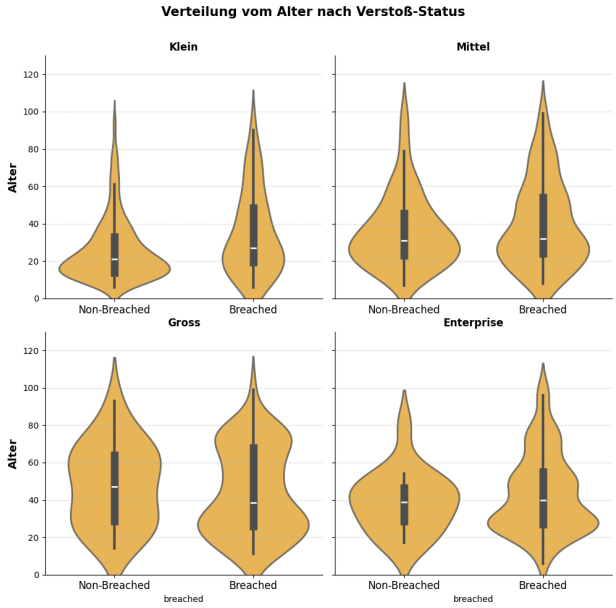


Figure 1: Altersverteilung der Unternehmen. Ältere Unternehmen scheinen häufiger unter denjenigen zu sein, die Opfer eines Cyber Events geworden sind.

Zusammenhang zwischen Unternehmensgröße, Wahrscheinlichkeit und finanziellen Folgen

Unsere Analyse zeigt: **je größer ein Unternehmen, desto höher die Wahrscheinlichkeit, Opfer eines Cyber-Breaches zu werden**. Gleichzeitig unterscheiden sich die finanziellen Folgen eines Vorfalls stark in Abhängigkeit von der Unternehmensgröße. Die Medianwerte verdeutlichen die Spannweite möglicher Verluste:

- **Kleine Unternehmen** (<50 Mitarbeitende): ca. 5'216 EUR
- **Mittelgroße Unternehmen** (50–249 Mitarbeitende): ca. 359'000 EUR
- **Große Unternehmen** (250–999 Mitarbeitende): ca. 1,97 Mio. EUR
- **Enterprise-Unternehmen** (>1000 Mitarbeitende): ca. 50,5 Mio. EUR

Während größere Organisationen aufgrund komplexer IT-Infrastrukturen und zahlreicher Mitarbeitender nahezu zwangsläufig häufiger von Vorfällen betroffen sind, können sie die Auswirkungen oft besser abfedern, da moderne Sicherheitssysteme den Schaden begrenzen.
Im Gegensatz dazu sind kleine und mittelständische Unternehmen zwar insgesamt seltener Ziel von Angriffen, doch wenn ein Breach eintritt, sind die finanziellen Folgen relativ zu Umsatz und Gewinn oft gravierender. Fehlende Investitionen in IT-Sicherheit und Mitarbeiterschulungen verschärfen dieses Risiko zusätzlich.
Die Ergebnisse machen deutlich: Cyber-Breaches stellen für alle Unternehmensgrößen erhebliche Risiken dar. Während große Unternehmen aufgrund ihrer Sichtbarkeit häufiger betroffen sind, laufen insbesondere kleinere Unternehmen Gefahr, dass ein einzelner schwerer Vorfall existenzbedrohende Konsequenzen hat.

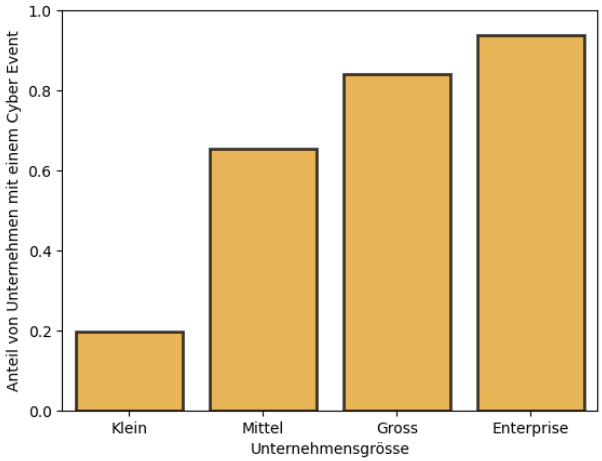


Figure 2: Wahrscheinlichkeit eines Breaches nach Unternehmensgröße.

