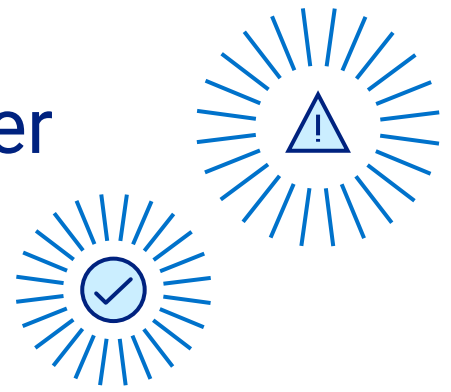


Checkliste für Krankenhäuser im Cybersecurity-Ernstfall



1. Patientenversorgung sicherstellen

2. Notbetrieb initiieren

- Grundvoraussetzung für den Notbetrieb: Offsite Backups gemäß 3-2-1-Regel
- BSI gemäß KRITIS-Pflicht informieren
- Remediation-Phase inkl. Schließen der Sicherheitslücken
- Fallback-System nutzen, um den Betrieb sicherzustellen, z. B.:
 - auf eigene dezentrale Backups der Krankenakten oder Backups bei externen (Cloud-)Dienstleistern zugreifen
 - Krankenakten auf Papier ausdrucken (hausintern oder durch Dienstleister)

3. Infrastruktur für die Wiederherstellung bereitstellen

- Entscheidung über Sofortmaßnahmen treffen, etwa:
 - in neue lokale Hardware investieren
 - auf die Cloud umsteigen (KRITIS-konforme Anbieter mit Hosting in DE/EU wählen)
- Neue Hardware oder Cloud-Umgebung in Betrieb nehmen



4. Backup-Integrität prüfen

- Backups auf Malware, manipulierte Dateien und schädliche Konfigurationen prüfen
- Sandbox zur Analyse verwenden
- Wiederherstellung zuerst in isolierter Testumgebung (Staging-System) testen
- Anomalien in Backup Logs suchen

5. Regelbetrieb schrittweise wiederherstellen

- Authentifizierung und Nutzeranmeldung ermöglichen
- Kommunikationssysteme wiederherstellen
- Weitere kritische Systeme priorisieren und aktivieren

6. Prävention und Zukunftssicherheit

- BCM-Pläne regelmäßig testen (inkl. Übungen mit dem Personal)
- Fallback Hardware für den Notfall vorhalten (oder entsprechende Verträge schließen)
- Cloud- und Managed-Service-Anbieter evaluieren
- Data Vaults (Datentresore) für höchste Backup-Sicherheit implementieren
- Regelmäßige Updates nach der 3-2-1-Regel durchführen