mertes.dev

Notfallkarte

SOFORTMASSNAHMEN (0–15 Minuten)

☐ System nicht weiter benutzen
☐ Keine Neustarts / keine Schreibzugriffe
☐ Netzwerkverbindung prüfen → ggf. isolieren
☐ Incident dokumentieren (Zeit, System, Symptome)
☐ Verantwortliche informieren

SCHADENSBEGRENZUNG (15–60 Minuten)

☐ Betroffene Systeme identifizieren
☐ Ausbreitung stoppen (z. B. Netzwerksegmentierung)
☐ Kritikalität bewerten (P1–P4)
☐ Backup-Verfügbarkeit prüfen

FORENSISCHE SICHERUNG

☐ Disk Image erstellen (bitweise Kopie)
☐ Optional: Memory Dump sichern
☐ Hashwerte bilden (Integrität!)
☐ Nur auf Kopien arbeiten

ANALYSE

☐ Ursache identifizieren (User, System, Angriff?)
☐ Umfang bestimmen (welche Systeme/Daten?)
☐ Logs und Metadaten analysieren
☐ Prüfen: gelöscht vs. verschlüsselt vs. beschädigt

RECOVERY

☐ Primär: Backup Restore
☐ Alternativ: File Recovery / Forensik
☐ Applikationen prüfen (DB, E-Mail etc.)
☐ Schrittweise Wiederherstellung

VALIDIERUNG

☐ Daten vollständig?
☐ Systeme funktionsfähig?
☐ Integrität geprüft (Hash / DB Consistency)?
☐ Fachbereich bestätigt?

WIEDERINBETRIEBNAHME

☐ Systeme kontrolliert online bringen
☐ Monitoring aktivieren
☐ Zugriff schrittweise freigeben

NACHBEREITUNG (PFLICHT!)

☐ Root Cause dokumentieren
☐ Schwachstellen beheben
☐ Backup-Strategie prüfen (RPO/RTO)
☐ Sicherheitsmaßnahmen verbessern

GOLDENE REGELN

✗ Kein hektisches „Fixen“ ohne Analyse
✗ Kein Arbeiten auf Originaldaten
✗ Kein Vertrauen in ungetestete Backups
✓ Immer strukturiert vorgehen
✓ Recovery ist ein Prozess, kein Tool
✓ Prävention ist günstiger als Wiederherstellung

INTERNER KONTAKT

Incident Owner: _____ IT-Verantwortlicher: _____ Externer Dienstleister: _____