WHITEPAPER

Business Continuity Management

Resilienz als Führungsentscheidung

Warum Wiederanlaufziele allein nicht genügen

Carsten Beck
Cybersecurity Auditor | ISO/IEC 27001 & ISO 22301 Lead Auditor
MAS Information Systems Management
Oktober 2026 · Version 1.0

Executive Briefing

Resilienz wird häufig über die Fähigkeit zur schnellen Wiederherstellung betrachtet. Die tatsächlich erreichte Wiederanlaufzeit ist jedoch das Ergebnis früherer Entscheide: welche Leistungen Vorrang haben, welche Vorkehrungen getroffen und welche Mittel dafür bereitgestellt wurden. Vorgelagert ist deshalb eine andere Frage: Welches Ausmass und welche Dauer einer Unterbrechung akzeptiert die Organisation, und wer entscheidet das?

Die bisherigen Whitepaper-Beiträge dieser Reihe zu Outsourcing, Audit und KI-Governance haben gezeigt, dass Verantwortung auch bei Auslagerungen intern bleibt und dass Anforderungen erst dann belastbar sind, wenn ihre Wirksamkeit nachgewiesen ist. Im Business Continuity Management (BCM) zeigt sich diese Logik besonders deutlich. Am Anfang steht ein Führungsentscheid, die Unterbrechungstoleranz: wie lange und in welchem Ausmass eine Leistung ausfallen darf. Die daraus abgeleiteten Anforderungen werden über Anwendungen und Infrastruktur bis zum Dienstleister nach unten vererbt. Diese Vererbungskette hat eine Gegenrichtung, den Rückweg. Auf ihm wird zunächst abgeglichen, ob die Zusagen zu den Anforderungen passen, und dann nachgewiesen, dass sie tatsächlich erfüllt werden, etwa durch Tests und Übungen. Ohne diesen Rückweg bleibt ein Wiederanlaufziel eine Absichtserklärung, auch wenn es genehmigt ist.

Leistungen hängen heute an gemeinsamen Plattformen und Dienstleistern, und gezielte Cyberangriffe suchen genau solche Knotenpunkte. Umso schwerer wiegt, dass der Rückweg typischerweise an drei Stellen bricht: an der Grenze zum Dienstleister, zwischen Kontinuitätsmanagement und Informationssicherheit und an der Annahme, dass ein System isoliert ausfällt und die übrige Umgebung intakt bleibt.

Der Rückweg ist damit notwendig, aber nicht hinreichend: Gelingt ein solcher Angriff, reicht auch ein nachgewiesenes Wiederanlaufziel nicht mehr aus. Solange unklar ist, ob die Angreifer noch Zugriff auf die Systeme haben, wird der Wiederanlauf zur Abwägung: Ein früher Wiederanlauf riskiert, ihnen den Zugriff zurückzugeben, ein später setzt einen Notbetrieb voraus, der so lange trägt. Diese Abwägung ist ein Geschäftsentscheid und selten vorbereitet. Fehlt der Notbetrieb, entscheidet der Druck.

Dieses Papier beschreibt, welche Entscheide und Nachweise nötig sind, damit Wiederanlaufziele tragen und die Organisation im Ereignisfall entscheidungsfähig bleibt. Die Methodik, mit der sie erarbeitet werden, setzt es voraus. Es richtet sich an Leitungs- und Aufsichtsgremien sowie an Verantwortliche in Business Continuity, Risiko, IT, Informationssicherheit, Beschaffung und Compliance. Kapitel 7 enthält Leitfragen für Leitungs- und Aufsichtsgremien, die Kapitel 3 bis 6 enthalten konkrete Prüfnachweise.

1 Ausgangslage: ein verschobenes Schadensbild

Kontinuitätsplanung orientiert sich in vielen Organisationen noch immer an klar begrenzten Störungen: Brand, Stromunterbruch, der Ausfall eines einzelnen Systems oder eines Standorts. Solche Ereignisse treffen einen abgrenzbaren Teil der Organisation, die Ursache ist bekannt, und die übrige Umgebung bleibt intakt. Die Wiederherstellung ist dann ein technisches Verfahren mit einem definierten Ziel.

Die schweren Ereignisse der letzten Jahre folgen einem anderen Muster. Sie erfassen mehrere Systeme, Standorte und oft auch Organisationsgrenzen zugleich, und auch die Wiederherstellungsfähigkeit selbst ist beeinträchtigt: Datensicherungen können kompromittiert sein und müssen vor dem Einspielen geprüft werden, zentrale Verzeichnis- und Identitätsdienste müssen neu aufgebaut werden, bevor anderes starten kann, und die Zielumgebung gilt als unsicher, bis das Gegenteil belegt ist. Wiederherstellen setzt damit Erkenntnisse voraus, die zum Zeitpunkt der Entscheidung nicht vollständig vorliegen.

Eine zweite Verschiebung betrifft die Zuständigkeit. Wo Leistungen ausgelagert sind, liegt die Wiederherstellung bei einer fremden Krisenorganisation, die meist gleichzeitig andere Kunden bedient und nach eigenen Prioritäten arbeitet. Die auslagernde Organisation erfährt den Fortschritt, statt ihn zu steuern. Ihre Wiederanlaufziele werden dann zu Anforderungen an einen Dienstleister, der sie nicht genehmigt hat und nur so weit kennt, wie sie vertraglich vereinbart sind.

Eine dritte Verschiebung betrifft die Ursache. Der Nachrichtendienst des Bundes (NDB) hält in seinem Lagebericht 2026 fest, dass die hybride Konfliktführung gegenüber Europa aggressiver wird und die Schweiz davon direkt betroffen ist, unter anderem durch Cyberangriffe. Hinzu kommen Ransomware-Angriffe auf kritische Infrastrukturen in der Schweiz. Nach Einschätzung des NDB ereignen sie sich ein- bis zweimal pro Monat und können den Betrieb über längere Zeit unterbrechen. Wer mit Absicht angreift, trifft bevorzugt die Abhängigkeiten, an denen mehrere Leistungen gleichzeitig hängen. Damit wird die Annahme unabhängiger Einzelausfälle selbst zum Risiko.

Alle drei Verschiebungen zusammen verändern die Steuerungsfrage. Sie lautet nicht mehr, wie schnell wiederhergestellt wird, sondern wie lange eine Organisation ohne eine Leistung auskommt, welche Alternativen in dieser Zeit tragen und wer über den Wiederanlauf entscheidet. Dazu gehört, auf welchem reduzierten, aber noch akzeptablen Niveau eine Leistung weiterlaufen kann. Das sind Führungsfragen, keine Verfahrensfragen.

> **Normativer und regulatorischer Rahmen**
>
> Orientierung bietet ISO 22301. Die Norm beschreibt die Anforderungen an ein Business-Continuity-Managementsystem und weist die Verantwortung der obersten Leitung zu. Welche Gremien im Einzelnen entscheiden, überlässt sie der Organisation. Ergänzende Leitfäden sind ISO 22313 zur Anwendung, ISO/TS 22317 zur Business-Impact-Analyse und ISO/IEC 27031 zur IKT-Bereitschaft.
>
> Regulatorische Vorgaben wie das FINMA-Rundschreiben 2023/1 im Finanzsektor oder die Richtlinie über das Kontinuitätsmanagement Bund gehen hier weiter und benennen die zuständigen Gremien (Abschnitt 2.2). Für kritische Infrastrukturen bietet der Leitfaden des Bundesamts für Bevölkerungsschutz eine methodische Grundlage. Verbindliche Vorgaben zu Ausfallsicherheit und Störungsbehebung sind in Vorbereitung: Der Bundesrat hat das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) im Februar 2026 beauftragt, bis Ende 2026 die Eckwerte für entsprechende Gesetzesentwürfe zu erarbeiten.

Regulatorische Vorgaben behandeln diese Führungsfragen ausdrücklich als Entscheide. Sie fragen nicht nur, wie Systeme geschützt sind, sondern auch, wie lange eine Leistung ausfallen darf, und sie bestimmen die zuständigen Gremien. Den Entscheid selbst nehmen sie der Organisation nicht ab. Sie setzen einen Mindeststandard. Dieses Papier zieht die regulatorischen Vorgaben heran, weil sie die Zuständigkeiten am deutlichsten regeln. Ihre Logik lässt sich auf Organisationen ausserhalb ihres Geltungsbereichs übertragen.

2 Der Managementprozess und seine Entscheidpunkte

Die Entscheidgrundlage für die Frage, wie lange der Ausfall einer bestimmten Leistung tolerierbar ist, liefert die Business-Impact-Analyse. Sie geht top-down vor und beginnt bei den Geschäftsprozessen, nicht bei den Systemen. Damit ist sie fachlich getrieben und wird von den Fachbereichen erarbeitet. Für jeden Prozess bewertet sie nach festgelegten Kriterien, wie sich die Auswirkungen eines Ausfalls über die Zeit entwickeln und ab wann sie untragbar werden. Zudem erfasst sie, wovon der Prozess abhängt: Personal, Systeme, Standorte und Dienstleister. Am Ende stehen priorisierte Zeitziele und Mindestniveaus.

Fachlich getrieben heisst allerdings nicht, dass jeder Fachbereich seine Einstufung selbst festlegt, und auch eine saubere Analyse beantwortet eine Frage nicht von selbst: Was gilt als kritisch, und was hat im Ereignisfall Vorrang? Diese Festlegung bestimmt im Voraus, wer im Ernstfall bedient wird und wer nicht. Das ist ein Führungsentscheid.

2.1 Die ausbleibende Priorisierung

Stuft eine Business-Impact-Analyse nahezu alle Geschäftsprozesse als kritisch ein, ohne daraus unterschiedliche Zeitziele und eine belastbare Reihenfolge abzuleiten, hat die eigentliche Priorisierung nicht stattgefunden. Ein häufiger Grund liegt in der Perspektive: Wer den eigenen Prozess einstuft, bewertet naturgemäss die Bedeutung für den eigenen Bereich, nicht die Auswirkung auf die Organisation als Ganzes. So gilt als hochkritisch, was im Alltag unentbehrlich scheint, obwohl sein Ausfall tagelang ohne ernste Folgen bliebe.

Die Verzerrung wirkt auch in die Gegenrichtung. In der Praxis kommt es vor, dass ein Geschäftsprozess in der Business-Impact-Analyse als kritisch eingestuft wird, die zugehörige Anwendung in der Schutzbedarfsanalyse der Informationssicherheit aber als nicht BCM-relevant gilt. Der Grund ist selten fachlich. Erst in der Schutzbedarfsanalyse wird sichtbar, was die Einstufung bedeutet: ein hoher Schutzbedarf beim Schutzziel Verfügbarkeit und damit hohe Anforderungen an die Anwendung, etwa Redundanz, Wiederherstellungstests oder Notfallpläne. Diese erscheinen zu aufwendig. Das Urteil richtet sich dann nicht nach dem Geschäft, sondern nach dem Aufwand, der aus ihm folgt.

