

Checklist

5.7 – Dreigingsinformatie

Thema: Organisatorisch | ISO 27002: 5.7 | Gerelateerd: 5.6, 8.8

Doelstelling

Aantonen dat de organisatie actuele dreigingsinformatie verzamelt, analyseert en gebruikt om beveiligingsmaatregelen proactief aan te passen aan het dreigingslandschap.

Verzamelen van dreigingsinformatie

- ☐ Is er een proces voor het structureel verzamelen van dreigingsinformatie (threat intelligence)?
- ☐ Worden bronnen zoals NCSC, Z-CERT, MISP, en sectorale ISAC's actief gemonitord?
- ☐ Worden kwetsbaarheidsdatabases (CVE, NVD) regelmatig geraadpleegd?
- ☐ Is er een abonnement op of toegang tot commerciële dreigingsinformatie waar relevant?
- ☐ Worden sociale media en darkweb gemonitord op relevante dreigingen voor de organisatie?

Analyse en duiding

- ☐ Wordt verzamelde dreigingsinformatie geanalyseerd op relevantie voor de organisatie?
- ☐ Worden dreigingen gekoppeld aan de eigen systemen en kwetsbaarheden (risk-based)?
- ☐ Is er een functionaris of team verantwoordelijk voor dreigingsanalyse?
- ☐ Wordt gebruik gemaakt van dreigingsmodellen zoals MITRE ATT&CK;?

Actie op dreigingsinformatie

- ☐ Leidt dreigingsinformatie aantoonbaar tot concrete beveiligingsmaatregelen of aanpassingen?
- ☐ Is er een proces voor snelle actie bij kritieke dreigingen (zero-days, actieve aanvallen)?
- ☐ Worden detectieregels (SIEM, IDS) bijgewerkt op basis van actuele dreigingsinformatie?
- ☐ Worden penetratietests en red-team oefeningen afgestemd op actuele dreigingen?

Rapportage en verbetering

- ☐ Worden dreigingstrends periodiek gerapporteerd aan het management?
- ☐ Is dreigingsinformatie input voor de jaarlijkse risicoanalyse?
- ☐ Worden lessen uit dreigingsinformatie gebruikt om bewustwordingstraining te verbeteren?



Wordt dreigingsinformatie gedeeld met relevante partners en ketenpartners?

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