

# Phase 11 – Notfallmanagement und Business Continuity

“„Nicht jeder Vorfall lässt sich verhindern – aber man kann vorbereitet sein.“

## Einleitung

Phase 11 – Notfallmanagement und Business Continuity ist ein Baustein auf dem Weg zu einem belastbaren ISMS für KMU. Die Phase verbindet organisatorische Sicht, technische Realität und die Anforderungen der Geschäftsführung.

## Ziel der Phase

Ziel ist es, die relevanten Informationen strukturiert zu erfassen, verständlich zu dokumentieren und als Grundlage für die nächsten Schritte nutzbar zu machen.

## Benötigte Teilnehmer

- Geschäftsführung oder IT-Entscheider
- Interner oder externer IT-Verantwortlicher
- Fachabteilungen nach Bedarf
- Datenschutz oder Qualitätsmanagement, falls vorhanden

## Arbeitsergebnisse der Phase

- Dokumentierte Ergebnisse der Bestandsaufnahme
- Offene Fragen und Risiken
- Erste Prioritäten für spätere Maßnahmen
- Grundlage für die nächste Phase

## Checkliste

## Notfallszenarien

## **Ziel**

Ransomware, Serverausfall, Internetausfall, Brand, Wasser, Stromausfall, Ausfall des Dienstleisters und Cloud-Ausfälle werden betrachtet. Szenarien müssen realistisch sein.

## **Warum ist das wichtig?**

Dieser Punkt sorgt dafür, dass Entscheidungen nicht auf Annahmen beruhen. Gerade in kleinen Unternehmen sind viele Informationen nicht dokumentiert, sondern nur einzelnen Personen bekannt. Durch die strukturierte Erfassung entsteht Transparenz und eine belastbare Grundlage für Risikoanalyse, Maßnahmenplanung und spätere Audits.

# Wiederaanlaufziele

## **Ziel**

RTO und RPO werden je Prozess oder System festgelegt. Entscheider müssen verstehen, welche Ausfallzeiten akzeptabel sind.

## **Warum ist das wichtig?**

Dieser Punkt sorgt dafür, dass Entscheidungen nicht auf Annahmen beruhen. Gerade in kleinen Unternehmen sind viele Informationen nicht dokumentiert, sondern nur einzelnen Personen bekannt. Durch die strukturierte Erfassung entsteht Transparenz und eine belastbare Grundlage für Risikoanalyse, Maßnahmenplanung und spätere Audits.

# Notfallkontakte

## **Ziel**

Geschäftsführung, IT-Dienstleister, Provider, Versicherer, Datenschutz, Rechtsberatung und Behördenkontakte werden dokumentiert. Im Notfall darf keine Suche beginnen.

## **Warum ist das wichtig?**

Dieser Punkt sorgt dafür, dass Entscheidungen nicht auf Annahmen beruhen. Gerade in kleinen Unternehmen sind viele Informationen nicht dokumentiert, sondern nur einzelnen Personen bekannt. Durch die strukturierte Erfassung entsteht Transparenz und eine belastbare Grundlage für Risikoanalyse, Maßnahmenplanung und spätere Audits.

# Kommunikationsplan

## **Ziel**

Es wird geregelt, wie intern und extern kommuniziert wird, wenn E-Mail oder Telefonie ausfallen. Alternative Kanäle müssen vorher bekannt sein.

## **Warum ist das wichtig?**

Dieser Punkt sorgt dafür, dass Entscheidungen nicht auf Annahmen beruhen. Gerade in kleinen Unternehmen sind viele Informationen nicht dokumentiert, sondern nur einzelnen Personen bekannt. Durch die strukturierte Erfassung entsteht Transparenz und eine belastbare Grundlage für Risikoanalyse, Maßnahmenplanung und spätere Audits.

# Restore-Verfahren

## **Ziel**

Wiederherstellungsschritte werden beschrieben und getestet. Ein Restore-Test ist der wichtigste Nachweis eines funktionierenden Backups.

## **Warum ist das wichtig?**

Dieser Punkt sorgt dafür, dass Entscheidungen nicht auf Annahmen beruhen. Gerade in kleinen Unternehmen sind viele Informationen nicht dokumentiert, sondern nur einzelnen Personen bekannt. Durch die strukturierte Erfassung entsteht Transparenz und eine belastbare Grundlage für Risikoanalyse, Maßnahmenplanung und spätere Audits.

# Entscheidungswege

## **Ziel**

Es wird festgelegt, wer Systeme abschalten, externe Hilfe beauftragen oder Kunden informieren darf. Unklare Entscheidungswege kosten im Ernstfall Zeit.

## **Warum ist das wichtig?**

Dieser Punkt sorgt dafür, dass Entscheidungen nicht auf Annahmen beruhen. Gerade in kleinen Unternehmen sind viele Informationen nicht dokumentiert, sondern nur einzelnen Personen bekannt. Durch die strukturierte Erfassung entsteht Transparenz und eine belastbare Grundlage für Risikoanalyse, Maßnahmenplanung und spätere Audits.

# Übungen

## Ziel

Notfallübungen oder Tabletop-Übungen prüfen, ob der Plan funktioniert. Schon eine jährliche Trockenübung bringt große Erkenntnisse.

## Warum ist das wichtig?

Dieser Punkt sorgt dafür, dass Entscheidungen nicht auf Annahmen beruhen. Gerade in kleinen Unternehmen sind viele Informationen nicht dokumentiert, sondern nur einzelnen Personen bekannt. Durch die strukturierte Erfassung entsteht Transparenz und eine belastbare Grundlage für Risikoanalyse, Maßnahmenplanung und spätere Audits.

# Typische Feststellungen

In KMU fehlen häufig aktuelle Dokumentationen, eindeutige Verantwortlichkeiten und regelmäßige Prüfungen. Das ist kein Vorwurf, sondern der Ausgangspunkt für den Aufbau eines ISMS.

# Hinweise für den IT-Berater

Wichtig ist eine pragmatische Sprache. Geschäftsführung und Fachbereiche müssen verstehen, welchen Nutzen die Phase für den Betrieb hat. Technische Details sind wichtig, sollten aber immer mit Geschäftsrisiken verbunden werden.

# Praxistipp

Am Ende jeder Phase sollte eine kurze Zusammenfassung erstellt werden: Was wurde erkannt, was ist kritisch, was ist offen und welche Entscheidung wird als nächstes benötigt?

# Ergebnis der Phase

Die Phase ist abgeschlossen, wenn die Ergebnisse so dokumentiert sind, dass eine andere fachkundige Person die Ausgangslage nachvollziehen und mit der nächsten Phase fortfahren kann.

---

Revision #4

Created 1 July 2026 08:11:31 by Stefan Kittel

Updated 1 July 2026 08:36:17 by Stefan Kittel