KRITIS-Checkliste für Mittelständler

Umsetzungshilfe – Stand: Juni 2025, digitoren.de

---

1. Prüfen der Betroffenheit

- Ist mein Unternehmen in einem KRITIS-Sektor tätig?
- Überschreitet mein Unternehmen die Schwellenwerte (Mitarbeiter, Umsatz, kritische Dienstleistungen)?
- Wurde eine offizielle Einstufung als KRITIS-Betreiber vorgenommen?

---

2. Verantwortlichkeiten festlegen

- Sicherheitsbeauftragten für KRITIS und Informationssicherheit benennen
- Zuständigkeiten und Vertretungsregelungen schriftlich festhalten
- Notfallmanagement-Team aufstellen

---

3. Risiko- und Vorfallmanagement

- Risikoanalyse und Schwachstellenbewertung durchführen
- Maßnahmenplan zur Risikominimierung aufstellen
- Vorfallmanagement-Prozess definieren (Erkennung, Meldung, Reaktion)

---

4. Informationssicherheitsmanagement (ISMS)

- Einführung eines ISMS (z. B. nach ISO 27001) planen
- Sicherheitsrichtlinien und -prozesse dokumentieren
- Regelmäßige Überprüfung und Aktualisierung des ISMS

---

5. Melde- und Berichtspflichten

- Meldewege und Ansprechpartner bei Behörden (z. B. BSI) festlegen
- Meldeprozess für IT-Sicherheitsvorfälle etablieren
- Fristen und Anforderungen für Berichte dokumentieren

---

6. Technische und organisatorische Maßnahmen

- IT-Infrastruktur absichern (Firewalls, Virenschutz, Zugriffsmanagement)
- Regelmäßige Backups und Wiederherstellungstests durchführen
- Zutritts- und Zugriffskontrollen implementieren
- Notfall- und Wiederanlaufpläne erstellen

---

7. Sensibilisierung und Schulung

- Mitarbeitende regelmäßig zu KRITIS und IT-Sicherheit schulen
- Awareness-Kampagnen und Phishing-Tests durchführen
- Dokumentation der Schulungen und Teilnehmer

---

8. Überprüfung & Weiterentwicklung

- Interne Audits und Überprüfungen der Maßnahmen durchführen
- Schwachstellen und Verbesserungen dokumentieren
- Maßnahmenplan regelmäßig aktualisieren

Hinweis: Diese Checkliste dient als Orientierungshilfe. Prüfen Sie stets die aktuellen gesetzlichen Vorgaben und branchenspezifischen Anforderungen.