Sottung Security Consulting
Informationssicherheit & Resilienz

Danach

NACH DEM VORFALL IST VOR DEM NÄCHSTEN VORFALL

Vorfall bewältigt. Und was nun?

Ob Cyberangriff, Ausfall eines Dienstleisters oder Stromausfall: Leitfaden zur Nachbereitung von Störungen und Vorfällen in Kernprozessen – mit Lessons Learned, Ursache-Wirkungs-Kette, Neubewertung der Risiken und Maßnahmen, die wirken.

Jürgen Sottung
KRITIS-Auditor · ISO 27001 Lead Auditor · externer ISB

Stand: November 2026
ssc-ism.de

DIE LAGE

Der Betrieb läuft wieder – und dann?

Ein Vorfall ist eine Ausnahmesituation. Tage im Krisenmodus, lange Nächte, viel Druck. Wenn der Betrieb wieder läuft, ist die Erleichterung groß – und das Tagesgeschäft wartet längst.

Genau an diesem Punkt hört in den meisten Organisationen die Arbeit am Vorfall auf. Es gibt keine Lessons-Learned-Runde, niemand rekonstruiert die Ursache-Wirkungs-Kette, die Risikobewertung bleibt unverändert – und die Maßnahmen, die den nächsten Vorfall verhindern oder begrenzen würden, werden nie umgesetzt.

Nicht nur eine Frage der IT

Nachbereitung lohnt sich bei jeder Störung, Beeinträchtigung oder jedem Ausfall wesentlicher Kernprozesse – auch wenn die Ursache komplett außerhalb der IT liegt:

Cyberangriff
Ransomware, kompromittierte Zugänge, Datenabfluss

Dienstleister
Ausfall eines kritischen Lieferanten oder Servicepartners

Infrastruktur
Strom, Wasser, Klima, Brand, Wasserschaden

Personal
Krankheitswelle, Ausfall von Schlüsselpersonen

Prozesse
Fehlbedienung, fehlerhafte Änderung, Qualitätsproblem

Umfeld
Lieferengpässe, Unwetter, Zugangsbeschränkungen

Warum die Nachbereitung so oft ausfällt

„Ist ja gut gegangen." Der Schaden war überschaubar, das Gefühl, etwas nachbereiten zu müssen, verfliegt schnell.

Erschöpfung und Rückstau. Die Beteiligten sind müde, liegengebliebene Arbeit drängt.

Angst vor der Schuldfrage. Wer Nachbereitung als Suche nach Schuldigen erlebt, sagt lieber nichts.

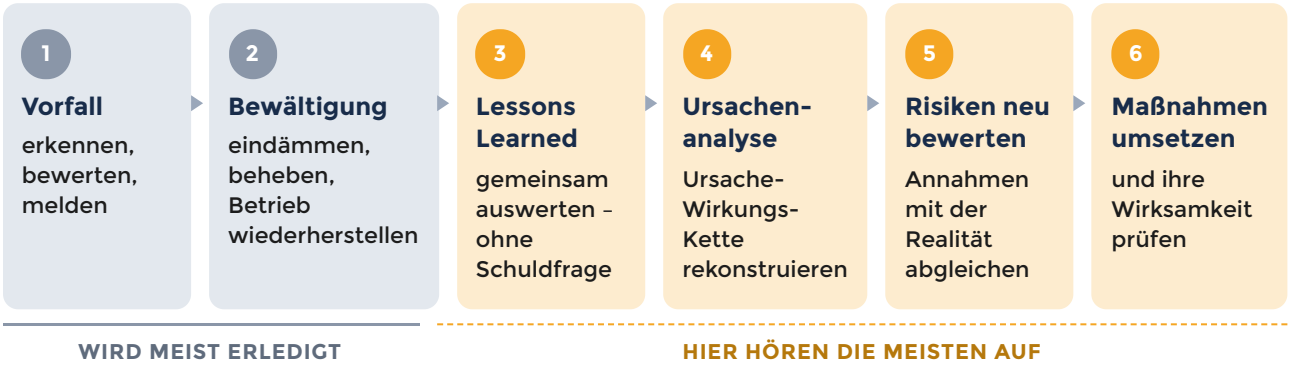
Niemand ist zuständig. Für die Bewältigung gibt es Rollen, für die Nachbereitung oft nicht.

