

Checklist

8.7 – Bescherming tegen malware

Thema: Technisch | ISO 27002: 8.7 | Gerelateerd: 8.8, 6.8

Doelstelling

Aantonen dat de organisatie passende maatregelen heeft genomen om systemen en gegevens te beschermen tegen malware, inclusief detectie, preventie en herstel.

Anti-malware maatregelen

- ☐ Is op alle eindpunten (laptops, servers, mobiel) anti-malwaresoftware geïnstalleerd?
- ☐ Wordt anti-malwaresoftware automatisch bijgewerkt met actuele signaturen?
- ☐ Is real-time bescherming (on-access scanning) ingeschakeld?
- ☐ Worden periodieke volledige scans uitgevoerd op alle systemen?
- ☐ Is anti-malware ook ingericht op e-mailgateways en webproxy's?

Preventieve maatregelen

- ☐ Is het uitvoeren van niet-goedgekeurde software (application whitelisting) beperkt?
- ☐ Zijn macro's in Office-documenten standaard uitgeschakeld of beperkt?
- ☐ Is autorun van externe media (USB, CD) uitgeschakeld?
- ☐ Worden medewerkers getraind in het herkennen van phishing en malware-aanvallen?
- ☐ Is er een proces voor veilig openen van e-mailbijlagen en downloads?

Detectie en respons

- ☐ Worden malwaredetecties centraal gelogd en gemonitord?
- ☐ Is er een procedure voor opvolging bij een malwaredetectie?
- ☐ Worden geïnfecteerde systemen direct geïsoleerd van het netwerk?
- ☐ Is er een herstelproces (clean-up, restore) beschreven en getest?

Beheer en rapportage

- ☐ Wordt de anti-malwarestatus (dekking, versies, uitzonderingen) periodiek gerapporteerd?
- ☐ Zijn uitzonderingen (systemen zonder anti-malware) onderbouwd en gecompenseerd?



Worden malware-incidenten geregistreerd en geanalyseerd op trends?



Is de anti-malwarestrategie afgestemd op actuele dreigingen (ransomware, supply chain)?

Verantwoordelijke:	_____	Datum controle:	_____
Afdeling:	_____	Score:	___ / 22
Reviewcyclus:	☐ Jaarlijks ☐ Na wijziging ☐ Na incident		Status: ☐ Voldoet ☐ Actiepunt ☐ N.v.t.