Risikomatrix: Risikoblindheit per Design

Ampel im Nebel

15. Januar 2026, 10:46
Frank Romeike [RiskNET]

Freitagmorgen, 06:20 Uhr: In der Leitwarte eines Industrieunternehmens blinkt eine rote Meldung auf. Nicht in der Produktion – zunächst nur in der IT. Der zentrale Identitätsdienst (Single Sign-on) ist ausgefallen, kurz darauf folgen Zugriffsprobleme im ERP und im MES. Binnen einer Stunde steht die Fertigung still, weil Auftragsdaten, Stücklisten und Freigaben nicht mehr verlässlich verfügbar sind. Der Schaden wächst im Minutentakt: Stillstandskosten, Vertragsstrafen, Expresslogistik, Überstunden, Kundenkommunikation – und eine Frage, die spätestens am Nachmittag im Vorstand landet: Wie konnte das passieren?

Der Vorfall lässt sich später auf eine scheinbar unspektakuläre Kette zurückführen: Eine Fehlkonfiguration in einer Cloud-*Policy*, kombiniert mit einem gestohlenen Admin-Token und einem automatisierten Angriffsskript. Ein Ereignis, das im jährlichen *Risiko*- Workshop als "selten" eingestuft wurde – und dessen Auswirkung man zwar als "existenzbedrohend" diskutierte, das aber in der Risikomatrix am Ende trotzdem bei "mittel" landete. Das Management beruhigte sich: "Mittel heißt: Wir haben alles im Griff."

Genau hier beginnt das Problem. In modernen, hochvernetzten IT-Infrastrukturen sind es gerade die seltenen, aber extrem teuren Ereignisse – die "fat tail"-Szenarien – die den Großteil des Gesamtrisikos tragen. Eine qualitative Matrix kann diese Realität in großen Umgebungen mit zehntausenden bis hunderttausenden Assets kaum noch abbilden. Sie komprimiert *Komplexität* zu einer Ampel – und macht damit aus einem existenziellen Thema eine scheinbar kontrollierbare Kategorie.

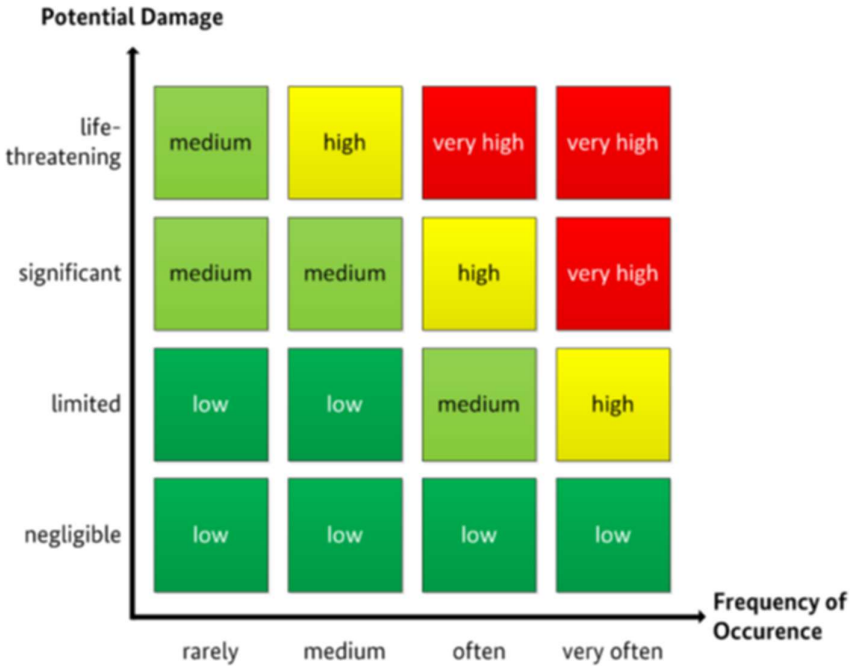

Abb. 01: Risikomatrix nach BSI-Standard 200-3 (Eintrittshäufigkeit vs. Schadensauswirkung).