Beide Verzerrungen haben dieselbe Ursache, und sie liegt nicht bei den Prozessverantwortlichen, sondern im Verfahren. Aus Sicht der Beteiligten ist jede einzelne Einstufung folgerichtig. Ohne gemeinsamen Massstab und ohne Abgleich über die Bereiche hinweg entsteht daraus aber keine Priorisierung. Die Richtlinie über das Kontinuitätsmanagement Bund trennt genau hier sauber: Erfasst werden die Betriebsfunktionen in der Führungslinie, also durch die Vorgesetzten der einzelnen Organisationseinheiten. Die Kriterien für die Bewertung ihrer Kritikalität legt dagegen die Leitung der Verwaltungseinheit fest. Der Massstab kommt von oben, die Anwendung von unten. Die Berner Kantonsverwaltung geht einen Schritt weiter und setzt den Massstab absolut. Sie spricht von vitalen Leistungen und meint damit Leistungen, deren Ausfall spätestens nach sieben Tagen untragbare Auswirkungen für Bevölkerung, Wirtschaft, Regierung oder Rechtsstaatlichkeit hätte. Eine feste Schwelle mag methodisch angreifbar sein, weil sie für alle Leistungen denselben Massstab anlegt. Eine Wiederanlauffrist ist sie nicht: Für die einzelnen vitalen Leistungen gelten eigene Ziele. In der Praxis ist sie wirksam: Sie erzwingt eine Aussage darüber, was nicht vital ist.

Die Folge einer unterlassenen Priorisierung zeigt sich erst im Ereignis. Eine Liste, auf der alles kritisch ist, ordnet nichts. Sie liefert dem Krisenstab keine Reihenfolge, und die Reihenfolge entsteht dann unter Zeitdruck, aus dem Bauch und ohne Legitimation. Die Priorisierung ist damit nicht entfallen. Sie ist von der Leitung an die Krisensituation delegiert worden.

2.2 Welche Entscheide anstehen

Die Priorisierung ist nicht der einzige Entscheid, den Business Continuity Management von der Führung verlangt. Aus ISO 22301 lassen sich fünf Fragen ableiten, die sie beantworten muss.

- **Was ist kritisch, und wie lange darf es ausfallen?** Festzulegen ist, nach welchen Kriterien Leistungen als kritisch gelten und ab wann ein Ausfall untragbar wird. Daraus folgt, bis wann eine Leistung wieder verfügbar sein muss und welche Vorrang hat, wenn nicht alles gleichzeitig wiederhergestellt werden kann.
- **In welchem Umfang muss eine Leistung erbracht werden?** Eine Leistung muss im Ereignisfall nicht vollständig verfügbar sein. Festzulegen ist, welches Mindestniveau genügt. Erst damit wird ein Notbetrieb planbar.
- **Welche Kontinuitätsstrategie wird gewählt?** Meist gibt es mehrere Wege: rasch wiederherstellen, auf eine Ausweichlösung umstellen, reduziert weiterarbeiten oder vorübergehend verzichten. Entscheiden muss die Leitungsebene, die das Risiko trägt. Mit ihrer Wahl verantwortet sie auch die Wege, die sie verworfen hat, und die Mittel, die der gewählte Weg erfordert.
- **Wer darf den Ereignisfall ausrufen, und wer gibt den Wiederanlauf frei?** Es muss vorab feststehen, wer einen Vorfall beurteilt und die Notfallpläne in Kraft setzt und wer über die Rückkehr in den Normalbetrieb entscheidet: als Rollen mit klarer Befugnis, besetzt mit benannten Personen und einer Stellvertretung.
- **Was geschieht, wenn Übungen Lücken zeigen?** Übungen und Tests zeigen, ob die Vorkehrungen tragen, auch bei wichtigen Dienstleistern. Zeigen sich Lücken, muss die oberste Leitung entscheiden: zusätzliche Mittel bereitstellen, die Architektur ändern, einen Vertrag neu verhandeln oder, soweit vertretbar, das Ziel anpassen. Diesen Entscheid trifft sie in der Managementbewertung (Ziff. 9.3 der Norm), der regelmässigen Überprüfung des Business-Continuity-Managementsystems.

Wer diese Entscheide trifft, regelt die Norm nur teilweise. Für die ersten vier verlangt sie Festlegungen und zugewiesene Befugnisse, aber nicht, welche Leitungsebene entscheidet. Diese Lücke füllen regulatorische Vorgaben: Die FINMA weist die Genehmigung der kritischen Funktionen und ihrer Unterbrechungstoleranzen dem obersten Leitungsorgan zu, die Richtlinie über das Kontinuitätsmanagement Bund der Leitung der Verwaltungseinheit die Kritikalitätskriterien, die Umsetzungsstrategie und die Abnahme der Pläne. Nur für den fünften Entscheid sind Verfahren und Zuständigkeit schon in der Norm festgelegt: die Managementbewertung durch die oberste Leitung.

Wo die Entscheide in der Norm stehen, zeigt Abbildung 1. Dargestellt ist der Aufbau von ISO 22301. Die roten Punkte markieren die fünf Führungsentscheide, die gestrichelten Linien den Rückfluss von Ergebnissen an die Leitung.

Dabei wird ein Muster sichtbar. Die ersten vier Entscheide beschreibt die Norm im Kapitel zum Betrieb (Kapitel 8), nicht im Kapitel zur Führung (Kapitel 5). Dieses verlangt, dass die oberste Leitung Rollen, Verantwortlichkeiten und Befugnisse zuweist. Es legt aber nicht fest, wer über Kritikalität, Toleranz, Mindestniveau, Strategie und Aktivierung entscheidet. Der fünfte Entscheid fällt dagegen in der Managementbewertung (Ziff. 9.3), auf Grundlage der Bewertung der Fähigkeiten (Ziff. 8.6).

Auch für die übrigen Entscheide gibt es einen Weg zurück zur Leitung. Die Managementbewertung berücksichtigt unter anderem die Informationen aus Business-Impact-Analyse und Risikobeurteilung sowie die Bewertung der Fähigkeiten (Ziff. 8.6), und zu ihren Ergebnissen gehören Entscheide über Änderungen an Business-Impact-Analyse, Risikobeurteilung, Strategien, Lösungen und Plänen. Die Norm stellt damit sicher, dass die Leitung die Ergebnisse kennt und Änderungen beschliessen kann. Sie stellt nicht sicher, dass die Leitung ihre Entscheidverantwortung auch wahrnimmt. In der Praxis werden die Ergebnisse deshalb oft nur zur Kenntnis genommen, während die eigentlichen Festlegungen dort fallen, wo die Norm sie beschreibt: im Betrieb. Will die Führung sie selbst treffen, muss sie diese bewusst an sich ziehen.

Besonders der fünfte Entscheid bleibt in der Praxis oft aus, obwohl die Managementbewertung genau dafür vorgesehen ist: die Konsequenz, wenn Übungen Lücken zeigen (Abschnitt 6.1).

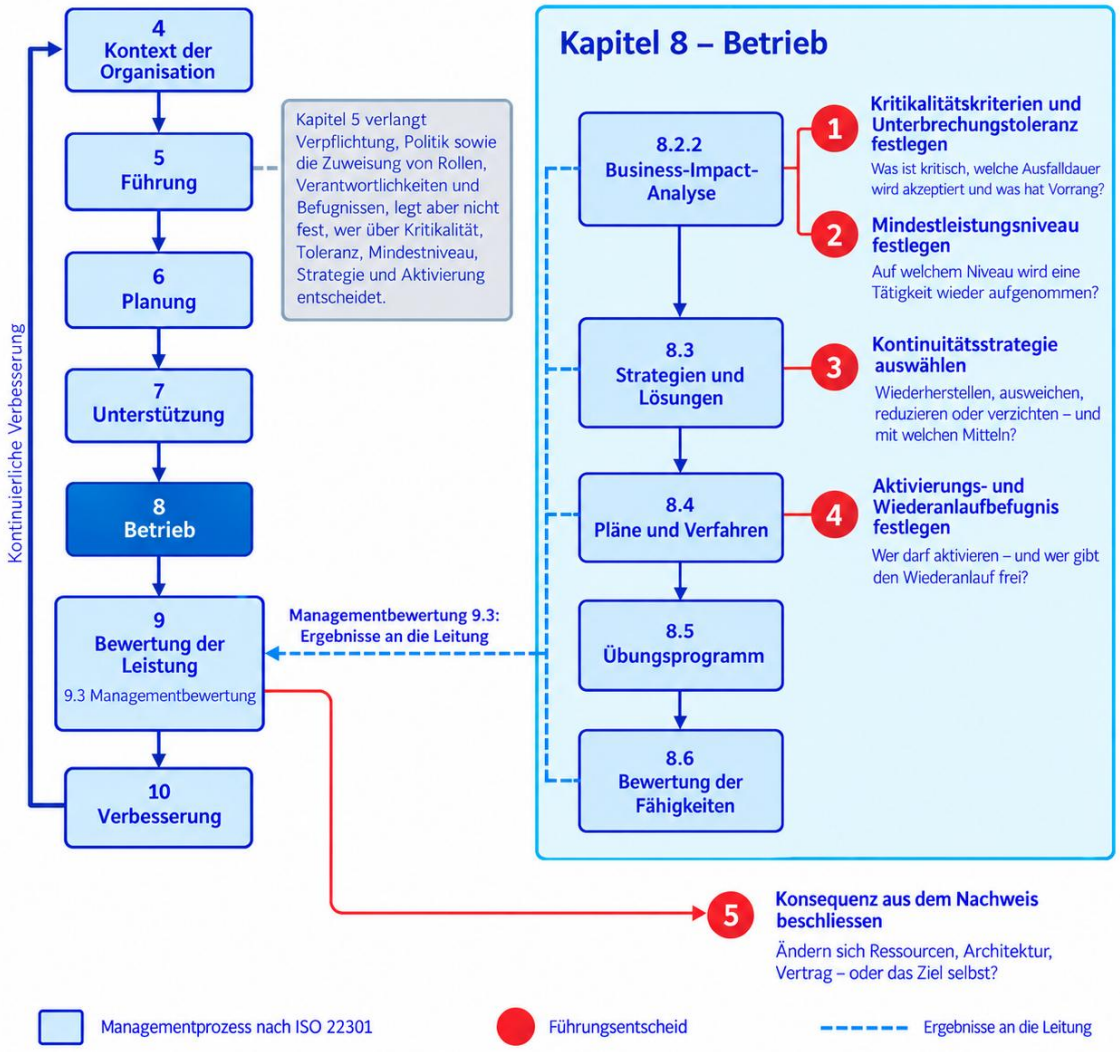


Abbildung 1: Der Managementprozess nach ISO 22301 und die fünf Führungsentscheide (eigene, vereinfachte Darstellung ohne Risikobeurteilung, Ziff. 8.2.3)

2.3 Von der Toleranz zum Nachweis

Wer über Unterbrechungstoleranzen entscheidet, muss die Grössen auseinanderhalten, mit denen sie beschrieben und umgesetzt werden. Der folgende Kasten fasst die wichtigsten Begriffe zusammen. Der Text zeigt anschliessend, wie sie zusammenhängen.

Begriffe und Abkürzungen

Maximal tolerierbare Unterbrechungsdauer (MTPD): Zeitspanne, nach der die Folgen einer Unterbrechung für die Organisation untragbar werden. Die Auswirkungen werden im Rahmen der Business-Impact-Analyse erhoben. Die Grenze, ab der sie untragbar werden, wird entschieden.

