

CIO Advisory

# Cyber-Resilienz

Wie Sie Präventions-, Verteidigungs- und Bewältigungsfähigkeiten wirksam vereinen



# Die ernste Lage der Cybersicherheit erfordert ein Umdenken

Die deutsche Wirtschaft ist ein äußerst attraktives Ziel für Cyberangriffe. 267 Mrd. EUR Schaden<sup>1</sup> entstand deutschen Unternehmen durch Cyberangriffe im Jahr 2024. Das sind 6% gemessen am Bruttoinlandsprodukt. Dem Schaden stehen rund 11,2 Mrd. EUR Investitionen deutscher Unternehmen in Cybersicherheit gegenüber.

Cyber-Resilienz wird mittlerweile zwar regulatorisch eingefordert, der Reifegrad der Unternehmen hinkt jedoch der wirtschaftlichen und gesellschaftlichen Kritikalität hinterher. Unternehmen bewerten Cybersicherheitsvorfälle als Geschäftsrisiko Nummer eins<sup>2</sup> und 35% der mittleren und kleinen Unternehmen bewerten ihre Cyber-Resilienz als unzureichend.<sup>3</sup>

Digitale Lieferketten rücken mit steigenden geopolitischen Spannungen verstärkt ins Visier staatlich gesteuerter Akteure, mit dem Ziel einer möglichst flächendeckenden und gravierenden Wirkung der Angriffe. Im Schnitt benötigen Unternehmen 277 Tage von der Identifikation bis zur vollständigen Eindämmung eines erfolgreichen Cyberangriffs. Es ist nicht mehr möglich, alle Angriffe zu verhindern, unabhängig von der Größe des Budgets. Unternehmen müssen eine ganzheitliche Cyber-Resilienz-Strategie verfolgen, mit der sie einen balancierten Ausbau ihrer Präventions-, Verteidigungs-, und Bewältigungsfähigkeiten forcieren und sich bestmöglich auf den Ernstfall vorbereiten.

## Aussitzen ist keine Option

- Die Digitalisierung der Geschäftsmodelle vergrößert die Angriffsfläche jeden Tag weiter
- Die Abhängigkeit der Unternehmen von digitalen Lieferketten steigt, 54% der Unternehmen sehen das Drittparteirisikomanagement als eine große Herausforderung
- Angreifer professionalisieren sich und werden mit steigenden geopolitischen Spannungen noch stärker staatlich subventioniert
- Neue Technologien beflügeln Effizienz und Wirksamkeit von Cyberkriminellen rasant
- Der Fachkräftemangel ist im Bereich Cybersecurity bereits groß und wächst weiter

## Unternehmen müssen jetzt handeln

- Unternehmen müssen aufhören eine reine Präventionsstrategie zu verfolgen oder „nur“ den Compliance Status anzustreben
- Unternehmen müssen ihre Fähigkeiten zur Verteidigung und Bewältigung von Cyberangriffen verbessern
- Erfolgreiche Unternehmen implementieren eine effektive Cyber-Resilienz-Strategie und Governance
- Dabei werden technische und organisatorische Präventions-, Verteidigungs-, und Bewältigungsfähigkeiten balanciert und vereint
- Cyber-Resilienz reduziert im Ernstfall die finanziellen Auswirkungen, sichert den Geschäftsbetrieb und erhöht die Fähigkeit, sich kontinuierlich anzupassen

## Kein leichtes Unterfangen

Wir unterstützen unsere Kunden seit langen Jahren in den Themen IT Compliance, Risiko und Sicherheit. Hinsichtlich Cyber-Resilienz sehen wir dabei aktuell immer wieder ähnliche Herausforderungen.

