

CHEFSACHE IT-SICHERHEIT

10 Punkte, die Geschäftsführer und Vorstände
jetzt im Blick haben sollten.

Inhaltsverzeichnis:

1. IT-Sicherheit ist Organpflicht – nicht nur Aufgabe der IT-Abteilung – 03
2. Welche Pflichten Ihr Unternehmen treffen: NIS2, DSGVO, StaRUG und Kundenvorgaben – 05
3. IT-Risikoregister & Frühwarnsystem: Welche Ausfälle bestandsgefährdend sind – 07
4. Identitäten & Zugriffe absichern: Der schnellste Weg ins Unternehmen führt über Accounts – 09
5. Backup ist nicht gleich Wiederherstellung: Warum Standard-Retention oft nicht reicht – 11
6. Notfallmanagement & Wiederanlauf: Wie handlungsfähig ist das Unternehmen im Ernstfall? – 13
7. Cloud-, SaaS- & Dienstleisterrisiken: Shared Responsibility endet nicht beim Provider – 14
8. Schwachstellen, Patches und externe Angriffsfläche beherrschen – 16
9. Meldepflichten & Datenschutz: Was muss wann dokumentiert und gemeldet werden? – 18
10. Security-Kultur, Schulungen und Reporting an die Leitung verankern – 20

EINORDNUNG

Warum dieses Thema auf die Agenda der Geschäftsleitung gehört

Cybersicherheit ist im Mittelstand endgültig vom IT-Thema zur Führungsaufgabe geworden. Die Frage ist längst nicht mehr, ob ein Unternehmen von Cyberrisiken betroffen sein kann, sondern wie gut Geschäftsleitung und Vorstand darauf vorbereitet sind, diese Risiken zu steuern, zu priorisieren und im Ernstfall handlungsfähig zu bleiben. Denn moderne Sicherheitsvorfälle treffen heute nicht nur Server und Anwendungen, sondern unmittelbar Wertschöpfung, Lieferfähigkeit, Reputation, Kundenerwartungen und Haftungsfragen. Wer IT-Risiken unterschätzt, riskiert deshalb nicht nur technische Störungen, sondern operative, regulatorische und wirtschaftliche Schäden.

Gleichzeitig ist die Lage für viele mittelständische Unternehmen unübersichtlich geworden. NIS2, DSGVO, StaRUG, Kundenanforderungen, Lieferkettenvorgaben und steigende Erwartungen von Versicherern, Prüfern und Auftraggebern wirken oft parallel. Hinzu kommt: Mit Cloud, SaaS und ausgelagerten Services werden IT-Strukturen zwar flexibler, aber nicht automatisch sicherer oder einfacher steuerbar. Die Verantwortung bleibt bei der Unternehmensleitung – auch dann, wenn Betrieb, Plattformen oder Teilprozesse an Dritte ausgelagert wurden

Genau hier setzt dieser Leitfaden an. Er übersetzt IT- und Cyber Risiken in Management-Sprache und zeigt die zehn Felder, in denen Geschäftsführer und Vorstände heute besonders gefordert sind: von Organpflicht und Risikofrüherkennung über Identitäten, Backups und Wiederanlauf bis hin zu Meldepflichten, Dienstleistersteuerung und Sicherheitskultur. Ziel ist kein technischer Deep Dive, sondern ein klarer Führungsrahmen für die Fragen, die auf Leitungsebene wirklich entschieden werden müssen.

Die gute Nachricht lautet: Wirksame Cybersicherheit beginnt nicht mit maximaler Komplexität, sondern mit Klarheit über Verantwortung, Prioritäten und Nachweisfähigkeit. Wer seine geschäftskritischen Risiken kennt, Sicherheitsmaßnahmen auf die richtigen Kronjuwelen ausrichtet und Wiederherstellung, Notfallmanagement sowie Reporting sauber verankert, schafft nicht nur regulatorische Anschlussfähigkeit, sondern stärkt die Resilienz des gesamten Unternehmens. So wird Cybersicherheit vom reaktiven Pflichtprogramm zu einem strategischen Enabler für Zukunftsfähigkeit. Gleichzeitig entsteht eine belastbare Grundlage, um handlungsfähig und glaubwürdig zu bleiben.

Cybersicherheit beginnt nicht mit maximaler Komplexität, sondern mit Klarheit über Verantwortungen, Prioritäten und Nachweisfähigkeit!



IT-Sicherheit ist Organpflicht – nicht nur Aufgabe der IT-Abteilung

IT-Sicherheit war lange ein Thema, das viele Geschäftsführungen gedanklich bei der IT-Abteilung verortet haben: Firewalls, Updates, Administratoren, externe Dienstleister. Diese Sicht ist heute überholt. Denn Cyberrisiken sind längst keine rein technischen Störungen mehr, sondern unternehmerische Risiken mit potenziell existenziellen Folgen – von Produktionsstillstand über Datenverlust bis hin zu Haftungs-, Bußgeld- und Reputationsschäden. Genau deshalb ist IT-Sicherheit rechtlich nicht mehr nur „Sache der IT“, sondern Teil ordnungsgemäßer Unternehmensführung. Für Geschäftsleiter ist das die eigentliche Zäsur: Nicht der einzelne Hackerangriff begründet das Haftungsrisiko, sondern eine Organisation, die Cyberrisiken nicht angemessen steuert, überwacht und dokumentiert. Wer IT-Sicherheit

nur operativ delegiert, ohne klare Governance, Berichtslinien und Kontrollmechanismen zu etablieren, bewegt sich heute in einem rechtlich riskanten Raum. Oppenhoff bringt es treffend auf den Punkt: IT-Sicherheit ist Aufgabe der Unternehmensleitung; Delegation ändert nichts daran, dass die Leitung Einhaltung, Umsetzung und Wirksamkeit der Sicherheitsstrategie überwachen muss. Rein rechtlich ist IT-Sicherheit damit keine IT-Option mehr, sondern Ausdruck der Organpflicht zur ordnungsgemäßen Geschäftsführung – vergleichbar mit Rechnungslegung, Compliance oder Risikomanagement. Diese Einordnung folgt aus den allgemeinen Sorgfalts- und Organisationspflichten des Gesellschaftsrechts und wird durch das neue Cybersicherheitsrecht noch einmal ausdrücklich geschärft.

Was das Gesetz heute wirklich verlangt

Die gesellschaftsrechtliche Basis ist klar: Geschäftsführer einer GmbH müssen nach **§ 43 GmbHG** die Sorgfalt eines ordentlichen Geschäftsmannes anwenden; für Vorstände einer AG gilt nach **§ 93 AktG** die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters. Ergänzend verlangt **§ 91 Abs. 2 AktG** geeignete Maßnahmen und insbesondere ein Überwachungssystem, damit bestandsgefährdende Entwicklungen früh erkannt werden. Cyberrisiken fallen heute ohne Weiteres in diese Kategorie, weil sie Verfügbarkeit, Integrität und Vertraulichkeit geschäftskritischer Systeme unmittelbar betreffen können. Mit **NIS2** und dem seit Dezember 2025 geltenden deutschen Umsetzungsgesetz ist diese Verantwortung nun ausdrücklich kodifiziert. Nach **§ 38 BSIG** müssen die Geschäftsleitungen wichtiger und besonders wichtiger Einrichtungen die Cyber-Risikomanagementmaßnahmen billigen, deren Umsetzung überwachen

und regelmäßig Schulungen absolvieren; zudem knüpft die Norm den Haftungsbezug ausdrücklich an schuldhaftes Pflichtverletzungen der Leitung. Parallel stellt die **NIS2-Richtlinie in Artikel 20** klar, dass Managementgremien die Maßnahmen genehmigen, ihre Umsetzung beaufsichtigen und für Verstöße haftbar gemacht werden können.

Wichtig ist dabei: Unternehmen, die nicht unmittelbar unter NIS2 fallen, können sich nicht entspannt zurücklehnen. Die gesetzlichen Leitplanken aus Sorgfaltspflicht, Organisationserfordernissen und Risikofrüherkennung gelten ohnehin. Hinzu kommt, dass NIS2 die Erwartungshaltung des Marktes verändert: Kunden, Versicherer, Prüfer, Banken und größere Auftraggeber werden Cyberresilienz zunehmend als Führungs- und Nachweisthema behandeln. Die praktische Messlatte steigt damit für den gesamten Mittelstand.

„Die IT kümmert sich darum“
reicht nicht mehr aus:

- **Verantwortung bleibt:** Aufgaben können delegiert werden, die Gesamtverantwortung aber nicht.
- **Keine Blinddelegation:** Zuständigkeiten, Ressourcen und Kontrollen müssen klar geregelt sein.
- **Risikoverständnis:** Die Leitung muss geschäftskritische Systeme und Ausfallrisiken kennen.
- **Management-Aufgabe:** Themen wie Incident Response, Backup, Wiederherstellung und Zugriffsschutz gehören auf die Agenda.
- **Neue Rolle:** Die Geschäftsleitung ist nicht nur Empfänger von Berichten, sondern aktiver Auftraggeber und Überwacher.
- **Nachweispflicht:** Entscheidend ist, dass angemessene Maßnahmen, Entscheidungen und Kontrollen belegt werden können.

Welche Erwartungen heute an Geschäftsführung und Vorstand gestellt werden

Ein modernes Leitungsorgan sollte heute mindestens vier Dinge sicherstellen. Erstens: Cyberrisiken müssen im unternehmerischen Risikobild sichtbar sein – nicht isoliert in einer IT-Ecke, sondern als Bestandteil der Gesamtsteuerung. Zweitens: Es braucht klare Verantwortlichkeiten, Eskalationswege und ein Mindestniveau an Sicherheitsmaßnahmen.

Drittens: Die Leitung muss regelmäßige Reports zur Sicherheitslage erhalten. Viertens: Entscheidungen, Prioritäten und Kontrollhandlungen müssen dokumentiert werden, damit Sorgfalt im Zweifel auch belegbar ist. Genau in diese Richtung weisen sowohl die gesellschaftsrechtlichen Pflichten als auch die NIS2-Governance-Anforderungen.

Beachten Sie diese Führungsfragen für die Praxis, um den Reifegrad der eigenen Organisation sichtbar zu machen:

- Welche Cyberrisiken können unseren Geschäftsbetrieb ernsthaft gefährden?
- Wer verantwortet Prävention, Incident Response und Wiederanlauf – und wie oft berichtet diese Funktion an die Geschäftsleitung?
- Wie belastbar sind unsere Backups, Wiederanlaufpläne und Zugriffsmodelle wirklich – und wann wurde das zuletzt überprüft?



Wer diese Fragen nicht belastbar beantworten kann, hat in der Regel kein Technikproblem, sondern ein Führungs- und Organisationsproblem!

Handlungsempfehlung für Geschäftsführer und Vorstände

Der erste Schritt ist nicht der Kauf eines Tools, sondern die klare Führungsentscheidung, Cyberrisiken als Organpflicht zu behandeln. Dazu gehört, eine verantwortliche Funktion mit Mandat zu benennen, ein regelmäßiges Reporting an die Leitung einzuführen, die

wesentlichen Cyberrisiken zu dokumentieren und zentrale Mindestmaßnahmen verbindlich zu machen – insbesondere bei Identitäten, Zugriffen, Incident Response, Backup und Wiederherstellung. So wird aus „Die IT kümmert sich darum“ ein belastbares Governance-Modell.

Sie können Security-Aufgaben delegieren – aber niemals die Verantwortung. IT-Sicherheit ist heute Teil ordnungsgemäßer Unternehmensführung. Wer Cyberrisiken nicht aktiv steuert, überwacht und dokumentiert, riskiert nicht nur operative Schäden, sondern auch persönliche Haftungsfolgen.

Welche Pflichten Ihr Unternehmen wirklich treffen: NIS2, DSGVO, StaRUG und Kundenvorgaben

Vier Treiber, ein Ergebnis: Sie kommen an Cyber-Pflichten kaum noch vorbei. Viele Geschäftsführungen stellen noch immer die falsche Frage: „Fallen wir überhaupt unter NIS2?“ Die bessere Frage lautet: **Über welchen Kanal treffen uns IT- und Cyberpflichten konkret?** Denn für mittelständische Unternehmen gibt es heute gleich vier relevante Treiber: erstens die direkte Regulierung über NIS2, zweitens die Sicherheits- und Meldepflichten aus der DSGVO, drittens die Pflicht zur Krisenfrüherkennung nach dem StaRUG und viertens den wachsenden Druck aus Kundenbeziehungen und Lieferketten. In der Praxis bedeutet das: Selbst wenn ein Unternehmen nicht unmittelbar

NIS2-reguliert ist, greifen regelmäßig andere Pflichten oder marktseitige Anforderungen mit sehr ähnlicher Wirkung. Für die Geschäftsleitung ist das die entscheidende Erkenntnis: **Die Frage ist nicht mehr, ob Cybersicherheit für Ihr Unternehmen relevant ist, sondern über welchen Hebel sie verbindlich wird.** Bei vielen Mittelständlern wirken sogar mehrere Ebenen gleichzeitig. Ein Unternehmen kann etwa nicht direkt unter NIS2 fallen, aber dennoch personenbezogene Daten verarbeiten, unter StaRUG ein Frühwarnsystem benötigen und von Kunden Nachweise zu Informationssicherheit, Backup, Wiederanlauf und Incident Handling verlangen müssen.