Unterbrechungstoleranz: Begriff der FINMA für das Ausmass der Unterbrechung einer kritischen Funktion, etwa Dauer oder erwarteter Schaden, das eine Organisation unter schwerwiegenden, aber plausiblen Szenarien zu akzeptieren bereit ist. Dieses Papier versteht darunter die von der Führung festgelegte Grenze. Sie wird über die MTPD und das Mindestleistungsniveau konkretisiert, ist aber nicht mit der MTPD gleichzusetzen. Wo nur die Zeitgrösse gemeint ist, steht «MTPD».

Mindestleistungsniveau (MBCO): Mindestumfang einer Leistung, der während einer Unterbrechung für die Organisation noch akzeptabel ist.

Wiederanlaufziel (RTO): Zeitraum, innerhalb dessen eine Tätigkeit nach einer Unterbrechung wieder auf dem Mindestleistungsniveau aufgenommen werden soll. Es liegt innerhalb der MTPD. Die technischen Wiederanlaufziele der Anwendungen und übrigen Ressourcen ergeben sich daraus und aus der gewählten Kontinuitätslösung.

Wiederherstellungspunkt (RPO): Maximal tolerierbarer Datenverlust, ausgedrückt als Zeitspanne. Er ist ein Zielwert. Der im Ereignis tatsächlich nutzbare Wiederherstellungspunkt kann weiter zurückliegen.

Erreichte Wiederanlaufzeit: In einem Test oder Ereignis tatsächlich gemessene Dauer bis zum Wiederanlauf. Erst sie belegt, ob das Wiederanlaufziel eingehalten wird, allerdings nur für das Szenario, den Umfang und die Messspanne, unter denen sie gemessen wurde.

Tragfähigkeit des Notbetriebs: Zeitspanne, während der ein Notbetrieb das Mindestleistungsniveau halten kann, bevor Belastung, Fehler und Rückführungslast ihn selbst zum grösseren Risiko machen. Sie begrenzt, wie spät die Wiederherstellung einschliesslich abhängiger Wiederanläufe und Datenabgleich abgeschlossen sein muss.

Leistung und Tätigkeit: «Leistung» bezeichnet, was die Organisation nach aussen erbringt, «Tätigkeit» die Arbeit im Geschäftsprozess, die sie trägt (im Sinn von ISO 22301). Die FINMA spricht von kritischen Funktionen, die Richtlinie des Bundes von Betriebsfunktionen.

«Dienstleister» und «Leistungserbringer» werden in diesem Papier gleichbedeutend verwendet und schliessen interne Leistungserbringer ein.

In der Praxis werden diese Grössen oft vermischt, dabei bauen sie aufeinander auf. Die Business-Impact-Analyse liefert die geschäftlichen Kontinuitätsanforderungen: maximal tolerierbare Unterbrechungsdauer, Mindestleistungsniveau und das Wiederanlaufziel der Tätigkeit im Sinn der Norm (ISO 22300). Auf dieser Grundlage werden, zusammen mit der Risikobeurteilung, Kontinuitätsstrategien und -lösungen ausgewählt. Erst daraus ergeben sich die technischen Wiederanlaufziele der Anwendungen, Systeme und übrigen Ressourcen, die diese Lösungen tragen. Ob sie erreicht werden, ist anschliessend nachzuweisen.

Dabei sind drei Zeitgrössen auseinanderzuhalten: das Wiederanlaufziel der Tätigkeit, das technische Wiederanlaufziel der Anwendung und die Tragfähigkeit des Notbetriebs. Das Wiederanlaufziel der Tätigkeit zählt ab der Störung. Es umfasst deshalb auch Erkennung, Eskalation und Entscheid, nicht nur die technische Wiederherstellung. Erreicht ist es, sobald die Tätigkeit wieder auf dem Mindestleistungsniveau läuft, über die wiederhergestellte Anwendung oder über einen Notbetrieb. Zur maximal tolerierbaren Unterbrechungsdauer braucht es eine Marge, weil Erkennung und Wiederanlauf im Ereignisfall selten so verlaufen

wie geplant. Davon zu unterscheiden ist das technische Wiederanlaufziel einer Anwendung. Ist sie wieder verfügbar, ist der Wiederanlauf über die Anwendung noch nicht abgeschlossen: Abhängige Wiederanläufe und Datenabgleich brauchen weitere Zeit. Wer das technische Ziel mit der maximal tolerierbaren Unterbrechungsdauer gleichsetzt, plant ohne Puffer für genau diese Anteile. Überbrückt ein Notbetrieb die Zeit bis zur Wiederherstellung, braucht das technische Ziel zudem eine eigene Begründung: Ein Notbetrieb trägt nur begrenzt, weil Belastung, Fehler und die wachsende Rückführungslast ihn mit der Zeit selbst zum Risiko machen (Abschnitte 4.1 und 4.2). Endet der Notbetrieb vor der Wiederherstellung, wird das Mindestleistungsniveau nicht mehr aufrechterhalten. Die Tragfähigkeit ist deshalb keine zweite Toleranzgrenze, sondern bestimmt, wie spät die Wiederherstellung einschliesslich abhängiger Wiederanläufe und Datenabgleich abgeschlossen sein muss. Die Rückführung in den Normalbetrieb folgt erst danach. Abbildung 2 zeigt diese Grössen im Verhältnis zueinander. Sie zeigt auch, was ein Notbetrieb leistet: Er verkürzt die Zeit ohne Leistung, bevor die Anwendung wieder verfügbar ist.

Eine Leistung kann innerhalb des Ziels wieder verfügbar sein und trotzdem nur einen Bruchteil des Normalbetriebs tragen. Ohne Mindestleistungsniveau bleibt jede Zeitangabe deshalb unvollständig.

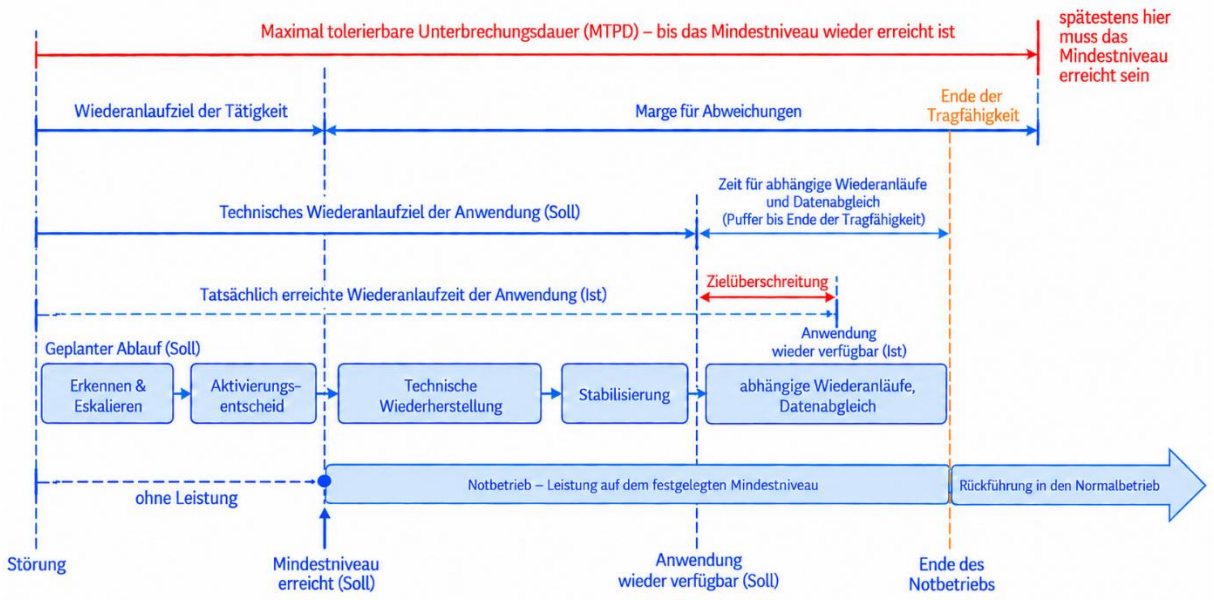


Abbildung 2: Maximal tolerierbare Unterbrechungsdauer, Wiederanlaufziele der Tätigkeit und der Anwendung, Tragfähigkeit des Notbetriebs und erreichte Wiederanlaufzeit (eigene Darstellung)

Kurze Toleranzen haben ihren Preis. Je kürzer die akzeptierte Unterbrechung und je höher das festgelegte Mindestleistungsniveau, desto höher sind in der Regel die Anforderungen an Redundanz, Wiederherstellungskapazität, Personalbereitschaft und vertragliche Absicherung. Eine Leitung kann deshalb nicht gleichzeitig sehr kurze Unterbrechungstoleranzen genehmigen und die dafür nötigen Mittel ungeprüft lassen, sonst bleibt die Zusage auf dem Papier. Auch darin liegt ein Grund, warum die Toleranz ein Führungsentscheid ist: Sie ist nicht nur eine Aussage über Risikoakzeptanz, sondern mittelbar auch über Architektur, Beschaffung und Kosten.

3 Die Vererbungskette und ihre drei Bruchstellen

Business Continuity Management ist im Kern eine Ableitungslogik. Aus der Kritikalität einer Leistung folgt, wie lange und in welchem Umfang sie ausfallen darf. Daraus ergeben sich das Wiederanlaufziel der Tätigkeit und, über die gewählte Kontinuitätsstrategie, die technischen Wiederanlaufziele der Anwendungen, die sie

tragen. Aus diesen wiederum folgen die Anforderungen an Infrastruktur, Daten und Standorte. Ist ein Dienstleister beteiligt, steht am Ende, was er zusichern muss. Jedes Glied leitet seine Anforderung vom darüberliegenden ab. Diese Abfolge ist die Vererbungskette; Abbildung 3 zeigt sie mit ihren drei Bruchstellen, die in den Abschnitten 3.2 bis 3.4 folgen. Die Begriffe stammen nicht aus ISO 22301. Vererbungskette und Bruchstellen sind ein Prüf- und Steuerungsmodell dieses Whitepapers, gebaut aus den Bausteinen der Norm: Business-Impact-Analyse, Abhängigkeiten, Strategien, Übungen und Bewertung.

Die Kette beginnt nicht bei der Technik, sondern bei der Leistung, die eine Organisation nach aussen erbringt, und bei dem Geschäftsprozess, der dahintersteht. Empfänger sind je nach Organisation zum Beispiel die Kundschaft, die Bevölkerung oder Patientinnen und Patienten. Die ersten beiden Glieder der Kette sind Erhebung: Man stellt fest, welche Leistungen es gibt und welche Prozesse sie tragen. Beim dritten Glied wird nicht mehr festgestellt, sondern entschieden. Erheben lassen sich die Auswirkungen eines Ausfalls. Ab wann sie untragbar werden, legt die Führung fest. Die Glieder darunter werden aus diesem Entscheid und aus der gewählten Kontinuitätsstrategie abgeleitet, einem weiteren Entscheid der Leitung.

3.1 Zwei Richtungen, von denen nur eine ausgebaut ist

Die Kette hat zwei Laufrichtungen. Abwärts vererbt sie Anforderungen. Aufwärts, auf dem Rückweg, geschieht zweierlei. Zuerst der Abgleich: Passen die Zusagen der unteren Glieder, entlang ihrer Abhängigkeiten betrachtet, zur Anforderung des obersten? Dann der Nachweis: Das unterste Glied muss belegen können, dass es die Anforderung tatsächlich trägt. Der Abgleich ist Voraussetzung für den Nachweis, ersetzt ihn aber nicht. Geschlossen ist die Kette erst, wenn beide Richtungen wirksam sind.

