Muster-Prüfprogramm

KRITIS

Nachweisprüfung

11 Prüfschritte · BSIG

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

§ 31 Abs. 1 und 2 BSIG · § 30 Abs. 2 Nr. 1 BSIG · NIS2-Richtlinie Art. 20 · § 31 Abs. 1 BSIG · § 31 Abs. 2 BSIG · § 30 Abs. 2 Nr. 2 und 3 BSIG · § 30 Abs. 2 Nr. 4 BSIG · § 30 Abs. 2 Nr. 9 und 10 BSIG · § 30 Abs. 2 Nr. 6 BSIG · § 32 Abs. 1 BSIG · § 39 Abs. 1 BSIG

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob ein Betreiber kritischer Anlagen die Risikomanagementmaßnahmen für seine kritischen Anlagen umgesetzt hat, die über das allgemeine Niveau hinausgehen, ob Systeme zur Angriffserkennung betrieben werden und ob die Meldepflichten erfüllt werden können. Sie beurteilt außerdem, ob der Nachweis für das Bundesamt durch Audits, Prüfungen oder Zertifizierungen vorbereitet ist: Umfang, Prüfer, Dokumentation und Umgang mit Mängeln.

GELTUNGSBEREICH

- Kritische Anlagen des Betreibers und die für ihren Betrieb notwendigen IT-Systeme, Komponenten und Prozesse
- Risikomanagementmaßnahmen nach den allgemeinen und den besonderen Anforderungen für Betreiber kritischer Anlagen
- Vorbereitung und Durchführung des Nachweises gegenüber dem Bundesamt
- Nicht Gegenstand: physische Resilienzmaßnahmen nach dem KRITIS-Dachgesetz und branchenspezifische Anforderungen, sofern nicht gesondert vereinbart

Prüfschritte 1 bis 3

Schritt 01 — § 31 Abs. 1 und 2 BSIG

Die kritischen Anlagen des Betreibers sind bestimmt und abgegrenzt; die für ihren Betrieb notwendigen IT-Systeme, Komponenten und Prozesse sind bekannt und dokumentiert.

Prüfhandlung Abgrenzung der kritischen Anlagen und die Liste der zugehörigen Systeme mit der Systemübersicht abgleichen.

Nachweise Dokumentation der kritischen Anlagen, Systemübersicht, Abhängigkeitsübersicht

Schritt 02 — § 30 Abs. 2 Nr. 1 BSIG; NIS2-Richtlinie Art. 20

Es besteht eine Risikoanalyse mit Sicherheitskonzepten für die kritischen Anlagen, sie ist aktuell und von der Leitung verantwortet.

Prüfhandlung Risikoanalyse und Sicherheitskonzepte lesen und Aktualität sowie Freigabe durch die Leitung prüfen.

Nachweise Risikoanalyse, Sicherheitskonzepte, Freigabevermerke der Leitung

Schritt 03 — § 31 Abs. 1 BSIG

Die Maßnahmen gehen für die kritischen Anlagen über das allgemeine Niveau hinaus und sind dem Aufwand nach nicht unverhältnismäßig zu den Folgen eines Ausfalls.

Prüfhandlung Prüfen, wie die Verhältnismäßigkeit der Maßnahmen für die kritischen Anlagen begründet und dokumentiert ist.

Nachweise Begründung zur Verhältnismäßigkeit, Maßnahmenkatalog der kritischen Anlagen

Prüfschritte 4 bis 6

Schritt 04

§ 31 Abs. 2 BSIG

Es werden Systeme zur Angriffserkennung eingesetzt, die laufend und automatisiert geeignete Parameter erfassen und auswerten und laufende Bedrohungen erkennen.

Prüfhandlung Systeme, abgedeckte Komponenten und Auswertung ansehen und die Abdeckung der Systeme der kritischen Anlagen prüfen.

Nachweise Architektur der Angriffserkennung, Abdeckungsübersicht, Auswertungen

Schritt 05

§ 30 Abs. 2 Nr. 2 und 3 BSIG

Die Maßnahmen zur Bewältigung von Sicherheitsvorfällen und zur Aufrechterhaltung des Betriebs sind umgesetzt und werden geübt.

Prüfhandlung Vorfalls- und Notfallpläne der kritischen Anlagen lesen und die Ergebnisse der letzten Übung ansehen.

