

Checklist

8.29 – Beveiligingstesten in ontwikkeling en acceptatie

Thema: Technisch | ISO 27002: 8.29 | Gerelateerd: 8.25, 8.28

Doelstelling

Aantonen dat beveiligingstesten worden uitgevoerd tijdens ontwikkeling en acceptatie om kwetsbaarheden te identificeren vóór inproductie.

Testbeleid en -strategie

- ☐ Is er een testbeleid dat beveiligingstesten verplicht stelt vóór livegang?
- ☐ Zijn beveiligingstestmethoden vastgesteld (SAST, DAST, penetratietest, code review)?
- ☐ Is beveiliging een formeel acceptatiecriterium voor nieuwe of gewijzigde systemen?
- ☐ Worden testresultaten gedocumenteerd en bewaard?

Typen beveiligingstesten

- ☐ Worden statische code-analyses (SAST) geautomatiseerd uitgevoerd?
- ☐ Worden dynamische applicatietests (DAST) uitgevoerd op webapplicaties?
- ☐ Worden penetratietests uitgevoerd voor kritieke of publiek toegankelijke systemen?
- ☐ Worden dependency-scans uitgevoerd op gebruikte bibliotheken en frameworks?
- ☐ Worden configuratiereviews uitgevoerd op systemen en cloudinfrastructuur?

Testomgeving en testdata

- ☐ Worden beveiligingstesten uitgevoerd in een omgeving die de productieomgeving nabootst?
- ☐ Wordt geen productiedata gebruikt in testomgevingen zonder maskering?
- ☐ Is de testomgeving gescheiden van de productieomgeving?
- ☐ Worden testomgevingen na gebruik opgeruimd om datalekage te voorkomen?

Opvolging van bevindingen

- ☐ Worden kritieke beveiligingsbevindingen verplicht verholpen vóór livegang?
- ☐ Is er een risicoafweging voor bevindingen die niet vóór livegang worden opgelost?
- ☐ Worden bevindingen geregistreerd en gemonitord op oplossing?



Worden herhaalde bevindingen geanalyseerd op structurele oorzaken?

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