Muster-Prüfprogramm

NIS2

Berechtigungsmanagement

13 Prüfschritte · NIS2

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

NIS2-Richtlinie Art. 21 Abs. 2 lit. i · BSI ORP.4 · NIS2-Richtlinie Art. 20 · ISO/IEC 27001:2022 Anhang A 5.15 · ISO/IEC 27001:2022 Anhang A 5.16 · ISO/IEC 27001:2022 Anhang A 5.18 · ISO/IEC 27001:2022 Anhang A 8.2 · NIS2-Richtlinie Art. 21 Abs. 2 lit. j · § 30 Abs. 2 Nr. 10 BSIG · ISO/IEC 27001:2022 Anhang A 8.5 · ISO/IEC 27001:2022 Anhang A 5.17 und 8.5 · ISO/IEC 27001:2022 Anhang A 8.15

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob die Organisation Zugriffe auf Netz- und Informationssysteme durch ein dokumentiertes, wirksames Verfahren steuert: vom Antrag über die Genehmigung und Vergabe bis zur regelmäßigen Überprüfung und zum Entzug. Sie beurteilt außerdem, ob erhöhte Rechte und der Fernzugriff zusätzlich abgesichert sind.

GELTUNGSBEREICH

- Fachanwendungen, Betriebssysteme, Datenbanken, Netzkomponenten und Verwaltungskonsolen, die für wesentliche Dienste oder Prozesse genutzt werden
- Benutzerkonten von Mitarbeitenden, Externen, Dienstleistern sowie technische Konten und Notfallkonten
- Prozesse für Eintritt, Wechsel und Austritt gemeinsam mit der Personalabteilung
- Nicht Gegenstand: physischer Zutritt und die Authentifizierung von Kundenzugängen, sofern nicht gesondert vereinbart

Prüfschritte 1 bis 3

Schritt 01

NIS2-Richtlinie Art. 21 Abs. 2 lit. i; BSI ORP.4

Eine Richtlinie zur Zugriffssteuerung besteht, ist von der Leitung freigegeben, aktuell und deckt Systeme, Daten und Standorte im Geltungsbereich ab.

Prüfhandlung Richtlinie lesen, Freigabe, Version und Datum der letzten Überprüfung feststellen und den Geltungsbereich mit der Systemübersicht abgleichen.

Nachweise Richtlinie mit Freigabevermerk und Änderungshistorie, Systemübersicht

Schritt 02

NIS2-Richtlinie Art. 20

Die Leitung wird über Berechtigungsrisiken informiert und trägt die Maßnahmen zum Risikomanagement mit.

Prüfhandlung Berichte und Protokolle der letzten zwölf Monate auf Themen zu Zugriffen und Berechtigungen durchsehen.

Nachweise Berichte an die Geschäftsleitung, Sitzungsprotokolle, Beschlüsse

Schritt 03

BSI ORP.4; ISO/IEC 27001:2022 Anhang A 5.15

Ein Rollen- und Berechtigungskonzept legt fest, welche Rolle welche Rechte erhält, und folgt dem Prinzip der geringsten Rechte.

Prüfhandlung Konzept für fünf ausgewählte Anwendungen mit den tatsächlich vergebenen Rechten vergleichen und Abweichungen erfragen.

Nachweise Rollenmatrix, Berechtigungskonzepte je Anwendung, Systemauszüge der Rechte

Prüfschritte 4 bis 6

Schritt 04 — BSI ORP.4

Für Systeme und Rollen sind Verantwortliche benannt, die Berechtigungen vor der Vergabe genehmigen.

Prüfhandlung Zehn Berechtigungsanträge auswählen und prüfen, ob die Genehmigung durch die fachlich verantwortliche Person vor der Vergabe vorliegt.

Nachweise Anträge oder Tickets mit Genehmigung und Zeitstempel, Liste der Verantwortlichen

Schritt 05 — BSI ORP.4; ISO/IEC 27001:2022 Anhang A 5.16

Neue Konten und Rechte beim Eintritt entsprechen dem Antrag und der Funktion.

Prüfhandlung Aus der Eintrittsliste der Personalabteilung eine Stichprobe ziehen und die vergebenen Rechte mit dem Antrag abgleichen.

Nachweise Eintrittsliste, Anträge, Auszug der vergebenen Rechte

Schritt 06 — BSI ORP.4; ISO/IEC 27001:2022 Anhang A 5.18

Bei einem Funktionswechsel werden nicht mehr benötigte Rechte entzogen.

Prüfhandlung Funktionswechsel der letzten zwölf Monate auswählen und die Rechte vor und nach dem Wechsel vergleichen.

Nachweise Liste der Wechsel, Rechteauszüge vor und nach dem Wechsel, Tickets

Prüfschritte 7 bis 9

Schritt 07 — BSI ORP.4; ISO/IEC 27001:2022 Anhang A 5.18

Konten ausgeschiedener Personen werden zeitnah gesperrt.