Sind wir direkt von NIS2 betroffen?

NIS2 erfasst in Deutschland seit Inkrafttreten des Umsetzungsgesetzes „wichtige“ und „besonders wichtige“ Einrichtungen. Das BSI geht von rund **29.500 betroffenen Unternehmen** und Organisationen aus. Erfasst werden unter anderem Sektoren wie Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheit, digitale Infrastruktur sowie bestimmte digitale Dienste; ausdrücklich genannt werden in der digitalen Infrastruktur auch Cloud-Computing-Dienste, Rechenzentrumsdienste, Managed Service Provider und Managed Security Service Provider. Als Management-Faustregel gilt: Relevant wird NIS2 typischerweise ab mittlerer Unternehmensgröße, also grob ab etwa 50 Beschäftigten und einer Größenordnung von über 10 Mio. Euro Umsatz bzw. Bilanzsumme, sofern das Unternehmen in einen

erfassten Sektor fällt. Für große Unternehmen liegen die Schwellen deutlich höher; häufig wird hier mit etwa 250 Beschäftigten sowie über 50 Mio. Euro Umsatz und über 43 Mio. Euro Bilanzsumme gearbeitet. Die genaue Einordnung muss im Einzelfall sauber geprüft werden, aber für viele mittelständische IT-Dienstleister, Cloud- und MSP-nahe Unternehmen sowie bestimmte Industrie- und Produktionsbetriebe ist das Thema näher, als es auf den ersten Blick scheint. Genau deshalb ist es gefährlich, NIS2 vorschnell als „Thema für KRITIS und Konzerne“ abzutun. Die Richtlinie hat den Kreis der adressierten Unternehmen massiv erweitert. Wer in einem relevanten Sektor tätig ist und eine gewisse Größenordnung erreicht, sollte seine Betroffenheit nicht schätzen, sondern strukturiert prüfen.

Was die DSGVO ohnehin verlangt

Schutzmaßnahmen:

Geeignete technische und organisatorische Maßnahmen müssen umgesetzt werden, wobei das Schutzniveau stets dem konkreten Risiko angemessen sein muss.

Schutzziele:

Vertraulichkeit, Integrität, Verfügbarkeit & Belastbarkeit der Systeme müssen sichergestellt sein, damit personenbezogene Daten geschützt und verarbeitet werden können.

Wiederherstellung:

Unternehmen müssen in der Lage sein, personenbezogene Daten und den Zugang zu ihnen nach einem Vorfall schnell und geordnet wiederherzustellen.

Meldepflicht:

Datenschutzverletzungen müssen unverzüglich und binnen 72 Stunden gemeldet werden, weshalb klare Meldewege und saubere Dokumentation erforderlich sind.

StaRUG: Frühwarnsystem für bestandsgefährdende Risiken – auch bei IT-Ausfällen

Ein dritter, oft unterschätzter Treiber ist das **StaRUG. § 1 StaRUG** verpflichtet die Mitglieder der Geschäftsleitung haftungsbeschränkter Unternehmensträger, Entwicklungen zu überwachen, die den Fortbestand der juristischen Person gefährden können. Das Gesetz verankert damit ausdrücklich die Pflicht zur Krisenfrüherkennung und zum Krisenmanagement. Für die Praxis heißt das: Ein schwerer Cyberangriff, der Ausfall des ERP-Systems, ein kompromittiertes Identitätssystem oder eine länger andauernde Betriebsunterbrechung sind nicht nur technische Störungen. Sie können bestandsgefährdende Entwicklungen sein und gehören deshalb in das unternehmerische

Frühwarn- und Risikomanagement. **NIS2 und DSGVO** definieren vor allem, wie Sicherheitsmaßnahmen und Reaktionsfähigkeit ausgestaltet sein müssen; StaRUG verschärft die Perspektive, indem es verlangt, solche Risiken frühzeitig zu erkennen, zu bewerten und in das Krisenmanagement zu überführen. Damit wird IT-Risiko endgültig zum Management-Thema: Nicht erst der eingetretene Schaden ist relevant, sondern die Frage, ob bestandsgefährdende Entwicklungen früh genug sichtbar gemacht und adressiert wurden. Wer kritische IT-Abhängigkeiten nicht in seinem Frühwarnsystem abbildet, hat kein reines IT-Problem, sondern eine Lücke in der Unternehmenssteuerung.

Kundendruck und Lieferkette: Quasi-NIS2 über den Vertrag

Selbst Unternehmen unterhalb der NIS2-Schwellen geraten heute häufig über ihre Kunden in einen faktischen Pflichtenkorridor. NIS2 verlangt ausdrücklich Maßnahmen zur Sicherheit in der Lieferkette und bei Beziehungen zwischen Einrichtungen und ihren unmittelbaren Anbietern oder Dienstleistern. Das BSI führt Lieferkettensicherheit ausdrücklich als Teil der NIS2-Risikomanagementmaßnahmen und stellt zusätzlich Best-Practice-Empfehlungen für Sicherheitsanforderungen an Lieferanten bereit. Die praktische Folge ist absehbar: NIS2-regulierte Unternehmen reichen Sicherheitsanforderungen an IT-Dienstleister, Cloud- und SaaS-Anbieter sowie andere kritische Zulieferer weiter. Das zeigt sich bereits heute in Sicherheitsfragebögen, Statusberichten, vertraglichen Sicherheitsklauseln, Audit- und Nachweisrechten sowie Anforderungen an Meldeprozesse und

Wiederherstellungszeiten. Dass solche Lieferantenprüfungen und Statusberichte inzwischen gelebte Praxis sind, zeigen etwa einschlägige **ISO-27001-orientierte Lieferanten-Checklisten** und Vertragsanforderungen zu Audit-Rechten und Wiederherstellungs-SLAs.

Für den Mittelstand ist das strategisch wichtig: Auch wer formal nicht reguliert ist, kann geschäftlich unter Druck geraten, weil Kunden ein belastbares Sicherheitsniveau inzwischen nicht mehr als Bonus, sondern als Voraussetzung für Zusammenarbeit behandeln. In vielen Branchen wird Informationssicherheit damit vom Compliance-Thema zum Wettbewerbsfaktor. Diese Schlussfolgerung ergibt sich unmittelbar aus den NIS2-Lieferkettenpflichten und den inzwischen üblichen Nachweis- und Auditmechanismen in Kunden-Lieferanten-Beziehungen.

Bedeutung für die Geschäftsleitung

Für Geschäftsführung und Vorstand folgt daraus eine einfache, aber wichtige Management-Logik: Sie sollten Ihr Unternehmen nicht nur auf direkte NIS2-Betroffenheit prüfen, sondern auf vier Ebenen gleichzeitig – Regulierung, Datenschutz, Krisenfrüherkennung und Kundenanforderungen. Erst diese Gesamtsicht zeigt, welche Pflichten und Erwartungen tatsächlich auf das Unternehmen wirken. Ein sinnvoller erster Schritt ist eine kurze C-Level-Bestandsaufnahme: Fallen wir potenziell in einen NIS2-Sektor? Welche personenbezogenen Daten und geschäftskritischen Systeme wären bei einem Vorfall betroffen? Welche IT-Ausfälle wären für unseren Geschäftsbetrieb bestandsgefährdend? Und welche

Sicherheitsnachweise erwarten Kunden oder Auftraggeber bereits heute von uns? Wer diese vier Fragen sauber beantwortet, schafft die Grundlage für alle Folgekapitel – vom Risikoregister über Identitäten und Backups bis hin zu Incident Response und Wiederanlauf. **Die entscheidende Frage lautet nicht, ob IT-Pflichten Ihr Unternehmen treffen, sondern über welchen Kanal.** Für die meisten mittelständischen Unternehmen wirken heute mindestens DSGVO und StaRUG; je nach Branche, Größe und Marktposition kommen NIS2 und vertragliche Lieferkettenanforderungen hinzu. Genau deshalb ist Cybersicherheit inzwischen keine Spezialdisziplin mehr, sondern ein Bestandteil belastbarer Unternehmensführung.

Welche Ausfälle für Ihr Unternehmen wirklich bestandsgefährdend sind

Viele Unternehmen haben zwar zahlreiche Sicherheitsmaßnahmen im Einsatz, aber keine belastbare Antwort auf eine einfache Management-Frage: Welche IT- und Cyberrisiken gefährden unseren Geschäftsbetrieb tatsächlich – und ab wann wird es kritisch? Genau hier setzt ein IT-Risikoregister an. Es übersetzt technische Risiken in unternehmerische Relevanz und macht sichtbar, welche Systeme, Prozesse und Abhängigkeiten für Umsatz, Lieferfähigkeit, Liquidität und Krisenfestigkeit wirklich kritisch sind. Das ist keine Kür, sondern zunehmend Teil dessen, was Regulatorik und gute Unternehmensführung erwarten. Nach **§ 30 BSIG** müssen betroffene Unternehmen Konzepte zur Risikoanalyse umsetzen; zu den gesetzlich genannten Risikomanagementmaßnahmen gehören außerdem ausdrücklich die Aufrechterhaltung des Betriebs, Backup-Management,

Wiederherstellung nach einem Notfall und Krisenmanagement. Auch das BSI beschreibt die NIS2-Risikoanalyse als systematische Bewertung von Risiken und geeigneten Gegenmaßnahmen. Ein gutes IT-Risikoregister ist deshalb kein Excel-Friedhof und keine technische Nebenliste der IT-Abteilung. Es ist ein Steuerungsinstrument für die Geschäftsleitung. Sein Zweck ist nicht, möglichst viele Gefährdungen aufzuschreiben, sondern Prioritäten zu schaffen: Welche Risiken sind für unser Unternehmen relevant, wie hoch ist ihr potenzieller Schaden, welche Gegenmaßnahmen existieren bereits – und wo besteht akuter Handlungsbedarf? Der **BSI-Standard 200-3** bündelt genau diese risikobezogenen Arbeitsschritte im IT-Grundschutz und stellt damit ein anerkanntes Vorgehen für die systematische Risikoanalyse bereit.

Was in ein gutes IT-Risikoregister gehört

Methodisch beginnt ein belastbares Risikoregister nicht bei Einzellücken, sondern bei den geschäftskritischen Prozessen und den davon abhängigen Anwendungen, IT-Systemen und Infrastrukturen. Genau diese Logik beschreibt der **BSI-Standard 200-3**: erst die relevanten Geschäftsprozesse und Objekte identifizieren, dann Schutzbedarf bestimmen und darauf aufbauend eine Risikoanalyse durchführen. In der NIS2-Logik kommt noch hinzu, dass Risiken nicht nur identifiziert, sondern auch bewertet, behandelt und regelmäßig überprüft werden müssen. In der Praxis heißt das: Für jedes wesentliche Risiko sollte klar erkennbar sein, welcher Prozess oder welches System betroffen

ist, wodurch das Risiko ausgelöst werden kann, welche Auswirkungen zu erwarten sind, wie hoch die Priorität ist, wer verantwortlich ist und welche Maßnahmen beschlossen wurden. Ob das später in einer spezialisierten GRC-Lösung, in einem ISMS-Tool oder zunächst in einer sauberen Tabellenstruktur dokumentiert wird, ist zweitrangig.

Entscheidend ist, dass daraus belastbare Management-Entscheidungen entstehen – etwa über Investitionen, Prioritäten, Notfallvorsorge oder externe Unterstützung. Diese Struktur folgt unmittelbar aus der BSI-Logik von Risikoidentifikation, -bewertung und -behandlung.

Die entscheidende Management-Frage: Welche Ausfälle wären bestandsgefährdend?

