

Checklist

8.5 – Beveiligde authenticatie

Thema: Technisch | ISO 27002: 8.5 | Gerelateerd: 8.2, 8.3

Doelstelling

Aantonen dat toegang tot systemen en applicaties uitsluitend plaatsvindt via beveiligde authenticatiemethoden, waarmee de identiteit van gebruikers betrouwbaar wordt vastgesteld.

Authenticatiebeleid

- ☐ Is er beleid voor authenticatie dat de minimale eisen per systeem/risiconiveau vastlegt?
- ☐ Is multi-factor authenticatie (MFA) verplicht voor toegang tot kritieke systemen?
- ☐ Is MFA verplicht voor beheerderstoegang en toegang op afstand?
- ☐ Worden zwakke of standaard wachtwoorden technisch geblokkeerd?
- ☐ Is vastgelegd welke authenticatiemethoden zijn toegestaan en welke niet?

Wachtwoordbeleid

- ☐ Voldoen wachtwoordeisen aan actuele richtlijnen (minimale lengte, complexiteit)?
- ☐ Worden wachtwoorden versleuteld opgeslagen (bcrypt, Argon2 of vergelijkbaar)?
- ☐ Is hergebruik van recente wachtwoorden technisch geblokkeerd?
- ☐ Is er een procedure voor veilig resetten van vergeten wachtwoorden?
- ☐ Worden medewerkers geïnformeerd over veilig wachtwoordgebruik en gebruik van een wachtwoordmanager?

Multi-factor authenticatie (MFA)

- ☐ Is MFA geïmplementeerd voor alle externe toegang (VPN, webportalen, e-mail)?
- ☐ Worden sterke tweede factoren gebruikt (TOTP-app, hardware token) in plaats van SMS?
- ☐ Is er een fallback-procedure bij verlies van de tweede factor?
- ☐ Worden MFA-uitzonderingen vastgelegd, onderbouwd en periodiek herzien?

Monitoring en incidenten

- ☐ Worden mislukte inlogpogingen gelogd en gemonitord?
- ☐ Is er een automatische blokkade na een aantal opeenvolgende mislukte pogingen?

☐ Worden verdachte inlogpatronen (ongebruikelijke tijden, locaties) gedetecteerd?

☐ Is er een procedure voor opvolging bij gedetecteerde accountcompromittatie?

Verantwoordelijke:	_____	Datum controle:	_____
Afdeling:	_____	Score:	___ / 22
Reviewcyclus:	☐ Jaarlijks ☐ Na wijziging ☐ Na incident		Status: ☐ Voldoet ☐ Actiepunt ☐ N.v.t.