

Checklist

8.27 – Principes voor veilige systeemarchitectuur en -engineering

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

Doelstelling

Aantonen dat beveiligingsprincipes worden toegepast bij het ontwerpen en bouwen van systemen en architecturen.

Beveiligingsarchitectuurprincipes

- ☐ Zijn beveiligingsarchitectuurprincipes (defense in depth, least privilege, fail secure) vastgelegd?
- ☐ Worden deze principes consequent toegepast bij het ontwerp van nieuwe systemen?
- ☐ Is er een architectuurboard of toetsingsproces voor beveiligingsarchitectuur?
- ☐ Worden beveiligingsprincipes ook toegepast bij cloudomgevingen en microservices?

Zero Trust architectuur

- ☐ Is Zero Trust als architectuurprincipe overwogen of geïmplementeerd?
- ☐ Wordt identiteitsverificatie afgedwongen voor elke toegangspoging, ook intern?
- ☐ Is netwerksegmentatie gecombineerd met identiteitsgebaseerde toegangscontrole?
- ☐ Wordt continue verificatie toegepast in plaats van eenmalige authenticatie per sessie?

Veilig ontwerp van componenten

- ☐ Worden single points of failure geïdentificeerd en geëlimineerd in kritieke systemen?
- ☐ Is het principe van 'security by default' toegepast (veilige standaardinstellingen)?
- ☐ Worden systemen ontworpen met minimale aanvalsoppervlakte (attack surface reduction)?
- ☐ Is scheiding van bevoegdheden technisch afgedwongen in de architectuur?
- ☐ Worden beveiligingscontroles ingebouwd in plaats van achteraf toegevoegd?

Review en toetsing

- ☐ Worden architectuurontwerpen beoordeeld op beveiligingsrisico's vóór implementatie?
- ☐ Is er een security architect of vergelijkbare rol betrokken bij systeemontwerp?
- ☐ Worden architectuurafwijkingen van beveiligingsprincipes gedocumenteerd en onderbouwd?



Worden architectuurbeslissingen periodiek herzien op actualiteit en effectiviteit?

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