Phase 5 – Bestehende Sicherheitsmaßnahmen

> *„Vorhandene Maßnahmen müssen nicht nur existieren, sondern wirksam sein.“*

Einleitung

Phase 5 – Bestehende Sicherheitsmaßnahmen bewerten 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

Patchmanagement

Ziel

Windows, Server, Office, Browser, Drittsoftware und Firmware werden betrachtet. Ungepatchte Systeme gehören zu den häufigsten Einfallstoren.

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.

Endpoint Security

Ziel

Antivirus, EDR, Firewall, Gerätekontrolle und Manipulationsschutz werden geprüft. Entscheidend ist die zentrale Verwaltung und Alarmierung.

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.

Backup und Restore

Ziel

Backupumfang, Zeitplan, Aufbewahrung, Offline-Schutz und Restore-Tests werden bewertet. Backups ohne getestete Wiederherstellung sind ein Scheinschutz.

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.

MFA und Zugriffsschutz

Ziel

Mehr-Faktor-Authentifizierung, Passwortregeln, Admintrennung und Zugriffsbeschränkungen werden geprüft. Besonders Cloud- und Fernzugriffe müssen abgesichert 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.

E-Mail-Sicherheit

Ziel

Spamfilter, Phishingschutz, SPF, DKIM, DMARC und sichere Anhänge werden bewertet. Viele Angriffe beginnen mit E-Mail.

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.

Netzwerksicherheit

Ziel

Firewallregeln, Segmentierung, VPN, WLAN-Sicherheit und offene Ports werden geprüft. Flache Netzwerke erhöhen das Schadensausmaß.

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.

Protokollierung und Monitoring

Ziel

Logs, Warnmeldungen, Systemüberwachung und Zuständigkeiten werden betrachtet. Ohne Monitoring werden Vorfälle oft erst spät erkannt.

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.

Physische Sicherheit

Ziel

Serverraum, USV, Zutritt, Brandschutz und Umgebung werden geprüft. Ein gestohlener oder beschädigter Server kann genauso kritisch sein wie ein Cyberangriff.

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 08:10:59 by Stefan Kittel
Updated 1 July 2026 08:35:17 by Stefan Kittel