In der Praxis ist die Abwärtsrichtung häufig deutlich besser ausgebaut als der Rückweg. Anforderungen werden gesetzt, Pläne entstehen, Einstufungen werden abgelegt, und die Kette sieht vollständig aus. Ob die Zusagen am unteren Ende die Toleranz am oberen Ende einhalten, wenn man sie entlang der Abhängigkeiten des Wiederanlaufs verfolgt, hat dagegen oft niemand geprüft.

Selbst wo priorisiert und genehmigt wurde, bleibt ein Wiederanlaufziel ein Sollwert. Über den Istwert sagt es nichts. Die erreichbare Wiederanlaufzeit ist eine Eigenschaft der Organisation, ihrer Architektur und ihrer Dienstleister: Sie wird nicht festgelegt, sondern ermittelt. ISO 22301 verlangt ausdrücklich eine Bewertung der Business-Continuity-Fähigkeiten. Zu bewerten ist nicht nur die Dokumentation, sondern die Fähigkeit selbst: ob die Organisation im Ereignisfall leisten kann, was geplant ist. Die Norm verlangt diese Bewertung in geplanten Abständen, zusätzlich nach einem Vorfall oder einer Aktivierung der Pläne und bei wesentlichen Änderungen. In vielen Organisationen ist das aber nicht oder nur in Ausschnitten geschehen. Deshalb sind Wiederanlaufziele in Audits so oft vorhanden und doch unbelegt.

Prüfnachweis: Vorzulegen sind für eine kritische Leistung zwei Zahlen: das genehmigte Wiederanlaufziel und die Wiederanlaufzeit, die zuletzt in einem Test oder Ereignis tatsächlich erreicht wurde. Fehlt die zweite Zahl, ist die erste unbelegt. Beide Zahlen müssen denselben Anfangs- und Endpunkt haben, und zur zweiten gehören Szenario und Umfang des Tests. Beginnt die Messung erst mit der technischen Wiederherstellung, belegt sie nur diesen Teil des Ziels.

Abbildung 3 zeigt die Kette mit beiden Laufrichtungen. Der Rückweg ist typischerweise an drei Stellen unterbrochen. Jede steht für eine andere Fehlerquelle: unpassende Zusagen, widersprüchliche Anforderungen und unzureichende Szenarioannahmen. Die roten Doppelstriche kennzeichnen die ersten beiden Bruchstellen, der gestrichelte rote Rahmen die dritte, die für die gesamte Kette gilt. Die folgenden Abschnitte beschreiben diese drei Bruchstellen.

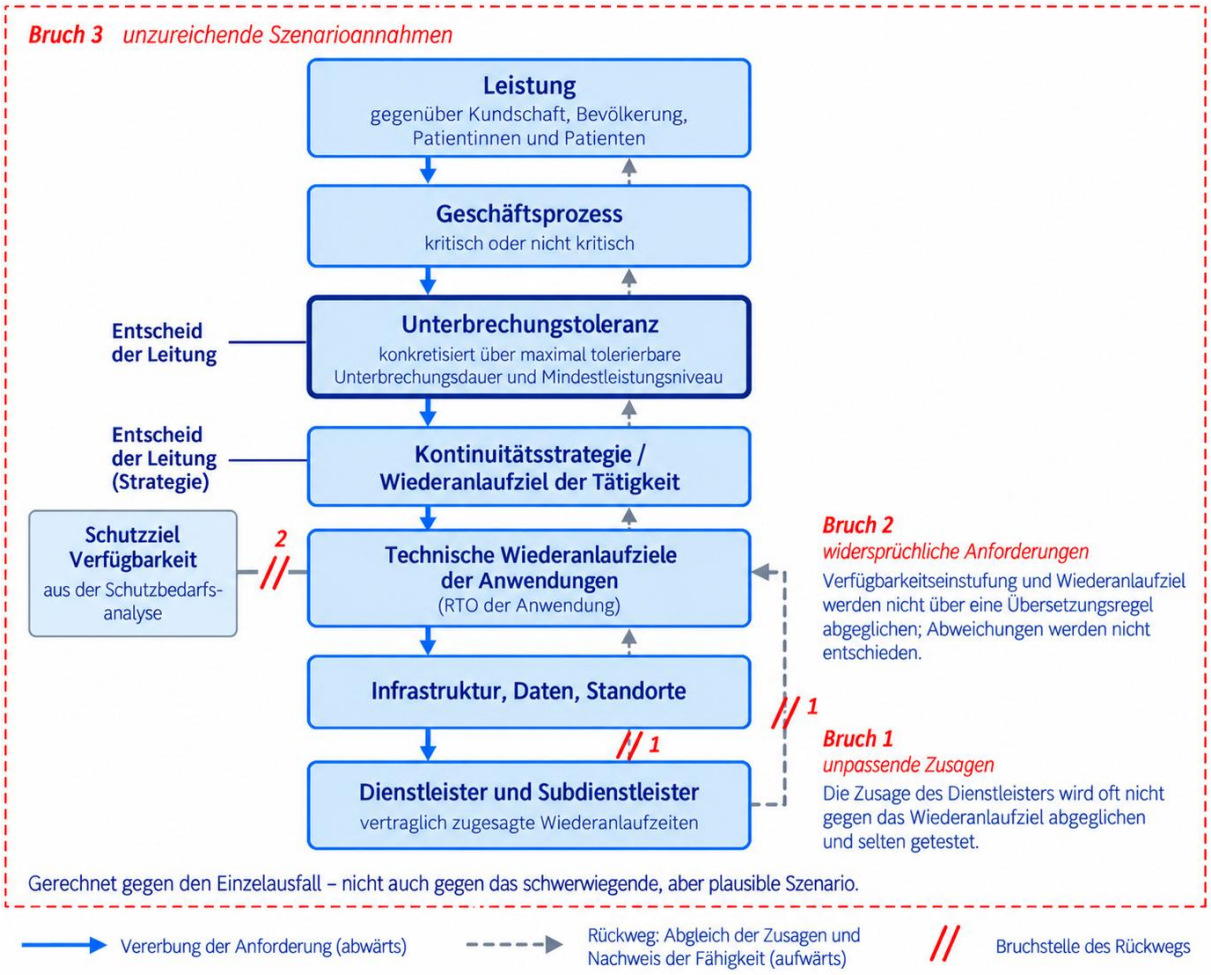


Abbildung 3: Die Vererbungskette und die drei Bruchstellen des Rückwegs (eigene Darstellung)

3.2 Bruch 1: Der Rückweg endet beim Leistungserbringer

Die Leitung genehmigt die Unterbrechungstoleranzen aus der Business-Impact-Analyse. Auf dieser Grundlage und entsprechend der gewählten Kontinuitätsstrategie leiten Fachbereich und Anwendungsverantwortliche das technische Wiederanlaufziel für die Anwendung ab. Betrieben wird die Anwendung häufig von einem Dienstleister, der seinerseits eine Wiederanlaufzeit zusichert. Ob diese Zusage das gesetzte Ziel überhaupt zulässt, ist in vielen Organisationen nie gerechnet worden.

Die Ursache ist selten Nachlässigkeit, sondern Organisation. Das Wiederanlaufziel geht auf die Business-Impact-Analyse zurück, die Wiederanlaufzusage entsteht in der Beschaffung, verhandelt aus einer Leistungs- und Preislogik heraus. Der Fachbereich ist zwar an beidem beteiligt, aber zu unterschiedlichen Zeitpunkten und oft durch unterschiedliche Personen. Zudem folgen beide unterschiedlichen Zyklen: Die Business-Impact-Analyse ist in geplanten Abständen und bei wesentlichen Änderungen zu überprüfen, der Vertrag wird meist nur bei seiner Erneuerung angepasst. Beide Dokumente sind vorhanden, beide sind unterzeichnet, und keine Stelle legt sie nebeneinander.

Normativ ist diese Lücke geschlossen. Die Business-Impact-Analyse hat die Abhängigkeiten zu bestimmen, einschliesslich Partnern und Lieferanten. Die Strategieauswahl ist daran zu messen, ob sie die Wiederaufnahme innerhalb der ermittelten Fristen und der vereinbarten Kapazität ermöglicht. Im Finanzsektor verlangt das FINMA-Rundschreiben 2023/1 zusätzlich, dass RTO und RPO mit den erforderlichen Leistungserbringern abgestimmt werden und ihre Einhaltung über Service Level Agreements oder Verträge geregelt oder durch andere geeignete Verfahren, Prozesse und Kontrollen sichergestellt wird. Die Lücke liegt damit

nicht in den Vorgaben, sondern in ihrer Umsetzung: Die Anforderung besteht seit Jahren, wird in der Praxis aber oft nicht erfüllt.

Eine Besonderheit gilt für interne Leistungserbringer, etwa in der Verwaltung oder bei konzerninternen Informatikdienstleistern. Mit ihnen besteht kein Vertrag im Marktsinn, sondern eine Leistungsvereinbarung. Die Verantwortung für die Betriebskontinuität bleibt trotzdem, wie bei externen Dienstleistern, vollständig bei der beziehenden Einheit. Interne Lieferbeziehungen sind deshalb kein Grund, auf den Abgleich zu verzichten. In der Praxis sind sie aber ein häufiger Ort, an dem er unterbleibt. Woran das liegen kann, beschreibt ein Pilotprojekt des Bundesamts für Cybersicherheit (BACS) und des Bundesamts für Umwelt (BAFU) mit zwei Industriebetrieben: Zentral bereitgestellte IT-Leistungen, etwa eines Mutterkonzerns, können die Wahrnehmung der Verantwortung vor Ort erschweren, insbesondere wenn Systeme, Änderungen und Notfallprozesse für die verantwortliche Einheit nicht transparent sind.

Prüfnachweis: Für dieselbe Leistung werden das aus der Business-Impact-Analyse abgeleitete technische Wiederanlaufziel der betroffenen Anwendung und die Wiederanlaufzusage des Dienstleisters nebeneinandergelegt. Sind die beiden Werte nie in einem Dokument oder einem Gespräch zusammengekommen, fehlt schon der Abgleich und damit die Voraussetzung für jeden Nachweis. Ob die Zusage im Ereignisfall tatsächlich hält, zeigt erst ein Test unter Beteiligung des Dienstleisters (Abschnitt 5.3).

3.3 Bruch 2: Zwei Stränge ohne Zusammenführungspunkt

Die Verfügbarkeitsanforderung aus der Business-Impact-Analyse und die Einstufung des Schutzziels Verfügbarkeit aus der Schutzbedarfsanalyse sind eng verwandt, aber nicht identisch. Die eine setzt an Leistung und Prozess an und ist zeitbezogen, die andere an Information oder Anwendung und arbeitet mit Stufen, oft hinterlegt mit Verfügbarkeitswerten in Prozent. Sie entstehen zudem in zwei getrennten Verfahren, zu zwei Zeitpunkten und in zwei Managementsystemen, typischerweise der Informationssicherheit nach ISO/IEC 27001 und dem Kontinuitätsmanagement nach ISO 22301. Eingestuft wird in beiden oft vom selben Fachbereich, zusammengeführt werden die Ergebnisse aber meist nicht.

