

Checklist

8.31 – Scheiding van ontwikkel-, test- en productieomgevingen

Thema: Technisch | ISO 27002: 8.31 | Gerelateerd: 8.25, 8.32

Doelstelling

Aantonen dat ontwikkel-, test- en productieomgevingen strikt gescheiden zijn om ongeautoriseerde wijzigingen en datalekken te voorkomen.

Omgevingssegregatie

- ☐ Zijn ontwikkel-, test- en productieomgevingen technisch gescheiden (aparte servers, netwerken, accounts)?
- ☐ Is toegang tot productie gescheiden van toegang tot ontwikkel- en testomgevingen?
- ☐ Worden wijzigingen in productie uitsluitend doorgevoerd via een gecontroleerd change management proces?
- ☐ Is er een acceptatieomgeving (OTAP) die de productieomgeving zo nauwkeurig mogelijk nabootst?

Toegang en autorisatie

- ☐ Hebben ontwikkelaars geen directe schrijftoegang tot productieomgevingen?
- ☐ Is toegang tot productiesystemen beperkt tot beheerders en operations-medewerkers?
- ☐ Worden productie-inloggegevens gescheiden beheerd van ontwikkel- en testomgeving?
- ☐ Is MFA verplicht voor toegang tot productieomgevingen?
- ☐ Worden productieparameters (database-credentials, API-keys) nooit opgeslagen in broncode?

Datascheiding

- ☐ Wordt productiedata nooit ongemaskeerd gebruikt in ontwikkel- of testomgevingen?
- ☐ Is er een geautomatiseerd proces voor het aanmaken van gemaskeerde testdata?
- ☐ Worden productiedatabases niet direct benaderd vanuit ontwikkel- of testomgevingen?
- ☐ Is de scheiding van data tussen omgevingen technisch afgedwongen?

Monitoring en naleving

- ☐ Worden pogingen tot directe toegang tot productie vanuit ontwikkelomgevingen gedetecteerd?
- ☐ Worden omgevingsconfiguraties periodiek gecontroleerd op correcte scheiding?
- ☐ Worden uitzonderingen (noodtoegang tot productie) gelogd en achteraf gereviewd?

☐ Is er een procedure voor het opschonen van test- en ontwikkelomgevingen na gebruik?

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