Problematisch ist die Einordnung "selten" + "existenzbedrohend" als "mittel" – ein typisches Muster bei seltenen, aber katastrophalen IT- und Cyberereignissen [Quelle: BSI (2017): BSI-Standard 200-3 - Risk Analysis based on IT-Grundschutz, Bonn 2017].

Der BSI-Standard 200-3 (Risikoanalyse auf Basis von IT-Grundschutz, siehe Abb. 01) hat in vielen Organisationen seine Berechtigung: Er schafft Struktur, gemeinsame Begriffe und eine auditierbare Dokumentation. Doch sobald IT-Landschaften hochdynamisch werden – Cloud, Microservices, Infrastructure as Code, Multi-Provider, 24/7-DevOps – stößt ein überwiegend qualitativer Bewertungsansatz an harte Grenzen. Die folgenden zehn Punkte ordnen die Grenzen kritisch ein – mit Blick auf große Infrastrukturen mit 100.000 Assets und mehr.

Skalierungsproblem: Asset-zentrierte Qualifizierung kollidiert mit IT-*Komplexität* und -Dynamik

Der klassische Einstieg vieler 200-3-Projekte lautet sinngemäß: "Wir kennen unsere Assets, wir kennen ihren Schutzbedarf, wir bewerten Risiken je Asset oder je Systemgruppe." Genau diese Logik bricht, sobald Infrastruktur nicht mehr aus einigen hundert Servern besteht, sondern aus zehntausenden virtuellen Ressourcen, Containern, Funktionen, Identitäten, API-Endpunkten, SaaS-Integrationen und Drittanbieter-Abhängigkeiten. In Cloud-Umgebungen sind Assets zudem flüchtig. Autoscaling erzeugt Instanzen für Minuten, Container werden im Sekundenbereich ersetzt, Serverless-Funktionen existieren als Konfiguration – nicht als "Server", den man inventarisieren könnte. Ein qualitatives, assetbasiertes Bewertungsmodell gerät hier in ein permanentes Hinterherlaufen: Der Aufwand steigt exponentiell, der Aktualitätsgrad sinkt linear.

Das Resultat ist eine riskante Illusion von Vollständigkeit. Formal wirkt das *Risikoinventar* sauber – faktisch wird es zum Schnappschuss einer Landschaft, die sich täglich ändert. In der Praxis entstehen dann typische Workarounds: man bewertet "Cluster", "Plattformen" oder "Anwendungen" pauschal. Das reduziert *Komplexität* – aber es verwischt genau die technischen Unterschiede, die für Eintrittswege und Auswirkungsmechanismen entscheidend sind. Zugespitzt: In einer Organisation mit

100.000 Assets und mehr kann eine Risikomatrix schnell zum "Wetterbericht von gestern" werden: gut formatiert, gut gemeint – aber für die operative Steuerung zu spät, risikoblind und zu grob.

Hoher Subjektivitätsgrad: Wenn *Risiko*-Kategorien mehr über Workshop-Dynamik als über Realität aussagen

Qualitative Einstufungen leben von Experteneinschätzungen. Das ist nicht per se falsch: Auch quantitative Modelle beginnen mit Annahmen. Der Unterschied liegt in der Disziplin der *Kalibrierung*. In vielen 200-3-Workshops werden Eintrittshäufigkeiten und Schadensauswirkungen als Begriffe diskutiert – ohne ein gemeinsames, numerisch hinterlegtes Verständnis. Siehe hierzu vertiefend den Beitrag "Grenzen einer qualitativen Bewertung".

Was bedeutet "selten"? Einmal in zehn Jahren? Einmal in 30 Jahren? Oder "hatten wir noch nicht"? Und was heißt "beträchtlich" – gemessen am EBIT, an der Liquidität, an der Produktionskapazität oder an regulatorischen Sanktionen? Ohne eine Operationalisierung sind Kategorien anfällig für psychologische Verzerrungen: Recency Bias (was gerade passiert ist), Availability Bias (was man sich leicht vorstellen kann), und – in großen Organisationen besonders verbreitet – politische Biases (welches *Risiko* heute Aufmerksamkeit bekommt). Das führt zu einem paradoxen Zustand: Je reifer ein Unternehmen organisatorisch ist, desto glatter werden die Bewertungsprozesse – und desto stärker verstecken sich Unsicherheiten hinter vermeintlich objektiven Begriffen. Wenn drei Teams denselben Szenario-Text lesen, entstehen oft drei unterschiedliche Matrix-Felder. Nicht weil jemand "falsch" liegt, sondern weil das Instrument die nötige Präzision nicht erzwingt.

