

Checklist

5.28 – Verzamelen van bewijsmateriaal

Thema: Organisatorisch | ISO 27002: 5.28 | Gerelateerd: 5.26, 5.27

Doelstelling

Aantonen dat bewijsmateriaal bij informatiebeveiligingsincidenten op een juridisch houdbare manier wordt verzameld, bewaard en beschermd.

Beleid en procedure

- ☐ Is er een procedure voor het verzamelen van digitaal bewijsmateriaal bij incidenten?
- ☐ Is de procedure afgestemd op juridische en forensische eisen (chain of custody)?
- ☐ Is vastgelegd wie bevoegd is bewijsmateriaal te verzamelen?
- ☐ Zijn medewerkers die bewijsmateriaal verzamelen getraind in forensische basistechnieken?

Technische maatregelen

- ☐ Worden forensische kopieën gemaakt van systemen vóór wijzigingen worden doorgevoerd?
- ☐ Worden logbestanden en geheugeninhoud veiliggesteld als onderdeel van de incidentrespons?
- ☐ Is er tooling beschikbaar voor forensisch onderzoek (imaging, log-analyse)?
- ☐ Worden hashwaarden gebruikt om de integriteit van bewijsmateriaal aan te tonen?
- ☐ Wordt bewijsmateriaal opgeslagen op een beveiligde, gecontroleerde locatie?

Bewaring en keten van bewaring

- ☐ Is de keten van bewaring (chain of custody) gedocumenteerd voor elk stuk bewijsmateriaal?
- ☐ Wordt vastgelegd wie toegang heeft gehad tot bewijsmateriaal en wanneer?
- ☐ Worden bewaartermijnen voor bewijsmateriaal afgestemd op juridische procedures?
- ☐ Is bewijsmateriaal beschermd tegen ongeautoriseerde toegang en manipulatie?

Juridische en externe samenwerking

- ☐ Is er afstemming met de juridische afdeling bij incidenten die tot rechtszaken kunnen leiden?
- ☐ Is er een procedure voor samenwerking met politie of justitie bij cybercriminaliteit?
- ☐ Worden externe forensische experts ingeschakeld bij complexe incidenten?



Is vastgelegd welke informatie wel en niet gedeeld mag worden met externe partijen?

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