/ MAURISEC.DE

FIELD NOTES / CHECKLIST 09

Backup ist erst gut, wenn der Restore funktioniert

PRUEFEN. BELEGEN. NACHHALTEN.

Prüfliste für Datensicherung und Wiederanlauf geschäftskritischer Dienste. Tests nur geplant und autorisiert durchführen; Produktivdaten sowie laufende Systeme schützen.

Pruefbereich / Team:

Datum:

- [ ] **01 / Mit den Fachverantwortlichen festlegen, welcher Datenverlust und welche Ausfallzeit je Dienst höchstens vertretbar sind.**

  Nachweis: Freigegebene Wiederanlaufziele, Datenverlustziele und priorisierte Dienste.

- [ ] **02 / Daten, Konfigurationen, Identitätsabhängigkeiten, Schlüssel, Installationsmedien und benötigte Lizenzen in die Wiederherstellungsplanung aufnehmen.**

  Nachweis: Abhängigkeitsliste und zugängliche Wiederanlaufunterlagen auch bei Ausfall des Hauptsystems.

- [ ] **03 / Sicherungskopien gegen Mitverschlüsselung oder Löschung absichern, etwa durch Offline-Kopien beziehungsweise geeignete unveränderbare Aufbewahrung.**

  Nachweis: Belegte Trennung und kontrollierter Test der Schutzwirkung; nicht lediglich ein zweites verbundenes Laufwerk.

- [ ] **04 / Backup-Verwaltung und privilegierte Zugänge vom normalen Betriebszugriff trennen; Wiederherstellungsbefugnisse eindeutig festlegen.**

  Nachweis: Rollen, getrennte Zugangspfade, Vertretung und überprüfte Berechtigungen.

- [ ] **05 / Sicherungen angemessen verschlüsseln und die Wiederverfügbarkeit der Schlüssel unabhängig vom ausgefallenen Produktivsystem testen.**

  Nachweis: Dokumentierter Schlüsselzugang und erfolgreicher Entschlüsselungstest durch Berechtigte.

/ MAURISEC.DE

FIELD NOTES / CHECKLIST 09

- [ ] **06 / Fehlgeschlagene und ausbleibende Sicherungen überwachen; Rückstau und Kapazitätsprobleme mit Verantwortlichen verfolgen.**

  Nachweis: Alarmtest, bearbeitete Fehler und nachvollziehbare Sicherungsläufe.

- [ ] **07 / Regelmäßig einen vollständigen Dienst in einer geeigneten isolierten Umgebung wiederherstellen; Datenintegrität und Fachfunktion prüfen.**

  Nachweis: Zeitmessung, verwendeter Sicherungsstand, Konsistenzprüfung und fachliche Abnahme.

- [ ] **08 / Einen Ransomware-Fall üben: sauberen Wiederherstellungspunkt bestimmen und erneute Einschleppung vor Wiederanbindung vermeiden.**

  Nachweis: Übungsprotokoll, Prüfungen auf Kompromittierung und dokumentierte Wiederanbindungsentscheidung.

- [ ] **09 / Erreichte Zeiten und tatsächlichen Datenstand mit den Zielen vergleichen; Lücken beheben und Wiederanlaufplan aktualisieren.**

  Nachweis: Soll-Ist-Abgleich, Maßnahmenliste und wiederholter Test nach wesentlichen Änderungen.

GEGENPROBE / AUTORISIERTE TESTUMGEBUNG

Eine repräsentative Testwiederherstellung isoliert durchführen und fachliche Nutzbarkeit sowie gemessene Wiederanlaufzeit prüfen.

GRENZEN UND VORAUSSETZUNGEN

Unveränderbarkeit ist nicht automatisch Offline-Trennung und schützt nicht vor jeder Fehlkonfiguration. Eine erfolgreiche Backup-Meldung beweist keinen nutzbaren Restore. Aufbewahrung, Löschung, Verschlüsselung und regionale Speicherung müssen zu Datenarten, Verträgen und rechtlichen Anforderungen passen. Produktions-Restores nicht unangekündigt zum Test verwenden.

PRIMAERQUELLEN / STAND 09.11.2026

CISA: #StopRansomware Guide
www.cisa.gov

NIST SP 800-184: Guide for Cybersecurity Event Recovery
csrc.nist.gov

BSI: Umsetzungshinweise CON.3 Datensicherungskonzept
www.bsi.bund.de