Phase 12 – Mitarbeitende sensibilisieren

> *„Menschen sind nicht das Problem – sie sind Teil der Sicherheitslösung.“*

Einleitung

Phase 12 – Mitarbeitende sensibilisieren 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

Grundlagenschulung

Ziel

Mitarbeitende lernen die wichtigsten Sicherheitsregeln. Inhalte sollten praxisnah und kurz 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.

Phishing erkennen

Ziel

Verdächtige E-Mails, Links, Anhänge und Absender werden erklärt. Phishing bleibt einer der häufigsten Angriffswege.

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.

Passwörter und MFA

Ziel

Sichere Passwörter, Passwortmanager und MFA werden verständlich erklärt. Ziel ist Akzeptanz, nicht Angst.

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.

Umgang mit Daten

Ziel

Vertrauliche Informationen, Kundendaten, Personaldaten und Ausdrucke werden behandelt. Informationssicherheit gilt auch außerhalb der IT-Systeme.

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.

Homeoffice und mobile Arbeit

Ziel

Private Netze, Geräte, Blickschutz, Transport und Verlust werden besprochen. Mobile Arbeit erweitert den Schutzbereich.

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.

Melden von Vorfällen

Ziel

Mitarbeitende müssen wissen, wie und an wen sie Vorfälle melden. Eine frühe Meldung ist wichtiger als Schuldzuweisung.

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.

Wiederholung

Ziel

Sensibilisierung ist kein einmaliges Ereignis. Kurze regelmäßige Impulse wirken besser als lange seltene Schulungen.

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 08:11:41 by Stefan Kittel
Updated 1 July 2026 08:36:27 by Stefan Kittel