Für die Geschäftsleitung wird es erst dann wirklich relevant, wenn klar ist, welche Ausfälle für das Unternehmen bestandsgefährdend werden können. Genau hier kommt die Business-Impact-Analyse ins Spiel. Der **BSI-Standard 200-4** beschreibt die Business-Impact-Analyse als Untersuchung dessen, was innerhalb des betrachteten Bereichs überhaupt abgesichert werden soll. Sie dient dazu, kritische Prozesse und Ressourcen sichtbar zu machen und die geforderten Wiederanlaufzeiten und Datenanforderungen festzulegen. Für das Management sind dabei vier Kennzahlen besonders hilfreich. Die MTPD beschreibt die maximal tolerierbare Ausfallzeit eines Prozesses, also den Zeitraum, ab dem gravierende Schäden eintreten. Die RTO beschreibt den Zeitraum vom Ausrufen des Notfalls bis zum Zeitpunkt der Wiederaufnahme eines Prozesses oder Systems. Die RPO definiert, wie aktuell die Daten nach einer Wiederherstellung

mindestens sein müssen. Und das MBCO legt fest, welches Mindestleistungsniveau der Notbetrieb erreichen muss, damit der Geschäftsbetrieb überhaupt sinnvoll fortgeführt werden kann. Diese Begriffe stammen aus dem BSI-Standard 200-4 und seinem Glossar und sind deshalb hervorragend geeignet, technische Diskussionen in Management-Sprache zu übersetzen. Managementtauglich formuliert lautet die Kernfrage also nicht: „Kann ein System ausfallen?“ Das kann grundsätzlich jedes System. Die entscheidende Frage lautet: Welcher Ausfall überschreitet unsere maximal tolerierbare Ausfallzeit – und bedroht damit Umsatz, Vertragsfähigkeit, operative Stabilität oder regulatorische Pflichten? Bestandsgefährdend ist nicht jeder IT-Störfall, sondern der Ausfall eines Kronjuwelen-Prozesses über die definierte Toleranz hinaus. Genau das muss ein gutes Zusammenspiel aus Risikoregister und Business-Impact-Analyse sichtbar machen.

Drei typische Beispiele aus dem Mittelstand

ERP-System: Fällt das ERP-System länger aus, betrifft das direkt Auftragsannahme, Einkauf, Faktura und Disposition. Aus einer technischen Störung wird schnell ein Geschäftsrisiko für Umsatz, Cashflow und Lieferfähigkeit. Deshalb sollte das Risiko im IT-Risikoregister mit MTPD, RTO und RPO hinterlegt werden, damit sichtbar wird, ob Backup und Wiederherstellung zur geschäftlichen Realität passen.

Identitäts- und Zugriffsmanagement: Wird ein zentrales Identitätssystem kompromittiert oder falsch konfiguriert, betrifft das oft gleichzeitig E-Mail, ERP, Cloud-Dienste und Admin-Zugänge. Aus einem technischen Fehler wird schnell ein organisationsweites Betriebsproblem. Deshalb sollte dieses Risiko im IT-Risikoregister klar priorisiert werden, um Zugriffsschutz und MFA zu stärken.

Produktionsnahe IT & OT: Kommt es zu Störungen in produktionsnaher IT, Maschinenanbindung oder logistischen Schnittstellen, sind oft Fertigung, Versand und Serviceprozesse betroffen. Aus einem technischen Ausfall wird schnell ein Risiko für Wertschöpfung, Lieferfähigkeit und Kundenzufriedenheit. Deshalb sollten diese kritischen Systeme im Risikoregister priorisiert werden.

Wo das Frühwarnsystem beginnt

Damit ein Risikoregister nicht nur dokumentiert, sondern steuert, braucht es ein Frühwarnsystem. Genau hier schlägt das StaRUG die Brücke zur Geschäftsleitung. **§ 1 StaRUG** verpflichtet die Mitglieder der Geschäftsleitung haftungsbeschränkter Unternehmensträger, Entwicklungen zu überwachen, die den Fortbestand der juristischen Person gefährden können. Werden solche Entwicklungen erkannt, müssen geeignete Gegenmaßnahmen ergriffen und gegebenenfalls die zuständigen Überwachungsorgane informiert werden. Das Gesetz ist damit kein reines Finanzmarkt- oder Restrukturierungsthema, sondern ein klarer Auftrag zur Krisenfrüherkennung. Für IT- und Cyber Risiken bedeutet das: Es genügt nicht, einmal im Jahr Risiken zu bewerten.

Die Geschäftsleitung braucht Indikatoren, an denen sich kritische Entwicklungen früh erkennen lassen. Typische Signale sind etwa wiederholte Störungen kritischer Systeme, Restore-Tests, die die geforderte RTO nicht erreichen, ansteigende Bestände offener kritischer Schwachstellen, auffällige Sicherheitsvorfälle oder eine zunehmende Abhängigkeit von einzelnen Providern, Personen oder Monolith-Systemen. Solche Abweichungen müssen in einem Management-Report sichtbar werden, bevor aus ihnen eine echte Krise wird. Diese Logik entspricht der Verbindung aus BSI-Risikomanagement und StaRUG-Früherkennung: Risiken systematisch erfassen, ihre Entwicklung beobachten und rechtzeitig gegensteuern.

Start für Mittelständler & Handlungsempfehlung für Geschäftsführer und Vorstände

Für mittelständische Unternehmen ist es meist nicht sinnvoll, sofort das gesamte Unternehmen in maximaler Detailtiefe zu analysieren. Pragmatischer ist ein Top-down-Ansatz: zuerst die zehn wichtigsten Geschäftsprozesse identifizieren, dann die dazugehörigen Anwendungen, IT-Services, Datenbestände und Abhängigkeiten ableiten und nur für diese Kronjuwelen eine saubere Business-Impact-Analyse und Risikobewertung aufbauen. Der **BSI-Standard 200-4** ist ausdrücklich für Institutionen beliebiger Art, Branche und Größe gedacht und bietet ein Stufenmodell für den Einstieg in BCM. Aus Managementsicht reicht für den Start oft schon eine sehr konkrete Fragelogik: Welche drei bis zehn Prozesse dürfen praktisch nicht ausfallen? Welche Systeme tragen diese Prozesse? Wie lange dürfen sie maximal gestört sein? Wie viel Datenverlust wäre tolerierbar? Und welche Gegenmaßnahmen

schließen die Lücke zwischen heutiger Realität und benötigter Resilienz? Genau aus dieser Logik ergeben sich später die richtigen Prioritäten für Backup, Wiederherstellung, Notfallvorsorge und Incident Response.

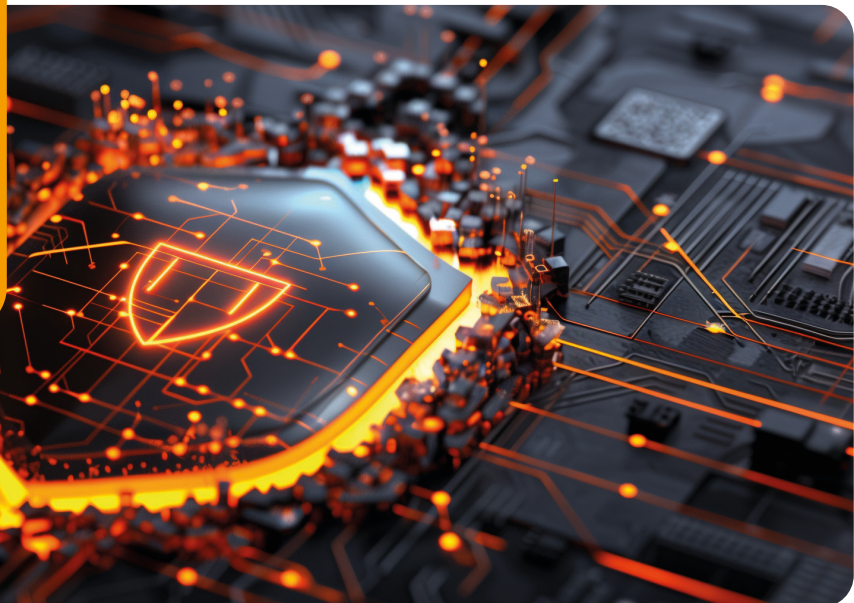
Der wichtigste erste Schritt ist nicht, sofort ein großes Governance-Projekt zu starten, sondern die geschäftskritischen Kronjuwelen sichtbar zu machen. Lassen Sie für die wichtigsten Prozesse Ihres Unternehmens ein kompaktes IT-Risikoregister mit klaren Verantwortlichkeiten aufbauen und hinterlegen Sie für diese Prozesse belastbare Zielgrößen wie MTPD, RTO und RPO. Ergänzen Sie das Ganze um wenige, aber aussagekräftige Frühwarnindikatoren, die regelmäßig im Management-Reporting auftauchen. So wird aus abstrakter Cybergefahr ein steuerbares Führungs- und Resilienzthema.

Identitäten & Zugriffe: Der schnellste Weg ins Unternehmen führt über Accounts

Viele Geschäftsführer und Vorstände denken bei Cyberangriffen noch immer zuerst an technische Angriffe auf Firewalls, Server oder Schwachstellen. Diese Gefahr ist real – aber in der Praxis führt der schnellste Weg ins Unternehmen heute oft über bereits vorhandene Konten. Laut dem Verizon 2025 Data Breach Investigations Report war **Credential Abuse mit 22 %** der häufigste Initialzugriffsvektor bei untersuchten Sicherheitsverletzungen; direkt dahinter folgte die **Ausnutzung von Schwachstellen mit 20 %**. Gleichzeitig betont Verizon, dass der menschliche Faktor in vielen Vorfällen weiterhin eine zentrale Rolle spielt und sich stark mit Social Engineering und missbrauchten Zugangsdaten überschneidet. Für die Unternehmensleitung ist das

eine zentrale Botschaft: Angreifer müssen heute nicht zwingend „durch die Firewall brechen“. Oft reicht es, sich mit einem kompromittierten oder überprivilegierten Konto als scheinbar legitimer Nutzer anzumelden. Ab diesem Moment agiert der Angreifer nicht mehr sichtbar „von außen“, sondern innerhalb der Vertrauenszone des Unternehmens – mit Zugriff auf E-Mail, Cloud-Dienste, ERP, Kollaborationsplattformen oder sogar administrative Funktionen. Genau deshalb sind Identitäten und Zugriffe heute einer der wirksamsten Hebel zwischen Prävention, Resilienz und Haftungsrisiko. Auch das BSI ordnet Personalsicherheit, Zugriffskontrolle und Asset-Management als zentrale Grundlagen der Informationssicherheit ein.

Der schnellste Weg ins Unternehmen führt oft nicht über eine technische Schwachstelle, sondern über ein kompromittiertes, schlecht geschütztes oder überprivilegiertes Konto.



Was NIS2 bei Identitäten und Zugriffen erwartet

NIS2 behandelt Identitäts- und Zugriffsschutz nicht als optionale Best Practice, sondern als Kernbestandteil des Cyber-Risikomanagements. Bereits **Artikel 21 Absatz 2** der Richtlinie nennt ausdrücklich Konzepte für die Zugriffskontrolle sowie die Verwendung von Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierungslösungen als relevante Risikomanagementmaßnahmen. Das BSI übersetzt diese Erwartung sehr greifbar: Ein einzelner Faktor wie ein Passwort ist nicht sicher genug; mehrere Faktoren sollen verhindern, dass manipulierte oder abgefangene Zugangsdaten allein für einen unbefugten Zugriff ausreichen. Besonders deutlich wird die Stoßrichtung in der **EU-Durchführungsverordnung 2024/2690**, die die technischen und

methodischen Maßnahmen für bestimmte NIS2-Sektoren konkretisiert. Dort werden unter anderem eindeutige Identitäten für Systeme und Nutzer, die Zuordnung eines Kontos zu einer einzelnen Person, sichere Authentifizierungsverfahren, das Blockieren von Nutzern nach einer festgelegten Zahl erfolgloser Anmeldeversuche, die regelmäßige Überprüfung privilegierter und administrativer Zugriffsrechte, das Prinzip Need-to-know, Least Privilege und die Trennung von Aufgaben ausdrücklich genannt. Gemeinsame Kennungen sollen nur ausnahmsweise zulässig sein und dann einem ausdrücklichen Freigabe- und Dokumentationsprozess unterliegen. Sie zeigt klar, welcher Reifegrad heute regulatorisch erwartet wird.