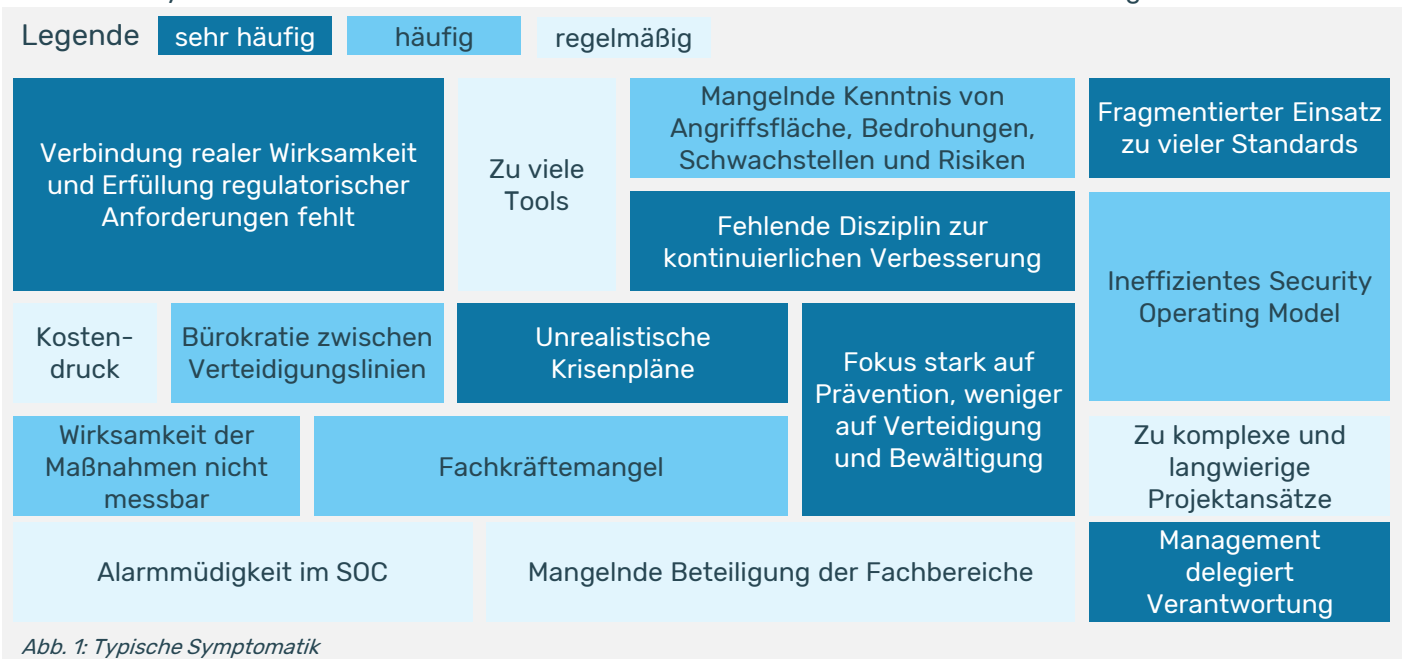


Abb. 1: Typische Symptomatik

<sup>1</sup>Quelle: Bitkom, Studie Wirtschaftsschutz 2024; <sup>2</sup>Quelle: Allianz, Risk Barometer 2024; <sup>3</sup>Quelle: WEF, Global Cyber Security Outlook 2025



## Welche Faktoren sind für Cyber-Resilienz entscheidend?

Grundvoraussetzungen für den Aufsatz einer wirksamen Cyber-Resilienz-Strategie sind die Kenntnis der Angriffsfläche und Bedrohungslage, das Verständnis realer Angriffstechniken und Schwachstellen. Darüber hinaus müssen die geschäftsbetrieblichen Auswirkungen und Risiken eines erfolgreichen Angriffs der Geschäftsleitung bekannt sein, um fundierte Entscheidungen zur Priorisierung der erforderlichen Maßnahmen treffen zu können und deren Umsetzung adäquat zu fördern. Regelmäßige Kontrollen und Verbesserungen sollten zur organisatorischen Routine gehören, genauso wie eine regelmäßige Reifegradmessung der Cyber-Resilienz. Um die Wirksamkeit der eingesetzten Budgets sicherzustellen, sollte das Betriebsmodell sicherheitsrelevanter Prozesse und Tools laufend auf Effizienz optimiert werden. Besonders wichtig ist zudem, dass Unternehmen die Bewältigung einer Cyberkrise üben, bevor es dazu kommt. Im Ernstfall entscheiden die ersten 24 Stunden nach einem Angriff über das Schicksal eines Unternehmens.

