

Checklist

5.26 – Reageren op informatiebeveiligingsincidenten

Thema: Organisatorisch | ISO 27002: 5.26 | Gerelateerd: 5.24, 5.25, 5.27

Doelstelling

Aantonen dat de organisatie informatiebeveiligingsincidenten effectief afhandelt om schade te beperken, systemen te herstellen en herhaling te voorkomen.

Incidentresponsproces

- ☐ Is er een vastgesteld incidentresponsproces met duidelijke stappen (detectie, indamming, herstel, evaluatie)?
- ☐ Zijn rollen en verantwoordelijkheden in het incidentresponsproces formeel belegd?
- ☐ Is het proces beschikbaar en bekend bij alle betrokkenen?
- ☐ Is er een crisisteam of CSIRT beschikbaar voor ernstige incidenten?
- ☐ Is het incidentresponsproces afgestemd op de AVG-meldplicht bij datalekken?

Indamming en herstel

- ☐ Is er een procedure voor het isoleren van gecompromitteerde systemen?
- ☐ Worden forensische sporen veiliggesteld vóór herstelacties worden uitgevoerd?
- ☐ Is er een procedure voor het herstellen van systemen vanuit een bekende goede toestand?
- ☐ Worden herstelde systemen gecontroleerd op volledigheid en veiligheid vóór hergebruik?
- ☐ Is vastgelegd hoe lang een incident maximaal mag duren per ernstniveau?

Communicatie tijdens incidenten

- ☐ Is vastgelegd wie communiceert met interne stakeholders tijdens een incident?
- ☐ Is vastgelegd wie communiceert met externe partijen (AP, NCSC, klanten, media)?
- ☐ Is er een crisiscommunicatieplan beschikbaar en actueel?
- ☐ Worden betrokken medewerkers tijdig en adequaat geïnformeerd tijdens een incident?

Documentatie en evaluatie

- ☐ Worden alle incidentactiviteiten gedocumenteerd in een incidentlog?
- ☐ Vindt na elk significant incident een post-incident review (PIR) plaats?

☐ Worden lessen uit incidenten structureel verwerkt in verbeterde procedures?

☐ Worden incidentstatistieken gerapporteerd aan het management?

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