Der Standard schafft hier methodische Leitplanken, aber er kann die grundlegende Subjektivität des qualitativen Ratings nicht auflösen – besonders nicht bei komplexen, seltenen Ereignissen, für die es intern kaum Erfahrungswerte gibt.

Fehlende belastbare Priorisierung: Wenn "hoch" zu häufig vorkommt, verliert es seine Steuerungswirkung

In großen IT-Landschaften existieren nicht zehn Risiken, sondern hunderte bis tausende relevante Szenarien – von Identitätsmissbrauch über API-Fehlkonfigurationen bis hin zu Lieferkettenrisiken und Cloud-Konzentrationsrisiken. Ein qualitatives System komprimiert diese Vielfalt auf wenige Kategorien. Das Ergebnis ist vorhersehbar: Viele Risiken landen in den oberen Klassen, weil die IT verständlicherweise lieber vorsichtig bewertet. Doch eine Priorisierung, die am Ende 40 "hohe" Risiken ausweist, ist keine Priorisierung mehr. Sie führt entweder zu Aktionismus ("Wir müssen alles gleichzeitig tun") oder zu Resignation ("Dann ist eben alles hoch"). Beides ist für Steuerung und Budgetierung fatal.

Gerade in Zeiten knapper Ressourcen benötigt das Management keine Ampel, sondern eine Rangliste mit Hebelwirkung: Wo reduziert ein Euro Sicherheitsinvestition den erwarteten oder den worst-case Schaden am stärksten? Ohne quantitative Ankerpunkte bleibt die Entscheidung häufig in der politischen Logik: Das sichtbarste *Risiko* gewinnt, nicht das teuerste. Die Risikomatrix ist hier wie ein grober Stadtplan für einen Flughafen: Sie zeigt, dass es Wege gibt, aber nicht, welcher Weg heute der schnellste ist.

Fehlende Aggregierbarkeit: Qualitative Bewertungen lassen sich kaum zu einer belastbaren Gesamtrisikoposition verdichten

Unternehmenssteuerung arbeitet mit Summen, Bandbreiten und Tragfähigkeiten: Wie groß ist das Gesamtrisiko? Welche Risikokonzentrationen bestehen? Welche Reserven brauchen wir? Diese Fragen verlangen Aggregation über Szenarien hinweg.

Qualitative Kategorien sind dafür nur begrenzt geeignet. Zwei "mittlere" Risiken ergeben nicht automatisch ein "hohes" *Risiko*, und zehn "geringe" Risiken können unter Umständen eine relevante Gesamtexponierung darstellen – etwa wenn sie alle denselben Engpass treffen (z. B. Identity Provider, Netzwerk-Kern, Cloud-Region). Ohne eine gemeinsame Skala für Verlustgrößen und Frequenzen bleibt Aggregation ein Pseudo-Rechnen: Man zählt Ampelfarben oder vergibt Punkte. Das kann für Kommunikation hilfreich sein, erzeugt aber keine belastbaren Kennzahlen für Risikotragfähigkeit, *Risikokapital* oder Entscheidungsvorlagen. Gerade dort, wo Governance und Prüfung steigen – etwa bei Vorstandsreportings oder integrierten ERM-Prozessen – wirkt ein rein qualitatives IT-Risikoportfolio wie ein Fremdkörper: Es liefert Zustandsbeschreibungen, aber keine finanzielle Risikosicht.

