Muster-Prüfprogramm

Active Directory und Entra ID

13 Prüfschritte · BSI, ISO 27001, BSIG

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

BSI APP.2.1 · BSI APP.2.2 · ISO/IEC 27001:2022 Anhang A 8.2 · § 30 Abs. 2 Nr. 10 BSIG · ISO/IEC 27001:2022 Anhang A 8.5 · ISO/IEC 27001:2022 Anhang A 5.16 und 5.18 · BSI ORP.4 · ISO/IEC 27001:2022 Anhang A 5.17 · ISO/IEC 27001:2022 Anhang A 5.16 · ISO/IEC 27001:2022 Anhang A 5.18 · ISO/IEC 27001:2022 Anhang A 8.15 und 8.16 · ISO/IEC 27001:2022 Anhang A 8.13

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob Active Directory und Entra ID nach einem klaren Administrationsmodell betrieben werden, ob hochprivilegierte Gruppen und Konten minimal und überwacht sind und ob Anmeldeverfahren, Dienstkonten, Gastzugänge und die Synchronisation zwischen beiden Verzeichnissen sicher eingerichtet sind. Sie beurteilt außerdem, ob der Verzeichnisdienst nach einer Kompromittierung wiederhergestellt werden kann.

GELTUNGSBEREICH

- Lokales Active Directory mit allen Domänen und Domänencontrollern
- Entra ID Mandant einschließlich bedingter Zugriffe, Gastkonten und Anwendungsregistrierungen
- Synchronisation zwischen lokalem Verzeichnis und Entra ID
- Nicht Gegenstand: Berechtigungen innerhalb einzelner Fachanwendungen

Prüfschritte 1 bis 3

Schritt 01 — BSI APP.2.1; BSI APP.2.2

Verantwortung und Betriebskonzept für die Verzeichnisdienste sind dokumentiert und aktuell.

Prüfhandlung Betriebskonzept lesen und mit der tatsächlichen Domänen- und Mandantenstruktur abgleichen.

Nachweise Betriebskonzept, Übersicht der Domänen und Vertrauensstellungen

Schritt 02 — BSI APP.2.2; ISO/IEC 27001:2022 Anhang A 8.2

Ein gestuftes Administrationsmodell trennt die Verwaltung der Verzeichnisdienste von der Verwaltung von Servern und Arbeitsplätzen.

Prüfhandlung Modell erläutern lassen und prüfen, ob Domänenadministratoren sich nur an dafür vorgesehenen Systemen anmelden.

Nachweise Beschreibung des Administrationsmodells, Anmelderestriktionen, Anmeldeprotokolle

Schritt 03 — ISO/IEC 27001:2022 Anhang A 8.2; BSI APP.2.2

Hochprivilegierte Gruppen und Rollen haben nur wenige, persönlich zugeordnete Mitglieder und werden regelmäßig überprüft.

Prüfhandlung Mitglieder der hochprivilegierten Gruppen und Entra-Rollen auslesen und mit genehmigten Zuordnungen abgleichen.

Nachweise Auslesung der Gruppen und Rollen, Genehmigungen, Rezertifizierungsprotokoll

Prüfschritte 4 bis 6

Schritt 04 § 30 Abs. 2 Nr. 10 BSIG; ISO/IEC 27001:2022 Anhang A 8.5

Administrative Anmeldungen und Fernzugriffe sind mit mehreren Faktoren geschützt; Regeln für bedingten Zugriff sind ohne ungeprüfte Lücken.

Prüfhandlung Regeln für bedingten Zugriff auswerten, Ausnahmen auflisten und den Registrierungsstand der Faktoren prüfen.

Nachweise Export der Regeln für bedingten Zugriff, Ausnahmeliste, Registrierungsbericht

Schritt 05 ISO/IEC 27001:2022 Anhang A 8.2

Notfallzugangskonten sind eingerichtet, geschützt hinterlegt, überwacht und werden getestet.

Prüfhandlung Anzahl, Hinterlegung und Überwachung der Notfallzugangskonten prüfen und den letzten Test ansehen.

Nachweise Notfallzugangsregelung, Alarmregel für Anmeldungen, Testprotokoll

Schritt 06 ISO/IEC 27001:2022 Anhang A 5.16 und 5.18; BSI ORP.4

Konten werden bei Eintritt, Wechsel und Austritt zeitnah angepasst; inaktive Konten werden deaktiviert.

Prüfhandlung Konten ohne Anmeldung seit 90 Tagen auslesen und fünf Austritte auf zeitnahe Deaktivierung prüfen.

