

Checklist

5.25 – Beoordeling van informatiebeveiligingsgebeurtenissen

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

Doelstelling

Aantonen dat informatiebeveiligingsgebeurtenissen worden beoordeeld om te bepalen of zij als incident moeten worden geclassificeerd en welke opvolging nodig is.

Beoordelingsproces

- ☐ Is er een vastgesteld proces voor het beoordelen van gemelde beveiligingsgebeurtenissen?
- ☐ Is vastgelegd wie verantwoordelijk is voor de initiële beoordeling (triage)?
- ☐ Worden gebeurtenissen beoordeeld op ernst, impact en urgentie?
- ☐ Is er een beslisboom of criteria om te bepalen of een gebeurtenis een incident is?
- ☐ Worden beoordelingen gedocumenteerd inclusief tijdstip en beslissing?

Classificatie en prioritering

- ☐ Is er een classificatieschema voor beveiligingsgebeurtenissen (laag/midden/hoog/kritiek)?
- ☐ Worden hoog-prioritaire gebeurtenissen direct geëscaleerd naar de CISO of crisisteam?
- ☐ Is vastgelegd binnen welke termijn een gebeurtenis moet worden beoordeeld per prioriteit?
- ☐ Worden datalekken direct getoetst aan de AVG-meldplicht (72-uurseis)?

Informatiebronnen en context

- ☐ Wordt bij de beoordeling gebruik gemaakt van logbestanden, SIEM-data en andere technische bronnen?
- ☐ Wordt dreigingsinformatie (threat intelligence) betrokken bij de beoordeling?
- ☐ Worden eerdere soortgelijke gebeurtenissen meegenomen in de beoordeling?
- ☐ Is er toegang tot externe bronnen (NCSC, leveranciers) voor context bij de beoordeling?

Rapportage en verbetering

- ☐ Worden beoordelingsresultaten gerapporteerd aan management of CISO?
- ☐ Worden fout-negatieven (gemiste incidenten) geanalyseerd om het beoordelingsproces te verbeteren?
- ☐ Worden trends in beveiligingsgebeurtenissen periodiek geanalyseerd?



Worden lessen uit beoordelingen gebruikt om detectieregels te verbeteren?

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