Vier Hebel für sicheres Identitäts- und Zugriffsmanagement

1) MFA und Passworthygiene – der schnellste Gewinn: Für viele Unternehmen ist MFA noch immer die einfachste und zugleich wirksamste Maßnahme, um identitätsbasierte Angriffe deutlich zu erschweren. Das gilt besonders für extern erreichbare Dienste wie E-Mail, VPN, Cloud-Portale, Remote-Zugänge und für alle administrativen Konten. Das BSI formuliert im Bereich Zwei-Faktor-Authentisierung

sehr eindeutig, dass der Login mit Passwort plus weiterem Faktor erfolgen sollte; in den NIS2-Unterlagen des BSI wird MFA zudem ausdrücklich als wesentliche Maßnahme hervorgehoben. Managementseitig ist das deshalb ein klassischer „Low Hanging Fruit“: Eine konsequente MFA-Pflicht reduziert nicht jedes Risiko, senkt aber die Eintrittswahrscheinlichkeit vieler Standardangriffe spürbar.

2) Admin-Konten & privilegierte Zugriffe streng behandeln: Noch kritischer als normale Nutzerkonten sind privilegierte Konten. Fällt ein Global Admin, Domain Admin oder anderes hoch privilegiertes Konto, reicht oft ein einziger erfolgreicher Zugriff, um große Teile der IT-Landschaft zu kontrollieren. Genau deshalb fordert die EU-Konkretisierung zu NIS2 die regelmäßige Überprüfung privilegierter und administrativer Konten. Auch der BSI-Grundsatz betont seit Jahren die sichere Verwaltung von Benutzern und Rechten; zudem

empfiehlt das BSI ausdrücklich, für einzelne Nutzer getrennte Konten mit unterschiedlichen Rechten zu verwenden. Im Active-Directory-Kontext hebt der BSI-Grundsatz zusätzlich hervor, dass alltägliche Arbeiten nicht mit hoch privilegierten Standard-Administratorkonten erfolgen sollten. Für Geschäftsführer und Vorstände ist die Konsequenz klar: Admin-Rechte gehören auf ein Minimum reduziert, sauber getrennt, stark abgesichert und eng überwacht.

3) Joiner-Mover-Leaver sauber regeln, sonst bleiben Risiken: Ein besonders unterschätztes Risiko liegt nicht in spektakulären Angriffen, sondern in unsauber verwalteten Konten und Berechtigungen. Wenn neue Mitarbeitende zu viele Rechte erhalten, Rollenwechsel nicht sauber nachgeführt werden oder Zugänge nach dem Austritt bestehen bleiben, entsteht ein klassisches Organisationsproblem mit direkter Sicherheitswirkung. Genau hier hilft der Joiner-Mover-Leaver-Ansatz: Beim Eintritt werden Rechte kontrolliert vergeben, beim Rollenwechsel

angepasst und beim Austritt konsequent entzogen. Die einschlägigen BSI-Anforderungen nennen ausdrücklich die regelmäßige Überprüfung vergebener Berechtigungen sowie den Berechtigungsentzug bei Veränderungen des Arbeitsverhältnisses; im BSI-Grundsatz wird außerdem gefordert, nicht benötigte Benutzerkennungen geeignet zu deaktivieren oder zu löschen. In der EU-Konkretisierung zu NIS2 spiegelt sich dieselbe Logik in der Forderung wider, Zugriffsrechte bereitzustellen, zu ändern, zu entfernen und zu dokumentieren.

4) Rechte-Reviews & Least Privilege machen Zugriff steuerbar: Viele Mittelständler leben mit gewachsenen Berechtigungsstrukturen, die im Alltag „irgendwie funktionieren“, aber kaum noch prüfbar sind. Genau hier entsteht aus operativer Bequemlichkeit ein Governance-Risiko. Die regulatorische Erwartung ist heute klar: Zugriffsrechte sollen nicht nur vergeben, sondern regelmäßig überprüft, angepasst und bei Bedarf entzogen werden. Die EU-Konkretisierung zu NIS2 nennt dafür

die Prinzipien Need-to-know, Least Privilege und Separation of Duties; BSI-nahe Anforderungskataloge greifen ergänzend die regelmäßige Überprüfung vergebener Berechtigungen auf. Für die Praxis bedeutet das nicht, jeden einzelnen Ordner manuell zu auditieren. Es bedeutet vielmehr, Rollenmodelle und Verantwortlichkeiten so aufzubauen, dass Berechtigungen nachvollziehbar, plausibel und periodisch rezertifizierbar werden. Aus Rechte-Chaos wird ein steuerbares Zugriffs-konzept.

Bedeutung für Geschäftsführer und Vorstände

Identitätsschutz ist kein Technikdetail, sondern eine Führungsaufgabe. Wer Identitäten und Zugriffe sauber steuert, senkt Angriffsrisiken, begrenzt Schäden und reduziert Haftungsrisiken. Auf Leitungsebene sollten daher MFA, privilegierte Konten, Rechte-Reviews und

der Entzug von Zugängen regelmäßig im Blick sein. Ein pragmatischer Einstieg sind MFA, die Trennung von Standard- und Admin-Konten, saubere Joiner-Mover-Leaver-Prozesse sowie regelmäßige Rechte-Reviews auf Basis eines klaren Rollenmodells.

Backup ist nicht gleich Wiederherstellung: Warum Standard- Retention oft nicht reicht

Viele Unternehmen wiegen sich beim Thema Datensicherung in Sicherheit, weil irgendwo im Stack bereits ein Backup existiert – beim Rechenzentrum, in der Cloud-Plattform oder direkt beim SaaS-Anbieter. Für die Geschäftsleitung ist genau das der kritische Denkfehler. Denn aus Sicht von Regulierung und Krisenfestigkeit reicht es nicht, dass technisch irgendeine Sicherung erstellt wird. Entscheidend ist, ob sich geschäftskritische Daten, Konfigurationen und Systeme innerhalb der geforderten Zeit und in der erforderlichen Datenqualität tatsächlich wiederherstellen lassen. Genau an dieser Stelle trennt sich Backup von echter Wiederherstellungsfähigkeit. NIS2 nennt ausdrücklich die Aufrechterhaltung des Betriebs, Backup-Management, Wiederherstellung nach einem Notfall und Krisenmanagement als Mindestbestandteile des Cyber-Risikomanagements; das BSI führt

diese Punkte in seinen NIS2-Infopaketen entsprechend als zentrale Pflichtbereiche auf. Für Geschäftsführer und Vorstände ist das eine wichtige Perspektivverschiebung: Die relevante Frage lautet nicht „Werden Sicherungen erstellt?“, sondern „Können wir nach einem Vorfall kontrolliert und rechtzeitig wieder arbeitsfähig werden?“ Das ist eine Führungsfrage, weil sie unmittelbar an Geschäftsfortführung, Lieferfähigkeit, Meldepflichten und Haftungsrisiken anknüpft. Ein Backup, das im Ernstfall nicht rechtzeitig, nicht vollständig oder nicht im benötigten Wiederherstellungspunkt nutzbar ist, erfüllt seinen Zweck nur sehr eingeschränkt. Der **BSI-Standard 200-4** ordnet genau deshalb Wiederanlauf, Wiederherstellung und BC-Strategien in ein systematisches Business-Continuity-Management ein, statt Backups isoliert als reine IT-Maßnahme zu behandeln.

Was NIS2 & DSGVO tatsächlich verlangen

NIS2 verlangt nicht bloß eine technische Datensicherung, sondern ein dokumentiertes und wirksames Backup- und Wiederherstellungsmanagement als Teil der Betriebskontinuität. **Artikel 21 der Richtlinie** nennt ausdrücklich „*business continuity, such as backup management and disaster recovery, and crisis management*“. Das BSI konkretisiert diese Stoßrichtung für NIS2-regulierte Unternehmen in seinen Leitfäden ebenfalls klar: Backup-Management und Wiederherstellung nach einem Notfall sind kein Anhängsel, sondern Bestandteil der geforderten Resilienz. Auch ohne NIS2 ist die Rechtslage deutlich. Artikel 32 DSGVO verlangt unter anderem die Fähigkeit, die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Zusätzlich

fordert dieselbe Norm ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen. Das bedeutet in der Praxis: Ein theoretisch vorhandenes Backup ohne belastbaren Restore-Prozess und ohne regelmäßige Tests liegt deutlich unter dem, was der Gesetzgeber unter angemessener Wiederherstellungsfähigkeit versteht. Damit wird die Abgrenzung sehr klar: NIS2 und DSGVO verlangen mehr als „*irgendwo gibt es schon Sicherungen*“. Gefordert ist eine Kombination aus Sicherheitsstrategie, Wiederherstellungsfähigkeit, klaren Zielzeiten, organisatorischer Einbettung und überprüfbarer Wirksamkeit. Genau deshalb ist Backup heute kein rein technisches Betriebsdetail mehr, sondern ein Bestandteil ordnungsgemäßer Governance.

RTO, RPO & Retention: Warum Standardvorgaben oft an Realität vorbeigehen

Ob ein Backup-Konzept ausreicht, lässt sich nicht aus der Standardkonfiguration eines Herstellers ableiten, sondern nur aus den Anforderungen des eigenen Geschäfts. Der **BSI-Standard 200-4** arbeitet deshalb mit klaren Zielgrößen: RTO beschreibt die geforderte Wiederanlaufzeit, also wie schnell ein Prozess oder System nach einem Notfall wieder verfügbar sein muss; RPO beschreibt die geforderte Aktualität der Datenwiederherstellung, also wie viel Datenverlust maximal tolerierbar ist. Der BSI-Standard macht zudem deutlich, dass RTO und RPO gewünschte Soll-Werte darstellen und in der Business-Impact-Analyse für zeitkritische Ressourcen hinterlegt werden. Für das

Management folgt daraus eine einfache Logik: Wenn Ihre geschäftlich definierte Wiederanlaufzeit oder Ihr akzeptabler Datenverlust nicht zu den tatsächlichen Sicherungs- und Wiederherstellungsmöglichkeiten passen, besteht ein reales Organisationsrisiko. Ein Anbieter-Standard kann technisch bequem sein und trotzdem geschäftlich unzureichend. Das gilt besonders in SaaS-Umgebungen, in denen Unternehmen oft annehmen, der Provider werde schon „alles Notwendige“ absichern. Die eigentliche Frage lautet aber: Unterstützen Frequenz, Wiederherstellungspunkt, Aufbewahrungszeit und Testbarkeit der Sicherungen die Anforderungen aus Ihrer Business-Impact-Analyse?

Das SaaS-Missverständnis: Backup des Anbieters ist nicht automatisch Ihr Recovery-Konzept

Gerade bei Cloud- und SaaS-Anwendungen zeigt sich besonders deutlich, warum Standard-Backups häufig nicht mit einem unternehmens-eigenen Recovery-Konzept gleichgesetzt werden dürfen. Anbieter sichern in erster Linie die Stabilität und Wiederherstellbarkeit ihrer Plattform im eigenen Betriebsmodell. Daraus folgt aber nicht automatisch, dass diese Sicherungen auch zu den fachlichen, zeitlichen und organisatorischen Anforderungen Ihres Unternehmens passen. Das ist keine Schwäche des Anbieters, sondern eine Frage des Verantwortungszuschnitts: Die Plattform stellt eine Standardfunktion bereit; ob diese Standardfunktion für Ihre Geschäftsprozesse, Ihr Risikoprofil und Ihre Melde- bzw. Wiederanlaufpflichten genügt,

bleibt Ihre Managemententscheidung. Diese Schlussfolgerung ergibt sich aus dem Zusammenspiel von NIS2-Resilienzanforderungen, DSGVO-Wiederherstellungsgebot und den BCM-Zielgrößen des BSI. Hinzu kommt ein weiterer Punkt, der in vielen Unternehmen zu spät erkannt wird: Für die Wiederaufnahme des Betriebs reicht es häufig nicht, nur Geschäftsdaten wiederherzustellen. Oft sind auch Konfigurationen, Rollen, Berechtigungen, Integrationen, Applikationsstände und betriebliche Abhängigkeiten entscheidend dafür, ob der Prozess wirklich wieder lauffähig ist. Der **BSI-Standard 200-4** denkt Wiederherstellung deshalb konsequent aus der Sicht der Geschäftsführung und nicht nur aus Sicht einzelner Datensätze.

