

Checklist

8.3 – Beperking van toegang tot informatie

Thema: Technisch | ISO 27002: 8.3 | Gerelateerd: 8.2, 5.15

Doelstelling

Aantonen dat toegang tot informatie en systeemfuncties wordt beperkt conform het toegangsbeveiligingsbeleid en de principes van least privilege en need-to-know.

Toegangsbeperkingsbeleid

- ☐ Is er beleid voor het beperken van toegang tot informatie op basis van functie en taak?
- ☐ Zijn de principes van least privilege en need-to-know technisch geïmplementeerd?
- ☐ Is vastgelegd welke gebruikers toegang hebben tot welke informatiecategorieën?
- ☐ Worden toegangsbeperkingen afgedwongen op applicatie- en databaseniveau?

Technische toegangscontroles

- ☐ Worden toegangsrechten tot bestanden en mappen beheerd via rolgebaseerde toegangscontrole (RBAC)?
- ☐ Is toegang tot gevoelige databronnen (databases, archieven) beperkt tot geautoriseerde gebruikers?
- ☐ Worden menuopties en applicatiefuncties beperkt tot wat de gebruiker nodig heeft?
- ☐ Is toegang tot productieomgevingen gescheiden van test- en ontwikkelomgevingen?
- ☐ Is toegang tot beheerfuncties beperkt tot systeembeheerders?

Gegevensgerichte toegangscontrole

- ☐ Is toegang tot persoonsgegevens beperkt conform de AVG (dataminimalisatie)?
- ☐ Worden gevoelige velden in databases gemaskeerd of versleuteld voor ongeautoriseerde gebruikers?
- ☐ Is toegang tot financiële gegevens beperkt tot medewerkers met een zakelijke noodzaak?
- ☐ Worden rapportages en exports van gevoelige data gecontroleerd op autorisatie?

Review en monitoring

- ☐ Worden toegangsbeperkingen periodiek gereviewed op correctheid en noodzaak?
- ☐ Worden pogingen tot ongeautoriseerde toegang gelogd en gesignaleerd?
- ☐ Worden toegangsrechten direct aangepast bij functiewijziging?



Worden afwijkingen in datatoegang gerapporteerd aan de eigenaar van de informatie?

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