Rechtlich wird diese fehlende Aggregierbarkeit zum *Risiko*: Das deutsche Rechtssystem verlangt ein Überwachungssystem zur frühzeitigen Erkennung bestandsgefährdender Entwicklungen (z.B. § 91 Abs. 2 AktG und § 1 *StaRUG*), und der Vorstand muss Risiken angemessen steuern (§ 93 AktG). In der Prüfungspraxis (u.a. *IDW PS 340* n.F.) wird damit zunehmend relevant, ob ein Risiko-früherkennungssystem nicht nur Risiken katalogisiert, sondern deren Tragweite für Fortbestand, Liquidität und Risikotragfähigkeit nachvollziehbar macht. Eine reine Ampel- bzw. Matrixlogik liefert jedoch weder eine konsolidierte Gesamtrisikoposition noch quantifizierte Bandbreiten für Verlusthöhen und Eintrittsraten. Damit fehlen belastbare Grundlagen für prüfungsfeste Vorstands- und Aufsichtsratsentscheidungen – etwa zur Priorisierung von Maßnahmen, zur Dimensionierung von Risikopuffern/Versicherungslimits oder zur Absicherung von Going-Concern-Annahmen im Abschluss.

Unzureichend für Ketten- und Kaskadeneffekte: Moderne IT-Risiken sind Netzwerkphänomene, keine Einzelfälle

Viele der heute kritischsten IT-Risiken entstehen nicht durch ein einzelnes Systemversagen, sondern durch Kaskaden: Ein Identitätsvorfall führt zu "lateral movement", ein API-Schlüssel öffnet eine Datenpipeline, ein Ausfall im Cloud-Backbone trifft mehrere Anwendungen gleichzeitig.

Risikomatrizen sind jedoch typischerweise zweidimensional: Eintrittshäufigkeit und Auswirkung. Abhängigkeiten werden zwar textlich beschrieben, aber selten konsequent modelliert. In großen Umgebungen ist das ein Kernproblem, weil "Auswirkung" weniger eine Eigenschaft eines Assets ist als eine Eigenschaft des gesamten Wertstroms. Ein Beispiel: Ein ERP-Ausfall ist in sich schon relevant. Existenzbedrohlich wird er, wenn er in eine Phase hoher Auslastung fällt, wenn parallel eine Supply-Chain-Störung besteht, oder wenn regulatorische Meldefristen nicht eingehalten werden. Das *Risiko* entsteht aus der Kopplung – nicht aus dem Asset.

In der Praxis zeigen gerade kritische Abhängigkeiten eine unangenehme Dynamik: Sie wachsen unbemerkt. Jede neue Schnittstelle, jede neue SaaS-Integration, jede neue Automatisierung erhöht die Vernetzung. Ein qualitatives Verfahren kann diese Netzwerkeffekte beschreiben, aber es kann sie kaum gewichten – und damit auch kaum steuern.

Fat Tails und Extremereignisse: Warum die Matrix das existenzbedrohende *Risiko* als "mittel" tarnt

Die IT-Risikowelt ist geprägt von Verteilungen mit "fetten Schwänzen" (fat tails): Viele Ereignisse sind klein oder moderat, einige wenige Ereignisse sind extrem – und diese wenigen dominieren die Gesamtschadenssumme. Das ist ein bekanntes Muster aus der Praxis von Cyber-Schäden, Großausfällen und Lieferkettenvorfällen: Nicht die typische Störung ist das Problem, sondern das seltene Eskalationsszenario. Genau diese Struktur kollidiert mit der Logik vieler Risikomatrizen. Abb. 01 zeigt es plastisch: "existenzbedrohend" kombiniert mit "selten" wird als "mittel" klassifiziert. Das wirkt auf den ersten Blick plausibel – denn die Matrix "belohnt" die geringe Eintrittshäufigkeit. Für fat-tail-getriebene Risiken ist das jedoch gefährlich, weil die Steuerungslogik kippt: Selten heißt nicht

harmlos; selten heißt oft nur: schlecht beobachtbar, schwer prognostizierbar, aber potenziell katastrophal.

Warum ist die Verzerrung so gravierend? Weil qualitative Kategorien implizit auf eine "typische" Welt verweisen. Sie bilden eher den Median ab: Was passiert in einem normalen Jahr? Fat-*tail-Risiken* fragen dagegen: Was passiert im schlechten Jahr – und wie überlebt das Unternehmen dann? Für existenzielle Fragestellungen zählt nicht die Häufigkeit des Normalfalls, sondern die Robustheit gegenüber Ausreißern. Praxisbeispiele für fat-tail-Szenarien sind zahlreich: Ransomware mit Domänen- und Backup-Komprimierung, kompromittierte Software-Lieferketten, großflächige Cloud-Region-Ausfälle, Fehler in zentralen Identity- oder Netzwerkkomponenten oder auch kombinierte Vorfälle (Incident + *Compliance* + Kommunikationskrise). Diese Ereignisse sind selten – aber wenn sie eintreten, entfalten sie eine nichtlineare Wirkung: Tage werden zu Wochen, IT wird zu Produktion, Störung wird zu Ergebniskrise. Kurz gesagt: In der Risikomatrix werden fat-*tail-Risiken* systematisch unterschätzt. Dies kann gravierend Auswirkungen auf die Existenz einer Organisation haben.