Beispiel Business Central: Warum 28 Tage zum Management-Risiko werden können

Besonders greifbar wird das am Beispiel Microsoft Business Central. Microsoft dokumentiert, dass sich eine Business-Central-Umgebung im Admin Center nur auf einen Zeitpunkt innerhalb der vergangenen 28 Tage zurücksetzen lässt; weiter zurück reicht die Restore-Möglichkeit nicht. Für Power-Plattform- und Dynamics-365-Produktionsumgebungen dokumentiert Microsoft ebenfalls eine Aufbewahrung automatischer System-Backups von bis zu 28 Tagen. Für die Geschäftsleitung ist das keine technische Randnotiz, sondern ein Steuerungsthema. Denn aus der 28-Tage-Grenze folgt: Wird ein Fehler, eine Manipulation oder ein schleichender Datenverlust erst später entdeckt, endet die vom Hersteller bereitgestellte Standard-Restore-Option trotzdem nach diesem Zeitraum. Ob 28 Tage ausreichen, hängt also nicht vom Produktstandard ab, sondern von Ihrem Geschäftsmodell, Ihrer Prüf- und Entdeckungszeit und den Anforderungen an Wiederherstellbarkeit. Für viele

mittelständische Unternehmen ist genau das der Punkt, an dem aus einem vermeintlich „vorhandenen Backup“ ein reales Resilienzrisiko wird. Diese Einordnung ist eine naheliegende Schlussfolgerung aus den Microsoft-Restore-Grenzen einerseits und den regulatorischen Anforderungen an zeitgerechte, wirksame Wiederherstellung andererseits. Wichtig ist dabei auch die begriffliche Klarheit: Backup ist nicht Archivierung. Eine 28-Tage-Restore-Funktion kann für operative Wiederherstellungsszenarien hilfreich sein, ersetzt aber nicht automatisch längere Anforderungen an Nachvollziehbarkeit, Prüfung, historische Rekonstruktion oder späte Fehlerentdeckung. Gerade deshalb muss die Geschäftsleitung bewusst entscheiden, wo Standardfunktionen genügen und wo zusätzliche Backup- oder Exportstrategien notwendig sind. Diese Differenzierung ergibt sich aus der unterschiedlichen Zielsetzung von BCM, Wiederherstellung und langfristiger Nachweis- bzw. Datenverfügbarkeit.

Restore statt nur Backup

In vielen mittelständischen Unternehmen ist nicht die Sicherung selbst das größte Problem, sondern die fehlende Validierung der Wiederherstellung. Ein Backup, das nie realistisch getestet wurde, ist eher Annahme als belastbarer Nachweis. Genau hier entstehen typische

Lücken: fehlende Zuordnung zu RTO und RPO, kein geübter Wiederanlaufplan, unklare Retention und fehlende Verantwortung – besonders bei Cloud- und SaaS-Systemen. Aus Managementsicht ist das kein Technik-, sondern ein Organisationsproblem.

Was die Geschäftsleitung jetzt tun sollte

Backup, Wiederherstellung und Retention sollten konsequent an den Anforderungen geschäftskritischer Systeme ausgerichtet werden. Entscheidend sind klare Zielwerte für Wiederanlaufzeit, tolerierbaren Datenverlust, Aufbewahrungsdauer und regelmäßig getestete

Restore-Prozesse. Erst dann lässt sich seriös beurteilen, ob Standardfunktionen des Herstellers ausreichen oder zusätzliche Backup-Services nötig sind. Besonders Cloud- und SaaS-Systeme verdienen dabei besondere Aufmerksamkeit.

Wie handlungsfähig ist das Unternehmen im Ernstfall?

Nicht jeder Sicherheitsvorfall lässt sich verhindern. Aber ob ein Unternehmen im Ernstfall strukturiert reagiert, Entscheidungen bündelt, Meldefristen einhält und den Betrieb kontrolliert wieder hochfährt, ist keine Frage des Zufalls – sondern eine Management-Entscheidung. Genau deshalb verlangen **NIS2** und die darauf aufbauenden **BSI-Leitlinien** nicht nur Prävention, sondern ausdrücklich auch Incident Handling, Business Continuity, Backup-Management, Wiederherstellung nach einem Notfall und Krisenmanagement als Bestandteile eines angemessenen Cyber-Risikomanagements. Für Geschäftsführer und Vorstände ist das die eigentliche Kernbotschaft dieses Kapitels: Ein Backup in der Konsole ist noch kein Wiederanlauf. Entscheidend ist, ob das Unternehmen unter realen Bedingungen handlungsfähig bleibt – mit klaren Rollen, belastbaren Notfallplänen, erreichbaren Ansprechpartnern, geübten Abläufen und einem funktionierenden Zusammenspiel zwischen IT, Fachbereichen, Kommunikation, Datenschutz und Leitungsebene. Der BSI-Standard 200-4 beschreibt BCM deshalb als methodischen Rahmen, mit dem ein Business Continuity Management System in einer Institution initiiert und gesteuert wird; die BSI-NIS2-Unterlagen verknüpfen diesen Rahmen ausdrücklich mit der Pflicht, ein Notfallmanagement zu etablieren.

Der BSI-Ansatz ist dabei bewusst ganzheitlich. Er denkt Notfallmanagement nicht als losen Ordner mit Checklisten, sondern als strukturierten Prozess: Risiken und geschäftskritische Abläufe werden analysiert, daraus werden Strategien und Wiederanlaufpläne abgeleitet, eine besondere Aufbauorganisation für den Ernstfall eingerichtet und die Wirksamkeit anschließend durch Tests und Übungen überprüft. Dass der **BCM-Prozess im BSI-Standard 200-4 entlang des PDCA-Zyklus** aufgebaut ist, unterstreicht genau diese Logik: planen, umsetzen, überprüfen und verbessern – nicht einmal dokumentieren und dann vergessen. Besonders wichtig ist dabei die Notfall- bzw. Krisenorganisation.

Der BSI-Standard 200-4 behandelt ausdrücklich den Aufbau einer **Besonderen Aufbauorganisation (BAO)** und verweist auf die organisatorische Abgrenzung zwischen Notfallstab und Krisenstab. Ergänzend beschreibt das BSI das Notfallhandbuch als Sammlung der Dokumente, die eine angemessene Reaktion auf Krisen und Notfälle unterstützen sollen. Für die Geschäftsleitung heißt das: Im Ernstfall darf nicht erst improvisiert werden, wer entscheidet, wer kommuniziert, wer technische Eindämmung steuert, wer externe Meldungen vorbereitet und wer gegenüber Kunden, Partnern oder Medien spricht. Diese Rollen müssen vorher festgelegt, vertreten und eingeübt sein.

Genau hier trennt sich Incident Response von hektischer Ad-hoc-Reaktion. Ein wirksamer Ablauf reicht von der Erkennung und Einordnung über Eindämmung und Priorisierung bis zur dokumentierten Wiederherstellung und zu Lessons Learned. Der entscheidende Unterschied zwischen Papier-Resilienz und echter Betriebsfähigkeit liegt im geübten Wiederanlauf: Nicht das dokumentierte Backup zählt, sondern der nachweislich funktionierende Restore.

Hinzu kommen klare Meldepflichten. Für NIS2-Vorfälle nennt das BSI eine Erstmeldung binnen 24 Stunden, eine weitere **Meldung binnen 72 Stunden und einen Abschlussbericht nach 30 Tagen**. Parallel verlangt die DSGVO bei meldepflichtigen Datenschutzverletzungen grundsätzlich eine Meldung binnen 72 Stunden. Ohne klare Incident-Response-Struktur drohen daher nicht nur längere Ausfälle, sondern auch Fristversäumnisse und zusätzliche rechtliche Risiken. Für die Geschäftsleitung ergeben sich daraus drei Kernfragen: Wer sitzt im Krisenstab? Welche Systeme und Prozesse müssen in welcher Reihenfolge wieder anlaufen? Und wann wurde dieser Ablauf zuletzt realistisch geübt? Wenn darauf keine belastbaren Antworten vorliegen, fehlt meist kein Tool, sondern ein wirksames Notfallmanagement.

Nicht das Backup auf dem Papier zählt, sondern der geübte Wiederanlauf unter realen Bedingungen. NIS2, BSI-Standard 200-4 und DSGVO verlangen nicht nur Schutzmaßnahmen, sondern belastbare Handlungsfähigkeit.



Cloud-, SaaS- und Dienstleisterrisiken steuern: Shared Responsibility endet nicht beim Provider

Cloud-Dienste, SaaS-Plattformen und externe IT-Dienstleister entlasten den operativen Betrieb. Sie entlasten aber nicht die Geschäftsleitung von ihrer Verantwortung für Sicherheit, Verfügbarkeit und Steuerbarkeit. Genau das beschreibt das **Shared-Responsibility-Modell** sehr klar: Je nach Modell – IaaS, PaaS oder SaaS – übernimmt der Anbieter mehr Teile des technischen Betriebs, aber Daten, Identitäten, Benutzerkonten, Zugriffskontrollen und Konfigurationen bleiben in wesentlichen Punkten Kundenthema. Microsoft formuliert das ausdrücklich so: Für alle Cloud-Bereitstellungsmodelle bleibt der Kunde für seine Daten und Identitäten verantwortlich; dazu gehören insbesondere Accounts, Rollen, MFA, Zugriffskontrollen und die Sicherheit der

Komponenten, die das Unternehmen selbst steuert. Für Geschäftsführer und Vorstände ist das die entscheidende Management-Botschaft: Mit der Auslagerung des Betriebs endet nicht die Organverantwortung. Im Gegenteil: Wer Cloud, SaaS, MSPs oder andere Dienstleister nutzt, vergrößert den eigenen Steuerungs- und Überwachungsauftrag. Denn Risiken entstehen nicht nur im eigenen Rechenzentrum, sondern auch in den Beziehungen zu Anbietern, Unterauftragnehmern, Integrationen und Plattformen. Das BSI beschreibt die Nutzung von Cloud-Diensten deshalb ausdrücklich als strategischen Schritt mit beträchtlichen Auswirkungen auf die eigene IT; Risiken und Verantwortlichkeiten müssen vor der Nutzung bewusst bewertet und geregelt werden.

Shared Responsibility heißt nicht: Der Provider kümmert sich um alles

Gerade im Mittelstand entsteht hier oft ein gefährlicher Irrtum. Viele Unternehmen gehen unausgesprochen davon aus, dass ein großer Cloud- oder SaaS-Anbieter Sicherheit, Verfügbarkeit und Wiederherstellung im Wesentlichen „mitliefert“. Tatsächlich verschiebt sich aber nur die Grenze der Zuständigkeit. In SaaS-Szenarien wie Microsoft 365 oder Dynamics 365 verwaltet der Anbieter zwar große Teile der Anwendung und Plattform, der Kunde bleibt aber für **Datenklassifizierung, Benutzer- und Rollenverwaltung, Zugriffsregeln, Sicherheitskonfigurationen** und viele Compliance-Entscheidungen verantwortlich. Microsoft benennt diese Kundenzuständigkeiten ausdrücklich, darunter Daten, Endpunkte, Benutzerkonten und Access Management.

Genau deshalb ist Shared Responsibility kein rein technisches Modell, sondern ein Governance-Thema. Die Geschäftsleitung muss wissen, welche Sicherheits- und Betriebsaufgaben der Anbieter übernimmt – und welche nicht. Wer diese Abgrenzung nicht versteht, bewertet Risiken falsch, baut Lücken in seiner Sicherheitsarchitektur auf und verlässt sich im Zweifel auf Leistungen, die vertraglich oder technisch gar nicht geschuldet sind. Dass diese Verantwortung nicht beim Provider endet, folgt auch aus der NIS2-Logik: Die Richtlinie verlangt Cyber-Risikomanagement gerade auch dort, wo Risiken aus Beziehungen zu direkten Lieferanten oder Dienstleistern entstehen.

NIS2 rückt Lieferkette, Cloud und Dienstleister ausdrücklich in den Fokus

NIS2 macht deutlich, dass Cybersicherheit nicht an der eigenen Unternehmensgrenze endet. Risiken in der Lieferkette sowie bei Cloud-, SaaS- und IT-Dienstleistern müssen deshalb aktiv gesteuert,

vertraglich abgesichert und kontinuierlich überwacht werden. Für Unternehmen wird damit auch die Sicherheit externer Abhängigkeiten zu einem festen Bestandteil wirksamen Cyber-Risikomanagements.

- **Pflichtfeld:** NIS2 behandelt Lieferkette, Cloud und Dienstleister als festen Bestandteil des Cyber-Risikomanagements.
- **Verantwortung:** Unternehmen müssen Risiken bei Providern, SaaS-Anbietern und IT-Dienstleistern aktiv steuern.
- **Vertragsbasis:** Sicherheitsanforderungen, Eskalationswege und Nachweise müssen vertraglich abgesichert werden.
- **BSI-Erwartung:** Risiken durch Dienstleister sind systematisch zu bewerten und laufend zu überwachen.
- **Management-Thema:** Cloud- und Dienstleisterrisiken sind damit keine reine IT-Frage mehr, sondern Führungsaufgabe.
- **Marktwirkung:** Auch nicht direkt regulierte Unternehmen geraten unter Druck, weil Kunden NIS2-Anforderungen weitergeben.

