Sottung Security Consulting
Informationssicherheit & Resilienz

Danach

KOMPAKT FÜR KLEINE UND MITTLERE UNTERNEHMEN

Ausfall überstanden. Und jetzt?

Wie Sie aus Störungen, Ausfällen und Sicherheitsvorfällen lernen – mit einer 60-Minuten-Nachbesprechung, einer einfachen Ursachensuche und einem Blatt zum Ausfüllen.

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

Stand: November 2026
ssc-ism.de

WARUM SICH DAS LOHNT

Nach dem Vorfall ist vor dem nächsten Vorfall

Der Server läuft wieder, die Rechnung ist bezahlt, der Dienstleister hat sich entschuldigt. Alle sind froh, dass es vorbei ist – und das Tagesgeschäft hat längst wieder übernommen.

Genau hier liegt die verpasste Chance. Ohne kurze Nachbereitung bleibt die Ursache bestehen, und derselbe Fehler kann wieder passieren. Dabei braucht es dafür weder einen Krisenstab noch ein Managementsystem – eine Stunde, die richtigen Fragen und ein Blatt Papier reichen für den Anfang.

Typische Ereignisse in kleinen und mittleren Unternehmen

Betrug per E-Mail
Eine gefälschte Rechnung oder geänderte Bankverbindung – und das Geld ist weg.

Schadsoftware
Ein Anhang wird geöffnet, Rechner oder Server sind verschlüsselt.

Ausfall des IT-Dienstleisters
Niemand erreichbar, als das System stand – oder das Problem lag beim Dienstleister selbst.

Cloud- oder Internetausfall
Branchensoftware, E-Mail oder Telefonie sind stundenlang weg.

Eine Person fehlt
Der Einzige, der sich mit der IT oder einem wichtigen Ablauf auskennt, ist krank oder im Urlaub.

Strom, Wasser, Brand
Ein Wasserschaden im Serverraum, ein Stromausfall, ein Kabelbrand.

Faustregel: Jedes Ereignis, das Ihren Betrieb spürbar gestört hat oder hätte stören können, ist eine Nachbesprechung wert. Auch ein Beinahe-Vorfall – etwa eine Betrugs-Mail, die gerade noch erkannt wurde.

SCHRITT 1

Die 60-Minuten-Nachbesprechung

Wann

Innerhalb von ein bis zwei Wochen – solange alle sich noch gut erinnern.

Wer

Alle Beteiligten, die Geschäftsführung und, wenn betroffen, der IT-Dienstleister.

Wie

Eine Stunde, eine Person moderiert, eine schreibt mit. Am Ende stehen Aufgaben mit Namen und Termin.

Fünf Fragen, die Sie stellen sollten

1. **Was ist genau passiert?** Der Ablauf in Stichpunkten: Wann fing es an, wann wurde es bemerkt, was wurde wann getan?
2. **Wie haben wir es bemerkt?** Durch Zufall, durch einen Kunden, durch den Dienstleister? Und wie lange hat das gedauert?
3. **Was lief gut?** Was soll beim nächsten Mal genauso laufen?
4. **Was lief schlecht?** Wen konnten wir nicht erreichen? Was wussten wir nicht? Was hat zu lange gedauert?
5. **Was ändern wir?** Konkrete Aufgaben – wer macht was bis wann?

Die wichtigste Regel: Fehler statt Schuldige

Wer Angst hat, bloßgestellt zu werden, erzählt nicht, was wirklich passiert ist. Fragen Sie deshalb nicht „Wer hat das gemacht?“, sondern „Warum konnte das passieren – und warum hatte es so große Folgen?“

SCHRITT 2

Die eigentliche Ursache finden

Der Auslöser ist selten die Ursache. Fragen Sie so lange „Warum?“, bis Sie bei etwas ankommen, das Sie ändern können.