Dynamische Bedrohungslage: Jahreszyklen und statische Klassen passen nicht zu permanenten Veränderungen

Zwischen zwei jährlichen *Risiko*- Reviews kann sich die Bedrohungslage fundamental ändern: neue Exploit-Ketten, neue Angriffstaktiken, neue Abhängigkeiten, neue Cloud-Services. Auch die interne Landschaft verändert sich: Releases, Migrationen, Berechtigungen, neue Schnittstellen. In DevOps-Organisationen ist Veränderung nicht Ausnahme, sondern Normalzustand.

Qualitative Bewertungen sind oft an Workshop- und Auditzyklen gebunden. Das ist verständlich – aber es erzeugt eine gefährliche Trägheit: Risiken werden dokumentiert, während Systeme sich weiterentwickeln. Die eigentliche Risikolage ist dann in Bewegung, die Bewertung bleibt stehen. In komplexen Umgebungen ist deshalb weniger die einmalige Bewertung entscheidend, sondern die Fähigkeit zur kontinuierlichen Messung: Wie viele kritische Fehlkonfigurationen existieren gerade? Wie schnell werden Patches ausgerollt? Wie viele privilegierte Identitäten sind aktiv? Solche Metriken sind nicht der Ersatz für Risikobewertung, aber sie sind das Frühwarnsystem. Ein rein qualitatives Verfahren integriert diese Operationalisierung oft nur begrenzt. Wer aus der IT verursachte Risikoszenarien heute steuern will, muss die Taktfrequenz erhöhen: von "jährlich bewerten" zu "laufend beobachten, regelmäßig nachkalibrieren".

Im Kontext einer dynamischen Bedrohungslage reicht ein periodisches "*Risiko*-Update" nicht aus: § 1 *StaRUG* verpflichtet die Geschäftsleitung, fortlaufend über Entwicklungen zu wachen, die den Fortbestand der juristischen Person gefährden können, und bei erkannten Gefährdungen unverzüglich geeignete Gegenmaßnahmen einzuleiten – praktisch bedeutet das ein permanentes Monitoring und eine laufende Analyse kritischer Frühwarnindikatoren (z. B. sicherheitsrelevante Störungen, Ausfallhäufungen, Control-Drift, signifikante Exposure-Änderungen in Cloud/Third Parties) statt einer rein statischen Einstufung in einer Risikomatrix.

Schwache Entscheidungsunterstützung für Investitionen: Ohne Euro-Wirkung bleibt Security-Budget nebulös

Vorstände und CFOs stellen inzwischen sehr konkrete Fragen: Welcher Sicherheitshebel bringt den größten Effekt? Was kostet das Restrisiko? Wie verändert sich die Verlustexponierung, wenn wir Zero Trust einführen, Backup-Architekturen härten oder Identity Governance ausbauen? Qualitative Kategorien geben darauf selten eine belastbare Antwort. Sie sagen: "Das *Risiko* ist hoch." Aber sie sagen nicht: "Dieses *Risiko* kostet uns im *Erwartungswert* X pro Jahr, und Maßnahme Y reduziert es um

Z." Das ist ein entscheidender Unterschied – nicht nur für Budgets, sondern auch für die strategische Planung und für das Verständnis von *Risikoappetit*.