Datenschutz und Auftragsverarbeitung: Verantwortung bleibt bei personenbezogenen Daten

Sobald Cloud- oder SaaS-Dienste personenbezogene Daten verarbeiten, kommt zusätzlich die DSGVO ins Spiel. **Artikel 28** verlangt, dass Verantwortliche nur solche Auftragsverarbeiter einsetzen, die hinreichende Garantien dafür bieten, geeignete technische und organisatorische Maßnahmen so umzusetzen, dass die Verarbeitung den Anforderungen der DSGVO entspricht. Außerdem muss die Verarbeitung durch einen Vertrag oder ein anderes verbindliches Rechtsinstrument geregelt sein. Das heißt für die Geschäftsleitung: Bei ausgelagerten Diensten genügt es nicht, auf Markenstärke oder Marktbekanntheit zu vertrauen; Auswahl, Prüfung und vertragliche Einbindung müssen belastbar sein.

Gerade in Cloud-Szenarien wird damit sichtbar, warum „Der Provider macht das schon“ kein tragfähiger Rechtsstandpunkt ist. Wer personenbezogene Daten über externe Dienste verarbeiten lässt, muss nicht nur die Plattform auswählen, sondern auch den Vertragsrahmen, die TOMs, die Unterauftragnehmer-Struktur und die operative Kontrollfähigkeit im Blick behalten.

Auch das BSI weist in seinen Cloud-Hinweisen darauf hin, dass die Nutzung von Cloud-Computing besonders kritisch wird, wenn personenbezogene Daten Dritter bei einem Anbieter gespeichert werden.

Datenschutz und Auftragsverarbeitung: Verantwortung bleibt bei personenbezogenen Daten

Kritische Anforderungen an Dienstleister dürfen nicht in Vertragsdetails oder Anhängen verschwinden, sondern müssen aktiv gesteuert

und regelmäßig überprüft werden. Gerade bei Sicherheit, Exit-Szenarien und Wiederherstellung braucht es klare Vorgaben für den Ernstfall.

Verträge:

Sicherheitsanforderungen, Eskalationswege und Zuständigkeiten müssen klar geregelt sein.

Exit-Szenarien:

Für Anbieterwechsel oder Ausfälle braucht es vorbereitete Ausstiegs- und Übergabepäne.

Wiederherstellungsrechte:

Unternehmen müssen sicherstellen, dass Daten, Konfigurationen und Zugriffe im Ernstfall wiederherstellbar sind.

Nachweise und laufende Kontrolle: Vertrauen ist kein Kontrollsystem

Ein häufiger Management-Irrtum besteht darin, Dienstleister einmalig auszuwählen und danach kaum noch aktiv zu steuern. Gute Governance verlangt mehr: Kritische Provider müssen risikobasiert eingeordnet, dokumentiert bewertet und regelmäßig überprüft werden. Das BSI betont in seinen NIS2-FAQ, dass Unternehmen sich auch mit Dienstleisterrisiken befassen müssen; Nachweise wie eine **ISO-27001-Zertifizierung** können dabei ein Indiz sein, ersetzen aber keine eigene Risikobewertung. Der BSI-C5-Katalog hilft zusätzlich, Mindestanforderungen an die Informationssicherheit von Cloud-Diensten transparent und prüfbar zu machen.

Für mittelständische Unternehmen ist das pragmatisch umsetzbar: Kritische Dienstleister – etwa für ERP, M365, Identitätsplattformen, Hosting, Backup oder Managed Security – sollten im Risikoregister als Abhängigkeiten erfasst werden. Statt Vollaudits braucht es oft schon eine strukturierte Due Diligence: Welche Zugriffe bestehen? Welche Daten sind betroffen? Welche Zertifikate, Prüfberichte oder Nachweise liegen vor? Wie sind Notfallvorsorge, Meldewege, Unterauftragnehmer und Exit geregelt? Das ist keine Überbürokratisierung, sondern der Unterschied zwischen blindem Outsourcing und steuerbarer Dienstleisterverantwortung.

Was die Geschäftsleitung jetzt tun sollte

Der wichtigste erste Schritt ist Transparenz über die eigenen Abhängigkeiten. Für jede geschäftskritische Cloud-, SaaS- oder MSP-Leistung sollte dokumentiert sein, welche Verantwortung beim Anbieter liegt, was intern verbleibt, welche Risiken im Ausfall- oder Sicherheitsfall

entstehen und welche vertraglichen Rechte gelten. Dazu sollten kritische Anbieter im Risikoregister geführt, Pflichten vertraglich geschärft, Exit-Szenarien vorbereitet und Nachweise regelmäßig eingefordert werden. So wird Outsourcing zu einem steuerbaren Betriebsmodell.

Schwachstellen, Patches und externe Angriffsfläche beherrschen

Die meisten erfolgreichen Angriffe scheitern nicht daran, dass Unternehmen keine „**High-End-Security**“ eingekauft haben. Sie gelingen, weil bekannte Schwachstellen zu lange offen bleiben, Systeme nicht sauber inventarisiert sind, alte Remote-Zugänge weiter im Internet hängen oder niemand mehr genau weiß, welche Dienste von außen überhaupt erreichbar sind. Das BSI formuliert es ungewöhnlich klar: Fast alle Cyberangriffe nutzen bekannte Schwachstellen. Gleichzeitig nennt das BSI das Aktualisieren von Software und Betriebssystemen sowie aktives Schwachstellenmanagement als zentrale

Schutzmaßnahmen. Für Geschäftsführer und Vorstände ist das ein wichtiges Signal. Ungepatchte Systeme, vergessene Internet-Systeme und unkontrollierte Exponierung sind kein unvermeidbares Schicksal, sondern in erster Linie Steuerungs- und Priorisierungsprobleme. Genau deshalb gehört dieses Thema nicht nur in die IT-Operation, sondern in die Führungslogik des Unternehmens: Was ist kritisch, was ist von außen erreichbar, was ist verwundbar, und wie schnell wird bei relevanten Funden gehandelt?

Die größte Gefahr sind oft nicht spektakuläre Zero-Day-Angriffe, sondern bekannte Schwachstellen, fehlende Patches und vergessene Internet-Systeme.



Warum Schwachstellen- und Patchmanagement Pflicht und nicht Kür ist

NIS2 verlangt ein systematisches Cyber-Risikomanagement. Dazu gehören nach den BSI-Infopaketen ausdrücklich die Behebung von Schwachstellen durch Patches, Konfigurationsänderungen oder andere Gegenmaßnahmen sowie eine Priorisierung nach Kritikalität und zeitlicher Einordnung. Die **EU-Durchführungsverordnung 2024/2690** geht noch weiter: Sie verlangt Verfahren dafür, dass Sicherheitspatches innerhalb angemessener Frist eingespielt, vor dem Einsatz in Produktivsystemen getestet, aus vertrauenswürdigen Quellen bezogen und auf Integrität geprüft werden. Wenn ein Patch bewusst nicht oder verzögert eingespielt wird, müssen zusätzliche Maßnahmen getroffen sowie die Restrisiken akzeptiert und die

Gründe dokumentiert werden. Damit ist die Management-Botschaft eindeutig: Patchen ist kein reiner Technikvorgang, sondern ein dokumentations- und haftungsrelevanter Führungsprozess. Wer Patches dauerhaft verschleppt, Ausnahmen nicht begründet oder kritische Schwachstellen in exponierten Systemen nicht priorisiert, hat kein Ressourcenproblem mehr, sondern ein Organisationsproblem. Die europäische NIS2-Konkretisierung verlangt zudem ausdrücklich, Informationen über technische Schwachstellen zu beobachten, wo sinnvoll Schwachstellenscans durchzuführen, kritische Schwachstellen ohne unangemessene Verzögerung zu behandeln und auch Nicht-Behebungen nachvollziehbar zu begründen.

Die externe Angriffsfläche: Was Angreifer vor Ihnen sehen

Besonders kritisch ist alles, was vom Internet aus erreichbar ist. Denn genau dort beginnt in vielen Fällen der erste Zugriff. Der **BSI-Lagebericht 2024** weist ausdrücklich darauf hin, dass insbesondere frei über das Internet erreichbare Webmail-Systeme ohne Multifaktor-Authentifizierung eine größere Angriffsfläche darstellen. Das ist nur ein Beispiel, aber ein sehr anschauliches: Angreifer suchen nicht zuerst nach Ihrem besten Sicherheitskonzept, sondern nach dem einfachsten Weg hinein. Aus Managementsicht ist die externe Angriffsfläche deshalb eine einfache, aber unbequeme Frage: Wissen

wir wirklich, welche Systeme, Portale, VPN-Zugänge, Subdomains, Testumgebungen, Cloud-Ressourcen und Admin-Oberflächen von außen erreichbar sind? Wenn diese Transparenz fehlt, sehen Angreifer die Angriffsfläche oft früher und vollständiger als das Unternehmen selbst. Genau hier beginnt wirksame Steuerung: nicht bei der letzten Stufe eines Security-Produkts, sondern bei der vollständigen Sicht auf öffentlich erreichbare Assets und deren Kritikalität. Das BSI verknüpft Asset-Management im NIS2-Kontext ausdrücklich mit regelmäßigen Audits und Kontrollen, um Schwachstellen frühzeitig zu erkennen.

Das eigentliche Problem sind oft nicht Zero Days, sondern alte Versäumnisse

Für den Mittelstand ist das eine gute Nachricht, auch wenn sie unbequem ist: Viele Risiken sind behebbar, weil sie nicht aus hochkomplexen Angriffen entstehen, sondern aus bekannten Versäumnissen. Typische Beispiele sind veraltete VPN- oder Fernzugriffssysteme, längst nicht mehr benötigte Dienste, Testsysteme mit alter Software, freistehende Webanwendungen ohne sauberes Update-Regime oder lokale Administrationsrechte, die im Alltag bequem, im Angriffsfall aber hochgefährlich sind. Die BSI-Unterlagen zu NIS2 und der Lagebericht stützen genau diese Richtung: Sicherheit entsteht nicht erst im Ausnahmefall, sondern vor allem durch konsequente Basishygiene,

Aktualität und Begrenzung unnötiger Angriffsflächen. Genau deshalb sollten Unternehmen Schwachstellen nicht nach Lautstärke, sondern nach Risiko priorisieren. Ein nicht gepatchtes, internet-exponiertes System mit hoher Geschäftsrelevanz ist für die Geschäftsleitung wichtiger als ein mittlerer Befund auf einem internen Nebensystem. Die **EU-Durchführungsverordnung** knüpft Schwachstellenmanagement ausdrücklich an Risikomanagement, Change Management und Security Testing. Das passt direkt zu den früheren Kapiteln dieses Leitfadens: Zuerst müssen die bestandskritischen Systeme bekannt sein, dann werden dort Exponierung und Patch-Dringlichkeit priorisiert.

Vier Management-Hebel, die sofort Wirkung haben:

- **Vollständige Transparenz über Assets und Exponierung:** Ohne ein aktuelles Inventar aller relevanten Systeme, Dienste und Anwendungen – on-premises wie in der Cloud – ist belastbares Schwachstellenmanagement kaum möglich. Nur wer seine Angriffsfläche kennt, kann Risiken frühzeitig erkennen und steuern.
- **Risikobasiertes Patch-Management mit klaren Fristen:** Nicht jedes Update ist gleich kritisch, aber internet-exponierte und geschäftskritische Systeme müssen priorisiert behandelt werden. Klare Fristen, Tests vor Produktiveinsatz und dokumentierte Ausnahmen machen aus Patches einen steuerbaren Prozess.
- **Reduktion der Angriffsfläche:** Nicht benötigte Verbindungen, Dienste und Zugänge sollten konsequent deaktiviert werden. Weniger Exponierung bedeutet weniger Angriffsfläche, weniger Patch-Druck und weniger unerwartete Risiken.
- **Verzahnung mit BCM und Risikoregister:** Kritische Schwachstellen an geschäftskritischen Systemen müssen im Management-Reporting sichtbar werden. Spätestens wenn ein offenes Internet-System ein Kronjuwel betrifft, wird aus einem IT-Thema ein unmittelbares Geschäftsrisiko.

