Muster-Prüfprogramm

Kryptografie und Schlüsselmanagement

12 Prüfschritte · NIS2, BSI, ISO 27001

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

NIS2-Richtlinie Art. 21 Abs. 2 lit. h · § 30 Abs. 2 Nr. 8 BSIG · BSI CON.1 · BSI TR-02102-1 · ISO/IEC 27001:2022 Anhang A 8.24 · BSI TR-02102-2 · DORA Art. 9 Abs. 4 lit. d · ISO/IEC 27001:2022 Anhang A 5.3 · ISO/IEC 27001:2022 Anhang A 8.13 · ISO/IEC 27001:2022 Anhang A 5.31

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob die Organisation den Einsatz kryptografischer Verfahren in einem Kryptokonzept regelt, nur anerkannte Verfahren und Schlüssellängen verwendet und Daten bei Übertragung und Speicherung nach ihrem Schutzbedarf verschlüsselt. Sie beurteilt außerdem, ob Schlüssel und Zertifikate von der Erzeugung bis zur Vernichtung kontrolliert verwaltet werden und ob die Organisation auf künftige Wechsel der Verfahren vorbereitet ist.

GELTUNGSBEREICH

- Verschlüsselung von Daten bei Übertragung und Speicherung in Anwendungen, Datenbanken, Datenträgern und Sicherungen
- Schlüsselverwaltung einschließlich Hardware-Sicherheitsmodulen, Schlüsseltresoren und Cloud-Schlüsseldiensten
- Interne und externe Zertifikate sowie eine eigene Public-Key-Infrastruktur, soweit vorhanden
- Nicht Gegenstand: die kryptografische Analyse einzelner Algorithmen

Prüfschritte 1 bis 3

Schritt 01 NIS2-Richtlinie Art. 21 Abs. 2 lit. h; § 30 Abs. 2 Nr. 8 BSIG; BSI CON.1

Ein Kryptokonzept legt fest, wo und wie kryptografische Verfahren eingesetzt werden, und ist freigegeben.

Prüfhandlung Kryptokonzept lesen, Freigabe und Aktualität prüfen und mit den eingesetzten Systemen abgleichen.

Nachweise Kryptokonzept mit Freigabevermerk

Schritt 02 BSI TR-02102-1

Zulässige Algorithmen und Schlüssellängen orientieren sich an anerkannten Empfehlungen; veraltete Verfahren sind ausgeschlossen.

Prüfhandlung Liste zulässiger Verfahren mit aktuellen Empfehlungen vergleichen und auf drei Systemen die tatsächlichen Einstellungen auslesen.

Nachweise Liste zulässiger Verfahren, Konfigurationsauszüge

Schritt 03 BSI CON.1; ISO/IEC 27001:2022 Anhang A 8.24

Ein Verzeichnis der eingesetzten kryptografischen Verfahren, Schlüssel und Zertifikate wird geführt.

Prüfhandlung Verzeichnis ansehen und mit einer Stichprobe aus Anwendungen und Schnittstellen auf Vollständigkeit prüfen.

Nachweise Kryptoinventar, Zertifikatsliste

Prüfschritte 4 bis 6

Schritt 04 — BSI TR-02102-2; ISO/IEC 27001:2022 Anhang A 8.24

Daten werden bei der Übertragung über Netze verschlüsselt; die TLS-Konfiguration entspricht den Vorgaben.

Prüfhandlung Externe und interne Dienste mit einem Prüfwerkzeug auf Protokollversionen und Verfahren testen.

Nachweise Prüfergebnisse der TLS-Konfiguration, Maßnahmen zu Abweichungen

Schritt 05 — ISO/IEC 27001:2022 Anhang A 8.24; DORA Art. 9 Abs. 4 lit. d

Gespeicherte Daten werden nach Schutzbedarf und Risikobewertung verschlüsselt, auch in Sicherungen.

Prüfhandlung Für drei Datenbestände mit hohem Schutzbedarf die Verschlüsselung von Datenbank, Speicher und Sicherung nachvollziehen.

Nachweise Schutzbedarfsfeststellung, Konfiguration der Verschlüsselung

Schritt 06 — ISO/IEC 27001:2022 Anhang A 8.24; BSI CON.1

Für Schlüssel ist der Lebenszyklus geregelt: Erzeugung, Verteilung, Speicherung, Wechsel, Sperrung und Vernichtung.

