

Checklist

5.21 – Beheer van informatiebeveiliging in de ICT-toeleveringsketen

Thema: Organisatorisch | ISO 27002: 5.21 | Gerelateerd: 5.19, 5.20

Doelstelling

Aantonen dat de organisatie de risico's in de ICT-toeleveringsketen (supply chain) beheerst, inclusief software, hardware en cloudcomponenten van derde partijen.

Inzicht in de toeleveringsketen

- Is er een overzicht van kritieke ICT-leveranciers en hun onderlinge afhankelijkheden?
- Zijn risico's van concentratie bij één leverancier of technologie geïdentificeerd?
- Worden sub-leveranciers (vierde partijen) in kaart gebracht voor kritieke diensten?
- Is vastgelegd welke componenten uit de keten als kritiek worden beschouwd?

Beveiligingseisen aan de keten

- Worden beveiligingseisen doorgecascadeerd naar sub-leveranciers?
- Is vastgelegd hoe leveranciers omgaan met softwareontwikkelingsbeveiliging (SSDLC)?
- Worden software-updates en patches van leveranciers gecontroleerd op authenticiteit?
- Is er beleid voor het gebruik van open-source componenten en bijbehorende risico's?
- Worden software bills of materials (SBOM) opgevraagd bij kritieke softwareleveranciers?

Risicobeheersing

- Worden supply chain-risico's meegenomen in de organisatiebrede risicoanalyse?
- Is er een procedure voor opvolging bij beveiligingsincidenten in de toeleveringsketen?
- Worden leveranciers gescreend op geopolitieke risico's (land van oorsprong, eigenaarschap)?
- Is er een alternatieve leverancier of exitstrategie voor kritieke ICT-componenten?

Monitoring en naleving

- Worden leveranciers in de keten periodiek beoordeeld op naleving van beveiligingseisen?
- Worden kwetsbaarheidsmeldingen in ketencomponenten actief gemonitord (NCSC, CVE)?
- Is er een proces voor snelle actie bij kritieke kwetsbaarheden in toeleveringsketensoftware?



Worden bevindingen gerapporteerd aan het management en opgenomen in risicobeheer?

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