Nachweise Liste inaktiver Konten, Austrittsmeldungen, Deaktivierungszeitpunkte

Prüfschritte 7 bis 9

Schritt 07 — ISO/IEC 27001:2022 Anhang A 5.17; BSI APP.2.2

Dienstkonten haben Verantwortliche, nur notwendige Rechte und starke, gewechselte oder verwaltete Kennwörter.

Prüfhandlung Dienstkonten auslesen, privilegierte Dienstkonten markieren und Alter der Kennwörter sowie Verantwortliche prüfen.

Nachweise Liste der Dienstkonten mit Verantwortlichen, Kennwortalter, Rechte

Schritt 08 — ISO/IEC 27001:2022 Anhang A 8.5; BSI APP.2.2

Kennwortregeln sind angemessen, und veraltete Anmeldeprotokolle und Verschlüsselungsverfahren sind abgeschaltet.

Prüfhandlung Kennwortrichtlinien und Einstellungen zu veralteten Protokollen auslesen; Ergebnisse eines Prüfwerkzeugs für Verzeichnisdienste ansehen.

Nachweise Richtlinienauszug, Bericht des Prüfwerkzeugs

Schritt 09 — ISO/IEC 27001:2022 Anhang A 8.2

Der Server für die Synchronisation zwischen lokalem Verzeichnis und Entra ID ist wie ein Domänencontroller geschützt.

Prüfhandlung Administration, Netzzugang und Berechtigungen des Synchronisationsservers und seiner Dienstkonten prüfen.

Nachweise Systemdokumentation, Mitglieder der lokalen Administratoren, Rechte des Synchronisationskontos

Prüfschritte 10 bis 13

Schritt 10 ISO/IEC 27001:2022 Anhang A 5.16

Gastkonten und externe Identitäten werden genehmigt, befristet und regelmäßig überprüft.

Prüfhandlung Gastkonten auslesen, älteste und inaktive Gäste markieren und den Überprüfungsprozess nachvollziehen.

Nachweise Liste der Gastkonten, Einstellungen für Einladungen, Überprüfungsnachweise

Schritt 11 ISO/IEC 27001:2022 Anhang A 5.18

Anwendungsregistrierungen und erteilte Einwilligungen werden kontrolliert; Nutzer können Anwendungen keine weitreichenden Rechte erteilen.

Prüfhandlung Einstellungen zur Einwilligung durch Nutzer prüfen und Anwendungen mit hohen Berechtigungen auflisten.

Nachweise Einwilligungseinstellungen, Liste der Anwendungen mit Berechtigungen

Schritt 12 ISO/IEC 27001:2022 Anhang A 8.15 und 8.16; BSI APP.2.2

Anmeldungen und Änderungen an Verzeichnisobjekten werden protokolliert, zentral ausgewertet und bei Auffälligkeiten alarmiert.

Prüfhandlung Überwachungsregeln für Änderungen an privilegierten Gruppen ansehen und einen Alarm nachvollziehen.

Nachweise Überwachungsrichtlinie, Regelkatalog, Alarmbeispiel

Schritt 13 ISO/IEC 27001:2022 Anhang A 8.13; BSI APP.2.2

Eine Wiederherstellung des Verzeichnisdienstes nach Kompromittierung ist geplant, gesichert und getestet.

Prüfhandlung Wiederherstellungsplan lesen, Sicherungen der Domänencontroller prüfen und den letzten Wiederherstellungstest ansehen.

Nachweise Wiederherstellungsplan, Sicherungsnachweise, Testprotokoll

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Betriebskonzept der Verzeichnisdienste und Administrationsmodell
2. Auslesung privilegierter Gruppen und Entra-Rollen
3. Export der Regeln für bedingten Zugriff mit Ausnahmen
4. Regelung zu Notfallzugangskonten
5. Liste der Dienstkonten mit Verantwortlichen
6. Liste der Gastkonten und Anwendungen mit Berechtigungen
7. Bericht eines Prüfwerkzeugs für Verzeichnisdienste
8. Wiederherstellungsplan und Testprotokoll

TYPISCHE FESTSTELLUNGEN

- Domänenadministratoren melden sich an normalen Arbeitsplätzen an.
- Hochprivilegierte Gruppen enthalten Dienstkonten und ausgeschiedene Mitarbeitende.
- Ausnahmen vom zweiten Faktor sind breit gefasst und nicht befristet.
- Dienstkonten haben seit Jahren unveränderte Kennwörter und Administratorrechte.
- Gastkonten bleiben nach Projektende aktiv.
- Eine Wiederherstellung des Verzeichnisdienstes wurde nie geübt.

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