Was das kostet: Derselbe Fehler passiert ein zweites Mal. Die gleichen Lücken in Erreichbarkeit, Entscheidungswegen und Wiederanlauf zeigen sich erneut. Und im nächsten Audit lautet die Frage: „Was haben Sie aus dem Vorfall gelernt?"

DER VOLLSTÄNDIGE KREISLAUF

Vom Vorfall zur Verbesserung – in sechs Schritten

Bewältigung ist nur die Hälfte. Wirksam wird Vorfall- und Notfallmanagement erst, wenn aus dem Ereignis Erkenntnisse, neue Risikobewertungen und umgesetzte Maßnahmen werden.



Was Normen und Gesetz erwarten

GRUNDLAGE	ANFORDERUNG
ISO/IEC 27001:2022 Anhang A 5.27, Abschnitt 10.2	Erkenntnisse aus Informationssicherheitsvorfällen nutzen; bei Abweichungen Ursachen ermitteln, Korrekturmaßnahmen umsetzen und deren Wirksamkeit überprüfen.
ISO 22301 / BSI-Standard 200-4 Business Continuity Management	Notfälle und Krisen nachbereiten, Notfallvorsorge und -pläne auf Basis der Erfahrungen bewerten und verbessern.
§ 30 Abs. 2 BSIG	Risikomanagementmaßnahmen umfassen u. a. die Bewältigung von Sicherheitsvorfällen (Nr. 2), die Aufrechterhaltung des Betriebs und Krisenmanagement (Nr. 3) sowie Verfahren zur Bewertung der Wirksamkeit (Nr. 6).
§ 32 Abs. 1 Nr. 4 BSIG	Die Abschlussmeldung an das BSI enthält Angaben zur zugrunde liegenden Ursache sowie zu den getroffenen und laufenden Abhilfemaßnahmen.
§ 38 Abs. 1 BSIG	Die Geschäftsleitung muss die Risikomanagementmaßnahmen umsetzen und ihre Umsetzung überwachen.

Für alle, nicht nur für NIS-2: Für NIS-2-pflichtige Einrichtungen und KRITIS-Betreiber ist die Nachbereitung faktisch Pflicht – spätestens die Abschlussmeldung verlangt Ursache und Abhilfe. Für alle anderen ist sie schlicht der günstigste Weg, den nächsten Ausfall zu verhindern.

SCHRITT 3

Die Lessons-Learned-Runde

Eine strukturierte Besprechung, in der alle Beteiligten den Vorfall gemeinsam auswerten. Ziel ist nicht, Schuldige zu finden, sondern zu verstehen, was passiert ist und was sich ändern muss.

Wann

Innerhalb von ein bis zwei Wochen nach Abschluss der Bewältigung – solange die Erinnerung frisch ist. Bei langen Ereignissen zusätzlich eine Zwischenrunde.

Wer

Alle Beteiligten: betroffene Fachbereiche, IT, Haustechnik, Dienstleister, Krisenstab, ISB, BCM-Beauftragte, bei Personenbezug der DSB. Die Leitung mindestens zur Ergebnisvorstellung.

Wie

60 bis 120 Minuten, neutral moderiert. Ergebnisse werden protokolliert, Maßnahmen bekommen Verantwortliche und Termine.

Die Leitfragen

1. **Was ist passiert?** Zeitleiste rekonstruieren: erster Hinweis, Erkennung, Eskalation, Meldung, Eindämmung, Wiederanlauf.
2. **Wie wurde der Vorfall erkannt?** Durch Technik, Beschäftigte, Kunden oder Dienstleister – und wie lange hat das gedauert?
3. **Was hat gut funktioniert?** Was davon wollen wir bewusst beibehalten?
4. **Was hat nicht funktioniert?** Erreichbarkeit, Entscheidungswege, Informationen, Zugänge, Notfallpläne, Dienstleister, Kommunikation.
5. **Was hätten wir früher sehen können?** Welche Warnsignale oder Beinahe-Vorfälle gab es – und warum wurden sie nicht ernst genommen?
6. **Was ändern wir konkret?** Maßnahmen mit Verantwortlichen und Terminen – nicht nur Absichtserklärungen.