### Faktor 1: Wissen

- Aktuelle und genaue Kenntnis der individuellen Bedrohungslage und Angriffsfläche
- Sachkundiges Verständnis realer Angriffstechniken, deren Schadwirkung auf den Geschäftsbetrieb sowie die Identifikation von Schwachstellen
- Konsistente Quantifikation und verständliche Kommunikation der geschäftsbetrieblichen Auswirkungen an die Geschäftsleitung

### Faktor 2: Priorisierung

- Ableitung relevanter und umsetzbarer Maßnahmen
- Einwertung von Aufwänden und Wirkung der Maßnahmen auf den Cyber-Resilienz-Reifegrad
- Allokation von Budgets wird am Return on Security Invest gemessen
- Adäquate Gewichtung von Präventions-, Verteidigungs-, und Bewältigungsmaßnahmen



Abb. 2: Die vier Erfolgsfaktoren der Cyber-Resilienz

### Faktor 4: Vorbereitung

- Aktuelle und getestete Wiederherstellungspläne
- Cyber-Resilienz-bezogene Krisenstabsübungen
- Minutiöses testen, lernen und verbessern der Rollen und Verantwortlichkeiten in einer Cyberkrise
- Regelmäßige Übungen zur Erhöhung der Erkennungs- und Reaktionsgeschwindigkeit relevanter Tools, Ressourcen und Anbieter
- Auswahl externer Partner für die Krise (z.B. Anwälte, IT-Forensik, PR-Agentur) vor der Krise

### Faktor 3: Effizienz

- Förderung der Umsetzung durch die Geschäftsleitung und das Management der Fachbereiche
- Regelmäßige unabhängige Kontrolle der Umsetzung ist Routine des laufenden Betriebs
- Erreichung strategischer Ziele wird regelmäßig quantifiziert und berichtet
- Kontinuierliche Effizienzsteigerung und Kostenoptimierung der sicherheitsrelevanten Projekt-, Anbieter-, Ressourcen-, Tool- und Prozesslandschaft



# Das plenum Cyber-Resilienz-Rahmenwerk nutzen

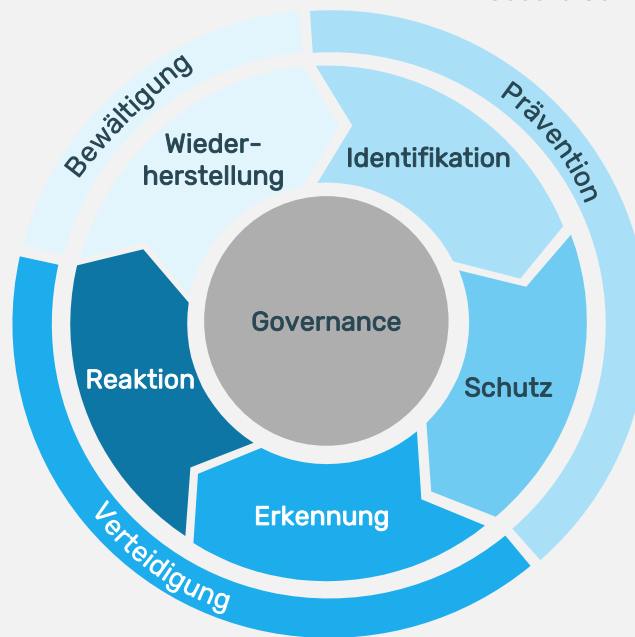
plenum hat aktuelle internationale Standards genutzt und Erfahrungen aus langjähriger Praxis einfließen lassen, um ein Cyber-Resilienz-Rahmenwerk zu erstellen. Den Kern des Rahmenwerks bildet eine Cyber-Resilienz-Governance, die Präventions-, Verteidigungs- und Bewältigungsfähigkeiten wirksam vereint und adäquat ausbalanciert. Wir empfehlen Unternehmen, den Reifegrad im ersten Schritt gegen ein Set an Schlüsselkontrollen zu bewerten. Im Anschluss kann die Breite und Tiefe erforderlicher Analysen an den individuellen Geschäfts- und Risikokontext passgenau ausgerichtet werden.

## Governance

- Geschäftskontext und Führung
- Rollen und Verantwortlichkeiten
- Richtlinien und Prozesse
- Risikomanagementrahmen
- Cybersecurity in Lieferketten

## Identifikation & Schutz

- Offensives Testen und Risikobewertung
- Asset- und Schwachstellenmanagement
- Kontinuierliche Verbesserung
- IAM, PAM und Authentifizierung
- Resilienz IT-Infrastruktur
- Kultur, Awareness und Training
- Datensicherheit
- Secure Software Development Lifecycle



## Wiederherstellung

- BCM und Krisenmanagement
- IT-Notfallmanagement
- Forensik und Sicherung
- Wiederherstellung von Daten und Systemen

## Erkennung & Reaktion

- Kontinuierliche Überwachung, SIEM
- Analyse von Anomalien, SOAR
- Threat Hunting
- Incident Response Management
- Analyse und Mitigierung
- Reporting und Kommunikation

Abb. 3: Das plenum Cyber-Resilienz-Rahmenwerk



# Quick-Check Cyber-Resilienz

Wo steht Ihr Unternehmen in Bezug auf Cyber-Resilienz? Ganz am Anfang, fokussiert auf regulatorische Compliance, oder bereits auf dem Weg zu einer umfassenden, strategischen Cyber-Resilienz-Lösung? Reflektieren Sie Ihre Einschätzung gerne entlang folgender Fragestellungen.