Prüfhandlung Regelung lesen und für zwei Schlüssel den Lebenszyklus mit Datum des letzten Wechsels nachvollziehen.

Nachweise Regelung zum Schlüsselmanagement, Protokolle des Schlüsselwechsels

Prüfschritte 7 bis 9

Schritt 07 DORA Art. 9 Abs. 4 lit. d; ISO/IEC 27001:2022 Anhang A 8.24

Schlüssel werden geschützt gespeichert, etwa in Hardware-Sicherheitsmodulen oder Schlüsseltresoren, mit eng begrenztem Zugriff.

Prüfhandlung Speicherorte der Schlüssel erfragen, nach Schlüsseln im Quellcode oder in Konfigurationsdateien suchen lassen und Zugriffsrechte prüfen.

Nachweise Berechtigungsauszug des Schlüsseltresors, Ergebnis der Suche nach eingebetteten Schlüsseln

Schritt 08 ISO/IEC 27001:2022 Anhang A 8.24

Zertifikate werden zentral überwacht, rechtzeitig erneuert und bei Kompromittierung gesperrt.

Prüfhandlung Überwachung der Ablaufdaten vorführen lassen und Ausfälle durch abgelaufene Zertifikate der letzten zwölf Monate erfragen.

Nachweise Zertifikatsübersicht mit Ablaufdaten, Erneuerungsprotokolle, Vorfallliste

Schritt 09 ISO/IEC 27001:2022 Anhang A 5.3

Aufgaben in der Schlüsselverwaltung sind getrennt; kritische Vorgänge erfordern das Vier-Augen-Prinzip.

Prüfhandlung Rollen in der Schlüsselverwaltung und Protokolle kritischer Vorgänge wie der Erzeugung von Hauptschlüsseln prüfen.

Nachweise Rollenkonzept, Protokolle mit zwei Beteiligten

Prüfschritte 10 bis 12

Schritt 10 — BSI CON.1; ISO/IEC 27001:2022 Anhang A 8.13

Schlüssel sind gesichert, sodass verschlüsselte Daten und Sicherungen wiederhergestellt werden können.

Prüfhandlung Sicherung der Schlüssel erläutern lassen und den letzten Wiederherstellungstest verschlüsselter Daten ansehen.

Nachweise Konzept zur Schlüsselsicherung, Protokoll des Wiederherstellungstests

Schritt 11 — ISO/IEC 27001:2022 Anhang A 5.31

Rechtliche Vorgaben zum Einsatz und zur Ausfuhr kryptografischer Verfahren sind berücksichtigt.

Prüfhandlung Prüfen, ob für Standorte und Reisen außerhalb der EU rechtliche Einschränkungen ermittelt wurden.

Nachweise Rechtskataster, Regelung für Auslandsstandorte

Schritt 12 — BSI TR-02102-1

Die Organisation plant den Wechsel auf neue Verfahren, auch mit Blick auf quantensichere Kryptografie.

Prüfhandlung Erfragen, ob Systeme mit langlebigen Daten und fest eingebauten Verfahren erfasst sind und ein Plan für den Wechsel besteht.

Nachweise Analyse der Kryptoagilität, Migrationsplan

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Kryptokonzept
2. Liste zulässiger Verfahren und Schlüssellängen
3. Kryptoinventar und Zertifikatsübersicht
4. Prüfergebnisse der TLS-Konfiguration
5. Regelung zum Schlüsselmanagement mit Rollen
6. Berechtigungsauszug der Schlüsseltresore oder Hardware-Sicherheitsmodule
7. Protokoll des letzten Wiederherstellungstests verschlüsselter Daten
8. Planung zum Wechsel kryptografischer Verfahren

TYPISCHE FESTSTELLUNGEN

- Ein Kryptokonzept fehlt oder nennt Verfahren, die nicht mehr empfohlen werden.
- Schlüssel und Kennwörter liegen im Quellcode oder in Konfigurationsdateien.
- Zertifikate laufen unbemerkt ab und verursachen Ausfälle.
- Interne Dienste akzeptieren veraltete Protokollversionen.
- Sicherungen sind verschlüsselt, der Schlüssel ist aber nicht gesondert gesichert.
- Es gibt keine Übersicht, welche Systeme bei einem Wechsel der Verfahren betroffen wären.

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