

Checklist

5.6 – Contact met speciale belangengroepen

Thema: Organisatorisch | ISO 27002: 5.6 | Gerelateerd: 5.5, 8.8

Doelstelling

Aantonen dat de organisatie relevante contacten onderhoudt met vakorganisaties, beveiligingsgemeenschappen en kennisnetwerken om actuele dreigingsinformatie te verkrijgen en best practices te delen.

Identificatie van relevante netwerken

- ☐ Zijn relevante beveiligingsgemeenschappen en kennisnetwerken geïdentificeerd?
- ☐ Neemt de organisatie deel aan sectorale ISAC's of vergelijkbare netwerken?
- ☐ Is vastgelegd wie namens de organisatie deelneemt aan externe beveiligingsnetwerken?
- ☐ Worden contacten en lidmaatschappen periodiek beoordeeld op relevantie?

Informatie-uitwisseling

- ☐ Worden dreigingsinformatie en kwetsbaarheidsmeldingen uit netwerken actief gebruikt?
- ☐ Is er een proces voor het vertalen van externe dreigingsinformatie naar interne maatregelen?
- ☐ Worden beveiligingswaarschuwingen (bv. NCSC-adviezen) direct doorgezet naar relevante teams?
- ☐ Deelt de organisatie (geanonimiseerde) beveiligingsinformatie terug met het netwerk waar toegestaan?

Kennisdeling en vakkennis

- ☐ Nemen beveiligingsmedewerkers deel aan conferenties, webinars of vakbijeenkomsten?
- ☐ Is er budget en tijd beschikbaar voor externe kennisopbouw en netwerken?
- ☐ Worden opgedane kennis en inzichten intern gedeeld met het beveiligingsteam?
- ☐ Is de organisatie aangesloten bij relevante brancheorganisaties (VNG, IBD, etc.)?

Vertrouwelijkheid en gedragsregels

- ☐ Zijn gedragsregels vastgesteld voor het delen van vertrouwelijke informatie in externe netwerken?
- ☐ Is het TLP-protocol (Traffic Light Protocol) bekend en toegepast bij informatie-uitwisseling?
- ☐ Worden medewerkers geïnformeerd over wat wel en niet gedeeld mag worden?

Verantwoordelijke:

Datum controle:

Afdeling:		Score:	___ / 18
Reviewcyclus:	☐ Jaarlijks ☐ Na wijziging ☐ Na incident	Status:	☐ Voldoet ☐ Actiepunt ☐ N.v.t.