DORA als Benchmark für den Mittelstand

Implikationen für Aufsichtsgremien


Nicola Oetker-Hilker, Geschäftsführende Gesellschafterin der Feingeist Board Advisors GmbH & Co.KG, Krefeld; Dr. Ralf Winckler, Managing Director TNP Consultants, Feingeist Board Advisors GmbH & Co.KG, Krefeld

Arten und Anzahl der Eintrittshäufigkeit von speziell digitalen Unternehmensrisiken stellen die Risiko-Resilienz nicht nur von Unternehmen im Finanzsektor stetig auf den Prüfstand. Der Aufsichtsrat muss sich intensiv mit dem Risikomanagement seines Unternehmens beschäftigen und sich von dessen Wirksamkeit überzeugen (§ 111 AktG). Über die gesetzlichen Anforderungen an die Erfüllung der Sorgfaltspflicht des einzelnen Aufsichtsratsmitgliedes hinaus nimmt die Relevanz ebenso für fakultative GmbH Aufsichtsräte zu. Ein bestenfalls entscheidungsorientiertes Risikomanagement kann helfen, den Anforderungen der Business Judgement Rule bei unternehmerischen Entscheidungen gerecht zu werden. Empfohlen wird ein Blick auf DORA und deren Standards als mögliche Benchmark, um potenzielle Risiken lokalisieren, verstehen, bewerten und beheben zu können.

I. Risiko Selbsteinschätzung

1. Beginnen wir ganz persönlich

Nutzen Sie als Mitglied im Aufsichtsgremium sensible Informationen auf Ihren persönlichen elektronischen Geräten, wie z.B. geheime Strategiepläne, Details zu Vorstandsvergütungen oder vertrauliche Finanzdaten? Wie steht es um den Schutz dieser sensiblen Daten z.B. durch Zero-Knowledge Verschlüsselung?

Das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG), das seit dem 26. April 2019 in Kraft ist, stellt deutliche Anforderungen an die Absicherung von Geschäftsgeheimnissen. Ein Geschäftsgeheimnis liegt vor, wenn zum Schutz der betreffenden sensiblen Informationen im Unternehmen angemessene Geheimhaltungsmaßnahmen getroffen worden sind.

Zwei Konsequenzen folgen für Unternehmensorgane und damit auch für den Aufsichtsrat. Erstens sind Schutzmaßnahmen zu treffen und zweitens müssen sie angemessen sein. Fehlt eines dieser Kriterien, kann das Unternehmen die Ansprüche nach GeschGehG nicht geltend machen. Im Regelfall ist auch keine alternative Anspruchsgrundlage einschlägig und die Gesellschaft kann im Innenverhältnis ggf. Regress gegenüber Geschäftsführung und Aufsichtsrat nehmen. Hier kann es sich um erhebliche Haftungsbeträge handeln. Der Abschluss einer D&O-Versicherung mag zwar beruhigen, bedeutet aber keinesfalls einen Freibrief.

Was als „angemessen" angesehen werden kann, bedarf der Konkretisierung, z.B. durch Rechtsprechung. Daher kann derzeit keine sichere Empfehlung ausgesprochen werden. Gut beraten sind Geschäftsführung und Aufsichtsrat aber, wenn sie wie folgt vorgehen:

1. Identifizierung und Kategorisierung aller geheimhaltungsbedürftigen Informationen;
2. Installation nach dem Risikograd abgestufter organisatorischer, technischer und rechtlicher Maßnahmen;

INHALT

Keywords
Business Judgement Rule; Cybersecurity; Digitale Resilienz; DORA (Digital Operational Resilience Act); GeschGehG; IKT; Risikomanagement

Normen
§§ 91, 93, 107, 111, 116; § 117 Abs. 3 AkG

3. Aktualisierung und Überprüfung aller Schutzmaßnahmen in regelmäßigen Abständen.

Geschäftsgeheimnisse und damit relevante streng vertrauliche Unternehmensdaten müssen unter anderem abgesichert, das bedeutet, nicht ohne Weiteres zugänglich sein.