Was die Geschäftsleitung jetzt tun sollte

Die entscheidende Führungsfrage lautet nicht: „Haben wir ein Schwachstellen-Tool?“, sondern: Kennen wir unsere extern erreichbaren Systeme, priorisieren wir Schwachstellen nach Geschäftsrelevanz und Exponierung, und werden Ausnahmen sauber entschieden

und dokumentiert? Wer das klar steuert, senkt das Risiko erfolgreicher Angriffe oft stärker als mit vielen Einzelmaßnahmen. Denn die gefährlichsten Lücken sind häufig bekannte Schwachstellen, alte Systeme und offene Zugänge ohne klare Zuständigkeit.

Was muss wann dokumentiert und gemeldet werden?

Kaum ein Bereich erzeugt im Ernstfall so viel operative Unsicherheit wie die Frage: Müssen wir jetzt melden – und wenn ja, wem, bis wann und mit welchen Inhalten? Genau hier entscheidet sich oft, ob ein Cybervorfall „nur“ technisch beherrscht wird oder zusätzlich zu einem Compliance- und Haftungsproblem eskaliert. Unter NIS2 gelten enge Fristen für erhebliche Sicherheitsvorfälle; unter der DSGVO kommen

eigene Meldepflichten für Datenschutzverletzungen hinzu. Gleichzeitig verlangen beide Regime eine nachvollziehbare Dokumentation der Vorfälle, der Bewertungen und der ergriffenen Maßnahmen. Für Geschäftsführer und Vorstände ist das der entscheidende Punkt: Es geht nicht nur um das Melden, sondern auch um die Beweisfähigkeit, dass rechtzeitig, informiert und angemessen gehandelt wurde.

NIS2: Drei Meldefenster statt einer einzigen Frist

Für erhebliche Sicherheitsvorfälle sieht NIS2 ein gestuftes Meldeverfahren vor. Das BSI beschreibt für Deutschland drei Stufen: eine frühe Erstmeldung **innerhalb von 24 Stunden**, eine Meldung innerhalb von 72 Stunden und eine Abschluss- oder Folgemeldung nach 30 Tagen beziehungsweise spätestens einem Monat. Die NIS2-Richtlinie selbst nennt dieselbe Struktur in Artikel 23: Early Warning binnen 24 Stunden, Incident Notification binnen 72 Stunden und Final Report spätestens einen Monat nach der Meldung. In Deutschland erfolgt die Meldung in der Regel an das BSI über das BSI-Portal. Wichtig ist dabei die Einordnung, wann ein Vorfall überhaupt als erheblich beziehungsweise signifikant gilt. Nach **Artikel 23 NIS2** ist das insbesondere dann der Fall, wenn der Vorfall eine schwerwiegende Betriebsstörung oder finanzielle Verluste verursacht oder verursachen kann oder wenn andere natürliche oder juristische Personen erhebliche materielle

oder immaterielle Schäden erleiden können. Das BSI übersetzt diese Schwelle in seinen NIS2-Unterlagen entsprechend in schwerwiegende Betriebsstörungen, finanzielle Verluste und Schäden bei Dritten; die **EU-Durchführungsverordnung 2024/2690** konkretisiert für bestimmte Sektoren zusätzlich Fallgruppen und Schwellenwerte. Für die Praxis heißt das: Die **24-Stunden-Meldung** ist keine perfekte Abschlussanalyse, sondern eine Frühwarnung. In der 72-Stunden-Meldung wird die Lage vertieft, und der Abschlussbericht dokumentiert Ursachen, Auswirkungen, Abhilfemaßnahmen und Lernerkenntnisse. Wer darauf wartet, bis jedes Detail forensisch geklärt ist, wird die Fristen oft reißen. Managementseitig ist deshalb ein Vorgehen nötig, das frühe Lagebilder zulässt und später sauber ergänzt wird. Das entspricht sowohl der NIS2-Systematik als auch der Anleitung des BSI.

DSGVO: Datenschutzverletzungen binnen 72 Stunden melden

Parallel dazu gilt das Datenschutzrecht. **Artikel 33 DSGVO** verpflichtet den Verantwortlichen, eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden an die zuständige Aufsichtsbehörde zu melden, sofern die Verletzung voraussichtlich nicht ohne Risiko für die Rechte und Freiheiten natürlicher Personen ist. Wird die 72-Stunden-Frist überschritten, muss die Verzögerung begründet werden. Außerdem muss ein Auftragsverarbeiter eine ihm bekannt gewordene Verletzung dem Verantwortlichen unverzüglich melden. Die Mindestinhalte der DSGVO-Meldung sind ebenfalls klar vorgegeben: Art der Verletzung, soweit möglich Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, Kontaktdaten des Datenschutzbeauftragten oder einer Anlaufstelle, wahrscheinliche Folgen sowie bereits ergriffene

oder vorgeschlagene Abhilfemaßnahmen. Die DSGVO erlaubt zudem ausdrücklich, Informationen schrittweise nachzureichen, wenn sie nicht gleichzeitig bereitgestellt werden können. Für die Leitungsebene ist das wichtig: Auch hier gilt praktisch eher „rechtzeitig vorläufig“ als „perfekt zu spät“. Zusätzlich verlangt Artikel 34 DSGVO, betroffene Personen unverzüglich zu benachrichtigen, wenn die Datenschutzverletzung voraussichtlich ein hohes Risiko für ihre Rechte und Freiheiten zur Folge hat, sofern nicht Ausnahmen greifen, etwa durch wirksame Schutzmaßnahmen wie Verschlüsselung oder nachträgliche Maßnahmen, die das hohe Risiko beseitigen. Damit wird klar: Ein schwerer Cybervorfall kann neben der Behördenmeldung auch Kommunikationspflichten gegenüber Betroffenen auslösen.

Das Doppelregime: Wann NIS2, wann DSGVO – und oft beides

In vielen realen Vorfällen greifen NIS2 und DSGVO gleichzeitig. Eine Ransomware-Lage mit Produktionsstillstand und kompromittierten personenbezogenen Daten kann einerseits ein erheblicher Sicherheitsvorfall im Sinne von NIS2 sein und andererseits eine Datenschutzverletzung im Sinne von Artikel 33 DSGVO. Dann laufen zwei Prüfungen parallel: einmal die Frage nach der Auswirkung auf Dienste, Betrieb und Dritte, und einmal die Frage nach dem Risiko für die Rechte und Freiheiten betroffener Personen. Die Fristen ähneln sich teilweise, die Rechtsgrundlagen, Empfänger und Prüfungskriterien sind aber nicht identisch.

Für die Praxis ist deshalb ein zentraler Vorfallsprozess entscheidend. Sobald ein schwerer Incident erkannt wird, muss systematisch geprüft werden: Liegt ein NIS2-relevanter erheblicher Sicherheitsvorfall vor? Sind personenbezogene Daten betroffen? Müssen zusätzlich Kunden, Auftraggeber, Versicherer oder Betroffene informiert werden? Ein solcher Entscheidungsprozess ist kein Bürokratiezusatz, sondern die Voraussetzung dafür, Fristen sauber zu steuern und keine Meldepflicht zu übersehen. Diese Schlussfolgerung ergibt sich direkt aus den parallelen Melde- und Dokumentationsanforderungen von NIS2 und DSGVO.

Beweisfähigkeit: Warum Dokumentation mehr ist als Administration

Neben den Meldefristen ist die Dokumentation der zweite große Hebel dieses Kapitels. Die DSGVO ist hier eindeutig: Der Verantwortliche muss Verletzungen des Schutzes personenbezogener Daten einschließlich aller relevanten Fakten, ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen dokumentieren, und zwar auch dann, wenn der Vorfall am Ende nicht meldepflichtig war. Diese Dokumentation muss der Aufsichtsbehörde ermöglichen, die Einhaltung von Artikel 33 zu überprüfen. Auch im NIS2-Kontext ist Dokumentation kein Nebenaspekt. Das BSI verweist darauf, dass die Meldung an das **BSI aus § 32 BSIG** folgt und dass Vorfallsbehandlung, Meldeprozess und Maßnahmen nachvollziehbar dokumentiert sein müssen; zudem nennt das BSI Dokumentation ausdrücklich als Teil der Pflichten unter NIS2. Wer innerhalb von 72 Stunden belastbar berichten und nach einem Monat einen Abschlussbericht abgeben

soll, braucht intern ohnehin eine saubere Vorfallschronologie, eine belastbare Ursachen- und Wirkungsbewertung und nachvollziehbare Entscheidungen zu Eindämmung, Wiederherstellung und Kommunikation. Für Geschäftsführer und Vorstände ist genau das der Punkt der Beweisfähigkeit. Im Ernstfall genügt es nicht zu sagen, man habe „nach bestem Wissen“ gehandelt. Entscheidend ist, ob sich später nachvollziehen lässt, wann der Vorfall erkannt wurde, welche Informationen vorlagen, wie Risiko und Meldepflicht bewertet wurden, wer entschieden hat, welche Maßnahmen angeordnet wurden und warum. Diese Anforderung ergibt sich zwar nicht als einzelnes Schlagwort „Beweisfähigkeit“ aus einer Norm, wohl aber unmittelbar aus den Dokumentationspflichten von DSGVO und NIS2 sowie aus der allgemeinen Notwendigkeit, fristgerechtes und angemessenes Handeln gegenüber Behörden und Prüfern belegen zu können.

Was bei einem Sicherheitsvorfall intern mindestens festgehalten werden sollte

- **Zeitlinie:** Erkennung, Eskalation, interne Bewertung und externe Meldungen dokumentieren.
- **Sachverhalt:** Betroffene Systeme, Dienste, Daten und mögliche Ursachen festhalten.
- **Bewertung:** Einstufung nach NIS2 und DSGVO sowie die Auswirkungen bewerten.
- **Entscheidungen:** Dokumentieren, ob gemeldet wurde, an wen und auf welcher Grundlage.
- **Maßnahmen:** Eindämmung, Wiederherstellung, Kommunikation und Lessons Learned festhalten.

Was die Geschäftsleitung jetzt tun sollte

Die wichtigste Führungsaufgabe ist ein einheitlicher Incident- und Meldeprozess, der NIS2 und DSGVO gemeinsam abdeckt. Vorab muss klar sein, wer Vorfälle bewertet, wer entscheidet, wer Meldungen

freigibt und wie Datenschutz, Recht, IT und Kommunikation eingebunden sind. Nur so lassen sich 24- und 72-Stunden-Fristen sicher einhalten und hektische Ad-hoc-Abstimmungen vermeiden.

Security-Kultur, Schulungen und Reporting an die Leitung verankern

NIS2 endet nicht bei Technik, Prozessen und Tools. Die Richtlinie zieht die Verantwortung bewusst bis in die Führungskultur hinein: Geschäftsleitungen müssen Cyber-Risikomanagementmaßnahmen billigen, ihre Umsetzung überwachen und können für Verstöße haftbar gemacht werden. Gleichzeitig verlangt Artikel 20 NIS2, dass Mitglieder der Leitungsorgane Schulungen absolvieren; Artikel 21 nennt zudem ausdrücklich Cybersecurity-Trainings, Basic Cyber Hygiene und Verfahren zur Bewertung der Wirksamkeit der Maßnahmen als Bestandteil des Pflichtenprogramms. Cybersicherheit ist damit nicht nur ein Umsetzungsprojekt, sondern eine dauerhafte Führungs- und

Steuerungsaufgabe. Für Geschäftsführer und Vorstände ist das die eigentliche Abschlussbotschaft dieses Leitfadens: Sicherheitskultur beginnt oben. Wenn die Leitung Cybersicherheit nur als IT-Thema behandelt, bleibt auch die Organisation dabei stehen. Wenn sie das Thema dagegen sichtbar priorisiert, regelmäßig nach Risiken fragt, Entscheidungen nachvollziehbar trifft und sich selbst schulen lässt, verändert das die Aufmerksamkeit, die Reaktionsgeschwindigkeit und am Ende auch das Sicherheitsniveau des gesamten Unternehmens. Genau diese Logik steckt in Artikel 20 NIS2: Governance, Schulung und Aufsicht sind keine Kür, sondern gesetzlich verankert.