Prüfhandlung Austrittsliste zu einem Stichtag mit den aktiven Konten abgleichen und die Zeit zwischen Austritt und Sperrung ermitteln.

Nachweise Austrittsliste, Kontenliste mit Status und Sperrdatum, Sperrprotokoll

Schritt 08 — BSI ORP.4; ISO/IEC 27001:2022 Anhang A 5.18

Berechtigungen werden in festgelegten Abständen durch die Verantwortlichen überprüft und Befunde nachverfolgt.

Prüfhandlung Letzte Überprüfung ansehen: Umfang, Rücklauf, Fristen und ob entzogene Rechte tatsächlich entfernt wurden.

Nachweise Berichte der Rezertifizierung, Bestätigungen der Verantwortlichen, Tickets zum Entzug

Schritt 09 — BSI ORP.4; ISO/IEC 27001:2022 Anhang A 8.2

Privilegierte Konten sind inventarisiert, auf das Nötige beschränkt und von der normalen Arbeit getrennt.

Prüfhandlung Privilegierte Konten direkt aus den Systemen auslesen, mit dem Inventar vergleichen und prüfen, ob Administratorkonten für E-Mail oder Internet genutzt werden.

Nachweise Inventar privilegierter Konten, Systemauszüge der Administratorgruppen, Genehmigungen

Prüfschritte 10 bis 13

Schritt 10 NIS2-Richtlinie Art. 21 Abs. 2 lit. j; § 30 Abs. 2 Nr. 10 BSIG; ISO/IEC 27001:2022 Anhang A 8.5

Mehrfaktor-Authentifizierung ist für Fernzugriff und privilegierte Zugänge eingesetzt, Ausnahmen sind begründet und genehmigt.

Prüfhandlung Konfiguration von VPN, Remote-Zugängen und Verwaltungskonsolen prüfen und die Ausnahmen mit ihrer Begründung durchgehen.

Nachweise Konfigurationsauszüge, Liste der Ausnahmen mit Genehmigung

Schritt 11 BSI ORP.4

Technische Konten, Dienstkonten und Notfallkonten sind erfasst, haben eine verantwortliche Person und ein geregeltes Passwortverfahren.

Prüfhandlung Dienst- und Notfallkonten aus den Systemen ableiten und für eine Stichprobe Verantwortliche und Passwortverfahren erfragen.

Nachweise Inventar der technischen Konten, Verfahrensbeschreibung, Nachweis der Passwortänderung

Schritt 12 ISO/IEC 27001:2022 Anhang A 5.17 und 8.5

Die Anforderungen an Passwörter und andere Authentisierungsmerkmale sind festgelegt und technisch durchgesetzt.

Prüfhandlung Festgelegte Regeln mit den Einstellungen in Verzeichnisdienst und zentralen Anwendungen vergleichen.

Nachweise Richtlinie, Konfigurationsauszüge

Schritt 13 ISO/IEC 27001:2022 Anhang A 8.15

Änderungen an Berechtigungen und die Nutzung privilegierter Konten werden protokolliert und ausgewertet.

Prüfhandlung Protokollierung für privilegierte Aktivitäten prüfen und eine Auswertung samt Reaktion auf einen Fund nachvollziehen.

Nachweise Protokollkonfiguration, Auswertungen, Meldungen und Tickets

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Richtlinie zur Zugriffssteuerung und Berechtigungsvergabe
2. Rollen- und Berechtigungskonzepte, Rollenmatrix
3. Inventar der Systeme und der privilegierten sowie technischen Konten
4. Ein- und Austrittslisten der Personalabteilung für die letzten zwölf Monate
5. Berichte der letzten Rezertifizierung mit Nachverfolgung
6. Systemauszüge zu Benutzern, Gruppen und Administratorrechten zu einem Stichtag
7. Konfigurationsnachweise zu Mehrfaktor-Authentifizierung und Kennwortregeln
8. Berichte an die Geschäftsleitung zum Thema Zugriffe

TYPISCHE FESTSTELLUNGEN

Die Überprüfung der Berechtigungen findet nicht statt oder wird ohne Prüfung der Details bestätigt.

Konten ausgeschiedener Personen bleiben über Wochen aktiv, weil die Meldung der Personalabteilung fehlt.

Privilegierte Konten sind nicht vollständig inventarisiert, einzelne Administratoren nutzen ihr Konto für den Alltag.

Dienstkonten haben keine verantwortliche Person und ein Passwort, das seit Jahren unverändert ist.

Mehrfaktor-Authentifizierung gilt mit nicht begründeten Ausnahmen, insbesondere für Dienstleister.

Rollen sind nicht dokumentiert, Rechte werden durch Kopieren vorhandener Benutzer vergeben.

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