Praxistipp

Ihr Unternehmen muss nachweisen, dass es sein Know-how durch nach außen hin erkennbare, objektive und angemessene Maßnahmen zur Geheimhaltung geschützt hat. Die Ansprüche an Unterlassung und Schadensersatz durch die Geschädigten sind durch das GeschGehG nachhaltig gestärkt worden.

2. Wie steht es um Ihr Aufsichtsgremium?

Ist Ihr Aufsichtsgremium fit in Digitalkompetenz und verfügt es über entsprechende Kenntnisse im Bereich des Risikomanagements?

Eine Studie der ECBE und hkp basierend auf Geschäftsberichten aus dem Jahr 2022 von DAX, MDAX und SDAX Unternehmen zeigt deutlichen Handlungsbedarf. 160 Unternehmen wurden befragt und haben auf der Grundlage von Eigeneinschätzung sowie teilweise auf Grundlage von Beurteilung durch einen externen Partner ihre Kenntnisse in aufsichtsratsrelevanten Themen bewertet:

Interne Kontrolle, Risikomanagement und Digitalisierung liegen laut Studie beim Gesamtranking deutlich im unteren Bereich mit 41 % bzw. 32 %. Knapp 2/3 der befragten Aufsichtsräte der Daxfamilie trauen sich demnach nur geringe Kenntnisse und Kompetenzen in zwei immer wichtiger werdenden Themenblöcken zu.

II. Einschätzung von Geschäftsrisiken

Demgegenüber nimmt der Anstieg von Unternehmensrisiken weltweit zu. Laut Allianz Risk Barometer 2024 bilden Cybervorfälle wie Ransomware-Angriffe, Datenschutzverletzungen und IT-Unterbrechungen im Jahr 2024 die größte Sorge für Unternehmen weltweit. An zweiter Stelle steht die eng miteinander verknüpfte Gefahr der Betriebsunterbrechung. Naturkatastrophen (von Platz 6 auf Platz 3 im Vergleich zum Vorjahr), Feuer, Explosion (von Platz 9 auf Platz 6) und politische Risiken und Gewalt (von Platz 10 auf Platz 8) sind die größten Aufsteiger in der neuesten Zusammenstellung der wichtigsten globalen Geschäftsrisiken, die auf den Erkenntnissen von mehr als 3.000 Risikomanagementexperten basieren. Die Aufforderung zum Handeln wird deutlich bei Betrachtung der Entwicklung der Top 10 Geschäftsrisiken weltweit im Allianz Risk Barometer in 2024.

Ranking pro Nennung

	N*	DAX	MDAX	SDAX
Branchenerfahrung/Geschäftsfelder	69 %	68 %	74 %	65 %
ESG, Nachhaltigkeit, CSR	64 %	60 %	65 %	61 %
Leitungs-/Kontrollerfahrung	60 %	61 %	53 %	66 %
Finanzen, Rechnungslegung, Abschlussprüfung	60 %	58 %	54 %	70 %
Personal	54 %	67 %	50 %	42 %
Compliance, Corporate Governance, Recht	50 %	49 %	47 %	56 %
Internationale Erfahrung	45 %	44 %	49 %	42 %
Digitalisierung, Technologie, IT	41 %	39 %	41 %	43 %
Strategie	39 %	47 %	32 %	36 %
Interne Kontrolle & Risikomanagement	32 %	31 %	30 %	37 %

*Über alle Unternehmen der DAX-Indexfamilie

Abb. 1: Relevanz von Risikomanagement und Digitalkompetenz, Quelle: ECBE Studie, hkp group 2023

III. Call to Action

Aus dem Vergleich des Rankings der Einschätzung eigener Kompetenzen im Aufsichtsgremium einerseits und der Benennung der Top 10 Geschäftsrisiken andererseits ergibt sich ein Gap, das es für Leitungsorgane und Aufsichtsgremien im Besonderen zu schließen gilt. Ein Call-to-Action, das handlungsorientiert und klar zum Handeln auffordert:

Die Beschäftigung mit den Themen Cybersicherheit, IKT (Informations-, Kommunikations- Technologien)-Risikomanagement, Geschäftskontinuität sind „Muss-Themen" für den Aufsichtsrat und ein fundiertes Wissen ist nicht zuletzt im Aktiengesetz für den Aufsichtsrat beziehungsweise dessen Prüfungsausschuss für das Risikomanagement festgelegt (§ 116 i.V.m. § 93 sowie § 117 Abs. 3 AktG).