Schulungspflicht: nicht nur für Mitarbeitende, sondern ausdrücklich auch für die Leitung

NIS2 verlangt ausdrücklich, dass Mitglieder der Leitungsorgane geschult werden. **Artikel 20 Absatz 2** verpflichtet die Mitgliedstaaten sicherzustellen, dass die Mitglieder der Managementgremien Schulungen absolvieren; zugleich sollen die betroffenen Unternehmen ähnliche Schulungen auch ihren Mitarbeitenden regelmäßig anbieten, damit Risiken erkannt und Cyber-Risikomanagementmaßnahmen eingeordnet werden können. Das BSI greift diese Pflicht in seinen NIS2-Informationspaketen und FAQ ausdrücklich auf und stellt klar, dass § 38 Absatz 3 BSIG auch die Geschäftsleitungen wichtiger und besonders wichtiger Einrichtungen zur Teilnahme an Schulungen verpflichtet. In der BSI-Handreichung zur Geschäftsleitungsschulung wird außerdem

auf die gesetzliche Definition von „regelmäßig“ als alle drei Jahre verwiesen. Das ist für die Praxis wichtiger, als es auf den ersten Blick wirkt. Viele Unternehmen haben Awareness bislang als Pflichtschulung für Mitarbeitende verstanden – häufig einmal jährlich, oft eher formal. NIS2 verschiebt diese Perspektive: Auch die Leitung muss in die Lage versetzt werden, Risiken zu erkennen, Maßnahmen zu bewerten und deren Auswirkungen auf die bereitgestellten Dienste zu verstehen. Management-Schulungen sind damit keine Reputationsmaßnahme, sondern eine Voraussetzung dafür, die eigene Aufsichts- und Entscheidungsverantwortung überhaupt sachgerecht wahrnehmen zu können.

Sicherheitskultur ist kein Soft Topic, sondern ein Risikotreiber

Artikel 21 NIS2 nennt ausdrücklich Basic Cyber Hygiene Practices and Cybersecurity Training sowie Human Resources Security als Teil der Cyber-Risikomanagementmaßnahmen. Das ist regulatorisch bemerkenswert, weil es zeigt: Der Gesetzgeber betrachtet den menschlichen Faktor nicht als Randthema, sondern als festen Bestandteil eines wirksamen Sicherheitsprogramms. Das BSI greift diese Sicht im **IT-Grundschutz** ebenfalls auf; dort gehören Sensibilisierung und Schulung zur Informationssicherheit zu den grundlegenden Bausteinen des Sicherheitsmanagements. Für die Geschäftsleitung heißt das: Sicherheitskultur entsteht nicht durch einzelne E-Learnings, sondern durch Wiederholung, Vorbildwirkung und klare Erwartungen. Mitarbeitende

müssen wissen, woran sie Phishing, verdächtige Zugriffe oder ungewöhnliche Systemreaktionen erkennen. Führungskräfte müssen Sicherheitsfragen nicht nur an die IT delegieren, sondern in Projekten, Investitionen und Veränderungen sichtbar mitführen. Und Fehler oder Beinahe-Vorfälle müssen so behandelt werden, dass daraus gelernt wird, statt nur nach Schuldigen zu suchen. Genau dadurch wird aus Awareness ein belastbarer Steuerungsfaktor. Diese Schlussfolgerung ergibt sich aus der Kombination aus NIS2-Schulungspflicht, Cyber-Hygiene-Anforderungen und den BSI-Grundschutzbausteinen zur Sensibilisierung.

Reporting an die Leitung: von Meldungen zu echten Steuerungsgrößen

Ebenso wichtig wie Schulungen ist das regelmäßige Reporting an die Unternehmensleitung. NIS2 verlangt nicht nur Maßnahmen, sondern auch **Verfahren zur Bewertung ihrer Wirksamkeit**. Das BSI formuliert dazu in seinen NIS2-Unterlagen sehr klar, dass die Unternehmensleitung regelmäßig über den Status der Informationssicherheit und bestehende Risiken informiert werden muss. Auch im IT-Grundschutz ist das verankert: Dort gibt es ausdrücklich die Anforderung Management-Berichte zur Informationssicherheit. Für Geschäftsführer und Vorstände bedeutet das: Ein gutes Security-Reporting besteht nicht aus langen technischen Statusmails, sondern aus wenigen, verständlichen

Steuerungsgrößen. Relevant sind nicht 200 Einzelfunde, sondern Trends und Abweichungen, die Entscheidungen auslösen. Dazu gehören etwa die Entwicklung kritischer Risiken, der Status besonders kritischer Schwachstellen, Patch-Verzögerungen bei internet-exponierten Systemen, Backup- und Restore-Erfolgsquoten, die Anzahl schwerer Incidents, Reaktions- und Wiederanlaufzeiten, Schulungsquoten, Phishing-Meldeverhalten oder offene Maßnahmen aus Audits und Vorfällen. Dass sich Wirksamkeit regelmäßig bewerten und dem Management berichten lassen muss, folgt direkt aus Artikel 21 Absatz 2 Buchstabe f NIS2 und den BSI-Hinweisen zu Management-Berichten.

Eskalationskriterien & Management-Reviews machen das Thema steuerbar

Reporting allein genügt allerdings nicht. Es braucht auch klare Regeln dafür, wann aus einer Kennzahl, einem Vorfall oder einer Abweichung ein Thema für die Geschäftsleitung wird. **Die EU-Durchführungsverordnung 2024/2690** verlangt, dass Rollen, Verantwortlichkeiten und Befugnisse von den Leitungsorganen in geplanten Abständen sowie bei signifikanten Vorfällen oder wesentlichen Änderungen überprüft und bei Bedarf aktualisiert werden. Das ist ein starker Hinweis darauf, dass Security-Steuerung nicht statisch gedacht wird: Wenn Risiken steigen, Vorfälle passieren oder sich das Betriebsmodell verändert, muss auch die Leitung ihre Steuerungs- und Eskalationslogik

nachschärfen. Praktisch heißt das: Die Geschäftsleitung sollte nicht nur einen Monats- oder Quartalsreport erhalten, sondern auch definieren, bei welchen Schwellenwerten sofort eskaliert wird. Beispiele wären ein signifikanter Sicherheitsvorfall, das Verfehlen definierter RTO- oder RPO-Ziele, wiederholt nicht bestandene Restore-Tests, ein kritischer Befund bei einem Schlüsseldienstleister oder eine Häufung schwerer Phishing- oder Identitätsvorfälle. Erst solche Eskalationskriterien machen aus Reporting echte Führungssteuerung. Diese Logik passt unmittelbar zu den NIS2-Anforderungen an Governance, Wirksamkeitsbewertung und laufende Verantwortung der Managementgremien.

Cybersicherheit wird erst dann dauerhaft steuerbar, wenn sie Teil der Führungskultur wird. NIS2 verlangt deshalb nicht nur Technik und Prozesse, sondern auch geschulte Leitungsorgane, regelmäßige Schulungen für Mitarbeitende, verständliche Management-Berichte, klare Eskalationskriterien und wiederkehrende Reviews der Wirksamkeit. So wird aus IT-Sicherheit ein belastbarer Führungsanspruch – und aus Pflicht gelebte Steuerung.

Fazit: Cybersicherheit wird zur Führungsqualität

Die zehn Punkte dieses Leitfadens zeigen vor allem eines: Cybersicherheit ist heute kein Spezialthema für die IT-Abteilung mehr, sondern ein Prüfstein für **gute Unternehmensführung**. Ob Organpflicht, Pflichtenmix, Risikoregister, Identitäten, Backup, Wiederanlauf, Dienstleistersteuerung, Schwachstellenmanagement, Meldeprozesse oder Sicherheitskultur – alle diese Themen laufen am Ende auf dieselbe Führungsfrage hinaus: Ist Ihr Unternehmen in der Lage, Cyberrisiken strukturiert zu steuern und im Ernstfall kontrolliert zu handeln?

Dabei geht es nicht darum, jede technische Detailfrage selbst zu beantworten. Es geht darum, die richtigen Fragen zu stellen, belastbare Informationen einzufordern, Prioritäten zu setzen und Entscheidungen nachvollziehbar zu dokumentieren. Genau darin liegt heute der Unterschied zwischen reaktiver IT-Verwaltung und echter Cyber-Resilienz auf Unternehmensebene.

Für viele mittelständische Unternehmen ist das keine Aufgabe, die mit einem Einzelprojekt erledigt ist. Cybersicherheit ist vielmehr ein laufender Führungsprozess: Risiken verändern sich, Geschäftsmodelle werden digitaler, regulatorische Erwartungen steigen und Abhängigkeiten von Identitätsplattformen, Cloud-Diensten, ERP-Systemen und externen Dienstleistern nehmen zu. Umso wichtiger ist es, nicht nur punktuell zu reagieren, sondern eine belastbare Struktur aufzubauen, in der Prävention, Wiederherstellung, Krisenfähigkeit und Nachweisbarkeit zusammenwirken.

Am Ende ist Cybersicherheit damit nicht nur Schutz vor Angriffen. Sie wird zu einem Faktor für Stabilität, Vertrauenswürdigkeit und Wettbewerbsfähigkeit. Wer hier als Geschäftsführung oder Vorstand aktiv steuert, reduziert nicht nur Haftungsrisiken, sondern stärkt die Handlungsfähigkeit des Unternehmens in einer Lage, in der digitale Widerstandsfähigkeit zunehmend über Geschäftserfolg mitentscheidet.

Der nächste sinnvolle Schritt

Die entscheidende Frage nach der Lektüre dieses Leitfadens lautet nicht, ob Handlungsbedarf besteht, sondern wo die größten Lücken in Ihrem Unternehmen heute tatsächlich liegen. Sind Ihre geschäftskritischen Risiken klar priorisiert? Sind Identitäten, Zugriffe, Backups und Wiederanlauf wirklich belastbar organisiert? Gibt es für Cloud-, SaaS- und Dienstleisterabhängigkeiten klare Verantwortlichkeiten, Nachweise und Exit-Szenarien? Und erhält die Geschäftsleitung regelmäßig

genau die Informationen, die sie für fundierte Entscheidungen braucht?

Wenn Sie diese Fragen nicht **für alle kritischen Bereiche belastbar beantworten** können, lohnt sich ein strukturierter Realitätscheck. Genau dort entsteht der größte Mehrwert: nicht durch noch ein Einzeltool, sondern durch Transparenz über Risiken, Verantwortlichkeiten und konkrete Prioritäten für die nächsten Schritte.

Unser pragmatischer Vorschlag: Strukturiert starten, gezielt priorisieren

Starten Sie mit einer kompakten Bestandsaufnahme Ihrer geschäftskritischen Systeme, Risiken und Wiederherstellungsanforderungen. So wird schnell sichtbar, wo Ihr Unternehmen bereits gut aufgestellt ist – und wo in Themen wie Identitätsschutz, Backup, Wiederanlauf oder Managed Security gezielt nachgeschärft werden sollte.

Wir gehen die Einordnung strukturiert mit Ihnen an. Dabei unterstützen wir mittelständische Unternehmen dabei, Sicherheitsanforderungen nicht nur technisch, sondern vor allem organisatorisch und betrieblich belastbar umzusetzen – mit pragmatischen Services, klarer Priorisierung und dem Blick auf das, was im Ernstfall wirklich zählt.



Lassen Sie uns gemeinsam Ihre Digitale Zukunft gestalten


Die abtis Gruppe führt als IT-Dienstleister den Mittelstand mit strategischer Beratung, effizienten Projekten und maßgeschneiderten Managed Services sicher in die digitale Zukunft. Die Gruppe verfügt über mehr als 20 Jahre Erfahrung in der Planung, der Umsetzung und dem Betrieb von Microsoft-Plattformen. Sie betreut bereits mehr als 250.000 Anwender der Cloud-Plattformen Microsoft 365 und Azure. Die abtis Gruppe ist Mitglied der Microsoft Intelligent Security Association (MISA), Fokuspartner von Microsoft für den Mittelstand und Gewinner des Microsoft Accelerate Innovation Awards 2023. Dabei deckt abtis alle Lösungsbereiche von Microsoft ab: von Modern Work über Security, Business Applications, Infrastructure (Azure), Digital & App Innovation (Azure) bis hin zu Data & AI (Azure).

abtis Holding AG • Wilhelm-Becker-Straße 11b • 75179 Pforzheim



Nehmen Sie Kontakt mit uns auf.

 www.abtis.de

 +49 7231 4431 - 100

 vertrieb@abtis.de

Genderhinweis: Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

© 2026 **Alle Rechte vorbehalten.** Dieses Dokument ist urheberrechtlich geschützt. Sämtliche Inhalte dienen der Dokumentation. Jede andere Nutzung, insbesondere die Weitergabe an Dritte, die Verbreitung oder die Bearbeitung, auch in Teilen, ist ohne schriftliche Einwilligung der abtis Holding AG untersagt. Die verwendeten Firmen-, Marken- und Produktnamen und Warenzeichen sind eingetragene Markenzeichen oder Warenzeichen der jeweiligen Inhaber und werden hiermit anerkannt.