Cyberrisiko als Existenzfaktor: Der Angriff als Auslöser oder Risiko der Restrukturierung

Sanierungskonferenz 2026

Heidelberg, 18. September 2026

Agenda

1 Cyberrisiken und Handlungsempfehlungen

2 Bedeutung und Umsetzung im Sanierungskonzept

Die nackten Zahlen: Deutschland im Fadenkreuz

Cybercrime verursacht in Deutschland Schäden in Milliardenhöhe

Entwicklungen im Bereich und deren Konsequenzen für Unternehmen in der heutigen Zeit

Fakten und Zahlen im Jahr 2026

67% der deutschen Unternehmen waren **von Daten- und IT-Geräte-Diebstahl, Industriespionage oder Sabotage** betroffen

Weitere 29% vermuteten einen Vorfall

Fast jedes Unternehmen in Deutschland ist schon betroffen gewesen – oder weiß es noch nicht

Der deutschen Wirtschaft entstand 2025 ein Gesamtschaden von **289,2 Mrd. €** – **deutlich mehr** als im Jahr 2024 (266,6 Mrd. €)

Der entstandene Schaden entspricht in etwa dem **halben Bundeshaushalt** Deutschlands

Einordnung der Situation

- Wir sprechen von einer der **größten wirtschaftlichen Bedrohungen unserer Zeit**
- Laut BKA-Bundeslagebild Cybercrime 2025: **335.000** verübte **Cybercrime-Fälle** in Deutschland im Jahr 2025
- Etwa zwei Drittel der Taten (207.888) wurden aus dem Ausland oder von unbekannten Tatorten aus begangen

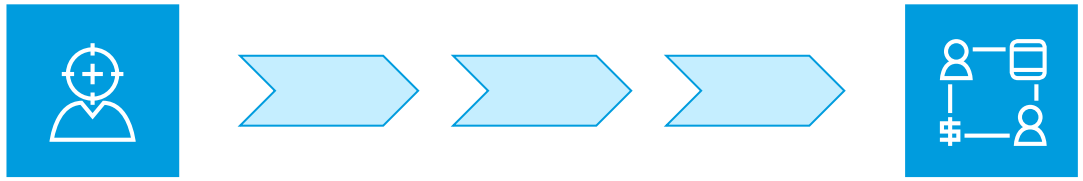
Das Täterfeld: Hochorganisiert, professionell, arbeitsteilig

Cyberkriminelle zeigen professionelle Strukturen und eine hohe Schattenwirtschaft auf – Cybercrime-as-a-Service, KI und die geopolitische Dimension prägen das Täterfeld

Strukturen der Cyberkriminalität

Cyberkriminalität – kein Hobby von Einzeltätern in dunklen Kellern

- Cyberkriminalität hat sich **massiv professionalisiert**
- Was früher vereinzelte Angriffe waren, ist heute eine **hochorganisierte Schattenwirtschaft** mit klarer Arbeitsteilung
- Ransomware-Betreiber, deren Partner und spezialisierte Access Broker arbeiten Hand in Hand
- Auch 2025 war das Geschäftsmodell **„Cybercrime-as-a-Service"** von zentraler Bedeutung. „Underground Economy" bietet ihre **kriminellen Dienstleistungen** in industriellen Maßstäben an
- **Künstlichen Intelligenz** dürfte diesen Trend weiter verstärken



Cybercrime als politische Bedrohung

- Zusätzlich zunehmende **geopolitische Dimension** zu beobachten
- Bundesinnenminister Alexander Dobrindt betonte: „Wir beobachten eine zunehmende Ausweitung **geopolitischer Konflikte in den digitalen Raum** und stellen fest, dass die hybride Bedrohung in Deutschland erkennbar angestiegen ist. Dabei verschwimmen die Grenzen zwischen finanziell und politisch motivierten Cyber-Gruppierungen immer mehr."
- Ziele waren **primär öffentliche Einrichtungen und Behörden**, aber auch Logistikdienstleister und Unternehmen des verarbeitenden Gewerbes

Die wachsende Angriffsfläche

Digitalisierung erweitert die Angriffsfläche: Täglich werden neue Schwachstellen bekannt, Fälle zeigen die systemische Abhängigkeit von funktionierender IT

Schwachstellen und Angriffspunkte

Täglich werden ∅ **119 neue Schwachstellen** bekannt – ein **Anstieg von 24 %** von 2024 auf 2025

Betroffen sind **Fachanwendungen, Serverinfrastrukturen und Smartphone-Apps**

Besonders gefährlich: **Zero-Day-Schwachstellen**, für die es noch keine Sicherheitsupdates gibt