Dass die beiden Werte voneinander abweichen, ist nicht ungewöhnlich, teils aus fachlichen Gründen, teils aus den Anreizen, die Abschnitt 2.1 beschreibt. Problematisch wird es, wenn diese Abweichung weder erkannt noch aufgelöst wird. Die Informationssicherheit prüft die Verfügbarkeitseinstufung, die BCM-Funktion das Wiederanlaufziel, und die Differenz prüft niemand.

Dabei ist die Koordination nicht nur sinnvoll, sondern teils vorgeschrieben. In der Bundesverwaltung verlangt die Informationssicherheitsverordnung (ISV), dass die Verwaltungseinheiten ihr Managementsystem für Informationssicherheit (ISMS) mit dem ordentlichen Risikomanagement, dem betrieblichen Kontinuitätsmanagement und dem Krisenmanagement koordinieren. Betrieben wird das ISMS von den Informationssicherheitsbeauftragten im Auftrag der Informationssicherheitsverantwortlichen. Auf der Seite der Informationssicherheit ist die Koordination damit klar zugeordnet. Koordination schafft Schnittstellen und Abgleich, aber keine Befugnis, über die Werte des jeweils anderen Systems zu entscheiden. Vergleichbar werden die beiden Werte zudem erst über eine Übersetzungsregel, die festlegt, welche Verfügbarkeitsstufe welcher Wiederanlauffrist entspricht. Das setzt voraus, dass die Stufen über eine zulässige Ausfalldauer definiert sind. Eine prozentuale Verfügbarkeit allein lässt sich nicht in eine Frist übersetzen, weil derselbe Wert aus vielen kurzen oder wenigen langen Unterbrüchen entstehen kann. Am einfachsten ist es, die Verfügbarkeitseinstufung der Anwendung aus der Business-Impact-Analyse abzuleiten, statt sie getrennt zu erheben. Die Regel und die Schwelle, ab der eine Abweichung eskaliert wird, legt die Leitung fest. Über die einzelne Abweichung entscheidet die dafür zuständige Ebene. Offen bleibt meist, wer die Abweichung zusammenführt und zur Entscheidung vorlegt. Entscheidend ist nicht, wer diese Aufgabe übernimmt, sondern dass sie jemandem zugewiesen ist.

Die Folge zeigt sich im Ereignisfall, entsteht aber lange vorher. Gebaut und betrieben wird die Anwendung nach dem einen Wert, erwartet wird im Ereignisfall womöglich der andere. Liegt der Wert, nach dem gebaut wurde, unter dem erwarteten, ist die Lücke eingebaut. Entschieden hat darüber niemand.

Prüfnachweis: Für dieselbe Anwendung werden die Verfügbarkeitseinstufung aus der Schutzbedarfsanalyse und das aus der Business-Impact-Analyse abgeleitete technische Wiederanlaufziel anhand der Übersetzungsregel verglichen. Fehlt die Regel, ist schon der Vergleich nicht möglich. Weichen die Werte ab, muss nachvollziehbar sein, wer auf welcher Ebene entschieden hat und welche einheitliche Anforderung daraus folgt.

3.4 Bruch 3: Gerechnet gegen den Einzelausfall

Die ersten beiden Bruchstellen liegen an Gliedern der Kette. Die dritte betrifft eine Annahme, auf der die ganze Kette beruht. Jede Wiederanlaufrechnung setzt ein Szenario voraus, und in der Praxis ist es meist der klassische Einzelausfall: ein System fällt aus, bei intakter Umgebung, verfügbarem Personal, funktionierendem Dienstleister und nutzbaren Datensicherungen.

Unter dieser Annahme geht die Rechnung auf, beim flächigen Ereignis nicht mehr. Der Grund wird in keiner einzelnen Einstufung sichtbar: Alle Wiederanläufe konkurrieren um dieselben Ressourcen. Personal, Wiederherstellungskapazität, Netzwerkbandbreite und die Aufmerksamkeit des Dienstleisters sind genau einmal vorhanden. Ob ein Wiederanlaufplan die Fristen aller betroffenen Leistungen gleichzeitig einhalten kann, unter Berücksichtigung von Reihenfolge, parallelen Arbeiten, Abhängigkeiten und gemeinsam genutzten Ressourcen, ist in vielen Organisationen nie geprüft worden, und eine verbindliche Reihenfolge des Wiederanlaufs existiert nicht. Die fehlende Priorisierung aus Abschnitt 2.1 wird hier zum Kapazitätsproblem.

Die FINMA verlangt von Banken, schwerwiegende, aber plausible Szenarien zu berücksichtigen. Das schliesst auch seltene Szenarien ein, solange ihr Eintreten unter realistischen Annahmen möglich ist. Die FINMA räumt dabei ein, dass manche Szenarien, etwa Pandemien, Kriege oder eine langanhaltende Strommangellage, möglicherweise nicht ohne Einbezug des Staates zu bewältigen sind, und erwartet trotzdem Vorarbeiten im Rahmen der eigenen Möglichkeiten. In der Bundesverwaltung werden departementsübergreifende Szenarien wie eine nationale Strommangellage zentral koordiniert, weil ihre Auswirkungen und die nötigen Massnahmen über die einzelne Verwaltungseinheit hinausreichen. Für Cybervorfälle gilt Ähnliches: Könnte etwa die Funktionsfähigkeit der Bundesverwaltung gefährdet sein oder könnten mehrere Departemente betroffen sein, kann die Fachstelle des Bundes für Informationssicherheit im Staatssekretariat für Sicherheitspolitik (SEPOS) die Federführung für die Bewältigung übernehmen oder sie mit Zustimmung der betroffenen Verwaltungseinheit und des Departements dem BACS übertragen (Art. 12 Abs. 5-7 ISV). Für die einzelne Organisation heisst das: Ihre eigene Reihenfolge des Wiederanlaufs muss mit den Prioritäten vereinbar sein, die im flächigen Ereignis von aussen gesetzt werden.

Prüfnachweis: Zu prüfen ist, ob der Wiederanlaufplan die Fristen der kritischen Leistungen mit der verfügbaren Wiederherstellungskapazität auch dann einhält, wenn mehrere Systeme gleichzeitig betroffen sind, und wer die Reihenfolge festlegt, wenn nicht alles gleichzeitig wiederhergestellt werden kann. Gibt es auf die zweite Frage keine dokumentierte Antwort, ist die Kette gegen ein Szenario gerechnet, das im flächigen Ereignis nicht eintritt.

Die drei Bruchstellen wirken unabhängig voneinander, treffen aber dasselbe Ziel: Bruch 1 und Bruch 2 enden beim technischen Wiederanlaufziel der Anwendung, Bruch 3 betrifft die Annahme, unter der es gerechnet wird. Gemeinsam erzeugen sie eine Dokumentationslage, die vollständig erscheint und im Ereignisfall nichts ordnet. Der Entscheid, der daraus folgt, ist Gegenstand des nächsten Kapitels.

4 Der Entscheid im Ereignisfall

Nach einem Cyberangriff, der Systeme kompromittiert hat, zeigt sich, wo der Rückweg an seine Grenzen kommt. Dort ist die Wiederherstellung nicht mehr nur eine technische Frage, sondern eine Führungsfrage. Gerade den Moment, in dem über den Wiederanlauf entschieden werden muss, behandeln viele Kontinuitätsplanungen nur am Rande.

4.1 Wiederanlauf im Kompromittierungsfall

Beim klassischen Ausfall folgt die Wiederherstellung einem Verfahren. Im Kompromittierungsfall steht zunächst die Bewältigung des Vorfalls im Vordergrund. Ob der Angreifer tatsächlich keinen Zugriff mehr hat, lässt sich aber meist erst hinreichend belastbar beurteilen, wenn Eindämmung und Analyse abgeschlossen sind, und das braucht Zeit. Der Wiederanlauf wird damit zum Geschäftsentscheid unter Unsicherheit. Wer früh startet, riskiert, dem Angreifer den Zugriff zurückzugeben. Wer wartet, verlängert den Notbetrieb. Fehlt dieser, dauert die Unterbrechung an. Mit jedem Tag wachsen die aufgestaute Arbeit und der Druck von aussen. Diese Abwägung ist keine technische. Treffen muss sie die Führung.

Führungsentscheid heisst nicht, dass die Leitung im Ereignisfall jedes System selbst freigibt. Sie setzt vorab den Rahmen, also die Unterbrechungstoleranz und das Risiko, das sie zu tragen bereit ist. Wer innerhalb dieses Rahmens über den Wiederanlauf entscheidet, muss vorgängig festgelegt sein, ebenso die Eskalationsschwellen und die Fälle, die der Leitung vorbehalten bleiben.

Hinzu kommt, dass der tatsächlich nutzbare Wiederherstellungspunkt weiter zurückliegen kann, als der Zielwert (RPO) vorsieht. Gemeint ist die jüngste Datensicherung, deren Vertrauenswürdigkeit hinreichend belegt ist, und nicht einfach die jüngste verfügbare. Je länger ein Angreifer unentdeckt im System war, desto grösser kann die Abweichung vom Zielwert und damit der tatsächlich hinzunehmende Datenverlust werden. Dass die Zeit bis zur Entdeckung eher zu- als abnimmt, stützt der Digital Defense Report 2026 von Microsoft, der für die untersuchten Vorfälle eine längere Verweildauer der Angreifer ausweist als im Vorjahr.

In vielen Organisationen ist der Wiederanlauf-Entscheid nur teilweise vorbereitet. Die Business-Impact-Analyse liefert die zeitliche Grenze. Im Business Continuity Plan fehlt dagegen häufig die Antwort darauf, unter welchen Bedingungen der Wiederanlauf innerhalb dieser Grenze freigegeben werden darf. Die häufigere Folge ist dann nicht, dass falsch entschieden wird, sondern dass niemand entscheidet: Der Krisenstab wartet auf eine forensische Aussage, die in der erhofften Eindeutigkeit nicht kommt, und die maximal tolerierbare Unterbrechungsdauer läuft ab. Auch das ist ein Entscheid, nur ein unbewusster.

Wie diese Abwägung in der Praxis aussieht, zeigte der Angriff auf die Berliner Landesverwaltung im August 2026. Zwei Senatsverwaltungen wurden vorsorglich vom Landesnetz getrennt. In dieser Zeit war unter anderem die Auszahlung von Wohngeld an rund 50 000 Haushalte gefährdet. Nach rund neun Tagen wurden sie wieder an das Landesnetz angebunden, während die forensischen Untersuchungen fortgeführt wurden. Der Fall zeigt zweierlei. Der Wiederanlauf nach einer Kompromittierung findet nicht erst statt, wenn alle Unsicherheit beseitigt ist. Und ob die Bevölkerung in der Zwischenzeit ihre Leistungen erhält, hängt davon ab, ob ein Notbetrieb besteht.