Neben der legalen Verpflichtung ergibt sich die Notwendigkeit, sich mit digitaler Resilienz auseinander zu setzen aus dem weltweit drastischen Anstieg von Cyberangriffen. Diese Angriffe erfolgen branchenübergreifend, treffen die betroffenen Unternehmen ohne merkliche Vorwarnung und richten jährlich hohe finanzielle Schäden sowie Reputationsschäden an. Die vom Bitkom e.V. im Jahr 2023 erhobenen Gesamtschäden für Unternehmen allein in Deutschland betrugen 205,9 Mrd. Euro.

Laut Bitkom e.V. ist die Betroffenheit in den Punkten digitaler Diebstahl von Geschäftsdaten und digitale Sabota-

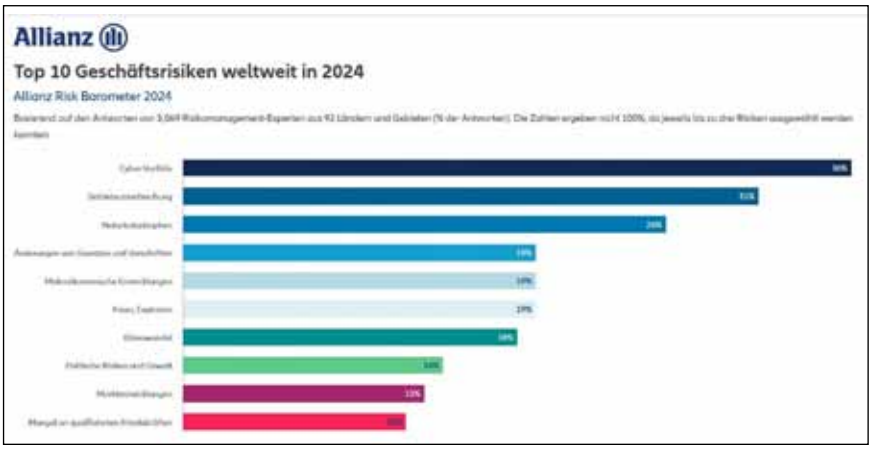

Abb. 2: Top 10 Geschäftsrisiken in 2024 (Quelle: Allianz)

Abb. 3: Durch Cyberangriffe verursachter Gesamtschaden (Quelle: bitkom)

ge von Informations- und Produktionssystemen mit über 70 Prozent der befragten Unternehmen besonders hoch.

Wie also können und sollten sich Unternehmen auch außerhalb des Finanzsektors und mit ihnen ihre Aufsichtsgremien vertiefend dem Thema Cybersecurity nähern?

IV. DORA als Benchmark für den Mittelstand

1. Von der Pflicht für den Finanzsektor

Im Finanzsektor gilt ab dem 17. Januar 2025 der Digital Operational Resilience Act (DORA) gemäß der Verordnung EU 2022/2554 verpflichtend für europäische Unternehmen sowie für ihre Dienstleister. Das heißt, für externe Partner und Dienstleister in der Wertschöpfungskette findet die EU-Verordnung ebenso Anwendung. Die digitale Resilienz wird damit für Finanzdienstleister ebenso entscheidend wie ihre finanzielle Stabilität. Das wesentliche Kernelement ist das sogenannte IKT-Risikomanagement. DORA setzt einheitliche Standards für die Informationssicherheit und deren kontinuierliche Überwachung. Finanzunternehmen sind verpflichtet, bestehende IKT-Risiken systematisch zu identifizieren, sie zu bewerten und zu steuern. Damit geht die Entwicklung einer DOR (digitale operationale Resilienz)-Strategie einher, die neben dem internen Risikomanagement das Drittparteienrisikomanagement betrifft. Der bisherige Kontroll- und Governance-Rahmen muss erweitert werden, damit u.a. die Überwachung von Verträgen mit IKT-Drittdienstleistern inkludiert werden kann. Ein wesentlicher Baustein von DORA sind die erweiterten Anforderungen an das IKT-Geschäftsfortführungsmanagement, damit im Krisenfall die Fortführung der kritischen und wichtigen Funktionen des Finanzinstitutes sichergestellt ist. Auch wurde eine breitere Anzahl an Risikofaktoren berücksichtigt, wie z.B. Naturkatastrophen, Insider-Angriffe, soziale oder politische Instabilität oder klimawandelbedingte Risiken. Somit wird den unterschiedlichen Risikogruppen Rechnung getragen und eine Inklusion der Top 10 Geschäftsrisiken weltweit laut Allianz Risk Barometer sichtbar.

