

Checklist

8.20 – Netwerkbeveiliging

Thema: Technisch | ISO 27002: 8.20 | Gerelateerd: 8.21, 8.22

Doelstelling

Aantonen dat netwerken worden beveiligd en beheerd om systemen en informatie te beschermen tegen ongeautoriseerde toegang en aanvallen.

Netwerkbeveiligingsbeleid

- ☐ Is er beleid voor netwerkbeveiliging dat eisen stelt aan architectuur, toegang en monitoring?
- ☐ Is de netwerktopologie gedocumenteerd en actueel?
- ☐ Worden netwerken ingedeeld in zones op basis van risico en vertrouwelijkheid?
- ☐ Worden beveiligingseisen meegenomen bij wijzigingen in de netwerkinfrastructuur?

Perimeterbeveiliging

- ☐ Is een firewall ingericht op de grens tussen intern netwerk en internet?
- ☐ Worden alleen noodzakelijke poorten en protocollen opengesteld (default deny)?
- ☐ Is een Web Application Firewall (WAF) ingericht voor publiek toegankelijke webapplicaties?
- ☐ Worden inkomende en uitgaande verbindingen gecontroleerd en gefilterd?
- ☐ Is DDoS-bescherming ingericht voor publiek toegankelijke diensten?

Interne netwerksegmentatie

- ☐ Is het interne netwerk gesegmenteerd in zones (DMZ, productie, beheer, gebruikers)?
- ☐ Worden kritieke systemen geïsoleerd in een apart netwerksegment?
- ☐ Is laterale beweging (east-west traffic) tussen segmenten beperkt en gemonitord?
- ☐ Wordt micro-segmentatie of Zero Trust toegepast voor kritieke omgevingen?

Beheer en monitoring

- ☐ Is netwerktoegang voor beheer gescheiden van regulier gebruikersverkeer?
- ☐ Worden netwerkcomponenten (switches, routers) centraal beheerd en geconfigureerd?
- ☐ Wordt netwerkverkeer gemonitord op anomalieën en bedreigingen (IDS/IPS)?



Worden netwerkconfiguraties regelmatig geauditeerd op correctheid en veiligheid?

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