

Checklist

5.15 – Toegangsbeveiliging

Thema: Organisatorisch | ISO 27002: 5.15 | Gerelateerd: 5.18, 8.2, 8.3

Doelstelling

Aantonen dat toegang tot informatie en systemen wordt beheerst op basis van vastgesteld beleid, zodat alleen geautoriseerde personen toegang hebben.

Toegangsbeveiligingsbeleid

- ☐ Is er een vastgesteld toegangsbeveiligingsbeleid?
- ☐ Zijn de principes van least privilege en need-to-know formeel verankerd in het beleid?
- ☐ Is het beleid van toepassing op alle systemen, applicaties en netwerken?
- ☐ Wordt het toegangsbeleid minimaal jaarlijks herzien?
- ☐ Is het beleid gecommuniceerd aan systeemeigenaren en beheerders?

Toegangscontrole per systeem

- ☐ Is voor elk systeem vastgelegd wie toegang heeft en op basis waarvan?
- ☐ Worden toegangsrechten beheerd via een centraal identity management systeem (IAM/AD)?
- ☐ Is single sign-on (SSO) ingericht voor het vereenvoudigen en centraliseren van toegangsbeheer?
- ☐ Zijn gastaccounts en tijdelijke accounts voorzien van een verloopdatum?

Netwerktogang

- ☐ Is netwerktogang gesegmenteerd op basis van functies en risiconiveaus?
- ☐ Is draadloze netwerktogang beveiligd conform actuele standaarden (WPA3 of vergelijkbaar)?
- ☐ Worden gasten en externe medewerkers op een apart netwerksegment geplaatst?
- ☐ Is Zero Trust netwerktogang (ZTNA) overwogen of ingericht voor kritieke systemen?

Monitoring en review

- ☐ Worden toegangspogingen en -activiteiten gelogd?
- ☐ Worden toegangsrechten minimaal jaarlijks gereviewed door proceseigenaren?
- ☐ Worden ongebruikte accounts gesignaleerd en geblokkeerd of verwijderd?

☐ Worden afwijkingen in toegangspatronen actief gemonitord?

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