

Checklist

5.16 – Identiteitsbeheer

Thema: Organisatorisch | ISO 27002: 5.16 | Gerelateerd: 5.15, 5.17, 8.2

Doelstelling

Aantonen dat identiteiten van gebruikers en systemen worden beheerd gedurende de volledige levenscyclus, van aanmaak tot verwijdering.

Aanmaak en beheer van identiteiten

- ☐ Is er een formeel proces voor het aanmaken van gebruikersaccounts?
- ☐ Wordt elke gebruiker voorzien van een unieke, persoonlijke identiteit (geen gedeelde accounts)?
- ☐ Worden accounts aangemaakt op basis van een goedgekeurd verzoek van HR of leidinggevende?
- ☐ Is er een centrale directory of IAM-systeem voor het beheer van alle identiteiten?
- ☐ Worden systeemaccounts en serviceaccounts apart beheerd en gedocumenteerd?

Levenscyclusbeheer

- ☐ Worden accounts direct geblokkeerd bij uitdiensttreding of contractbeëindiging?
- ☐ Worden accounts na een vastgestelde inactiviteitsperiode automatisch geblokkeerd?
- ☐ Is er een proces voor periodieke review van actieve accounts?
- ☐ Worden accounts van langdurig afwezige medewerkers tijdelijk geblokkeerd?

Privileged identity management

- ☐ Worden beheerdersidentiteiten (admin-accounts) apart beheerd van reguliere accounts?
- ☐ Is Privileged Access Management (PAM) ingericht voor beheerderstoegang?
- ☐ Worden beheerdersaccounts alleen gebruikt voor beheerstaken, niet voor dagelijks werk?
- ☐ Is just-in-time (JIT) toegang ingericht voor privileged accounts?

Audit en rapportage

- ☐ Worden wijzigingen in identiteiten en rechten gelogd en bewaard?
- ☐ Worden orphaned accounts (accounts zonder actieve medewerker) periodiek opgespoord?
- ☐ Is er rapportage over de staat van identiteitsbeheer aan de CISO of management?



Worden bevindingen uit identity-reviews aantoonbaar opgevolgd?

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