CHECKLISTE

# IT-Notfall — erste Stunde

Was intern klären, bevor die Technik beginnt

| | |
|---|---|
| **Dokument-ID** | BR-CHK-003 |
| **Version** | 1.0 |
| **Stand** | 27. Juni 2026 |
| **Klassifizierung** | Öffentlich — kostenloser Ratgeber |
| **Autor** | Benjamin Raulf, BR-Systems |
| **Herausgeber** | BR-Systems · IT-Systemhaus · Unterlüß |
| **Kontakt** | info@br-systems.eu · 0179 160 1700 |

> Bei Ransomware, Totalausfall oder Datenverlust zählt die erste Stunde. Diese Liste hilft Geschäftsführung und IT-Verantwortlichen, Ruhe zu bewahren und die richtigen Schritte nicht zu vergessen.

## Sofort (0–15 Minuten)

- ☐ Betroffene Systeme vom Netz trennen — nicht herunterfahren, wenn Ransomware aktiv ist
- ☐ Keine Löschungen „auf Verdacht“
- ☐ Interne Meldekette starten (GF, IT, Datenschutz wenn personenbezogene Daten)
- ☐ Uhrzeit und Symptome notieren (Screenshots, Fehlermeldungen)

## Klären (15–60 Minuten)

- ☐ Was ist betroffen? (Dateien, Server, E-Mail, ERP)
- ☐ Gibt es ein aktuelles Backup — wann war der letzte erfolgreiche Restore-Test?
- ☐ Externe Dienstleister und Verträge parat (IT-Partner, Versicherung, Anwalt)
- ☐ Passwörter von betroffenen Konten zurücksetzen — nach Abstimmung
- ☐ Kunden und Lieferanten: nur informieren, wenn es zwingend ist — Text vorher abstimmen

## Nachbereitung

- ☐ Ursache dokumentieren und Maßnahmenplan mit Terminen
- ☐ Restore-Test und Backup-Strategie überprüfen
- ☐ Lessons Learned intern besprechen — ohne Schuldzuweisungen