Die fortschreitende Digitalisierung und Vernetzung **erweitert die Angriffsflächen stetig**

Erläuterung

- **Jedes neue System**, jedes IoT-Gerät, jede Cloud-Anbindung kann potenzielle Einfallstore bieten
- Cyberkriminelle **nutzen zunehmend Schwachstellen** in Perimetersystemen wie Firewalls und VPN-Zugängen aus
- Ein Beispiel, das die systemische Abhängigkeit illustriert: Das **fehlerhafte Update** eines Sicherheitsprodukts von CrowdStrike am 19. Juli 2024 führte zu weltweiten IT-Ausfällen mit erheblichen wirtschaftlichen Schäden
- Ein Vorfall, der zeigt, wie **abhängig** moderne Unternehmen von funktionierender IT-Infrastruktur sind

RSM US Middle Market Business - Index Sonderbericht: Cybersicherheit 2026

KI, wirtschaftliche Unsicherheit und geopolitische Spannungen verschärfen die Cyberbedrohungslage im Mittelstand

Cyberbedrohungen nehmen strukturell zu

- KI, geopolitische Spannungen und wirtschaftlicher Druck verschärfen die Cyberbedrohungslage deutlich
- Mittelstand bleibt aufgrund begrenzter Ressourcen, gewachsener IT-Strukturen und Reifelücken besonders angreifbar
- Erforderlich sind klare Gegenmaßnahmen – von Cyberstrategie und KI-Vorhaben bis hin zu Cloud-Steuerung und Risikovorsorge

Der Mittelstand bleibt besonders verwundbar

- 18 % der befragten Führungskräfte aus dem Mittelstand berichten von Datenschutzverletzungen im letzten Jahr
- 24 % der mittelständischen Unternehmen waren von Ransomware-Angriffen oder -Forderungen betroffen
- Mittelständler liegen bei Budget, Personal und Governance häufig hinter größeren Marktteilnehmern zurück

Vertrauen in Maßnahmen ist hoch – Reifegrad oft noch nicht

- 96 % vertrauen ihren bestehenden Schutzmaßnahmen
- Gleichzeitig bestehen Lücken bei Incident Response, Identitätskontrollen, KI-Governance und Wiederanlauffähigkeit

Identität wird zum zentralen Risikofeld

- Angreifer „brechen“ häufig nicht ein, sondern „loggen sich ein“
- Schwache Berechtigungen, unklare Zugriffsmodelle und nicht-menschliche Identitäten erhöhen das Risiko zusätzlich

Cybersecurity als Steuerungs- und Resilienzthema

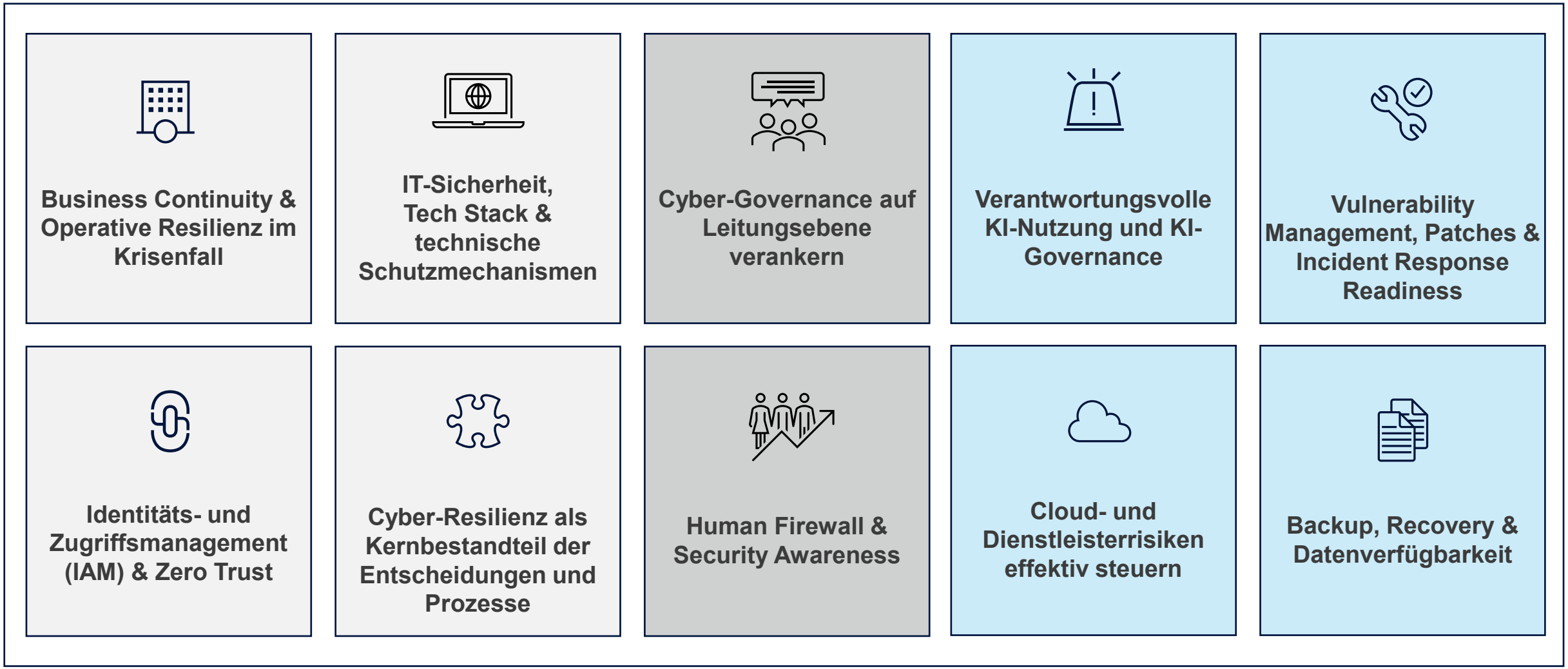
- Cyberrisiken beeinflussen Steuerung, Stabilität und Fortführungsfähigkeit von Unternehmen unmittelbar
- Entscheidend sind klare Prioritäten, wirksame Governance und ein risikoorientierter Mitteleinsatz