Die wichtigste Regel: Fehler statt Schuldige

Wer befürchtet, bloßgestellt zu werden, verschweigt Fehler. Fragen Sie nach Bedingungen, nicht nach Personen: Nicht „Wer hat das übersehen?“, sondern „Warum konnte das übersehen werden – und warum hatte es so große Folgen?“

SCHRITT 4

Die Ursache-Wirkungs-Kette

Der Auslöser eines Vorfalls ist selten seine Ursache. Die eigentliche Ursache liegt meist in Bedingungen, die den Auslöser erst so folgenreich gemacht haben.

Methode 1: Fünfmal „Warum?“ – ein Beispiel

Warum 1	Die Server waren verschlüsselt. – Weil sich Schadsoftware im Netz ausbreiten konnte.
Warum 2	Weil der Angreifer Administratorrechte erlangt hatte.
Warum 3	Weil ein Administrator-Konto ohne zweiten Faktor genutzt wurde – auch für E-Mail und Internet.
Warum 4	Weil es keine Trennung von Admin- und Arbeitskonten gab und Ausnahmen nie überprüft wurden.
Ursache	**Privilegierte Zugänge waren nicht gesteuert – das Risiko war bekannt, aber nie entschieden.**

Ebenso wichtig ist, warum der Schaden so groß wurde: Die Backups lagen im selben Netz und wurden mit verschlüsselt. Das betrifft nicht die Wahrscheinlichkeit, sondern die Auswirkung – und gehört genauso zur Kette.

Methode 2: Ursachen nach Bereichen sammeln

Bei komplexen Ereignissen hilft eine Sammlung nach Bereichen, angelehnt an das Ishikawa-Diagramm. Sie verhindert, dass die Analyse bei der Technik stehen bleibt:

Mensch
Wissen, Sensibilisierung, Belastung, Vertretung

Technik
Konfiguration, Wartung, Redundanz, Überwachung

Organisation
Rollen, Zuständigkeiten, Entscheidungswege

Prozesse
Abläufe, Änderungen, Meldeweg, Wiederanlauf

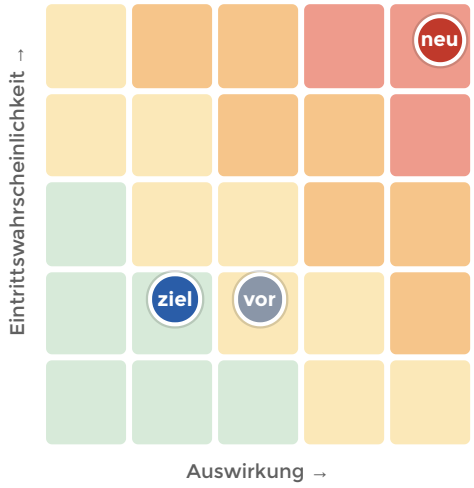
Dienstleister
Abhängigkeiten, Verträge, Reaktionszeiten, Alternativen

Umfeld
Standorte, Versorgung, Zeitpunkt (Wochenende, Urlaub)

SCHRITT 5

Risiken neu bewerten

Ein Vorfall ist der härteste Realitätscheck für jede Risikoanalyse. Er zeigt, welche Annahmen zu optimistisch waren – bei der Eintrittswahrscheinlichkeit, bei der Auswirkung oder bei beidem.



Was die Matrix zeigt

- **vor:** So war das Risiko vor dem Vorfall bewertet – „mittel, akzeptiert".
- **neu:** Der Vorfall zeigt: Das Szenario ist real, und der Schaden ist deutlich größer als angenommen.
- **ziel:** Mit Maßnahmen soll das Risiko wieder in einen bewusst tragbaren Bereich.

Das neu bewertete Risiko entscheidet die Leitung: behandeln, übertragen, vermeiden oder bewusst tragen.