Der Form nach ist die Lücke bereits adressiert. ISO 22301 verlangt eine Reaktionsstruktur mit benannter Befugnis zur Aktivierung, Pläne mit Aktivierungskriterien und ein Verfahren für die Rückführung in den Normalbetrieb. Das FINMA-Rundschreiben verlangt, dass der Business Continuity Plan die auslösenden Gegebenheiten und die Entscheidungsprozesse beschreibt. Auch in der öffentlichen Verwaltung gibt es solche Regeln. Die Berner Kantonsverwaltung legt ausdrücklich fest, dass die Direktionen auch über die Überführung in den Normalbetrieb entscheiden. Offen bleibt meist, was dieser Entscheidungsprozess im Kompromittierungsfall enthalten muss.

Vier Elemente gehören vorbereitet:

- **Wer entscheidet.** Eine vorab festgelegte Rolle mit benannten Personen, nicht eine Funktion, die im Ereignisfall erst gesucht wird. Dazu eine Regelung für den Fall, dass diese nicht erreichbar sind.
- **Auf welcher Informationsgrundlage.** Welche Aussagen müssen vorliegen, in welcher Form, und welche Unsicherheit wird ausdrücklich in Kauf genommen.
- **Welche Optionen bestehen.** Teilwiederanlauf einzelner Leistungen, Betrieb mit reduziertem Funktionsumfang, Neuaufbau statt Wiederherstellung. Wer nur eine Option hat, entscheidet nicht.
- **Ab wann der Notbetrieb selbst das grössere Risiko ist.** Notbetrieb belastet das Personal, erhöht die Fehlerrate und lässt die Arbeit wachsen, die später zurückgeführt werden muss. Ab einem gewissen Punkt kann das schwerer wiegen als das Restrisiko eines Wiederanlaufs. Wo er genau liegt, zeigt sich erst in der Situation. Vorab festzulegen sind die Kriterien, an denen er sich erkennen lässt, und wer ihn feststellt. Die geplante Tragfähigkeit (Abschnitt 2.3) liefert dafür den Ausgangswert.

Ob diese Elemente tragen, zeigt sich nicht im Plan, sondern in der Übung. Ein Entscheid unter Unsicherheit lässt sich in einer Planbesprechung oder Stabsübung durchspielen, lange bevor er im Ereignis fällt.

Prüfnachweis: Der Business Continuity Plan einer kritischen Leistung wird mit einer einzigen Frage gelesen: Steht darin, wer unter welchen Bedingungen den Wiederanlauf freigibt? Enthält er nur Wiederherstellungsschritte und Zeitziele, ist der Entscheid nicht vorbereitet.

4.2 Notbetrieb als vergessene Kontinuitätsstrategie

Das vierte Element führt auf ein grundsätzlicheres Problem. Die Abwägung zwischen frühem und spätem Wiederanlauf setzt voraus, dass es eine Zeit ohne Systeme gibt, welche die Organisation aushalten kann. Ob es sie gibt, ist eine Strategiefrage, und sie wird selten gestellt.

ISO 22301 verlangt die Auswahl geeigneter Kontinuitätsstrategien und hält mit dem Mindestleistungsniveau die Grösse bereit, die reduzierten Betrieb beschreibbar macht. In der Praxis lautet die gewählte Strategie trotzdem häufig «schnell wiederherstellen». Das ist oft kein Entscheid gegen Ausweichlösung, reduzierten Betrieb oder Verzicht, sondern ein Entscheid ohne sie.

Verschärfend kommt hinzu, dass Rückfallverfahren bei der Digitalisierung oft nicht mitgedacht wurden. Gemeint sind manuelle oder papierbasierte Abläufe, mit denen eine Leistung auch ohne IT weiterläuft. Sie verschwinden schleichend: Je länger ein Prozess vollständig digital läuft, desto weniger bleibt von ihnen übrig. Die Formulare existieren nicht mehr, Partner nehmen nur noch elektronische Übermittlung an, und niemand im Team hat den alten Ablauf je ausgeführt. Das ist ein Strategieentscheid mit erheblicher Tragweite, der nie als solcher getroffen wurde.

Notbetrieb muss allerdings nicht manuell sein. Er kann auch darin bestehen, dass eine Leistung technisch entkoppelt weiterläuft, lokal und ohne Anbindung an zentrale Netze oder Dienste. Für industrielle Anlagen nennen BACS und BAFU die Fähigkeit zum autonomen Weiterbetrieb ohne Netzwerkanbindung ausdrücklich als Faktor der Cyberresilienz. Im Kompromittierungsfall wird diese Fähigkeit besonders wichtig.

Die Trennung vom Netz ist oft eine der ersten Eindämmungsmassnahmen. Wer entkoppelt weiterarbeiten kann, verliert dadurch weniger Leistung und gewinnt Zeit für die Analyse. Wer es nicht kann, bezahlt die Eindämmung mit der Unterbrechung.

Wer den Notbetrieb bewusst plant, gleich in welcher Form, muss vier Fragen beantworten: Welche Leistungen werden überhaupt aufrechterhalten, und welche fallen bewusst aus? In welcher Qualität und mit welchem Durchsatz? Wer informiert Kundschaft, Aufsicht und Partner, und wann? Und wie lange ist er tragfähig, bevor er selbst zum grösseren Risiko wird? Die BCM-Richtlinien der Berner Kantonsverwaltung verlangen

einen Teil davon ausdrücklich: Das Ergebnis der Business-Impact-Analyse umfasst einen Beschrieb des Notbetriebs samt der benötigten Ressourcen, mit besonderem Augenmerk auf Alter und Verfügbarkeit der Daten. Zu den Plänen gehört zudem das Vorgehen zur Rückführung in den Normalbetrieb.

Gerade diese Rückführung wird am häufigsten unterschätzt. Ein Notbetrieb erzeugt Daten und Vorgänge, die später nacherfasst und in die Systeme zurückgeführt werden müssen. Diese Rückführungslast wächst mit jedem Tag und kann bei längerem Notbetrieb die technische Wiederherstellung zeitlich deutlich übersteigen. Wer den Notbetrieb ohne die Rückführung plant, verschiebt das Problem lediglich.

Ein belastbarer Notbetrieb ist damit mehr als eine Notlösung für den Fall, dass die Wiederherstellung misslingt. Erst er macht den Wiederanlauf nach einer Kompromittierung zu einem echten Entscheid. Fehlt er, entscheidet der Druck und nicht der Erkenntnisstand.

Prüfnachweis: Für eine kritische Leistung ist zu klären, welche Kontinuitätsstrategie gewählt wurde und wer diese Wahl wann getroffen hat. Liegt als Antwort nur der Wiederherstellungsplan vor, wurde keine Strategie gewählt, sondern eine vorausgesetzt.

5 Resilienz unter Dienstleisterabhängigkeit

Der erste Whitepaper-Beitrag dieser Reihe hat den Grundsatz dargelegt, dass die Verantwortung bei Auslagerungen intern bleibt. Spätestens beim Wiederanlauf zeigt sich, ob sie trägt: ob eine Organisation die ausgelagerte Leistung noch steuert oder auf die Krisenorganisation ihres Dienstleisters wartet. Drei Aspekte sind dafür zentral.

5.1 Korrelierte Ausfälle

Unter Klumpenrisiko wird üblicherweise verstanden, dass viele Leistungen bei einem einzigen Dienstleister ausgelagert sind. Diese Betrachtung ist richtig, greift für die Kontinuität aber zu kurz. Entscheidend ist, welche Leistungen gleichzeitig ausfallen, auch wenn sie bei verschiedenen Dienstleistern liegen. Korrelierte Ausfälle sind die Dienstleisterseite des flächigen Ereignisses, gegen das die Kette nach Abschnitt 3.4 meist nicht gerechnet ist.

Ob Leistungen gleichzeitig ausfallen, zeigt sich oft erst in der Technik dahinter. Zwei Dienstleister mit getrennten Verträgen können dieselbe Cloud-Region, denselben Identitätsdienst, dasselbe Rechenzentrum oder denselben Subdienstleister nutzen. Verträge können solche Abhängigkeiten offenlegen und sollten es auch. Die Überschneidung zeigt sich aber erst, wenn jemand die Angaben aller Verträge nebeneinanderlegt.

Die Szenariobeispiele der FINMA decken beide Formen ab. Der längere Ausfall durch die Insolvenz eines wichtigen Dienstleisters betrifft das klassische Klumpenrisiko. Ein länger anhaltendes Verbot ausländischer Regierungen, nach dem dort ansässige Cloud-Anbieter oder andere Dienstleister Schweizer Firmen nicht mehr bedienen dürfen, kann dagegen mehrere Dienstleister zugleich treffen. In beiden Fällen fallen Leistungen aus, ohne dass ein technischer Defekt vorliegt.

Wie nahe das zweite Szenario an der Realität liegt, zeigte ein verwandter Fall im Juni 2026. Anthropic musste seine neuesten KI-Modelle aufgrund einer Exportkontrollanweisung der US-Regierung für sämtliche Kunden weltweit sperren, auch auf den grossen Cloud-Plattformen, über die sie bezogen wurden. Wer das Modell über verschiedene Plattformen und damit über getrennte Verträge nutzte, war gleichermassen betroffen: Die Abhängigkeit lag nicht beim Vertragspartner, sondern beim Anbieter dahinter. Der direkte Zugang zu Fable 5 war knapp drei Wochen gesperrt, auf den Cloud-Plattformen war die Wiederfreigabe zunächst nur angekündigt. Wer seine Anwendungen so gebaut hatte, dass sie auf ein anderes Modell ausweichen konnten, blieb handlungsfähig. Diese Fähigkeit ist keine Vertragsfrage, sondern eine Frage der

Kontinuitätsstrategie (Abschnitt 5.2). Wie KI-Anbieter vertraglich gesteuert werden, behandelt das Whitepaper KI-Governance dieser Reihe.

Prüfnachweis: Für die kritischen Leistungen ist aufzuzeigen, welche gemeinsamen technischen Abhängigkeiten ihre Dienstleister haben. Fehlt eine solche Übersicht, ist das Klumpenrisiko nur vertraglich, nicht technisch erfasst.

5.2 Substituierbarkeit als Massstab

Substituierbarkeit bezeichnet, ob und wie schnell sich eine ausgelagerte Leistung durch einen anderen Anbieter oder eine eigene Lösung ersetzen lässt. Die europäische Finanzmarktregulierung (DORA) berücksichtigt sie ausdrücklich bei der Einstufung kritischer IKT-Drittdienstleister. Schweizer Organisationen sind davon in der Regel nicht unmittelbar erfasst. Die FINMA verlangt eine Voraussetzung dafür: Bei wesentlichen Auslagerungen muss ein geordneter Ausstieg möglich sein, also eine Rückführung ins Unternehmen oder eine Übertragung auf einen anderen Dienstleister. Wie schnell ein solcher Wechsel gelingt, beantwortet erst die Substituierbarkeit. Für die Kontinuitätsbetrachtung ist sie deshalb nützlicher als die blosse Ausstiegsmöglichkeit, weil sie eine prüfbare Frage stellt: Gibt es eine Alternative, und in welcher Zeit wäre sie nutzbar?

Der Unterschied ist erheblich. Wo eine Leistung kurzfristig ersetzbar ist, begrenzt die Substitution den Schaden. Wo nicht, etwa weil Daten in einem proprietären Format liegen, kein zweiter Anbieter den Markt bedient oder die Migration Monate dauert, hängt die Einhaltung der Unterbrechungstoleranz der obersten Ebene allein an der Krisenorganisation eines Dienstleisters, sofern keine eigene Ausweich- oder Notbetriebslösung besteht. Eine nie gegen diese Toleranz gerechnete Zusage (Abschnitt 3.2) wiegt dann doppelt, weil es keinen Ausweg gibt. Das ist keine vertragliche Frage mehr, sondern eine strategische.