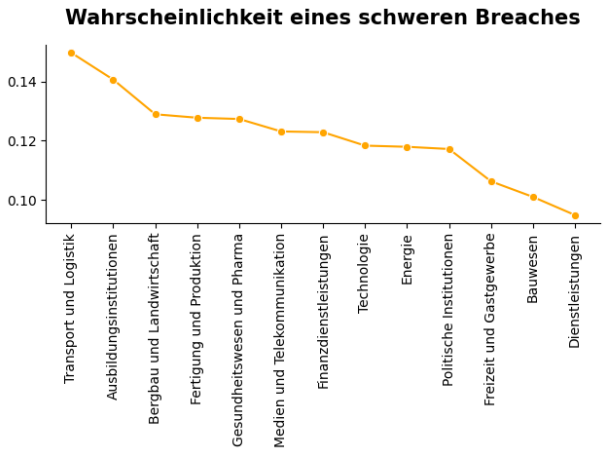
Branchenspezifische Unterschiede bei Cyber-Breaches

Unsere Analyse zeigt deutliche Unterschiede in der Betroffenheit einzelner Branchen innerhalb der DACH-Region. Besonders auffällig ist, dass

die Branche **Transport und Logistik** am stärksten von Cyber-Breaches betroffen ist. Ähnlich wie im Texas Report belegen auch unsere Daten, dass Unternehmen dieser Branche ein zentrales Ziel von Angriffen darstellen. Ein möglicher Grund liegt in der hohen Abhängigkeit von digital gesteuerten Lieferketten, Echtzeitdaten und vernetzten IT/OT-Systemen. Jede Störung hat unmittelbare operative und wirtschaftliche Folgen – was Angriffe besonders attraktiv macht.

An zweiter Stelle folgen **Ausbildungsinstitutionen**. Sie sind häufig Ziel von Angriffen, da sie in großem Umfang personenbezogene Daten wie Identitäten, Prüfungsleistungen oder Forschungsdaten speichern, gleichzeitig aber oft nur über eingeschränkte Budgets für IT-Sicherheit verfügen. Diese Kombination aus hoher Datenrelevanz und vergleichsweise schwacher Absicherung macht sie besonders anfällig.

Auf dem dritten Platz liegt die Branche **Bergbau und Landwirtschaft**. Hier spielen vor allem die zunehmende Digitalisierung und der Einsatz von IoT-gestützten Maschinen sowie automatisierten Produktionsprozessen eine Rolle. Durch die oft weit verstreuten Standorte und die begrenzte IT-Sicherheitsinfrastruktur sind diese Systeme besonders exponiert, was Cyberangriffe erleichtert und deren Folgen verschärfen kann.



Wichitigkeit von Schutzmassnahmen und Abschirmung

Basierend auf unserer Analyse gehen wir davon aus, dass in der DACH-Region rund **30 % der Unternehmen** in irgendeiner Form bereits von einem Cyber-Breach betroffen waren. Dieser Wert liefert eine erste Orientierung zur generellen Betroffenheit im Unternehmensumfeld und stimmt auch mit den Zahlen aus unterschiedlichen Reports überein (z.B KPMG)

Darüber hinaus lassen sich im Rahmen eines *technographischen Ansatzes* nur jene Unternehmen betrachten, deren Systeme auch ohne den Einsatz von illegalen Tools oder Grauzonen-Praktiken **öffentlich sichtbar und analysierbar** sind. Bei diesen Firmen zeigte sich eine deutlich erhöhte Breach-Rate von **rund 40 %**. Dies deutet darauf hin, dass bereits die bloße Sichtbarkeit im Netz ein erhebliches zusätzliches Risiko für erfolgreiche Angriffe darstellt.

Unter diesen Unternehmen zeigte sich zudem ein klares Muster: **Firmen mit einem dokumentierten Breach verfügten über eine deutlich größere externe Angriffsfläche**. Dazu zählen beispielsweise mehr öffentlich erreichbare IP-Adressen, eine höhere Anzahl an Subdomains sowie der Einsatz zusätzlicher externer Produkte wie z.B *WordPress, SharePoint oder Shopify*. Je breiter und vielfältiger diese Angriffsfläche, desto größer die Wahrscheinlichkeit, dass Schwachstellen unentdeckt bleiben und von Angreifern ausgenutzt werden.

Mit anderen Worten: **Sichtbarkeit nach außen korreliert stark mit Verwundbarkeit**. Unternehmen, die ihre Angriffsfläche effektiv reduzieren, verringern dadurch nicht nur die Angriffsmöglichkeiten, sondern auch die Wahrscheinlichkeit, selbst zu den bereits betroffenen Firmen zu gehören.

