Muster-Prüfprogramm

BSI-Grundschutz

Backup und Wiederherstellung

13 Prüfschritte · BSI-Grundschutz

13 Prüfschritte mit Kriterium, Fundstelle, Prüfhandlung und erwarteten Nachweisen. 8 Unterlagen zur Anforderung und die typischen Feststellungen.

BSI CON.3 · BSI DER.4 · NIS2-Richtlinie Art. 21 Abs. 2 lit. c · ISO/IEC 27001:2022 Anhang A 8.13 · ISO/IEC 27001:2022 Anhang A 5.23 · NIS2-Richtlinie Art. 21 Abs. 2 lit. f

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob die Organisation Daten und Systeme so sichert, dass sie nach einem Ausfall, einem Fehler oder einem Angriff innerhalb der geforderten Zeit und mit dem geforderten Datenstand wiederhergestellt werden können. Entscheidend ist der Nachweis, dass die Wiederherstellung funktioniert, nicht nur, dass Sicherungen laufen.

GELTUNGSBEREICH

- Server, virtuelle Maschinen, Datenbanken, Fachanwendungen und Dateiablagen im Rechenzentrum und, soweit relevant, an Standorten
- Daten in Cloud- und SaaS-Diensten, soweit die Organisation für ihre Sicherung verantwortlich ist
- Sicherungssoftware, Speichersysteme, Medien und Aufbewahrungsorte
- Nicht Gegenstand: Archivierung zur Erfüllung von Aufbewahrungspflichten, sofern nicht gesondert vereinbart

Prüfschritte 1 bis 3

Schritt 01 — BSI CON.3

Ein Datensicherungskonzept besteht, ist freigegeben und aktuell.

Prüfhandlung Konzept lesen, Freigabe und Datum der letzten Überprüfung feststellen und die Verantwortlichen erfragen.

Nachweise Datensicherungskonzept mit Freigabevermerk und Version

Schritt 02 — BSI CON.3; BSI DER.4

Zulässiger Datenverlust und Wiederanlaufzeit je System sind aus den Anforderungen der Geschäftsprozesse abgeleitet.

Prüfhandlung Vorgaben je System mit den Ergebnissen der Auswirkungsanalyse vergleichen und Abweichungen erfragen.

Nachweise Übersicht der Vorgaben je System, Auswirkungsanalyse

Schritt 03 — BSI CON.3

Alle relevanten Systeme und Daten sind in die Sicherung einbezogen.

Prüfhandlung Systemübersicht und Konfigurationsverwaltung mit den Sicherungsaufträgen abgleichen und nicht gesicherte Systeme ermitteln.

Nachweise Systemübersicht, Liste der Sicherungsaufträge

Prüfschritte 4 bis 6

Schritt 04 — BSI CON.3

Verfahren, Zeitpunkte und Aufbewahrungsdauer der Sicherungen entsprechen den Vorgaben des Konzepts.

Prüfhandlung Konfiguration der Sicherungsaufträge für eine Stichprobe von Systemen mit dem Konzept vergleichen.

Nachweise Auszug der Jobkonfiguration, Konzept

Schritt 05 — BSI CON.3

Sicherungsläufe werden überwacht, Fehler werden bearbeitet und nachvollziehbar abgeschlossen.

Prüfhandlung Protokolle eines Monats ansehen, Fehlläufe auswählen und die Bearbeitung bis zum Abschluss verfolgen.

Nachweise Sicherungsprotokolle, Meldungen und Tickets zu Fehlläufen

Schritt 06 — BSI CON.3; NIS2-Richtlinie Art. 21 Abs. 2 lit. c; ISO/IEC 27001:2022 Anhang A 8.13

Sicherungen sind vor Manipulation und Verschlüsselung durch Schadsoftware geschützt, etwa durch getrennte Zugangsdaten und unveränderbare oder getrennt gelagerte Kopien.

Prüfhandlung Zugriffsrechte auf Sicherungssystem und Medien prüfen und feststellen, ob mindestens eine Kopie aus der Produktionsumgebung nicht änderbar ist.

Nachweise Berechtigungsauszug, Architekturübersicht, Konfiguration unveränderbarer Speicher

Prüfschritte 7 bis 9

Schritt 07 — BSI CON.3

Sicherungsmedien und gespeicherte Sicherungen sind gegen unbefugten Zugriff geschützt, bei Bedarf verschlüsselt.

Prüfhandlung Verschlüsselungseinstellungen und Zugriffsrechte prüfen und die Schlüsselverwaltung ansehen.