5.3 Was vertraglich verankert sein muss

Die im Whitepaper IT-Outsourcing & Governance dieser Reihe beschriebenen Verträge sichern Informationssicherheit, Reporting, Auditrechte und Exit. Für die Betriebskontinuität kommen drei Punkte hinzu, die in Standardverträgen regelmässig fehlen:

- **Zugesicherte Wiederanlaufzeiten für die eigenen kritischen Leistungen,** nicht allgemeine Verfügbarkeitszusagen über das Jahr. Eine Verfügbarkeit von 99,9 Prozent sagt wenig darüber, wie lange ein einzelner Ausfall dauern darf.
- **Die Teilnahme an Übungen,** einschliesslich des Rechts, den Dienstleister in ein Szenario einzubeziehen, das ihn selbst zum Ausfallgrund macht.
- **Die Priorisierung im Ereignisfall.** Wenn ein Dienstleister gleichzeitig alle Kunden wiederherstellen muss, entscheidet seine Reihenfolge über die eigene Wiederanlaufzeit. Wo diese Reihenfolge nicht geregelt ist, ist sie offen.

ISO 22301 verlangt, die Business-Continuity-Fähigkeiten relevanter Lieferanten zu bewerten. Die FINMA verlangt für ausgelagerte kritische Prozesse zudem ausdrücklich, dass der Disaster-Recovery-Plan die externen Abhängigkeiten, die vertraglichen Regelungen und alternative Lösungen berücksichtigt. Die alternativen Lösungen sind dabei der anspruchsvollste Teil, weil sie eine Rückfallebene verlangen, die ohne den betroffenen Dienstleister trägt.

Wie Priorisierung, Wiederherstellungsdauer und Rückfallebene zusammenwirken, wenn die Krisenorganisation beim Dienstleister liegt, zeigt der Angriff auf die Südwestfalen-IT.

Fallvignette: Südwestfalen-IT

Am 30. Oktober 2023 legte ein Ransomware-Angriff die Systeme der Südwestfalen-IT lahm, eines kommunalen IT-Zweckverbands in Nordrhein-Westfalen. Betroffen waren 72 Mitgliedskommunen und nach Angaben des Verbands rund 1,6 Millionen Bürgerinnen und Bürger. Für dieses Whitepaper ist nicht der Angriffsweg der interessante Teil, sondern der Wiederanlauf.

Erstens wurde die Reihenfolge im Ereignis festgelegt: Gut zwei Wochen nach dem Angriff wurde gemeinsam mit dem erweiterten Krisenstab eine Priorisierung der wiederherzustellenden Fachverfahren erarbeitet. Erst danach begann die schrittweise Wiederherstellung.

Zweitens zeigt der Verlauf die Grössenordnung der Aufgabe: Der Krisenmodus dauerte nach Angaben des Dienstleisters elf Monate und endete Ende September 2024. Betroffen waren rund 1460 Server, von denen 871 neu aufgesetzt werden mussten. Die über 700 Datensicherungen waren intakt, mussten aber einzeln geprüft werden, bevor sie eingespielt werden konnten.

Drittens mussten die Kommunen parallel eigene Behelfslösungen etablieren, teilweise über den Postweg und mit manuellen Verfahren. An der Priorisierung der Fachverfahren wirkten sie mit. Die technische Wiederherstellung und Freigabe lagen jedoch beim gemeinsamen IT-Dienstleister und seiner Krisenorganisation.

Diese Konstellation findet sich auch in der Schweiz. Gemeinden und Kantone beziehen Fachanwendungen von gemeinsamen Informatikdienstleistern, oft in öffentlicher Trägerschaft. Die Bundesverwaltung bezieht ihre Informatikleistungen vor allem von internen Leistungserbringern, ergänzt durch externe Dienstleister. Auch dort liegt die Krisenorganisation beim Dienstleister, die Verantwortung für die Leistung gegenüber der Bevölkerung aber bei der Auftraggeberin. Bei Südwestfalen-IT hob selbst die öffentlich-rechtliche Trägerschaft diese Abhängigkeit im Ereignisfall nicht auf. Wie weit Schweizer Gemeinden auf diese Abhängigkeit vorbereitet sind, deutet ein weiteres Pilotprojekt des BACS im Kanton Aargau an. Nach der Selbstbewertung der 14 teilnehmenden Gemeinden werden externe IT-Dienstleister grossmehrheitlich nicht systematisch gesteuert. Klare Sicherheitsanforderungen, definierte Eskalationswege und vorbereitete Alternativen bei IT-Ausfällen sind meist unzureichend, und häufig fehlt eine klare Priorisierung der geschäftskritischen Prozesse.

Prüfnachweis: Für die wichtigsten Dienstleister stellen sich zwei Fragen: Wurde ihre zugesicherte Wiederanlaufzeit schon einmal getestet? Und welche eigenen Leistungen würden bei ihnen gleichzeitig ausfallen? Dazu kommt die unbequeme Anschlussfrage: Welche Rückfallebene trägt, solange man auf den Wiederanlauf beim Dienstleister keinen Einfluss hat?

6 Übungen als Wirksamkeitsnachweis

Die bisherigen Kapitel beschreiben Anforderungen und Entscheide. Ob sie tragen, zeigt sich im Ereignis oder, besser vorab, in einer Übung. Je nach Form belegt eine Übung nicht nur die angemessene Gestaltung (Design Effectiveness), sondern auch, dass eine Vorkehrung tatsächlich funktioniert. Wie weit diese Aussage als Wirksamkeit im Betrieb (Operating Effectiveness) trägt, hängt davon ab, welche Fähigkeit tatsächlich geprüft wurde, unter welchen Bedingungen und für welchen Zeitraum die Schlussfolgerung gelten soll. ISO 22301 verlangt dafür ein Programm, nicht eine Übung: Szenarien, die zu den Kontinuitätszielen passen, klar definierte Ziele, eine Auswertung und eine Durchführung in geplanten Abständen sowie bei wesentlichen Änderungen. Für die Bundesverwaltung hält der Bundesrat in den Erläuterungen zu seiner Risikopolitik fest,

dass die Funktionen im Not- und Krisenfall im Voraus zugeordnet und die geplanten Abläufe getestet werden müssen.

Übungen unterscheiden sich erheblich in Aufwand und Aussagekraft. Diese Unterschiede werden in der Praxis selten explizit gemacht, was dazu führt, dass ein durchgeführter Plan-Review und eine Gesamtübung im Reporting gleich aussehen.

Wie Tabelle 1 zeigt, liefert eine Gesamtübung mit Dienstleisterbeteiligung den umfassendsten Nachweis über Organisationsgrenzen hinweg, ersetzt aber den technischen Nachweis einzelner Wiederherstellungsfähigkeiten nicht zwingend. Die übrigen Stufen prüfen Ausschnitte, was legitim ist, solange ihre Aussagekraft nicht überschätzt wird. Die FINMA verlangt Tests unter schwerwiegenden, aber plausiblen Szenarien, einschliesslich der Wiederherstellungsabhängigkeiten zu Drittparteien.

Ebenso wichtig wie die Stufe ist das Szenario. Geübt wird häufig der klassische Einzelausfall. Ein Cyberangriff mit kompromittierten Systemen fehlt dagegen oft, obwohl gerade er die Entscheide verlangt, die sich nur in der Übung vorbereiten lassen. Wer nur den Einzelausfall übt, bestätigt die Annahme des Einzelausfalls, statt sie zu prüfen. Die Szenarien müssen dabei nicht neu erfunden werden. Das Handbuch zum Risikomanagement Bund sieht vor, dass Risiken mit potenziell grossen Auswirkungen als Übungsszenario dienen. Sie sind dort bereits im «credible worst case» beschrieben.

Stufe	Was geprüft wird	Grenzen
Plan-Review	Plausibilität, Vollständigkeit, Aktualität und Konsistenz der Pläne	Prüft ausschliesslich den dokumentierten Zustand; keine Aussage über Ausführbarkeit
Funktionstest	Technische Lösungen wie Datensicherung, Umschaltung, Kommunikationsmittel	Isolierte Betrachtung; die Konkurrenz um Ressourcen bleibt unsichtbar
Planbesprechung (Tabletop)	Rollenverständnis, Zuständigkeiten, Abhängigkeiten, Entscheidwege	Zeitdruck und Informationslücken lassen sich nur simulieren; Ausführbarkeit und tatsächliche Dauer werden nicht nachgewiesen
Übung einzelner Plansequenzen	Einzelne Wiederanlauf-Sequenzen innerhalb des zuständigen Teams, erreichte Zeiten	Kein Zusammenspiel über Teamgrenzen; Abhängigkeiten bleiben ausgeblendet
Stabs- und Stabsrahmenübung	Zusammenarbeit in der BCM-Organisation über Führungslinie, Prozesse und Wiederanlauf-Teams	Der reale Systemzustand wird angenommen, nicht hergestellt
Gesamtübung mit Dienstleisterbeteiligung	Zusammenspiel von Fachbereich, IT, Dienstleistern und Leitung über die gesamte Kette	Aufwendig und koordinationsintensiv, nur begrenzt oft durchführbar; ersetzt den technischen Nachweis einzelner Wiederherstellungen nicht zwingend

Tabelle 1: Übungsstufen und ihre Aussagekraft (eigene Darstellung in Anlehnung an gängige BCM-Praxis)

6.1 Fehlende Übungen und fehlende Konsequenzen

Der naheliegende Befund ist, dass nicht oder nur teilweise geübt wird. Übungsprogramme fehlen, oder Übungen beschränken sich auf Plan-Reviews und Funktionstests, die keinen Entscheid verlangen. Auch das

in Abschnitt 5.3 erwähnte Pilotprojekt des BACS zeigt in der Selbstbewertung der teilnehmenden Gemeinden Lücken bei der praktischen Übung von Notfall- und Wiederherstellungsabläufen. Wo nicht geübt wird, fehlt der Rückweg. Wo nur Ausschnitte geübt werden, bleibt er lückenhaft.

Weniger offensichtlich ist ein zweiter Befund, der gerade dort auftritt, wo geübt wird: Dieselben Erkenntnisse treten über mehrere Übungszyklen hinweg auf, ohne dass sich etwas geändert hätte.

Typische Beispiele: Die Wiederherstellung dauert länger als das Ziel, das Ergebnis wird protokolliert, das Ziel bleibt unverändert. Ein Dienstleister nimmt zum wiederholten Mal nicht teil, weil der Vertrag es nicht vorsieht. Die Rückführung der im Notbetrieb entstandenen Daten wird als offener Punkt vermerkt und steht im Folgejahr wieder auf der Liste.