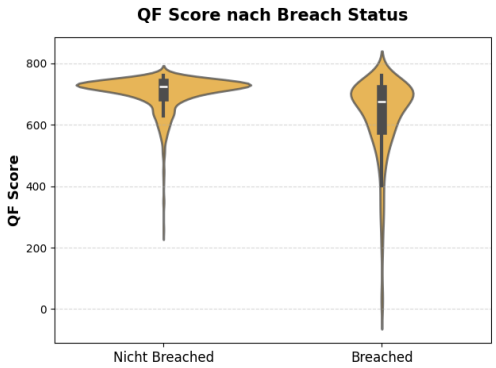
Quantum Fort Score

Neben internen Datenquellen berücksichtigt dieser Bericht auch Analysen auf Basis unseres proprietären **Quantum Fort Score** – einer von unseren Cybersecurity- und Data-Science-Teams entwickelten Kennzahl. Dieser Score bewertet die Sicherheitslage einer Organisation anhand einer Vielzahl von Faktoren, darunter Angriffsflächen-Exposition, Abhängigkeiten von Drittanbietern, Reifegrad interner Richtlinien, historische Sicherheitsvorfälle sowie die Einhaltung relevanter Compliance-Vorgaben. Es handelt sich dabei nicht um einen oberflächlichen Benchmark, sondern um einen statistisch validierten Indikator, der die Cyber-Resilienz messbar macht.

Unsere Ergebnisse zeigen, dass Unternehmen, die eine Sicherheitsverletzung erlitten haben, deutlich niedrigere Cyber-Scores aufweisen. So liegt der durchschnittliche Score bei betroffenen Unternehmen bei **627.6**, während nicht-betroffene Organisationen im Schnitt **703.1** erreichen. Dieser Unterschied ist statistisch signifikant (mit einem p-Wert von $<$ **0,05**) und bestätigt, dass der Score nicht nur mit Risiken korreliert, sondern ein aussagekräftiger Prädiktor dafür ist.

Die Ergebnisse unterstreichen die praktische Relevanz unseres Bewertungsmodells: Den eigenen Score zu verbessern, bedeutet nicht nur, eine höhere Kennzahl im Bericht zu erzielen, sondern aktiv die Angriffsfläche gegenüber realen Cyber-Bedrohungen zu reduzieren. Unternehmen mit höheren Scores zeigen konsistent bessere Erkennungs- und Reaktionsfähigkeiten, geringere Risiken im Zusammenhang mit Lieferanten sowie eine stärkere Ausrichtung an gängigen Cybersecurity-Frameworks. Der Score fungiert somit sowohl als Diagnoseinstrument als auch als Fahrplan für eine proaktive Verteidigungsstrategie.

Auch wenn der numerische Unterschied der durchschnittlichen Scores auf den ersten Blick moderat wirken mag, ist zu beachten, dass der Quantum Fort Score eine ganzheitliche Bewertung der Cyber-Hygiene vornimmt. Dazu gehören unter anderem Notfall- und Business-Continuity-Planung, Compliance-Fähigkeit und operative Resilienz – nicht nur die reine Eintrittswahrscheinlichkeit eines Angriffs. Schon moderate Verbesserungen im Score spiegeln daher substanziellen Fortschritt in mehreren zugrunde liegenden Risikodimensionen wider.



Cyber-Breaches mit Auswirkungen auf Privatpersonen

Auch wenn die meisten Vorfälle Unternehmen und Institutionen betreffen, gibt es immer wieder Beispiele, die zeigen: Cyberangriffe machen nicht vor Einzelpersonen Halt. Und die Bandbreite ist erstaunlich.
Ein **Landwirt** wiederum war Opfer eines **Ransomware-Angriffs** mit den gravierenden Folgen. So wurde auch das **E-Mail-Postfach und der Kalender einer Justizsenatorin** angegriffen, was ein klassischer Fall von Datendiebstahl ist. In einer Schweizer Gemeinde gelang es Angreifern, sich Zugang zum **privaten E-Mail-Account eines Gemeindepräsidenten** zu verschaffen und in seinem Na-

men Nachrichten zu verschicken - ein typisches Beispiel für Identitätsmissbrauch. Selbst hochrangige Politikerinnen und Politiker sind betroffen, wie ein **DDoS-Angriff auf die Webseite einer Ministerin** zeigt.