2. Zum Nutzen für KMUs im Mittelstand

In ähnlicher, teilweise nahezu gleicher Art und Weise sind mittelständische Unternehmen von den genannten Risiken betroffen. DORA übersetzt für den Mittelstand bedeutet gleichsam eine verstärkte Verbesserung von bestehenden Abwehrmechanismen, vorab die Wahrnehmung und Einschätzung derselben. Die Risikobetrachtung wird ausgeweitet auf relevante Dienstleister, insbesondere IT-Dienstleister, die meist vollen Zugang zu den kritischen IT-Schnittstellen besitzen und so ungewollt selbst zum Risiko werden können. DORA kann als Katalysator genutzt werden für ein effektives Geschäftsprozessmanagement (BPM). In diesem können proaktive, anpassungsfähige und resiliente Ansätze entwickelt werden, um mögliche Risiken frühzeitig zu lokalisieren, sie wahrzunehmen, einzuschätzen und die geeigneten Abwehrmechanismen zu aktivieren.

Für mittelständische Unternehmen können Aufbau und Implementierung eines IKT-Risikomanagements eine erhebliche Belastung darstellen. Die Umsetzung eines IKT-Risikosystems erfordert ein tiefes Verständnis komplexer technologischer Zusammenhänge. Themen wie Datenintegrität und Cloudsicherheit erfordern hohe

Kernziele und Schlüsselaspekte von DORA

- Stärkung der Resilienz
  - Sicherstellung der Widerstandsfähigkeit gegenüber Störungen der IKT
  - Testen der Resilienz durch regelmäßige Stresstests
- Harmonisierung von Anforderungen
- Einführung einheitlicher Standards für das Management operationeller Risiken im gesamten EU-Finanzsektor
  - Einführung resistenter Systeme zur Identifizierung, Bewertung und Überwachung digitaler Risiken
  - Regelmäßige Risikobewertung für alle IKT-Prozesse und -Systeme
  - Verpflichtung zur Transparenz und Berichterstattung
- Schutz vor Cyberbedrohungen
- Management und Prävention von Cyberattacken, IT-Ausfällen und Datenverlusten
  - Verpflichtung zur Meldung schwerwiegender IKT-Vorfälle an die zuständigen Behörden
  - Einheitliche Meldeformate für alle Unternehmen im Finanzsektor
- Förderung einer nachhaltigen und robusten IKT-Infrastruktur für den Finanzsektor und dessen Dienstleister
  - Unternehmen sind verpflichtet, Risiken, die durch Drittanbieter entstehen, umfassend zu überwachen und zu steuern
  - Einführung von Anforderungen an die Verträge mit IKT-Dienstleistern, einschließlich Notfallplänen und Exitstrategien
  - Erweiterung des Due-Diligence-Prozesses bei der Auswahl von Drittanbietern
- Stärkung von Governance und Verantwortlichkeiten:
  - Unternehmensführung und Aufsichtsräte tragen die Verantwortung für die Umsetzung von DORA
  - Schulungen und Festlegung klarer Verantwortlichkeiten im Risikomanagement
  - Etablierung klarer Berichts- und Überwachungsmechanismen für digitale Risiken

Aufmerksamkeit. Die Implementierung intern oder mittels einer externen Beratung kann zu erheblichen Kosten führen. Dies erfordert eine sorgfältige Planung und Priorisierung im Rahmen der Governance.

Die Einführung eines IKT-Risikomanagementsystems ist eine interdisziplinäre Aufgabe, bei der unterschiedliche Abteilungen (IT, Rechts bzw. Compliance, Risikomanagement und interne Revision) gemeinsam zusammenarbeiten müssen. Quick Wins bei der Identifikation von Gaps, der Entwicklung eines maßgeschneiderten Lösungsansatzes und die Optimierung von Prozessen stehen zunächst im Fokus. Es gilt insbesondere für KMUs den richtigen Kipppunkt zwischen zunehmender Belastung und Bürokratie und der Steigerung digitaler Resilienz zu finden.