Nachweise Vorfalls- und Notfallpläne, Übungsprotokolle

Schritt 06

§ 30 Abs. 2 Nr. 4 BSIG

Die Lieferkette der kritischen Anlagen ist betrachtet, Dienstleister mit Zugriff sind vertraglich auf Sicherheitsanforderungen verpflichtet.

Prüfhandlung Verträge und Bewertungen von drei Dienstleistern der kritischen Anlagen prüfen.

Nachweise Dienstleisterverzeichnis, Verträge, Bewertungen

Prüfschritte 7 bis 9

Schritt 07 — § 30 Abs. 2 Nr. 9 und 10 BSIG

Zugriffskontrolle und Mehrfaktor-Authentifizierung sind für die Systeme der kritischen Anlagen umgesetzt.

Prüfhandlung Berechtigungen und Authentifizierung für die Systeme der kritischen Anlagen in einer Stichprobe prüfen.

Nachweise Berechtigungsauszüge, Konfiguration der Mehrfaktor-Authentifizierung

Schritt 08 — § 30 Abs. 2 Nr. 6 BSIG

Konzepte und Verfahren zur Bewertung der Wirksamkeit der Maßnahmen bestehen und werden angewendet.

Prüfhandlung Verfahren zur Wirksamkeitsbewertung und die Ergebnisse der letzten zwölf Monate ansehen.

Nachweise Prüfplan, Berichte der Wirksamkeitsbewertung, Maßnahmenliste

Schritt 09 — § 32 Abs. 1 BSIG

Erhebliche Sicherheitsvorfälle können an die gemeinsame Meldestelle gemeldet werden: Frühwarnung binnen 24 Stunden, Meldung binnen 72 Stunden, Abschlussmeldung nach einem Monat.

Prüfhandlung Meldeprozess, Zuständigkeiten und Vorlagen prüfen und eine Meldung oder Übung auf Einhaltung der Fristen untersuchen.

Nachweise Meldeprozess, Vorlagen, Nachweis der Übung oder Meldung

Prüfschritte 10 bis 11

Schritt 10 § 39 Abs. 1 BSIG

Der Nachweis gegenüber dem Bundesamt ist geplant: Umfang, Nachweisart (Audit, Prüfung oder Zertifizierung), Termin im Turnus von drei Jahren und Prüfer sind festgelegt.

Prüfhandlung Nachweisplanung mit dem vom Bundesamt festgelegten Termin abgleichen und Eignung der Prüfstelle sowie Unabhängigkeit prüfen.

Nachweise Nachweisplanung, Beauftragung der Prüfstelle, Terminmitteilung des Bundesamts

Schritt 11 § 39 Abs. 1 BSIG

Festgestellte Sicherheitsmängel werden mit Frist und Verantwortlichen erfasst, nachverfolgt und gegenüber dem Bundesamt darstellbar behoben.

Prüfhandlung Mängellisten früherer Nachweise ansehen und den Stand der Behebung prüfen.

Nachweise Mängelliste, Maßnahmenplan, Nachweise der Behebung

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Dokumentation der kritischen Anlagen und der zugehörigen Systeme
2. Risikoanalyse und Sicherheitskonzepte
3. Begründung zur Verhältnismäßigkeit der Maßnahmen
4. Beschreibung der Angriffserkennung mit Abdeckungsübersicht
5. Vorfalls- und Notfallpläne mit Übungsprotokollen
6. Meldeprozess mit Vorlagen und Zuständigkeiten
7. Nachweisplanung und Berichte früherer Audits, Prüfungen oder Zertifizierungen
8. Mängelliste mit Maßnahmenplan

TYPISCHE FESTSTELLUNGEN

Die Abgrenzung der kritischen Anlagen und der notwendigen IT-Systeme ist nicht aktuell, Abhängigkeiten sind nicht erfasst.

Die Angriffserkennung deckt einen Teil der Systeme der kritischen Anlagen nicht ab.

Die Verhältnismäßigkeit der Maßnahmen ist nicht begründet, besondere Maßnahmen für die kritischen Anlagen sind nicht erkennbar.

Die Meldefähigkeit wurde nie geübt, die Vertretung der zuständigen Personen ist ungeklärt.

Der Nachweis wird zu spät vorbereitet, der Umfang der Prüfung deckt die kritischen Anlagen nicht vollständig ab.

Mängel früherer Prüfungen sind ohne Frist und Verantwortliche und werden nicht nachverfolgt.

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