Nachweise Konfigurationsauszug, Konzept zur Schlüsselverwaltung

Schritt 08 — BSI CON.3

Mindestens eine Kopie wird räumlich getrennt vom Produktivsystem aufbewahrt.

Prüfhandlung Aufbewahrungsorte ansehen und die räumliche und organisatorische Trennung beurteilen.

Nachweise Standortliste der Kopien, Besichtigungsnotiz oder Nachweis des Dienstleisters

Schritt 09 — BSI CON.3; ISO/IEC 27001:2022 Anhang A 8.13

Wiederherstellungen werden regelmäßig getestet; Ergebnis und benötigte Zeit werden mit den Vorgaben verglichen.

Prüfhandlung Testplan und Testprotokolle der letzten zwölf Monate prüfen und, wenn möglich, eine Wiederherstellung beobachten.

Nachweise Testplan, Testprotokolle mit Zeitmessung, Abweichungsmeldungen

Prüfschritte 10 bis 13

Schritt 10 — BSI CON.3; BSI DER.4

Das Wiederherstellungsverfahren ist dokumentiert, Verantwortliche sind benannt und die Dokumentation steht auch bei Ausfall der Hauptumgebung bereit.

Prüfhandlung Handbuch lesen, Ablageorte prüfen und feststellen, ob die Unterlagen offline erreichbar sind.

Nachweise Wiederherstellungshandbuch, Verantwortlichenliste, Ablagekonzept

Schritt 11 — BSI CON.3

Aufbewahrungs- und Löschfristen der Sicherungen sind festgelegt und werden eingehalten.

Prüfhandlung Fristen mit den Einstellungen der Sicherungssoftware und den vorhandenen Beständen vergleichen.

Nachweise Fristenregelung, Bestandsauszug der Sicherungen

Schritt 12 — ISO/IEC 27001:2022 Anhang A 5.23

Bei Cloud- und SaaS-Diensten ist geklärt, wer welche Daten sichert, und die Zusage des Anbieters ist nachweisbar.

Prüfhandlung Verträge und Leistungsbeschreibungen zur Datensicherung lesen und Nachweise zu Sicherung und Wiederherstellung anfordern.

Nachweise Vertragsauszüge, Leistungsbeschreibung, Bestätigungen des Anbieters

Schritt 13 — NIS2-Richtlinie Art. 21 Abs. 2 lit. f

Die Verantwortlichen erhalten regelmäßig Kennzahlen zu Erfolgsquote, Testergebnissen und offenen Mängeln.

Prüfhandlung Berichte der letzten zwölf Monate ansehen und Maßnahmen zu festgestellten Mängeln verfolgen.

Nachweise Berichte, Maßnahmenliste

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Datensicherungskonzept und Wiederherstellungshandbuch
2. Vorgaben zu zulässigem Datenverlust und Wiederanlaufzeit je System
3. Systemübersicht und Liste der Sicherungsaufträge
4. Sicherungsprotokolle eines zusammenhängenden Monats
5. Testplan und Testprotokolle der Wiederherstellung
6. Berechtigungsauszug für Sicherungssystem und Medien
7. Verträge und Leistungsbeschreibungen von Cloud- und Sicherungsdienstleistern
8. Berichte zu Sicherungskennzahlen

TYPISCHE FESTSTELLUNGEN

- Wiederherstellungstests fanden nie oder nur für einzelne Dateien statt, nicht für komplette Systeme.
- Neue Systeme sind nicht in die Sicherung aufgenommen worden.
- Das Sicherungssystem ist mit denselben Administratorkonten erreichbar wie die Produktion.
- Es gibt keine Kopie, die vor Verschlüsselung durch Schadsoftware geschützt ist.
- Fehlgeschlagene Läufe werden nicht verfolgt, einzelne Systeme sind seit Wochen ohne gültige Sicherung.
- Die gemessene Wiederherstellungszeit liegt deutlich über der Vorgabe des Geschäftsbereichs.

Bibliothek Muster-Prüfprogramme

29 Muster-Prüfprogramme online

proauditmap.com/pruefprogramme/

Vollständiges Prüfpaket in ProAuditMap

proauditmap.com

ProAuditMap

Muster ohne Gewähr und keine Rechtsberatung. Gesetze, Verordnungen und Standards erscheinen nur als Fundstelle, Normtexte sind nicht abgedruckt. Passen Sie Umfang und Tiefe vor der Verwendung an Ihre Organisation, Ihre Risiken und die aktuelle Fassung der für Sie geltenden Vorschriften an. Stand: 13. Oktober 2026