

Checklist

5.24 – Planning en voorbereiding van het beheer van informatiebeveiligingsincidenten

Thema: Organisatorisch | ISO 27002: 5.24 | Gerelateerd: 5.25, 5.26, 6.8

Doelstelling

Aantonen dat de organisatie voorbereid is op het beheren van informatiebeveiligingsincidenten door vastgestelde processen, rollen, procedures en communicatielijnen.

Incidentbeheerbeleid en -proces

- ☐ Is er een vastgesteld incidentbeheerproces voor informatiebeveiligingsincidenten?
- ☐ Zijn rollen en verantwoordelijkheden in het incidentbeheer formeel belegd?
- ☐ Is het incidentbeheerproces gedocumenteerd en beschikbaar voor betrokkenen?
- ☐ Sluit het beveiligingsincidentproces aan op het algemene IT-incidentbeheerproces?
- ☐ Is het proces afgestemd op de AVG-meldplicht datalekken (72-uurseis)?

Classificatie en triage

- ☐ Is er een classificatiesysteem voor incidenten (ernst, impact, urgentie)?
- ☐ Is vastgelegd welke drempel een beveiligingsgebeurtenis tot een incident maakt?
- ☐ Worden incidenten snel getriageerd zodat prioriteit bepaald kan worden?
- ☐ Is er een procedure voor het herkennen van en omgaan met datalekken?

Respons en escalatie

- ☐ Is er een responsprocedure per type incident (malware, datalek, DDoS, etc.)?
- ☐ Zijn escalatielijnen vastgesteld (naar management, CISO, toezichthouder, politie)?
- ☐ Is er een procedure voor communicatie met externe partijen (AP, NCSC, media)?
- ☐ Is er een crisisteam of CSIRT beschikbaar voor ernstige incidenten?
- ☐ Worden betrokken systemen bij ernstige incidenten geïsoleerd conform procedure?

Oefening en verbetering

- ☐ Worden incidentresponsprocedures minimaal jaarlijks geoefend of gesimuleerd?
- ☐ Worden lessen uit incidenten structureel verwerkt in verbeterde procedures?

☐ Is er een post-incident review (PIR) proces na significante incidenten?

☐ Worden trends in incidenten gerapporteerd aan het management?

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