

Checklist

8.26 – Beveiligingseisen voor applicaties

Thema: Technisch | ISO 27002: 8.26 | Gerelateerd: 8.25, 8.27

Doelstelling

Aantonen dat beveiligingseisen voor applicaties worden vastgesteld, gedocumenteerd en geverifieerd tijdens ontwikkeling en aanschaf.

Vastleggen van beveiligingseisen

- ☐ Worden beveiligingseisen voor elke applicatie expliciet vastgesteld?
- ☐ Zijn eisen voor authenticatie, autorisatie, logging en encryptie per applicatie gedocumenteerd?
- ☐ Worden beveiligingseisen ook gesteld aan aangeschafte of uitbestede applicaties?
- ☐ Worden beveiligingseisen afgestemd op de classificatie van de te verwerken informatie?
- ☐ Is een dreigingsmodel beschikbaar voor kritieke applicaties?

Authenticatie en sessiebeheer

- ☐ Is sterke authenticatie (MFA) vereist voor applicaties met toegang tot gevoelige data?
- ☐ Worden sessiesleutels veilig gegenereerd en beheerd (voldoende entropie, time-out)?
- ☐ Is bescherming tegen sessiekaping (session fixation, CSRF) geïmplementeerd?
- ☐ Worden inactieve sessies automatisch beëindigd?

Invoervalidatie en outputbeveiliging

- ☐ Wordt alle gebruikersinvoer gevalideerd en gesaneerd (input validation)?
- ☐ Is bescherming tegen SQL-injectie, XSS en andere injectie-aanvallen geïmplementeerd?
- ☐ Worden foutmeldingen zo ontworpen dat ze geen gevoelige systeeminformatie lekken?
- ☐ Is output encoding toegepast om XSS te voorkomen?
- ☐ Worden bestandsuploads gecontroleerd op type, grootte en inhoud?

Verificatie en testen

- ☐ Worden beveiligingseisen getoetst tijdens acceptatietesten?
- ☐ Worden periodieke penetratietests uitgevoerd op kritieke applicaties?

- ☐ Worden OWASP Top 10-kwetsbaarheden actief getest?
- ☐ Worden bevindingen uit applicatiebeveiligingstests aantoonbaar opgevolgd?

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