NOTFALL-CHECKLISTE

Cyberangriff / IT-Sicherheitsvorfall

Was tun wenn es passiert ist? Sofortmassnahmen, Meldepflichten und Kommunikation.

WICHTIG: Diese Checkliste ausdrucken und offline verfügbar halten!

Phase 1: Sofortmaßnahmen (Erste 60 Minuten)

- ☐ Ruhe bewahren – keine übereilten Aktionen
- ☐ Betroffene Systeme NICHT ausschalten (Beweissicherung!)
- ☐ Betroffene Systeme vom Netzwerk isolieren (Kabel ziehen, WLAN aus)
- ☐ IT-Sicherheitsverantwortlichen informieren
- ☐ Geschaeftsführung informieren
- ☐ Zeitstempel und erste Beobachtungen dokumentieren
- ☐ Screenshots von Fehlermeldungen / Erpresserschreiben machen
- ☐ Keine Lösegeldforderungen bezahlen
- ☐ Passwörter für alle Admin-Konten SOFORT ändern
- ☐ Prüfen: Welche Systeme sind betroffen?

Phase 2: Analyse & Eindaemmung (Stunde 1-4)

- ☐ Art des Angriffs identifizieren (Ransomware, Phishing, DDoS...)
- ☐ Ausmaß des Schadens abschätzen
- ☐ Betroffene Daten identifizieren (personenbezogen?)
- ☐ Backup-Status prüfen (sind Backups sauber?)
- ☐ Forensische Sicherung der betroffenen Systeme
- ☐ Externe IT-Sicherheitsexperten hinzuziehen (z.B. ITSB Deutschland)
- ☐ Kommunikationskanal fuer Krisenstab einrichten

Phase 3: Meldepflichten (24-72 Stunden)

DSGVO-Meldepflicht (Art. 33):

- Meldung an Aufsichtsbehörde innerhalb von 72 Stunden
- Zuständige Behörde: Landesbeauftragter für Datenschutz
- Online-Meldeformular nutzen (www.lda.bayern.de)

NIS2-Meldepflicht:

- Frühwarnung innerhalb von 24 Stunden an BSI
- Detaillierte Meldung innerhalb von 72 Stunden
- Abschlussbericht innerhalb von 1 Monat

Weitere Meldungen prüfen:

- ■ Betroffene Personen informieren (Art. 34 DSGVO)?
- ■ Cyberversicherung informieren (Frist beachten!)
- ■ Strafanzeige bei Polizei erstatten
- ■ BSI-Meldung (bei KRITIS/NIS2-Betroffenheit)

Phase 4: Wiederherstellung

- ■ Systeme aus sauberem Backup wiederherstellen
- ■ Sicherheitslücke identifizieren und schliessen
- ■ Alle Passwörter zurücksetzen (alle Benutzer)
- ■ MFA für alle Konten aktivieren
- ■ Systeme schrittweise wieder ans Netz nehmen
- ■ Monitoring verstärken (erhöhte Wachsamkeit)
- ■ Funktionstest aller wiederhergestellten Systeme

Phase 5: Nachbereitung

- ■ Detaillierten Vorfallsbericht erstellen
- ■ Lessons Learned Workshop durchführen
- ■ Sicherheitsmaßnahmen anpassen
- ■ Mitarbeiterschulung durchführen
- ■ Notfallpläne aktualisieren
- ■ Nächsten Audit-Termin vereinbaren

ITSB Notfall-Hotline:089200011 380

E-Mail: help@itsb-deutschland.de