Ausgangslage und Kerndaten zur Studie

- RSM US Middle Market Business Index Sonderbericht: Cybersicherheit 2026
- Grundgesamtheit Mittelstand: 30 Mio. USD und 10 Mrd. USD Umsatz
- Marktgröße: rund 125.000 Unternehmen im modernen Mittelstand
- Befragung: 602 Führungskräfte (USA und Kanada)
- Branchen: Breite Abdeckung verschiedener Branchen des Mittelstands
- Befragungszeitraum: Januar & Februar 2026

Top-10-Handlungsempfehlungen

Stärkung der Cybersicherheit im Mittelstand: Top-10-Handlungsempfehlungen



Agenda

1 Cyberrisiken und Handlungsempfehlungen

2 Bedeutung und Umsetzung im Sanierungskonzept

Cyber Security – Standards und gesetzliche Vorgaben

Für Cyber Security sind verschiedene Standards und Frameworks etabliert; vor allem in den Branchen sind Standards de facto verpflichtend; grundsätzlich geringer Anteil an gesetzlichen Vorgaben

Bestehende Standards, Frameworks und gesetzliche Anforderungen im Cyber Security

Standards und Frameworks

Übergreifende Standards

ISO/IEC 27001
- Aufbau und Betrieb eines Information Security Management Systems (ISMS)
- Zertifizierbarer Nachweis

ISO/IEC 27701
- Erweiterung ISMS um Datenschutz
- Strukturierte Umsetzung von Privacy-Anforderungen

[…]

Branchen-Standards

TISAX
- Branchenstandard der Automobilindustrie
- Einheitliches Assessment und Austausch v. Prüfergebnissen

IEC 62443
- Sicherheitsstandard für industrielle Systeme (OT/ICS)
- Anforderungen an Hersteller, Integratoren und Betreiber

[…]

Frameworks

CIS Critical Security Controls
- Konkrete, priorisierte Sicherheitsmaßnahmen
- Fokus auf operative Umsetzung

NIST
- Rahmen für Cyber-Risiko-management (5 Funktionen)
- Strukturierung und Reifegradbewertung

[…]

Gesetzliche Anforderungen

Richtlinien

NIS2-Richtlinie
- EU-Vorgaben zu Cyber-security und Meldepflichten
- Mindestanforderungen an Organisationen

[…]

Cyber Security – IDW S 6

IDW S 6 als reine Orientierungshilfe im Umgang mit Cyber Security; keine klaren Vorgaben definiert; RSM Ebner Stolz profitiert daher durch starkes Netzwerk aus Cyber Security Experten