Hinter Cyberangriffen stehen auch unterschiedliche Motive. Sie beeinflussen sowohl die Wahl der Angriffsvektoren als auch die potenziellen Folgen für Betroffene. Häufige Motive sind:

- **Finanzieller Gewinn:** Viele Angriffe zielen direkt auf monetären Ertrag.
- **Politische Botschaften und Spionage:** Angriffe auf politisch exponierte Personen oder Institutionen dienen oft dazu, Informationen zu sammeln, Einfluss auszuüben oder Aufmerksamkeit für eine politische Botschaft zu erzeugen.
- **Reputation, Ruhmsucht und "for fun":** Manche Angreifer handeln aus Neugier, zum Prahlen in Szene oder schlicht „aus Spass" — etwa durch das Verschicken von Nachrichten aus fremden E-Mail-Accounts oder das Defacing von Webseiten. Solche Aktionen sind zwar nicht immer monetär motiviert, können aber hohen Reputationsschaden verursachen.
- **Sabotage und gezielte Schädigung:** In Einzelfällen steht die gezielte Schädigung eines Opfers im Vordergrund

Wichtig ist: Motive treten selten isoliert auf. Angreifer kombinieren oft finanzielle, politische und ego-getriebene Ziele, was die Schadenswirkung verstärkt und Abwehrmassnahmen komplexer macht. Die Auswahl des Angriffsvektors (Ransomware, Phishing, DDoS, Identitätsmissbrauch etc.) reflektiert dabei das beabsichtigte Ziel und die erwartete Wirkung des Angriffs.

Um solchen Risiken vorzubeugen, bieten wir eine praxisnahe Lösung an, die Privatpersonen unterstützt und dabei hilft ein sicheres Cyber System aufzubauen. Details dazu finden Sie unter Elite Protection.

Datensatzübersicht

Der für diese Analyse verwendete Datensatz umfasst **1'191 Sicherheitsvorfälle** in der DACH-Region (Deutschland, Österreich und Schweiz). Die Daten wurden durch unsere internen Methoden zur Datenaggregation erhoben, bei denen Informationen aus Open-Source-Intelligence, kommerziellen Threat-Intelligence-Feeds sowie aus überwachten Darknet-Quellen zusammengeführt wurden.

Jeder Eintrag enthält wesentliche Attribute, darunter die betroffene Organisation, den Sektor (privat oder staatlich), den Typ des Vorfalls (z. B. Cyberangriff, Datenleck, technische Schwachstelle) sowie relevante Metadaten. Dieses Merkmalset ermöglicht sowohl deskriptive Analysen als auch die Identifikation von Mustern und zentralen Risikofaktoren innerhalb der DACH-Länder.

Es ist jedoch zu beachten, dass trotz des breiten Ansatzes eine gewisse Untererfassung nicht ausgeschlossen werden kann. Besonders kleinere Organisationen oder nicht öffentlich gemachte Vorfälle sind möglicherweise nicht vollständig abgebildet.

Im Vergleich zu unserem Texas-Report wird zudem deutlich, dass es in den DACH-Ländern an gleichwertig hochwertigen und öffentlich zugänglichen Informationsquellen mangelt. Dies führt dazu, dass Analysen in diesem Raum stärker von fragmentierten und teils unvollständigen Daten abhängig sind.

Wir sind überzeugt, dass eine stärkere **Offenlegung und Open-Sourcing solcher Daten**

Forschenden helfen könnte, datengetriebene Entscheidungen zu treffen und fundiertere sowie statistisch robustere Schlussfolgerungen zu ziehen.

Schlusswort

Die Analyse zeigt klar: Cyber-Breaches sind in der DACH-Region weit verbreitet und betreffen vor allem Unternehmen mit komplexer IT-Landschaft, hoher Sichtbarkeit im Netz oder mangelnden Schutzmaßnahmen. Besonders KMU stehen vor der Herausforderung, mit begrenzten Ressourcen eine stetig wachsende Angriffsfläche abzusichern.

Branchenspezifische Unterschiede verdeutlichen zudem, dass kritische Sektoren wie Transport, Logistik und Landwirtschaft besonders im Fokus von Angreifern stehen. Gleichzeitig sind auch staatliche Institutionen und Ausbildungsstätten zunehmend betroffen.

Der **Quantum Fort Score** hat sich dabei als zuverlässiger Indikator erwiesen: Unternehmen mit niedrigen Scores sind signifikant häufiger Opfer von Breaches. Schon moderate Verbesserungen im Score spiegeln substanzielle Fortschritte in Cybersicherheit und Resilienz wider.

Unser Fazit: Organisationen in der DACH-Region müssen Cybersicherheit als strategische Kernaufgabe verstehen. Investitionen in kontinuierliche Modernisierung, Risikoreduktion und Compliance sind entscheidend, um die digitale Widerstandsfähigkeit nachhaltig zu stärken.