Treffen die Aussagen links oder rechts eher auf Ihre Organisation zu:	
Dokumentation ist wichtig	1 Durchsetzung und Umsetzung ist wichtig
Geschäftsleitung delegiert	2 Geschäftsleitung fördert
Beseitigung von Feststellungen	3 Mitigation realer Risiken
Compliance orientierte Metrik	4 Reifegrad und KRI-basierte Metrik
Theoretische Risikoanalysen	5 Risikoanalysen auf Basis realer Bedrohungen
Regulatorik priorisiert	6 Standards priorisiert, Regulatorik als Beiprodukt
Angriffsfläche unvollständig erfasst	7 Angriffsfläche automatisiert und aktuell erfasst
Awareness-Training computerbasiert jährlich	8 Umfassendes Cyber-Kultur-Programm
Pauschales Loggen und ineffizientes Monitoring	9 Gezieltes Loggen und optimiertes Monitoring
Netzwerk- & Cloudarchitektur verstehen wenige	10 Netzwerk- & Cloudarchitektur nach Best Practice
Zu viele Sicherheitstools gekauft, zu wenige Experten eingestellt, ineffiziente Prozesse	11 Experten eingestellt, Prozess- und Toollandschaft wird laufend optimiert
Bürokratie verlangsamt Reaktion auf Vorfälle	12 Zusammenspiel aus Experten, Prozessen und Tools steigert die Reaktionsgeschwindigkeit
Externe Meldungen funktionieren theoretisch	13 Externe Meldungen funktionieren praktisch
Krisen- und Notfallplan geschrieben und veraltet	14 Krisen- und Notfallplan getestet und verbessert
Keine Cyber-Versicherung oder Partner für eine Cyberkrise	15 Cyber-Versicherung und diversifizierte Landschaft an Partnern für eine Cyberkrise

## Mehrzahl der Antworten eher links?



Ihr Unternehmen fokussiert stark auf die Einhaltung regulatorischer Vorgaben und hat unter Umständen Lücken gegenüber gängigen Standards sowie nicht erkannte Risiken. Überprüfen Sie den Reifegrad gegen das Cyber-Resilienz-Rahmenwerk, um an den richtigen Stellen anzusetzen und eine ganzheitliche Cyber-Resilienz-Strategie zu entwerfen.

## Mehrzahl der Antworten eher rechts?



Ihr Unternehmen geht das Thema Cyber-Resilienz strategisch an und hat bereits einen hohen Cyber-Resilienz-Reifegrad. Eine individualisierte Reifegradbewertung gegen das plenum Cyber-Resilienz-Rahmenwerk begleitet von Interviews und tiefergehenden Analysen kann Ihnen jetzt bei der weiteren Optimierung und wirksamen Umsetzung der Cyber-Resilienz-Strategie helfen.



# plenum Leistungsangebot Cyber-Resilienz

Wir unterstützen Ihr Unternehmen individuell, ganzheitlich und bedarfsorientiert auf dem Weg zu einer höheren Cyber-Resilienz – vom initialen Orientieren, über das kontinuierliche Optimieren, bis hin zum realitätsnahen Testen. Sprechen Sie uns an und vereinbaren ein Termin mit unseren Experten.

## Orientieren

Unser Angebot für Unternehmen, die das Thema Cyber-Resilienz angehen möchten, aber die individuelle Bedrohungslage, Angriffsfläche und Risiken nur teilweise kennen.

## Optimieren

Unser Angebot für Unternehmen, die sich als „compliant“ einschätzen und nun wissen möchten, ob sie wirklich sicher sind oder wie sie noch effizienter werden können.

