

Checklist

5.17 – Authenticatie-informatie

Thema: Organisatorisch | ISO 27002: 5.17 | Gerelateerd: 5.16, 8.5

Doelstelling

Aantonen dat authenticatie-informatie (wachtwoorden, tokens, sleutels) veilig wordt beheerd gedurende de volledige levenscyclus.

Beheer van wachtwoorden

- ☐ Is er beleid voor het veilig beheren en gebruiken van wachtwoorden?
- ☐ Worden initiële wachtwoorden veilig verstrekt en bij eerste gebruik geforceerd gewijzigd?
- ☐ Is het gebruik van een wachtwoordmanager aanbevolen of verplicht voor medewerkers?
- ☐ Worden wachtwoorden nooit opgeslagen in platte tekst (onversleuteld)?
- ☐ Is er een veilig proces voor het resetten van vergeten wachtwoorden (zonder bypass van MFA)?

Wachtwoordkwaliteit en -beleid

- ☐ Voldoen wachtwoordeisen aan actuele richtlijnen (NIST, NCSC: minimale lengte, geen verplichte complexiteit)?
- ☐ Worden veelgebruikte of gecompromitteerde wachtwoorden technisch geblokkeerd?
- ☐ Is hergebruik van recente wachtwoorden technisch voorkomen?
- ☐ Worden wachtwoorden niet periodiek geforceerd gewijzigd tenzij er aanleiding is (NIST-richtlijn)?

Andere authenticatiemiddelen

- ☐ Worden hardwaretokens, smartcards en certificaten centraal beheerd en geregistreerd?
- ☐ Is er een procedure voor het blokkeren van verloren of gestolen authenticatiemiddelen?
- ☐ Worden cryptografische sleutels en certificaten beheerd conform een key management procedure?
- ☐ Is er beleid voor het vervangen van verlopen of gecompromitteerde sleutels en certificaten?

Bewustwording en handhaving

- ☐ Worden medewerkers getraind in veilig omgaan met wachtwoorden en authenticatiemiddelen?
- ☐ Is het delen van wachtwoorden expliciet verboden en worden overtredingen opgevolgd?
- ☐ Is er monitoring op gebruik van gecompromitteerde wachtwoorden (Have I Been Pwned-integratie)?



Worden bevindingen over zwakke authenticatie gerapporteerd aan de beveiligingsfunctionaris?

Verantwoordelijke:	_____	Datum controle:	_____
Afdeling:	_____	Score:	___ / 21
Reviewcyclus:	☐ Jaarlijks ☐ Na wijziging ☐ Na incident		Status: ☐ Voldoet ☐ Actiepunt ☐ N.v.t.