mertes.dev

Playbook

Incident Response & Data Recovery

Autor: Andre Mertes

26. April 2026

Inhaltsverzeichnis

1. Klassifikation von Vorfällen (Incident Typen)

Nicht jeder Datenverlust ist gleich kritisch. Eine schnelle Einordnung spart Zeit.
Typische Incident-Kategorien:

- **P1 – Kritisch:**
  Totalausfall produktiver Systeme, Ransomware, Datenbankverlust
- **P2 – Hoch:**
  Teilverlust von Daten, E-Mail-Ausfall, beschädigte Filesysteme
- **P3 – Mittel:**
  Einzelne Dateien oder Benutzer betroffen
- **P4 – Niedrig:**
  Testsysteme, nicht geschäftskritische Daten

Ziel: Priorisierung nach Business Impact, nicht nach technischer Komplexität.

2. Sofortmaßnahmen (First Response)

Grundregel: Jede unnötige Systeminteraktion kann Daten überschreiben.

Checkliste

- [ ] Schreibzugriffe stoppen (System ggf. isolieren)
- [ ] Betroffene Systeme vom Netzwerk trennen (bei Verdacht auf Angriff)
- [ ] Keine „Quick Fixes“ oder Neustarts ohne Analyse
- [ ] Incident dokumentieren (Zeitpunkt, Symptome, Änderungen)
- [ ] Verantwortliche informieren

Bei kritischen Systemen: kein produktiver Weiterbetrieb ohne Bewertung

3. Forensische Sicherung (Acquisition Phase)

Ziel ist ein forensisch sauberes Abbild, bevor Änderungen erfolgen.

Technische Maßnahmen

- Disk Imaging (bitweise Kopie)
- Speicherabbild (Memory Dump) bei laufenden Systemen
- Hashing (z. B. SHA-256) zur Integritätsprüfung

Best Practices

- Nur auf Kopien arbeiten, niemals auf Originalsystemen
- Write Blocker verwenden (physisch oder logisch)
- Zeitstempel (MAC Times) erhalten

4. Analysephase (Root Cause & Scope)

Jetzt geht es darum zu verstehen: Was ist passiert und wie weit reicht der Schaden?

Typische Analysepunkte

- Dateisystem-Metadaten (MFT, Inodes)
- Logfiles (System, Auth, Application)
- Benutzeraktivitäten (z. B. Shell-History)
- Netzwerkverkehr (falls vorhanden)

Wichtige Fragen

- Wurden Daten gelöscht, überschrieben oder verschlüsselt?
- Ist der Vorfall lokal oder systemisch?
- Gibt es Persistenzmechanismen (z. B. Malware)?

5. Wiederherstellung (Recovery Phase)

Die eigentliche Datenrettung erfolgt erst nach der Analyse.

Recovery-Strategien

1. Backup-Restore (bevorzugt)
   - Voll- oder inkrementelle Backups
   - Snapshot-Recovery (z. B. VM, Storage)
2. File-System-Recovery
   - Wiederherstellung über Metadaten
   - File Carving bei beschädigten Strukturen
3. Applikations-Level
   - Datenbanken (Point-in-Time Recovery)
   - E-Mail-Systeme (Mailbox Restore)

6. E-Mail Recovery Runbook

E-Mails sind oft geschäftskritisch und müssen separat betrachtet werden.

Ablauf

- Papierkorb / Soft Delete prüfen
- Server-seitige Backups analysieren
- Mailbox-Datenbanken wiederherstellen
- Lokale Clients prüfen (Cache-Dateien)

Hinweise

- Retention Policies beachten
- Journaling/Archivsysteme nutzen
- Wiederherstellung testen, bevor produktiv geschaltet wird

7. Validierung & Integritätsprüfung

Nach der Wiederherstellung ist vor der Freigabe.

Checks

- [ ] Hash-Vergleiche (falls vorhanden)
- [ ] Applikationstests (funktionieren Systeme?)
- [ ] Datenkonsistenz prüfen (z. B. Datenbanken)
- [ ] Benutzerabnahme (Fachbereich!)

8. Wiederinbetriebnahme (Restore to Production)

Vorgehen

- Systeme schrittweise wieder online bringen

- Monitoring aktivieren (Logs, Alerts)
- Zugriff kontrollieren freigeben

Kein „Big Bang“, sondern kontrollierter Rollout.

9. Lessons Learned & Härtung

Der wichtigste Teil wird oft übersprungen.

Analyse

- Was war die Root Cause?
- Warum hat Prävention versagt?
- Wie lange war die Downtime?

Maßnahmen

- Backup-Strategie verbessern (RPO/RTO anpassen)
- Monitoring erweitern
- Security-Härtung (Patching, MFA, Segmentierung)
- Mitarbeiterschulung

10. Minimal-Setup (Quick Wins)

Falls wenig Ressourcen vorhanden sind:

- Tägliche Backups + Offsite-Kopie
- Monatlicher Restore-Test
- Zentrale Log-Sammlung
- Definierter Incident Owner
- Dokumentiertes Mini-Playbook (z.B. dieses hier!)

11. Kompakte Notfall-Checkliste

Wenn Datenverlust auftritt:

1. System nicht weiter nutzen
2. Netzwerkverbindung prüfen / ggf. trennen
3. Incident dokumentieren
4. Backup-Verfügbarkeit prüfen
5. Forensische Kopie erstellen
6. Recovery planen – nicht improvisieren
7. Wiederherstellung durchführen
8. Ursache analysieren
9. Maßnahmen ableiten

Fazit

Ein funktionierendes Incident Response & Recovery Playbook reduziert nicht nur Ausfallzeiten, sondern verhindert Folgefehler – insbesondere vorschnelle, destruktive Maßnahmen. Das Ziel ist nicht nur Recovery, sondern kontrollierte, nachvollziehbare und reproduzierbare Wiederherstellung.