Beispiel: die gefälschte Bankverbindung

Was	Eine Rechnung über 8.400 € wurde auf ein falsches Konto überwiesen.
Warum?	Ein „Lieferant“ hatte per E-Mail eine neue Bankverbindung mitgeteilt.
Warum?	Die Buchhaltung hat die Änderung einfach übernommen – die E-Mail sah echt aus.
Ursache	**Es gab keine Regel, Änderungen von Bankdaten telefonisch zu prüfen.**

Der Betrag ist erfunden, das Muster ist typisch. Die Maßnahme ist einfach und kostet nichts: Bankdaten werden nur nach Rückruf unter der bekannten Telefonnummer geändert.

Zwei Hebel für Ihre Maßnahmen

Damit es seltener passiert

- Rückruf-Regel bei Bankdaten und Zahlungen
- Zwei-Faktor-Anmeldung für E-Mail und Fernzugriff
- Updates automatisch einspielen lassen
- kurze Schulung zu Betrugs- und Phishing-Mails
- Vertretung für wichtige Personen festlegen

Damit es weniger schlimm wird

- Datensicherung, die nicht mitverschlüsselt werden kann – und getestet ist
- Notfallliste mit Telefonnummern auf Papier
- Absprache mit dem IT-Dienstleister: Wer ist wann erreichbar?
- Plan B für die wichtigsten Abläufe

SCHRITT 3 · ZUM AUSFÜLLEN

Das Nachbereitungsblatt

Ein Blatt pro Ereignis genügt. Heben Sie es auf – beim nächsten Mal sehen Sie, ob sich etwas wiederholt.

Nachbereitung	
Was ist passiert?	
Wann? Wie lange?	
Was war betroffen?	
Was lief gut?	
Was lief schlecht?	
Die eigentliche Ursache	
Nachbesprechung am / mit	

#	Was ändern wir?	Wer?	Bis wann?	Erledigt
1				☐
2				☐
3				☐
4				☐

Nach drei Monaten: Haben die Maßnahmen gewirkt?	

ZUM SCHLUSS

Ist der Vorfall wirklich abgeschlossen?

- [ ] Eine Nachbesprechung mit allen Beteiligten hat stattgefunden.
- [ ] Wir kennen die eigentliche Ursache – nicht nur den Auslöser.
- [ ] Jede Maßnahme hat einen Namen und einen Termin.
- [ ] Notfallliste und Absprachen mit Dienstleistern sind aktualisiert.
- [ ] Die Geschäftsführung hat entschieden, was umgesetzt wird.
- [ ] In drei Monaten schauen wir nach, ob die Maßnahmen gewirkt haben.

Wann sich Hilfe von außen lohnt

- wenn der Schaden groß war oder Kunden betroffen waren,
- wenn die Beteiligten selbst in den Vorfall verwickelt sind – und eine neutrale Moderation brauchen,
- wenn Sie nicht sicher sind, ob Sie die eigentliche Ursache gefunden haben,
- wenn Kunden, Versicherer oder Aufsicht wissen wollen, was Sie aus dem Vorfall gelernt haben.

SSC Logbuch – die Nachbereitung mit dem Blick von außen

Moderierte Nachbesprechung, Ursachenanalyse und ein kurzer Bericht mit priorisierten Maßnahmen – zum Festpreis, den Sie nach einem kurzen Vorgespräch erhalten. Bei einem Folgeauftrag wird ein Teil angerechnet.

Mehr erfahren: ssc-ism.de/ssc-leistungen/ssc-logbuch

Vorgespräch vereinbaren: ssc-ism.de/kontakt · E-Mail: info@ssc-ism.de

Stand: November 2026. Dieser Leitfaden gibt einen allgemeinen Überblick aus der Praxis und ersetzt keine Rechts- oder Einzelfallberatung. Ausführliche Fassung für NIS-2-pflichtige Einrichtungen: „Nach dem Vorfall ist vor dem nächsten Vorfall“ auf ssc-ism.de. © Sottung Security Consulting – Weitergabe in unveränderter Form ausdrücklich erwünscht.