Muster-Prüfprogramm

Patch- und Schwachstellenmanagement

13 Prüfschritte · NIS2, ISO 27001

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

BSI OPS.1.1.3 · ISO/IEC 27001:2022 Anhang A 8.8 · ISO/IEC 27001:2022 Anhang A 5.9 · NIS2-Richtlinie Art. 21 Abs. 2 lit. f · NIS2-Richtlinie Art. 21 Abs. 2 lit. e

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob die Organisation bekannte Schwachstellen in Systemen und Software systematisch erkennt, nach Risiko bewertet und rechtzeitig behebt, und ob Ausnahmen kontrolliert und nachvollziehbar behandelt werden. Sie beurteilt außerdem, ob der Patchstand durch Auswertungen belegt wird.

GELTUNGSBEREICH

- Server, Arbeitsplatzsysteme, Netzwerk- und Sicherheitskomponenten, Datenbanken und Anwendungen in der Verantwortung der Organisation
- Firmware, Drittsoftware und Bibliotheken, soweit sie in Eigenentwicklungen eingesetzt werden
- Schwachstellenscans und die Verfahren zu Bewertung, Test, Einspielung und Ausnahmen
- Nicht Gegenstand: Penetrationstests, sofern nicht gesondert vereinbart; Systeme, die vollständig vom Dienstleister betrieben werden, nur über die Steuerung des Dienstleisters

Prüfschritte 1 bis 3

Schritt 01 — BSI OPS.1.1.3; ISO/IEC 27001:2022 Anhang A 8.8

Ein Prozess für Patch- und Schwachstellenmanagement besteht, ist freigegeben und legt Fristen nach Kritikalität fest.

Prüfhandlung Prozessbeschreibung lesen und prüfen, ob Fristen, Rollen, Ausnahmen und Eskalation festgelegt sind.

Nachweise Prozessbeschreibung mit Freigabe, Fristenmatrix

Schritt 02 — ISO/IEC 27001:2022 Anhang A 5.9

Ein aktuelles Inventar der Systeme und der eingesetzten Software dient als Grundlage.

Prüfhandlung Inventar mit Netzwerkscan oder Verzeichnisdaten abgleichen und nicht erfasste Systeme feststellen.

Nachweise Inventar, Vergleichsliste

Schritt 03 — BSI OPS.1.1.3

Informationsquellen zu Schwachstellen sind festgelegt und werden von benannten Personen ausgewertet.

Prüfhandlung Quellen und Zuständige erfragen und für eine aktuelle Schwachstelle den Weg von der Meldung bis zur Bewertung nachvollziehen.

Nachweise Quellenliste, Zuständigkeiten, Bewertungsnotiz zu einem Beispiel

Prüfschritte 4 bis 6

Schritt 04 — BSI OPS.1.1.3; ISO/IEC 27001:2022 Anhang A 8.8

Neue Schwachstellen werden auf ihre Relevanz und ihr Risiko bewertet, die Bewertung ist dokumentiert.

Prüfhandlung Aus einem Quartal fünf Schwachstellen mit hoher Kritikalität auswählen und die Bewertung nachvollziehen.

Nachweise Bewertungsprotokolle, Tickets

Schritt 05 — ISO/IEC 27001:2022 Anhang A 8.8

Schwachstellenscans laufen regelmäßig und decken die Systeme im Geltungsbereich ab.

Prüfhandlung Scanplan und Scanbereiche mit dem Inventar vergleichen und die letzten Berichte ansehen.

Nachweise Scanplan, Scanberichte, Abdeckungsübersicht

Schritt 06 — BSI OPS.1.1.3

Kritische Schwachstellen werden innerhalb der festgelegten Frist behoben, Fristüberschreitungen werden verfolgt.

Prüfhandlung Für eine Stichprobe kritischer Schwachstellen die Zeit von der Kenntnis bis zur Behebung ermitteln und mit der Frist vergleichen.

Nachweise Auswertung offener und geschlossener Schwachstellen, Tickets, Eskalationen

Prüfschritte 7 bis 9

Schritt 07 — BSI OPS.1.1.3

Patches werden vor dem Einspielen in der Produktion getestet, Rückfallmöglichkeiten sind vorhanden.