Genau hier liegt die Übersetzungsarbeit: CISOs werden von CEO und CFO meist erst dann gehört, wenn sie aus der IT resultierend Risikoszenarien in einer Finanzsprache ausdrücken – als erwarteter Jahresverlust, Bandbreiten potenzieller Schäden oder als messbarer Mehrwert einer Maßnahme. Trend Micro diagnostiziert in einer weltweiten Studie aus dem Jahr 2024 eine anhaltende Kommunikationslücke: Nur 54% der befragten Security-Leader sind überzeugt, dass die C-Suite die Cyberrisiken vollständig versteht; zugleich berichten 46%, dass die Messung des Business Value ihrer Security-Strategie ihre Glaubwürdigkeit im Board erhöht. (Trend Micro, 2024: IT Security Leaders Are Failing to Close a Boardroom Credibility Gap).

In großen Umgebungen geraten Programme ohne quantitative Steuerung schnell in eine paradoxe Lage: Die besten technischen Maßnahmen konkurrieren mit den sichtbarsten Projekten. Ein Security-Programm wird dann eher nach *Compliance*- Lücken oder Auditergebnissen priorisiert – nicht nach risikogewichteter Wirkung. Wer Security als Business-Thema behandeln will, braucht zumindest für die wichtigsten Szenarien eine Übersetzung in wirtschaftliche Größen. Die qualitative Matrix ist hierfür ein Einstieg – aber nicht der Zielzustand.

Nachvollziehbare Szenarien für Versicherungen, Aufsicht und Prüfung: Die Welt fragt nach Szenarien und Zahlen

Cyber- Versicherer, Wirtschaftsprüfer und Regulatorik entwickeln sich in Richtung stärkerer Nachvollziehbarkeit: nicht nur "haben Sie Kontrollen?", sondern "welches Verlustpotenzial tragen Sie – und wie begrenzen Sie es?" Auch Vorgaben wie NIS2 bzw. *DORA* oder branchenspezifische Aufsichten erhöhen den Druck auf belastbare Szenarioanalysen, Resilienztests und Reporting.

In dieser Welt wirkt eine Ampelbewertung schnell zu grob. Sie kann zeigen, dass man sich Gedanken gemacht hat – aber sie zeigt selten, wie robust die Organisation gegenüber Extremereignissen ist. Gerade bei fat-tail-Szenarien reicht "mittel" als Ergebnis nicht aus, wenn das Szenario im Ernstfall die Liquidität oder die Lieferfähigkeit gefährdet. Zudem steigt die Erwartung, dass Risiken in Zusammenhang mit Unternehmenskennzahlen diskutiert werden: Recovery-Zeiten, Ausfallkosten, Vertragsrisiken, Meldepflichten, Haftungsfragen. Qualitative Verfahren können diese Dimensionen aufnehmen – aber sie liefern sie oft nicht in einer Form, die externen Stakeholdern als Entscheidungsgrundlage genügt. Das Ergebnis ist häufig ein Nebeneinander: Für *Audit* und IT-Grundschutz existiert die qualitative Dokumentation, für Aufsicht und Management werden zusätzliche, meist ad-hoc Szenariopapiere erstellt. Effizienter wäre ein integrierter Ansatz.

Vom *Compliance*-Instrument zur risikobasierten Steuerung: Wie ein quantitativer Ansatz aussehen kann

IT- Grundschutz und der BSI-Standard 200-3 sind in vielen Organisationen der sichere Hafen: ein gemeinsames Vokabular, eine strukturierte Vorgehenslogik, eine kontrollorientierte Baseline. Genau dort liegt aber auch die zentrale Schwäche, wenn sie als primäres Steuerungsinstrument missverstanden werden. In hyperskaligen IT- und Cloud-Landschaften entsteht eine gefährliche Verwechslung: Kontrollabdeckung wird mit Risikoreduktion gleichgesetzt, Dokumentation mit Steuerbarkeit.

Der Grundschutz denkt von IT-Assets her – sinnvoll für Standardrisiken und *Audit*- Nachweise, aber zu grob für die Frage, die Vorstand, CFO, Behördenleiter oder CISO in Zeiten knapper Ressourcen beantworten müssen: Welche wenigen Entscheidungen senken das Gesamtrisiko nachweisbar am

