

Checklist

8.28 – Veilig coderen

Thema: Technisch | ISO 27002: 8.28 | Gerelateerd: 8.25, 8.26

Doelstelling

Aantonen dat veilige codeerpraktijken worden gehanteerd om kwetsbaarheden in software te voorkomen.

Secure coding standaarden

- ☐ Zijn secure coding guidelines vastgesteld en beschikbaar voor ontwikkelaars (OWASP, CERT)?
- ☐ Worden ontwikkelaars getraind in veilig programmeren?
- ☐ Zijn secure coding eisen opgenomen in de acceptatiecriteria voor code?
- ☐ Worden externe ontwikkelaars en contractors aan dezelfde secure coding eisen gehouden?

Veelvoorkomende kwetsbaarheden voorkomen

- ☐ Is bescherming tegen SQL-injectie geïmplementeerd (prepared statements, ORM)?
- ☐ Is bescherming tegen Cross-Site Scripting (XSS) geïmplementeerd (output encoding)?
- ☐ Is bescherming tegen Cross-Site Request Forgery (CSRF) geïmplementeerd?
- ☐ Worden geheugenbeheerproblemen (buffer overflow) voorkomen via veilige talen of controles?
- ☐ Worden hardcoded wachtwoorden en API-sleutels in broncode voorkomen via tooling?

Geautomatiseerde code-analyse

- ☐ Is statische analyse (SAST) geïntegreerd in de CI/CD-pipeline?
- ☐ Is dynamische analyse (DAST) ingericht voor webapplicaties?
- ☐ Worden dependency-scans (SCA) uitgevoerd op open-source componenten?
- ☐ Worden beveiligingsbevindingen uit geautomatiseerde scans verplicht opgepakt vóór release?

Code review en kwaliteitsbewaking

- ☐ Worden code reviews uitgevoerd met expliciete aandacht voor beveiliging?
- ☐ Is een vier-ogen-principe verplicht voor code-wijzigingen in productiebranches?
- ☐ Worden beveiligingsgerelateerde pull requests extra beoordeeld door een security-bewuste reviewer?
- ☐ Worden beveiligingslessen uit incidenten vertaald naar verbeterde coding guidelines?

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