

Checklist

8.24 – Gebruik van cryptografie

Thema: Technisch | ISO 27002: 8.24 | Gerelateerd: 8.25, 5.17

Doelstelling

Aantonen dat cryptografie wordt ingezet om de vertrouwelijkheid, integriteit en authenticiteit van informatie te waarborgen conform een vastgesteld cryptografiebeleid.

Cryptografiebeleid

- ☐ Is er een vastgesteld cryptografiebeleid dat het gebruik van encryptie regelt?
- ☐ Zijn toegestane algoritmen, sleutellengtes en protocollen vastgelegd (conform NCSC-richtlijnen)?
- ☐ Is verboden gebruik van verouderde algoritmen (MD5, SHA-1, DES, RC4) vastgelegd?
- ☐ Is het beleid afgestemd op wet- en regelgeving (AVG, NIS2, BIO2)?

Encryptie van data in rust

- ☐ Worden gevoelige gegevens versleuteld opgeslagen (databases, bestanden, back-ups)?
- ☐ Is full-disk encryptie ingeschakeld op laptops en mobiele apparaten?
- ☐ Worden back-ups versleuteld opgeslagen, ook in de cloud?
- ☐ Worden sleutels beheerd gescheiden van de versleutelde data?
- ☐ Zijn sterke algoritmen in gebruik (AES-256 of vergelijkbaar)?

Encryptie van data in transit

- ☐ Is TLS 1.2 of hoger verplicht voor alle netwerkcommunicatie met gevoelige data?
- ☐ Zijn verouderde protocollen (SSL, TLS 1.0/1.1) uitgeschakeld?
- ☐ Worden e-mails met gevoelige inhoud versleuteld verstuurd (S/MIME, PGP of beveiligd portaal)?
- ☐ Is HTTPS afgedwongen voor alle webapplicaties (HSTS)?

Sleutelbeheer

- ☐ Is er een sleutelbeheerprocedure die de volledige levenscyclus van sleutels regelt?
- ☐ Worden sleutels periodiek geroteerd conform de vastgestelde sleutellevensduur?
- ☐ Worden verlopen of gecompromitteerde sleutels tijdig ingetrokken?

- ☐ Is er een procedure voor herstel van versleutelde data bij verlies van sleutels?
- ☐ Worden cryptografische sleutels beschermd via een HSM of key management systeem?

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