Cyber Security im Rahmen des IDW S 6

IDW S 6

Inhalte zu Cyber Security im IDW S 6

- Cyber Security soll als Bestandteil der „digitalen Strategie“ ein Teil des strategischen Leitbildes sein. Es werden Vorkehrungen zur Abwehr von Cyber-Angriffen als elementarer Bestandteil der digitalen Strategie gefordert
- Ergänzende Informationen aus dem F&A:
  - Empfehlung zum Einsatz von Checklisten zur Bewertung vorgesehener Maßnahmen zur Abwehr von Cyber-Angriffen
  - Empfehlung von Experten, sofern eigene Expertise nicht ausreichend ist

„…pflichtgemäßen Ermessen des Konzepterstellers […] über die Auswirkungen […] zu berichten.“

Relevante Fragestellungen gemäß F&A zum IDW S 6

- Wie ist das IT-Zugriffs- / Berechtigungssystem organisiert?
- Wie wird das Netzwerk regelmäßig auf Intrusion geprüft?
- Wie häufig wird ein Backup erstellt?
- Liegt eine Zertifizierung der Informationssicherheit vor?
- Besteht eine Cybercrime-Versicherung?
- […]

Bedeutung für das Sanierungsgutachten

Cyber Security als Bestandteil des strategischen Leitbildes im IDW S 6; Bedeutung und Notwendigkeit adäquater Betrachtung im Sanierungsgutachten aufgrund der inhärenten Eigenschaften

Komponenten des strategischen Leitbildes

Scope des strategischen Leitbildes gemäß IDW S 6

- **Wesentlichen Geschäftsfelder**
- **Ressourcen & Fähigkeiten**
- **Langfristige Zielvorstellungen**
- **Grundstrategien**
  - **Digitale Strategie**
  - **ESG-Strategie**
- **Angestrebte Wettbewerbs-position**
- **Wertvorstellungen, Grundregeln und Verhaltensweisen**

Bedeutungsgrad Cyber Security

Die Gewichtung der Cyber Security im Sanierungsgutachten wird vor allem im Vergleich zu anderen strategischen Elementen wie der ESG-Strategie deutlich:

	Cyber Security	ESG
Scope	Konkretes Risikofeld	Breiter Rahmen
Bedeutung	Strategisch & operativ kritisch	Strategisch wichtig
Zeithorizont	Sofortige Auswirkung	Langfristige Wirkung
Steuerungs-logik	Incident-getrieben	Reporting-getrieben

Cyber Security erfordert eine adäquate Betrachtung, da hiermit entsprechende Risiken als auch mögliche Chancen einher gehen

Bewertungsansatz Cyber Security im Rahmen des IDW S 6

Adäquate Bewertung und Ausarbeitung der Cyber Security im Sanierungsgutachten erfordert einen strukturierten Prozess; begleitet durch hohe Expertise sowie effizientes und kostenbewusstes Handeln

Mehrstufiger Bewertungsansatz

Analyse

Phase 1 **Ist-Analyse der IT-Organisation mit folgendem Fokus**

- Prüfung von Aufbau-/ Ablauforganisation und Prozesse
- Durchführung einer übergeordneten Risikobewertung

Phase 2 **Unternehmensspezifische Schwachstellenanalyse**

- Durchführung eines modularen Penetrationstests
- Identifizierung von potenziellen technischen und organisatorischen Schwachstellen inklusive Risiken

Einsatz anerkannter Standards (bspw. ISO/IEC 27001, NIST)

Auswertung

Phase 3 **Identifikation von Handlungsempfehlungen**

- Ergebniskonsolidierung der Analysephasen
- Ableitung konkreter Handlungsempfehlungen

Zentrale Inhalte für das Sanierungsgutachten

Bei **Ausgestaltung** des **Cyber-Security-Inhalts** im Rahmen des Sanierungsgutachtens sollten **drei Anforderungen** sichergestellt werden:

Durch den gezielten Einsatz von Experten …
auch Zugang zu kuratiertem Netzwerk spezialisierter Cyber-Security-Unternehmen – passgenaue Expertise

… gelingt es Cyber Security effizient …
Standardisierte Prozesse mit fokussiertem Individualisierungsgrad – bei Einhaltung des Zeitplans

… sowie kostenbewusst zu adressieren
Effiziente Arbeitsweise sowie konsequente Begrenzung des Inhalts auf die wesentlichen Anforderungen

Exemplarischer Foliensatz im Sanierungsgutachten

[Unternehmen] historisch durch Cyberangriffe vorbelastet; erste Maßnahmen bereits eingeführt; individueller Bewertungsansatz im Rahmen Cyber Security durch RSM Ebner Stolz eingesetzt

