# Leseprobe

Zwei Auszüge als kostenfreie Vorschau: der Notfall-Erstcheck und die Sofortmaßnahmen-Karte Ransomware. Das vollständige Handbuch (9 Kapitel, ausfüllbar als PDF, Word und Markdown) erhalten Sie nach dem Kauf über Digistore24.

KAPITEL 2

# Notfall-Erstcheck

Diese Seite ist der Einstieg im Ernstfall. Erst einstufen, dann handeln — nicht umgekehrt.

## 1. Ruhe bewahren und einstufen

| Einstufung | Merkmale | Reaktion |
|---|---|---|
| Störung | Einzelner Arbeitsplatz oder einzelne Funktion betroffen, Arbeit geht eingeschränkt weiter | Normaler IT-Support, keine Meldekette |
| Notfall | Mehrere Mitarbeitende oder ein zentrales System betroffen (Server, Internet, Telefonie, Kasse/ERP) | Dieses Handbuch: Meldekette (Kapitel 4) + passende Sofortmaßnahmen-Karte (Kapitel 5) |
| Krise | Existenzbedrohend: Ransomware, vollständiger Datenverlust, längerer Komplettausfall | Meldekette + Leitung übernimmt, externe Hilfe einbinden, Meldepflichten prüfen (Kapitel 7) |

## 2. Die ersten fünf Minuten

1. Beobachtung notieren: Was geht nicht? Seit wann? Wer ist betroffen? (Protokollbogen, Kapitel 8 — ab jetzt mitschreiben.)
2. Einstufen anhand der Tabelle oben.
3. Bei Notfall oder Krise: erste Person der Meldekette anrufen (Kapitel 4). Telefon vor E-Mail — E-Mail könnte selbst betroffen sein.
4. Passende Sofortmaßnahmen-Karte aufschlagen (Kapitel 5) und Schritt für Schritt abarbeiten.
5. Nichts auf eigene Faust reparieren, neu starten oder löschen, bevor die Karte oder ein Fachmann es sagt — voreilige Neustarts vernichten Spuren und können Schäden vergrößern.

> **Wichtig:** Verdacht auf Ransomware oder Angriff? Betroffene Geräte vom Netzwerk trennen (Netzwerkkabel ziehen, WLAN aus) — aber NICHT ausschalten. Karte R (Kapitel 5) befolgen.

# Karte R — Ransomware

### WORAN SIE ES ERKENNEN

- Dateien lassen sich nicht öffnen, tragen fremde Endungen oder es erscheint eine Erpressernachricht.
- Ungewöhnliches Verhalten: unbekannte Anmeldungen, deaktivierter Virenschutz, massenhaft veränderte Dateien.

### SOFORT TUN

1. Betroffene Geräte sofort vom Netzwerk trennen: Netzwerkkabel ziehen, WLAN deaktivieren. Geräte NICHT ausschalten (Spuren im Arbeitsspeicher).
2. Meldekette starten — dies ist immer Notfall, bei Verschlüsselung Krise.
3. Backups schützen: Backup-Medien/Verbindungen sofort physisch trennen, bevor auch sie verschlüsselt werden.
4. Versicherung kontaktieren (Kapitel 3) BEVOR externe Forensik beauftragt wird.
5. Anzeige bei der ZAC erstatten (Kapitel 3); Meldepflicht Datenschutz prüfen (Kapitel 7). Erpressernachricht fotografieren, nichts daran verändern.

### AUF KEINEN FALL

- Lösegeld zahlen oder Kontakt zu Erpressern aufnehmen — erst Polizei und Versicherung einbinden, die Entscheidung trifft die Geschäftsführung mit Beratung.
- Geräte formatieren oder „bereinigen“, bevor Forensik und Versicherung zugestimmt haben — Beweismittel gehen verloren.
- Mit kompromittierten Systemen weiterarbeiten oder Passwörter darauf eingeben.

### ESKALATION

Sofort: externer IT-Dienstleister/Forensik (über Versicherung), ZAC, ggf. Datenschutzbehörde binnen 72 h. Wiederanlauf nur von sauberen Backups auf geprüften Systemen.