Der Grund ist selten Ignoranz. Die Erkenntnisse einer Übung fliessen meist in einen Massnahmenplan, während die Konsequenz an anderer Stelle liegen müsste: in den Ressourcen, in der Architektur, im Vertrag oder in der Unterbrechungstoleranz selbst. Die Richtlinie des Bundes sieht als Ergebnis einer Übung eine Beurteilung mit Massnahmenplan vor. Sie verlangt aber auch, die Business-Impact-Analyse, die Umsetzungsstrategie und die Pläne periodisch auf ihre Wirksamkeit zu überprüfen. Genau dort gehört die Konsequenz hin, doch die Verbindung wird selten gezogen. Oft fehlt zudem eine Stelle, welche die Nachverfolgung wahrnimmt: Die Rolle der BCM-Verantwortlichen ist nicht oder nur teilweise definiert, oder sie hat nicht die Befugnis, Konsequenzen einzufordern. Dabei verlangen etwa die Richtlinien des Bundes und des Kantons Bern ausdrücklich eine benannte BCM-verantwortliche Person, beim Bund zudem mit den nötigen Kompetenzen und Ressourcen. Zeigt eine Übung systematisch nicht erreichbare Ziele, stellt sie nicht nur die Ausführung infrage, sondern das Verhältnis von Ziel und Mitteln. Die Konsequenz kann bei den Ressourcen, der Architektur, den Verträgen oder beim Ziel selbst liegen. Ein Ziel darf dabei nur so weit angepasst werden, wie rechtliche und regulatorische Vorgaben und die tatsächlich tragbaren Auswirkungen es zulassen. Leichter erreichbar heisst nicht angemessen. Diese Konsequenz zu ziehen, ist der fünfte Führungsentscheid.

Prüfnachweis: Die Feststellungen der letzten drei Übungszyklen werden nebeneinandergelegt. Wiederkehrende Punkte sind selten nur ein Ausführungsproblem. Meist zeigen sie, dass die zuständige Entscheidungsebene nicht einbezogen wurde.

7 Leitfragen für Leitungs- und Aufsichtsgremien

Die folgenden Fragen eignen sich für eine Standortbestimmung. Sie zielen nicht auf technische Details, sondern auf die Entscheidgrundlage und darauf, ob die Leitung ihre Rolle tatsächlich wahrnimmt.

Zur Entscheidgrundlage

- Wissen wir, welche unserer Leistungen wie lange ausfallen dürfen? Und haben wir diesen Wert auf Grundlage der Erhebung in den Fachbereichen selbst entschieden oder nur übernommen? Falls bei uns fast alles kritisch ist: Wer legt im Ereignisfall die Reihenfolge fest?
- Haben wir für unsere kritischen Leistungen festgelegt, auf welchem Mindestniveau sie im Ereignisfall erbracht werden? Oder kennen wir nur die Zeit, nicht den Umfang?
- Haben wir bei der Genehmigung der Unterbrechungstoleranzen geprüft, ob die dafür notwendige Redundanz, Wiederherstellungskapazität und Bereitschaft auch finanziert sind?

Zur Kette bis zum Dienstleister

- Haben wir für unsere wichtigsten Leistungen einmal gerechnet, ob die zugesicherten Wiederanlaufzeiten unserer Dienstleister unsere eigenen Ziele überhaupt zulassen?

- Wissen wir, welche unserer Leistungen gleichzeitig ausfallen können, weil sie dieselbe Plattform, dieselbe Region oder denselben Subdienstleister nutzen? Und wissen wir, bei welchen Dienstleistern wir kurzfristig keine Alternative hätten?
- Sind die Verfügbarkeitseinstufungen unserer kritischen Anwendungen mit den Wiederanlaufzielen aus der Business-Impact-Analyse abgeglichen? Und ist geregelt, wer entscheidet, wenn sie voneinander abweichen?

Zum Entscheid im Ereignisfall

- Haben wir geregelt, wer im Kompromittierungsfall den Wiederanlauf freigibt, in welchem Rahmen und auf welcher Informationsgrundlage? Und welche Entscheide bleiben uns vorbehalten?
- Haben wir für unsere kritischen Leistungen einen Notbetrieb, der lange genug trägt, und wissen wir, ab wann er selbst zum grösseren Risiko wird? Und ist geplant, wie die dabei entstehende Arbeit anschliessend zurückgeführt wird?
- Sind die Rollen, die wir im Ereignisfall brauchen, mit benannten Personen und Stellvertretungen besetzt, erreichbar und für ihre Aufgabe ausgebildet? Und hat die für das Kontinuitätsmanagement verantwortliche Stelle die Befugnis, Konsequenzen einzufordern?

Zum Nachweis

- Kennen wir neben unseren Wiederanlaufzielen auch die zuletzt tatsächlich erreichte Wiederanlaufzeit, und wissen wir, unter welchen Bedingungen und über welche Spanne sie gemessen wurde?
- Nehmen unsere wesentlichen Dienstleister an unseren Übungen teil? Und haben wir je ein Szenario geübt, in dem der Dienstleister selbst der Ausfallgrund ist oder unsere Systeme kompromittiert sind?
- Tauchen in unseren Übungsberichten seit mehreren Zyklen dieselben Feststellungen auf? Und haben wir daraufhin in der Managementbewertung konkrete Entscheide zu Ressourcen, Architektur, Verträgen oder Zielen getroffen, oder haben wir die Empfehlungen nur zur Kenntnis genommen?

Wer diese Fragen heute nicht beantworten kann, hat damit einen konkreten Ausgangspunkt für das nächste Resilienz-Review.

Fazit

Drei Befunde ziehen sich durch dieses Whitepaper: die ausbleibende Priorisierung, die Brüche auf dem Rückweg und der unvorbereitete Wiederanlauf-Entscheid.

Was diese Befunde verbindet, ist kein methodisches Defizit. Business Continuity Management ist als Methodik ausgereift und normiert, und aus ISO 22301 lässt sich ableiten, wo entschieden werden muss. Meist fehlt es an zwei Dingen: an Entscheiden, die die Leitung bewusst selbst trifft, statt die Ergebnisse nur zur Kenntnis zu nehmen, und am Nachweis, dass das unterste Glied der Kette die Anforderung des obersten tatsächlich trägt. Selbst wo Übungen diesen Nachweis liefern, bleibt oft die Konsequenz aus.

Resilienz ist deshalb keine rein technische Eigenschaft. Sie ist eine Fähigkeit der Organisation, und ihre Grenzen werden durch Führungsentscheide bestimmt. Diese legen fest, was kritisch ist und welche Unterbrechung akzeptiert wird, auf welchem Niveau eine Leistung weiterläuft, welche Strategie sie mit welchen Mitteln sichert, wer im Ereignisfall entscheidet und welche Konsequenz aus Übungen folgt. Der Massstab ist nicht die Wiederherstellungsgeschwindigkeit, sondern ob die Organisation im Ereignisfall auf dieser Grundlage entscheidungsfähig ist.

Quellen

Anthropic, Statement on the US government directive to suspend access to Fable 5 and Mythos 5, 12. Juni 2026 (anthropic.com/news/fable-mythos-access); Redeploying Fable 5, 30. Juni 2026, aktualisiert am 1. Juli 2026 (anthropic.com/news/redeploying-fable-5); CNBC, «Anthropic says Trump admin has lifted export controls on Claude Fable 5 and Mythos 5», 30. Juni 2026.

BCM-Richtlinien der Kantonsverwaltung Bern vom 4. September 2024, insbesondere Ziff. 2.3, 5.4 Bst. a, f und g, 7.2, 7.3 und 7.5.

Bundesamt für Bevölkerungsschutz BABS, Leitfaden Schutz kritischer Infrastrukturen (erstmals 2015); zu den geplanten Vorgaben Motion 23.3001 und Medienmitteilung des Bundesrates vom 18. Februar 2026.

Bundesamt für Cybersicherheit BACS, Cyberresilienz-Assessment (CyRA). Zentrale Erkenntnisse aus dem Pilotprojekt im Kanton Aargau, 25. Juni 2026, insbesondere Ziff. 3, 5 und 8.

Bundesamt für Umwelt BAFU und Bundesamt für Cybersicherheit BACS, Cybersicherheit bei Störfallbetrieben. Erkenntnisse aus dem Pilotprojekt mit den kantonalen Vollzugsstellen, September 2026, insbesondere Ziff. 4.

FINMA-Rundschreiben 2018/3 «Outsourcing» vom 21. September 2017, in Kraft seit 1. April 2018.

FINMA-Rundschreiben 2023/1 «Operationelle Risiken und Resilienz – Banken» vom 7. Dezember 2022, in Kraft seit 1. Januar 2024, insbesondere Rz 10, 14–17, 84–95 und 101–110 (inkl. Fussnoten 25 und 27 zu den Szenarien).

Handbuch zum Risikomanagement Bund der Eidgenössischen Finanzverwaltung, Version vom 16. September 2024, insbesondere Ziff. 2.3.3, 6.2 und 6.3.

Informationssicherheitsverordnung (ISV, SR 128.1) vom 8. November 2023, Art. 5 Abs. 4, Art. 12 Abs. 5–8, Art. 36 Abs. 3 Bst. a und Art. 37 Abs. 2 Bst. a.

ISO 22301:2019 mit Amendment 1:2024, insbesondere Ziff. 5, 8.2 bis 8.6 und 9.3; ergänzend ISO 22313:2020, ISO/TS 22317:2021 (Business-Impact-Analyse), ISO/IEC 27001:2022 mit Amendment 1:2024 (Managementsystem für Informationssicherheit), ISO/IEC 27031:2025 (IKT-Bereitschaft); Begriffe wie MTPD und RTO nach ISO 22300:2025.

Microsoft, Digital Defense Report 2026, Berichtszeitraum Juli 2025 bis Juni 2026, insbesondere S. 35 (Verweildauer von Angreifern).

Nachrichtendienst des Bundes NDB, Sicherheit Schweiz 2026. Lagebericht des Nachrichtendienstes des Bundes, 25. Juni 2026, insbesondere S. 5, 9 und 66–67.

Richtlinie der Eidgenössischen Finanzverwaltung über das Kontinuitätsmanagement Bund vom 1. August 2024, insbesondere Ziff. 3.1, 3.3 und 4.1 bis 4.4.

Senatskanzlei Berlin, Pressemitteilung «Senatsverwaltungen wieder ans Landesnetz Berlin angebunden», 23. August 2026; Cyberangriff auf das Landesnetz: Informationen für Bürgerinnen und Bürger, berlin.de/cyberangriff (Stand 14. September 2026); heise online, Chronologie zum Cyberangriff auf die Berliner Verwaltung (abgerufen im September 2026).

Südwestfalen-IT und r-tec, Abschlussbericht Security Incident, 25. Januar 2024; Südwestfalen-IT, Bilanz ein Jahr nach dem Hackerangriff, Mitteilung vom 30. Oktober 2024.

Verordnung (EU) 2022/2554 (DORA), Art. 31 Abs. 2 Bst. d.

Weisungen des Bundesrates über die Risikopolitik des Bundes vom 26. Juni 2024 (BBl 2024 1662) mit Erläuterungen, insbesondere zu Ziff. 4 Abs. 6.

Hinweis

Dieses Whitepaper gibt ausschliesslich meine persönliche fachliche Einschätzung wieder und steht nicht für eine Behörde oder Aufsicht. Es darf unverändert weitergegeben und mit Quellenangabe zitiert werden. Kommerzielle Verwertung und Bearbeitungen bedürfen meiner vorherigen Zustimmung.



Fragen und Austausch willkommen

carsten@carsten-beck.ch

Alle Beiträge der Reihe

carsten-beck.ch/publikationen

linkedin.com/in/carstenbeck-grc