V. Geschäftsprozessmanagement als Schlüssel zum Erfolg

Ein wesentlicher Erfolgsfaktor bei der Umsetzung der DORA-Vorgaben ist ein effektives Geschäftsprozessmanagement (BPM). Ein gut strukturiertes BPM unterstützt Unternehmen nicht nur bei der Einhaltung regulatorischer Anforderungen, sondern bietet auch zahlreiche Vorteile, die weit über die DORA-Compliance hinausgehen:

1. **Optimierung und Risikominimierung:** Eine systematische Analyse und Optimierung der Geschäftsprozesse ist notwendig, Risiken frühzeitig zu identifizieren und zu minimieren. Dies schafft eine solide Basis für die Einhaltung der DORA-Vorgaben und verbessert gleichzeitig die betriebliche Effizienz.
2. **Erhöhte Transparenz und Kontrolle:** Ein klar definiertes BPM erhöht die Transparenz in den Arbeitsabläufen. Ziel ist Prozesskontrollen einzuführen, die es ermöglichen, Abweichungen frühzeitig zu erkennen und zu korrigieren. Dies sorgt für eine nahtlose Integration der DORA-Vorgaben in die Unternehmensprozesse.
3. **Effiziente Ressourcennutzung:** Der BPM-Ansatz hilft, Ressourcen optimal zu nutzen, indem Prozesse automatisiert und standardisiert werden. Dies reduziert nicht nur den Aufwand für die DORA-Compliance, sondern trägt auch zu einer insgesamt effizienteren Betriebsführung bei.
4. **Bessere Entscheidungsfindung:** Der Einsatz von BPM gewährt wertvolle Einblicke in die Unternehmensprozesse, die eine datengestützte Entscheidungsfindung ermöglichen. Ziel ist, fundierte Entscheidungen zu treffen, die IT-Sicherheitsstrategien und Risikomanagementmaßnahmen effektiv unterstützen.
5. **Kontinuierliche Verbesserung und Anpassungsfähigkeit:** Die Anforderungen im digitalen Raum entwickeln sich ständig weiter. Ein dynamisches BPM erlaubt, Prozesse kontinuierlich zu verbessern und flexibel auf neue Herausforderungen zu reagieren. Eine notwendige Voraussetzung ist,

dass die Prozesse stets auf dem neuesten Stand sind.

VI. Implikationen für den Aufsichtsrat

Das gesamte Aufsichtsgremium muss und kann nicht zu IT-Experten werden. Aber es kann Fachausschüsse bilden, die sich detailliert mit fachspezifischen Themen befassen und diese dem Plenum im Extrakt nahebringen. Der Prüfungsausschuss ist in vielen praktischen Fällen der meistgebildete Ausschuss. § 107 Abs. 3 AktG benennt die Pflicht des AR zur Überwachung von Governance-Systemen und Abschlussprüfung.

Der Aufsichtsrat kann aus seiner Mitte einen oder mehrere Ausschüsse bestellen, namentlich, um seine Verhandlungen und Beschlüsse vorzubereiten oder die Ausführung seiner Beschlüsse zu überwachen. Er kann insbesondere einen Prüfungsausschuss bestellen, der sich mit der Überwachung des Rechnungslegungsprozesses, der Wirksamkeit des internen Kontrollsystems, des Risikomanagementsystems und des internen Revisionssystems sowie der Abschlussprüfung, hier insbesondere der Auswahl und der Unabhängigkeit des Abschlussprüfers, der Qualität der Abschlussprüfung und der vom Abschlussprüfer zusätzlich erbrachten Leistungen, befasst. Der Prüfungsausschuss kann Empfehlungen oder Vorschläge zur Gewährleistung der Integrität des Rechnungslegungsprozesses unterbreiten. Dem Aufsichtsrat ist regelmäßig über die Arbeit der Ausschüsse zu berichten.

