

Checklist

8.21 – Beveiliging van netwerkdiensten

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

Doelstelling

Aantonen dat netwerkdiensten (intern en extern) veilig worden geconfigureerd, beheerd en gemonitord conform beveiligingseisen.

Inventarisatie van netwerkdiensten

- ☐ Is er een actueel overzicht van alle netwerkdiensten (DNS, DHCP, VPN, proxy, e-mail, etc.)?
- ☐ Zijn beveiligingseisen per netwerkdienst vastgelegd?
- ☐ Worden onnodige of verouderde netwerkdiensten uitgeschakeld?
- ☐ Is vastgelegd welke netwerkdiensten extern bereikbaar zijn en waarom?

Beveiliging van specifieke diensten

- ☐ Is DNS beveiligd tegen spoofing en hijacking (DNSSEC, DNS-over-HTTPS)?
- ☐ Is e-mail beveiligd met SPF, DKIM en DMARC?
- ☐ Worden VPN-verbindingen beveiligd met sterke encryptie en MFA?
- ☐ Is remote desktop (RDP, SSH) niet direct bereikbaar vanaf internet?
- ☐ Worden beheerpoorten (SSH, RDP, HTTPS-beheer) alleen toegankelijk via een jump server of VPN?

Uitbestede netwerkdiensten

- ☐ Zijn beveiligingseisen opgenomen in contracten met aanbieders van netwerkdiensten?
- ☐ Worden uitbestede netwerkdiensten gemonitord op beschikbaarheid en beveiliging?
- ☐ Is er een procedure voor incidenten bij uitbestede netwerkdiensten?
- ☐ Worden SLA's voor uitbestede netwerkdiensten periodiek gereviewd?

Monitoring en wijzigingsbeheer

- ☐ Worden wijzigingen in netwerkdienstconfiguraties via change management behandeld?
- ☐ Worden netwerkdiensten gemonitord op beschikbaarheid en afwijkingen?
- ☐ Worden certificaten voor netwerkdiensten (TLS) tijdig vernieuwd?

☐ Worden netwerkdienstconfiguraties periodiek geauditeerd?

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