stärksten? Eine qualitative Matrix kann hier kaum liefern. Sie ordnet, aber sie priorisiert weder methodisch fundiert noch robust. Sie macht vor allem die fat-tail-getriebenen Extremrisiken klein, weil seltene Ereignisse im Raster systematisch zu "mittel" zusammenfallen. Quantitative Verfahren setzen genau an dieser Stelle an: Sie behandeln *Risiko* nicht als Farbfeld, sondern als Verlustverteilung. Statt eine Eintrittshäufigkeit grob zu schätzen, werden Treiber explizit modelliert (z. B. Frequenz von Threat Events, Erfolgswahrscheinlichkeit, Detektions- und Reaktionszeiten, Recovery-Dauern, Abhängigkeiten zu Identität, Cloud-Regionen und kritischen Dienstleistern). Statt "hoch" oder "mittel" entsteht eine Bandbreite: erwarteter Jahresverlust, 90/95/99-Perzentile, Worst-Case-Szenarien – und damit eine Sprache, die in Finanz- und Budgetprozessen anschlussfähig ist.

Besonders entscheidungsrelevant wird Quantifizierung, wenn sie mit Sensitivitätsanalysen kombiniert wird. Tornado- oder Treiberanalysen zeigen, welche Parameter die Verlustverteilung dominieren: Ist es die Häufigkeit von Privilege-Compromise, die Zeit bis zur Isolation, die Wiederanlaufzeit von ERP/MES oder die Abhängigkeit von einem einzigen Identitätsdienst? So wird aus "wir brauchen mehr Security" eine priorisierte Liste: die zwei bis drei Stellhebel, die pro investiertem Euro die größte Reduktion im Tail bewirken.

Ein quantitativer Ergänzungsrahmen ist damit kein akademischer Luxus, sondern ein Entscheidungswerkzeug:

- Er macht "fat tails" sichtbar, statt sie in Klassen zu verwischen – inklusive der Frage, mit welcher Wahrscheinlichkeit existenzbedrohende Verluste eintreten.
- Er erlaubt Maßnahmenpriorisierung nach Wirkung: Welche Kontrolle reduziert Frequenz, welche senkt Verlusthöhe, welche verkürzt Recovery – und wie stark verschiebt sich dadurch die Verlustverteilung?
- Er unterstützt Sensitivitätsanalysen: Wo sind die größten Hebel (z. B. privilegierte Identitäten, Backup-Resilienz, Segmentierung, Cloud-*Policy*-Governance) und wo sind Investitionen nur kosmetisch?
- Er liefert eine Finanzsprache für Entscheidungen: erwartete Ausfallkosten, Bandbreiten, *Risiko*-Reduktion pro Maßnahme – statt triviale Ampelfarben.

In der Praxis lässt sich das mit etablierten Ansätzen umsetzen: Das FAIR-Modell (Factor Analysis of Information Risk) trennt *Risiko* explizit in Frequenz und Verlusthöhe und zerlegt beide in nachvollziehbare Faktoren; häufig ergänzt durch stochastische Simulationen, um Unsicherheit als Bandbreite zu modellieren. ISO 27005 bietet den Rahmen für Informationssicherheits-*Risikomanagement*, NIST liefert starke Perspektiven auf Controls und Resilienz – entscheidend ist jedoch das Prinzip: Die Top-Szenarien werden so quantifiziert, dass Budget- und Maßnahmenentscheidungen überprüfbar werden.

Fazit: Risikoszenarien transparent machen

Im Eingangsszenario – Fehlkonfiguration in einer Cloud-*Policy*, gestohlener Admin-Token, automatisiertes Skript, und wenige Minuten später stehen ERP, MES und Fertigung – hätte ein quantitativer Ansatz genau das sichtbar gemacht, was die Matrix kaschiert: nicht nur "selten", sondern eine relevante Wahrscheinlichkeit für einen mehrtägigen Produktionsstillstand mit starkem Ausreißerpotenzial. Eine Treiber- und Sensitivitätsanalyse hätte zudem gezeigt, dass die größten Hebel nicht in weiteren Checklisten liegen, sondern in der Absicherung privilegierter Identitäten (PAM/MFA/Conditional Access), in *policy*- as-code mit kontinuierlichen Guardrails, in schneller Isolation sowie in getesteter Wiederanlauffähigkeit (Backups, Restore-Übungen). Mit diesen

Maßnahmen wären sowohl erwarteter Verlust als auch *Tail-Risiko* messbar gesunken – und "mittel" wäre nicht zum Synonym für "wir haben es unterschätzt" geworden.