EXEMPLARISCH

Bewertungsergebnisse und Anforderungsprofil

Wesentliche Bewertungsergebnisse

- Analyse hat eine Vielzahl kritischer Komponenten und Risikofelder aufgezeigt
- Fokus liegt auf geschäftskritischen Assets und Prozessen, einem wirksamen Cyber-Risikomanagement sowie einer kontinuierlichen Überwachung
- RSM Ebner Stolz empfiehlt Maßnahmen zur Erhöhung der Transparenz von Cyberrisiken sowie den Aufbau eines toolbasierten Frühwarnsystems für eine effektive Risikobewertung und -steuerung

[Unternehmen] ist dem Bereich sonstige Unternehmen zuzuordnen

Kritische Infrastrukturen	Ausfall gefährdet öffentliche Sicherheit oder Grundversorgung	☐
Regulierte Unternehmen	Erhöhte Bedeutung mit zusätzlichen Cyber-Security-Vorgaben	☐
Sonstige Unternehmen	Keine Systemrelevanz, primär wirtschaftliche Auswirkungen	☒

Erforderliches Anforderungsprofil gemäß Klassifizierung

Standards	Bewährte Sicherheitsstandards (z. B. ISO/IEC 27001)
Systeme	Gesicherte IT-Systeme, Netzwerke und Datenbestände
Prozesse	Verbindliches Risiko-, Incident- und Notfallmanagement

Historie und Bewertungsansatz

Historische Ereignisse

- Ransomware-Angriff im Mai 2025: 3 Tage Produktionsstillstand, Datenverlust und finanzieller Schaden im sechsstelligen Bereich
- Kompromittierung von Zugangsdaten im Januar 2026: Fast-Überweisung im fünfstelligen Bereich sowie Reputationsschaden

Intern implementierte Standards und Maßnahmen

- Einführung von Multi-Faktor-Authentifizierung (MFA)
- Regelmäßige Awareness-Schulungen (verpflichtende für alle Mitarbeitenden)
- Zentrales Patch- und Update-Management

Bewertungsansatz

in den wesentlichen Analysefeldern zur Bewertung Cyber Security

Strategie	**Rollen**	**Assets & Prozesse**	**Risiko-mgmt.**	**Drittparteien**
Prävention	**Überwachung**	**Bewusstsein**	**Vorfall-mgmt.**	**Resilienz**

Exemplarischer Foliensatz im Sanierungsgutachten

Vielzahl kritischer Komponenten und Risikofelder identifiziert; Fokus auf kritische Assets und Prozesse, Cyber-Risiko-Management sowie Überwachung

EXEMPLARISCH

Kritische Komponente	Risiko	Handlungsbedarf
Security-Strategie und Governance ▪ Keine klar definierte Sicherheitsstrategie ▪ Keine verbindlichen Richtlinien ▪ Geringe Management-Einbindung	▪ Inkonsistente Maßnahmen ▪ Sicherheitslücken durch uneinheitliches Verhalten sowie mangelnde Priorisierung von Cyber Security	gering – hoch
Rollen und Ver-antwortlichkeiten ▪ Unklare Zuständigkeiten ▪ Überlastung einzelner Personen ▪ Fehlende Trennung von Aufgaben	▪ Sicherheitsaufgaben werden nicht wahrgenommen ▪ Operative Sicherheitslücken	
Kritische Assets und Prozesse ▪ Unvollständige Asset-Transparenz ▪ Fehlende Priorisierung und unklare Abhängigkeiten	▪ Schutzmaßnahmen greifen nicht ▪ Kritische Systeme unzureichend geschützt ▪ Hohe Ausfallrisiken	
Cyber-Risiko-management ▪ Risiken werden nicht strukturiert erfasst ▪ Fehlende Risikobewertung ▪ Keine regelmäßige Aktualisierung	▪ Risiko von Blind Spots ▪ Falsche Priorisierung von Maßnahmen ▪ Veraltete Risikolage	
Überwachung ▪ Unvollständige Protokollierung ▪ Keine zentrale Auswertung von Logdaten ▪ Fehlende Alarmierungsmechanismen	▪ Sicherheitsrelevante Ereignisse bleiben z.T. unentdeckt ▪ Verzögerte Reaktion auf Sicherheitsvorfälle	

Ihre Ansprechpartner

Christoph Elzer

Partner
Restrukturierung
München

christoph.elzer@ebnerstolz.de
Mobil +49 170 2155212

John Hoffmann

Partner, CISA, CIA
Geschäftsbereich IT-Revision
Stuttgart

John.Hoffmann@ebnerstolz.de
Mobil +49 152 21775698