

Checklist

8.22 – Segregatie van netwerken

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

Doelstelling

Aantonen dat netwerken zijn gesegmenteerd om de verspreiding van aanvallen te beperken en kritieke systemen te beschermen.

Segregatiestrategie

- ☐ Is er een vastgestelde strategie voor netwerksegmentatie op basis van risico en vertrouwelijkheid?
- ☐ Zijn de criteria voor netwerksegmentatie gedocumenteerd (functie, risico, gebruikersgroep)?
- ☐ Is de netwerksegmentatie afgestemd op de informatieclassificatie?
- ☐ Wordt netwerksegmentatie herzien bij significante wijzigingen in de architectuur?

Technische implementatie

- ☐ Zijn VLAN's of vergelijkbare technieken ingericht voor netwerksegmentatie?
- ☐ Is er een DMZ ingericht voor systemen die zowel intern als extern bereikbaar zijn?
- ☐ Zijn productie-, test- en ontwikkelomgevingen netwerktechnisch gescheiden?
- ☐ Is het beheersnetwerk (OOB management) gescheiden van het productieve netwerk?
- ☐ Worden OT/ICS-netwerken gescheiden van IT-netwerken?

Toegangscontrole tussen segmenten

- ☐ Worden firewallregels gebruikt om verkeer tussen segmenten te controleren?
- ☐ Is het principe van default deny toegepast voor inter-segment verkeer?
- ☐ Worden firewallregels periodiek gereviewd en overbodige regels verwijderd?
- ☐ Is er logging van verkeer tussen netwerksegmenten?

Gasten en externe toegang

- ☐ Is gastnetwerk volledig gescheiden van het interne bedrijfsnetwerk?
- ☐ Hebben gasten uitsluitend internettoegang en geen toegang tot interne systemen?
- ☐ Is wifi voor medewerkers gescheiden van gastwifi?

☐ Worden IoT-apparaten geplaatst in een apart netwerksegment?

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