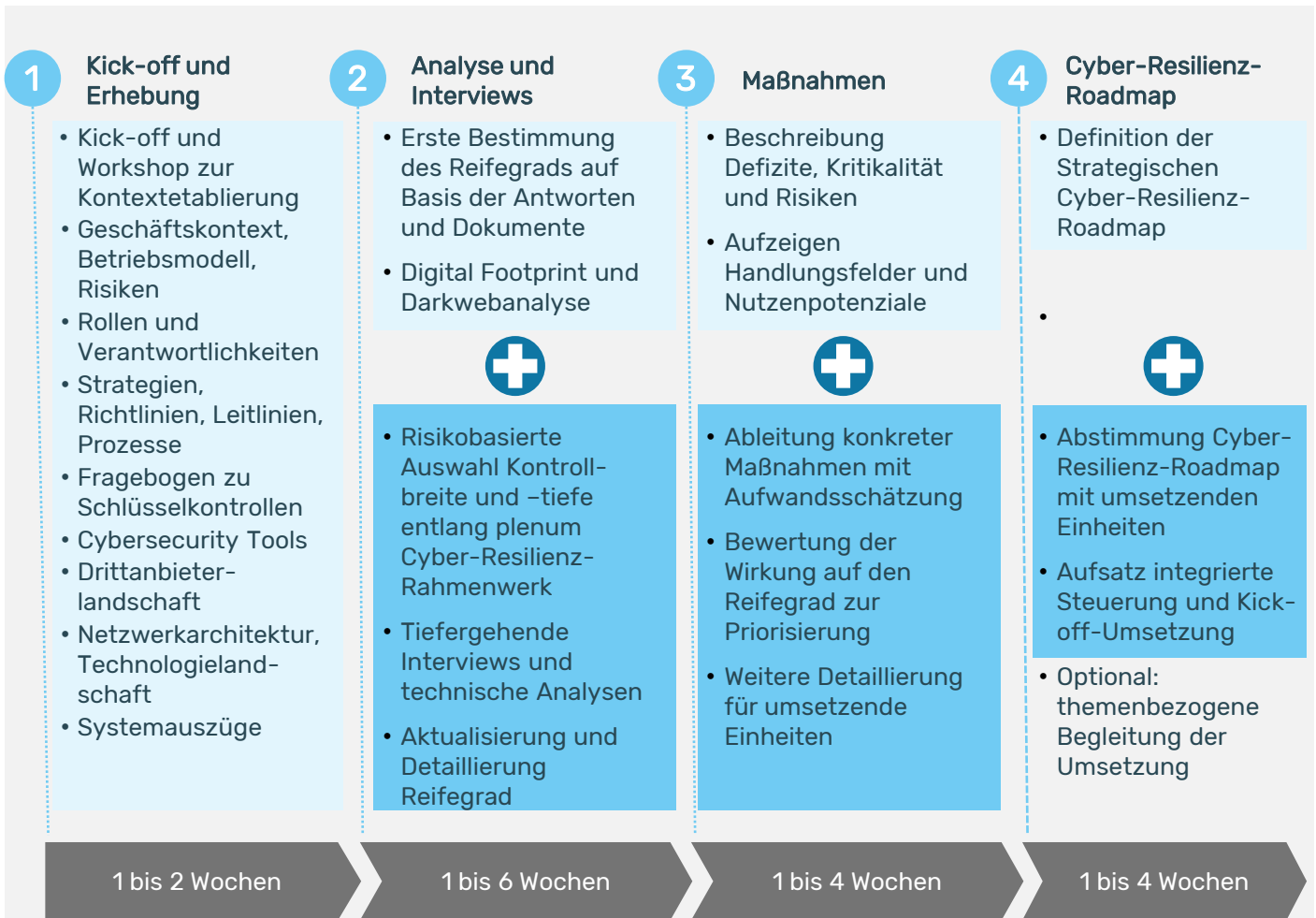


Abb. 4: Typisches Projektvorgehen Orientieren (hellblau hinterlegt) und Optimieren (dunkelblau hinterlegt).

## Vorbereiten

Unser Angebot für Unternehmen, die ihre Organisation gezielt auf die Situation eines erfolgreichen Cyberangriffs vorbereiten wollen.

- Cyber-Resilienz-Krisenübung zur Überprüfung und Stärkung der Krisen-„Readiness“
- Planung und Durchführung von Übungen zur Verbesserung der Erkennungs- und Reaktionszeiten
- Aufsatz oder Review eines umfangreichen Cyber-Resilienz-Testprogramms gemäß DORA
- Test und Optimierung interner und externer Meldeprozesse