Regelmäßige Weiterbildungen zu aktuellen Trends im Risikomanagement sind angeraten, um als Sparringspartner auf Augenhöhe die richtigen Fragen stellen zu können. Externe Experten können fallweise wertvolle Einblicke in spezifische Risiken bieten. Nur so kann der Aufsichtsrat die Wirksamkeit des IKT-Risikomanagements überprüfen und ebenso auf die Einhaltung rechtlicher Anforderungen (§ 91 Abs. 2 AktG) achten.

Es ist die Pflicht der Aufsichtsgremien sicherzustellen, dass die von der Geschäftsleitung implementierte Risikostrategie mit den Zielen des Unternehmens übereinstimmt. Auch ist dem Aufsichtsrat regelmäßig vom Vorstand zu berichten, damit die Prüfung der Angemessenheit der Methoden zur Risikobewertung und -überwachung möglich ist. Ein IKT-Risikomanagement System kann für die Wahrnehmung der Überwachungs- und Kontrollfunktion des Aufsichtsrates eine wertvolle Unterstützung sein, wenn es entscheidungsorientiert auf Grund der klar strukturierten Abwägung möglicher Risiken basiert ist. Aufsichtsräte treffen insbesondere bei der Beschlussfassung über zustimmungsbedürftige Geschäfte unternehmerische Entscheidungen im Sinne der Business Judgement Rule.

§ 93 Abs. 1 Satz 2 AktG benennt die Voraussetzungen, unter denen keine Pflichtverletzung des Organmitglieds vorliegt, obwohl dem Unternehmen ggf. ein Schaden entstanden ist. In der Praxis werden diese Voraussetzungen, die erfüllt sein müssen, damit die „Haftungsfreistellung" der Business Judgement Rule greift, in fünf Tatbestandsmerkmale gesplittet, die kumulativ erfüllt sein müssen:

- Unternehmerische Entscheidung,
- Wohl der Gesellschaft,
- Keine Sonderinteressen,
- Angemessene Information und
- Guter Glaube

Die Beweislast dafür, dass die Voraussetzungen der Business Judgement Rule erfüllt sind, trägt das Aufsichtsratsmitglied selbst. Die Einführung von zentralen Verantwortlichkeiten im Unternehmen im Rahmen des Risikomanagements, die Einführung bzw. Adaption von DORA als Benchmark in Abhängigkeit des Umfeldes des individuellen Unternehmens können dem Aufsichtsrat helfen, seine Überwachungsfunktion effektiv wahrnehmen zu können. Und mehr noch können unternehmerische Entscheidungen für alle Unternehmensorgane auf einer risikobewerteten Grundlage getroffen werden.

VII. Fazit

Die Umsetzung der DORA-Verordnung bietet mittelständischen Unternehmen trotz höherer Belastungen bei der Einführung zahlreiche Chancen, ihre digitale Resilienz zu stärken und sich zukunftssicher aufzustellen. Mit der Unterstützung neutraler Dritter und einem effektiven BPM kann es gelingen, notwendige Anforderungen zu formulieren und effizient zu erfüllen, Risiken zu minimieren und damit die Marktpositionierung zu stärken. Das ist operativ die Aufgabe des Vorstandes und der Geschäftsleitung. Aufsichts- und Beirat sollen in der Lage sein, die digitale Resilienz in ihrer Struktur zu verstehen, das relevante Thema zum Top-Thema auf ihrer Tagesordnung zu machen und die Operative als Sparringspartner bei der Umsetzung zu unterstützen. Zudem können mögliche Haftungsrisiken im Rahmen der Business Judgement Rule minimiert werden.

DORA bietet dabei als EU-Richtlinie eine Benchmark, mit deren Beschäftigung und sinnvoll abgewandelten Regeln für KMUs ein professionellerer Umgang mit Bereich des Risikomanagements entstehen kann. Die Risiken und Kritikalität des individuellen Geschäftsmodells bestimmen die Größe der Umsetzungsmaßnahmen und den Reifegrad der vorhandenen digitalen Resilienz. Damit können Cybersicherheit, Betriebsstabilität und das Vertrauen der Stakeholder geschützt werden. Mit Hilfe einer pragmatischen und an das jeweilige Unternehmen angepassten Umsetzung können KMU ihre Anforderungen effizient und kosteneffektiv adressieren.