01

Checkliste

Die 7 Bausteine eines IT-Sicherheitskonzepts

02 Vorwort

Ein IT-Sicherheitskonzept ist weit mehr als eine Sammlung technischer Massnahmen.

Es ist ein ganzheitlicher Leitfaden, der zeigt, wie ein Unternehmen seine Daten, Systeme und Prozesse schützt – und dabei Verantwortung, Strukturen und Rollen klar benennt.

Diese Checkliste soll eine Orientierung geben:

Sie zeigt die sieben wichtigsten Bausteine, die in keinem IT-Sicherheitskonzept fehlen dürfen.
Sie richtet sich an KMU, Stiftungen und Organisationen, die mit sensiblen Daten arbeiten und den Spagat zwischen rechtlichen Vorgaben, technischer Sicherheit und menschlichem Handeln meistern müssen.

03

Die 7 Bausteine im Überblick

1. Ziele und Geltungsbereich

- Welche Systeme, Daten und Prozesse fallen in den Schutzbereich?
- Definition der besonders schützenswerten Daten (z. B. Patientendaten, Finanzdaten, interne Protokolle).
- Abgrenzung: Was gehört nicht dazu?

2. Risikobewertung

- Analyse möglicher Bedrohungen (Cyberangriffe, Datenverlust, menschliches Fehlverhalten).
- Einschätzung der Eintrittswahrscheinlichkeit und des Schadensausmasses.
- Dokumentation der Ergebnisse als Grundlage für Massnahmen.

3. Schutzmassnahmen

- **Technisch:** Firewalls, Backups, Multi-Faktor-Authentifizierung, Verschlüsselung
- **Organisatorisch:** klare Regeln für Zugriffsrechte, definierte Prozesse für Updates, Notfallpläne
- **Physisch:** Zutrittskontrollen zu Serverräumen, sichere Aufbewahrung von Datenträgern

04

Die 7 Bausteine im Überblick

4. Rollen und Verantwortlichkeiten

- **Geschäftsleitung** trägt die Gesamtverantwortung.
- **IT-Abteilung oder externe Partner** setzen Massnahmen um.
- **Mitarbeitende** sind im Alltag in der Pflicht (Passwörter, E-Mail-Sicherheit).
- **Stiftungsräte oder Verwaltungsräte** geben zusätzliche Vorgaben.

5. Abläufe und Prozesse

- Prävention: Regelmässige Schulungen, klare Regeln für den Umgang mit Daten.
- Incident-Response-Plan: Wer macht was im Ernstfall?
- Wiederherstellung: Wie werden Systeme schnellstmöglich wieder funktionsfähig gemacht?
- Kommunikation: Wer wird wann informiert (intern & extern)?

6. Rechtliche und organisatorische Vorgaben

- Schweizer Datenschutzgesetz (DSG) und EU-DSGVO
- Statuten von Stiftungen oder internen Gremien
- Branchenspezifische Standards (z. B. ISO 27001, FINMA-Richtlinien)
- Dokumentation aller Anforderungen, damit sie überprüfbar bleiben

05

Die 7 Bausteine im Überblick

7. Kontinuierliche Verbesserung

- Regelmässige Überprüfung und Aktualisierung des Konzepts
- Tests: Penetrationstests, Wiederherstellungsübungen, Audits
- Feedback einholen – von Mitarbeitenden, Kunden, Aufsichtsbehörden
- Dokumentieren, anpassen, verbessern: Das Konzept lebt.

06 Schlusswort

Ein IT-Sicherheitskonzept ist kein Selbstzweck. Es ist eine Haltung: Verantwortung übernehmen, klare Sprache wählen, verbindlich handeln.

So entsteht Sicherheit nicht nur auf technischer Ebene, sondern auch in der Zusammenarbeit mit Mitarbeitenden, Kunden und Partnern.

Ein gelebtes Konzept sorgt dafür, dass alle Beteiligten wissen, worauf es ankommt – und dass Vertrauen entsteht.

Kurz gesagt: Ein IT-Sicherheitskonzept ist dann erfolgreich, wenn es nicht nur geschrieben, sondern gelebt wird.

07

Hast Du noch Fragen?

Wir helfen Dir gerne weiter.

PLUS PLUS

Felsenaustrasse 17, 3004 Bern
031 511 22 33
team@plusundplus.ch
www.plusundplus.ch