Zwei Hebel für Maßnahmen

Eintrittswahrscheinlichkeit senken

- Zugänge absichern, MFA, getrennte Admin-Konten
- Wartung, Patchen, Härtung
- Dienstleister sorgfältig auswählen und steuern
- Schulung, klare Abläufe, Vier-Augen-Prinzip
- Beinahe-Vorfälle erfassen und auswerten

Auswirkung begrenzen

- Redundanzen und Ausweichlösungen, zweiter Lieferant
- getrennte, unveränderliche Backups
- getestete Notfall- und Wiederanlaufpläne
- Notfall- und Kommunikationsübungen
- früher erkennen, schneller handeln

Nicht vergessen: Ein Vorfall zeigt oft, dass Wiederanlaufzeiten, Abhängigkeiten oder Notfallkontakte nicht stimmen. Business-Impact-Analyse und Notfallpläne gehören deshalb nach jedem größeren Ereignis auf den Prüfstand.

DER BLICK VON AUSSEN

Warum die eigene Nachbereitung oft zu kurz greift

Wer täglich im Prozess steckt, hält Umwege, Provisorien und Abhängigkeiten für normal. Nach einem Vorfall wird diese Betriebsblindheit zum Risiko: Die Analyse bleibt beim Offensichtlichen stehen.

Die interne Brille

- **Scheuklappen:** Bekanntes wird nicht mehr hinterfragt.
- **Befangenheit:** Beteiligte bewerten ihr eigenes Handeln.
- **Hierarchie:** Offenheit endet dort, wo Vorgesetzte mit am Tisch sitzen.
- **Zeitdruck:** Intern gewinnt immer das Tagesgeschäft.

Der externe Blick

- **Neutral:** keine eigene Rolle im Vorfall, keine Abteilungsinteressen.
- **Erfahren:** Muster aus vielen Organisationen und Branchen.
- **Prüfend:** weiß, was Auditor, Aufsicht und Versicherer nach einem Vorfall fragen.
- **Moderierend:** sorgt dafür, dass auch Unbequemes ausgesprochen wird.

Aus der Praxis: Die Wäscherei

In einer Klinik hängt die Versorgung mit Wäsche an einem einzigen externen Dienstleister. Im Alltag fällt das niemandem auf – die Wäsche kommt ja. Fällt dieser Dienstleister aus, fehlen innerhalb kurzer Zeit Bettwäsche, OP-Textilien und Dienstkleidung. Die Patientenversorgung ist betroffen, ohne dass ein einziges IT-System gestört ist.

Eine interne Nachbereitung würde den Ausfall des Dienstleisters als Ursache festhalten. Der externe Blick fragt weiter: Warum gab es keinen zweiten Anbieter, keinen Notvorrat, keine vertraglich vereinbarte Ersatzlösung – und warum stand diese Abhängigkeit in keiner Risikoanalyse?

Aus der Prüferpraxis: Im Audit frage ich nach dem letzten größeren Vorfall – und danach, was sich seitdem verändert hat. Eine dokumentierte Nachbereitung mit umgesetzten Maßnahmen überzeugt mehr als jede Richtlinie zum Vorfallmanagement.

SCHRITT 6 · VORLAGE ZUM AUSFÜLLEN

Maßnahmen umsetzen – und nachhalten

Erkenntnisse ohne Umsetzung sind nur gut gemeint. Jede Maßnahme braucht einen Verantwortlichen, einen Termin und ein Kriterium, an dem sich ihre Wirksamkeit prüfen lässt. Offene Punkte gehören in die Managementbewertung – bis sie erledigt sind.

Nachbereitung Vorfall / Störung	
Ereignis / Kennung	
Betroffene Kernprozesse	
Zeitraum (erkannt – abgeschlossen)	
Meldung an Behörde / Aufsicht	☐ nicht erforderlich (Begründung): ☐ erfolgt am:
Auslöser	
Ursache(n)	
Was gut funktioniert hat	
Was nicht funktioniert hat	
Betroffene Risiken (alt → neu)	
Lessons-Learned-Runde am / mit	

#	Maßnahme	Hebel*	Verantwortlich	Termin	Wirksamkeit geprüft durch
1					
2					
3					
4					

* W = senkt die Eintrittswahrscheinlichkeit · A = begrenzt die Auswirkung

BIA / Notfallpläne angepasst	☐ ja ☐ nicht erforderlich
Restrisiko entschieden durch / am	
Wiedervorlage in der Managementbewertung	

CHECKLISTE

Ist Ihr Vorfall wirklich abgeschlossen?