Prüfhandlung Ablauf des Tests und der Freigabe an zwei aktuellen Patches nachvollziehen.

Nachweise Testprotokolle, Freigaben, Rückfallplan

Schritt 08 — BSI OPS.1.1.3; ISO/IEC 27001:2022 Anhang A 8.8

Ausnahmen werden begründet, durch eine zuständige Stelle genehmigt, befristet und durch Ersatzmaßnahmen abgesichert.

Prüfhandlung Liste der Ausnahmen ansehen und für eine Stichprobe Begründung, Genehmigung, Befristung und Ersatzmaßnahmen prüfen.

Nachweise Ausnahmeliste mit Genehmigungen und Ersatzmaßnahmen

Schritt 09 — BSI OPS.1.1.3

Systeme und Software ohne Herstellerunterstützung sind erkannt und werden mit einem Plan behandelt.

Prüfhandlung Inventar nach Systemen ohne Unterstützung filtern und Pläne zur Ablösung oder Absicherung prüfen.

Nachweise Liste der Systeme ohne Unterstützung, Ablösepläne, Risikoakzeptanz

Prüfschritte 10 bis 13

Schritt 10 — ISO/IEC 27001:2022 Anhang A 8.8

Der Patchstand umfasst alle Arten von Komponenten: Betriebssysteme, Anwendungen, Netzwerkgeräte, Firmware und Drittsoftware.

Prüfhandlung Patchstandsberichte je Komponentenart ansehen und Lücken in der Abdeckung ermitteln.

Nachweise Patchstandsberichte, Abdeckungsübersicht

Schritt 11 — NIS2-Richtlinie Art. 21 Abs. 2 lit. f

Die Wirksamkeit wird durch erneute Scans oder Berichte zum Patchstand belegt.

Prüfhandlung Für behobene Schwachstellen prüfen, ob ein erneuter Scan den Erfolg bestätigt.

Nachweise Folgescans, Abschlussvermerke

Schritt 12 — NIS2-Richtlinie Art. 21 Abs. 2 lit. f

Kennzahlen zu Patchstand und Fristeinhaltung werden an die Verantwortlichen berichtet und führen zu Maßnahmen.

Prüfhandlung Berichte der letzten zwölf Monate lesen und Entscheidungen zu Abweichungen nachvollziehen.

Nachweise Kennzahlenberichte, Protokolle, Maßnahmenlisten

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

Für Schwachstellen in eigenen Produkten und Diensten gibt es, soweit zutreffend, ein Verfahren zur Entgegennahme und Bearbeitung von Meldungen.

Prüfhandlung Meldeweg, Zuständigkeiten und die Bearbeitung eines Beispiels prüfen.

Nachweise Verfahrensbeschreibung, Kontaktadresse, Bearbeitungsnachweis

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Prozessbeschreibung zum Patch- und Schwachstellenmanagement mit Fristenmatrix
2. Inventar der Systeme und Software
3. Scanplan und Schwachstellenberichte der letzten Quartale
4. Auswertung offener und geschlossener Schwachstellen mit Behebungsdauer
5. Patchstandsberichte je Komponentenart
6. Liste der Ausnahmen mit Genehmigungen und Ersatzmaßnahmen
7. Liste der Systeme ohne Herstellerunterstützung und Ablösepläne
8. Kennzahlenberichte an die Verantwortlichen

TYPISCHE FESTSTELLUNGEN

- Das Inventar ist unvollständig, deshalb fehlen Systeme im Scan und im Patchprozess.
- Fristen sind festgelegt, werden für kritische Schwachstellen aber regelmäßig überschritten, ohne Eskalation.
- Netzwerkgeräte und Firmware sind nicht Teil des Patchprozesses.
- Ausnahmen laufen unbefristet und ohne Ersatzmaßnahmen.
- Systeme ohne Herstellerunterstützung sind in Betrieb, ein Ablöseplan fehlt.
- Die Behebung wird nicht durch einen erneuten Scan bestätigt.

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