- [ ] Die Zeitleiste des Ereignisses ist rekonstruiert und dokumentiert.
- [ ] Eine Lessons-Learned-Runde mit allen Beteiligten hat stattgefunden – auch mit Fachbereichen und Dienstleistern.
- [ ] Auslöser und Ursache(n) sind unterschieden und benannt.
- [ ] Die Analyse betrachtet Mensch, Technik, Organisation, Prozesse, Dienstleister und Umfeld – nicht nur die IT.
- [ ] Die betroffenen Risiken sind neu bewertet – Wahrscheinlichkeit und Auswirkung.
- [ ] Maßnahmen haben Verantwortliche, Termine und Wirksamkeitskriterien.
- [ ] Die Leitung hat über Maßnahmen und Restrisiken entschieden.
- [ ] Business-Impact-Analyse, Notfallpläne und Erreichbarkeiten sind angepasst.
- [ ] Die Abschlussmeldung (falls meldepflichtig) enthält Ursache und Abhilfemaßnahmen.
- [ ] Die Wirksamkeit der Maßnahmen wird geprüft – etwa in einer Übung oder im internen Audit.
- [ ] Beinahe-Vorfälle werden künftig ebenfalls erfasst und ausgewertet.

Woran Sie sehen, ob Nachbereitung wirkt

Zeit bis zur Erkennung

Wie lange vergeht zwischen Beginn und Erkennen eines Ereignisses?

Zeit bis zum Wiederanlauf

Wie schnell ist der Kernprozess wieder verfügbar – im Vergleich zum Ziel?

Wiederkehrende Ursachen

Tauchen dieselben Ursachen in mehreren Vorfällen auf?

PROBIEREN SIE UNS AUS

SSC Logbuch – die Nachbereitung mit dem Blick von außen

Ein klar umrissener Einstieg: Sie hatten einen Vorfall, eine Störung oder einen Ausfall – wir bereiten ihn gemeinsam mit Ihnen nach. Mit dem neutralen Blick von außen und der Erfahrung aus Audits, Beratung und über 25 Jahren IT-Management.

1 · Moderierte Lessons-Learned-Runde

2 bis 3 Stunden mit allen Beteiligten, vor Ort oder per Teams – neutral moderiert, ohne Schuldfrage.

2 · Ursachenanalyse

Rekonstruktion der Zeitleiste und der Ursache-Wirkungs-Kette – über IT, Organisation, Prozesse und Dienstleister hinweg.

3 · Ergebnisbericht

Priorisierte Maßnahmen nach beiden Hebeln, Hinweise zur Neubewertung der Risiken und zur Anpassung der Notfallplanung.

Festpreis nach Vorgespräch

In einem kurzen Vorgespräch klären wir Ereignis, Beteiligte und Rahmen. Danach erhalten Sie ein Festpreisangebot – ohne Überraschungen.

Anrechnung bei Folgeauftrag

Entscheiden Sie sich im Anschluss für die Umsetzung mit uns, rechnen wir einen Teil des Preises für SSC Logbuch an.

Vorgespräch vereinbaren

30 Minuten per Microsoft Teams zur Klärung von Ereignis, Rahmen und Angebot. Den Termin wählen Sie direkt online.

Termin wählen: ssc-ism.de/kontakt

E-Mail: info@ssc-ism.de · Notfall- und Krisenprozesse dauerhaft aufbauen: SSC Anker · externer ISB: SSC Lotse

Jürgen Sottung – KRITIS-Auditor, ISO 27001 Lead Auditor, BCM-Beauftragter und externer ISB. Über 25 Jahre IT-Management als Führungskraft, heute auf der Seite der Prüfung und Beratung.

Stand: November 2026. Dieser Leitfaden gibt einen allgemeinen Überblick aus der Praxis und ersetzt keine Rechts- oder Einzelfallberatung. Quellen: ISO/IEC 27001:2022 (Abschnitt 10.2, Anhang A 5.27); ISO 22301; BSI-Standard 200-4; §§ 30, 32, 38 BSIG. © Sottung Security Consulting – Weitergabe in unveränderter Form ausdrücklich erwünscht.