‘Beleid logische toegangsbeveiliging gemeente Meppel’

Auteur: CISO
Datum: november 2021
Versie: 1.0

Inhoudsopgave

1. Logische toegangsbeveiliging.

1.1. Inleiding

Het beleid logische toegangsbeveiliging is erop gericht de beveiliging van de gemeentelijke informatiesystemen en de informatie binnen de informatiesystemen van de gemeente Meppel te waarborgen.

'Logische toegangsbeveiliging is het geheel aan maatregelen welke tot doel hebben, de toegang tot gegevens en informatiesystemen te beheersen zodat gegevens, informatiesystemen en resources worden bescherm tegen ongeautoriseerde acties'.(zoals: raadplegen, verwijderen, wijzigen en gebruik.)

Met ingang van 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) in werking getreden en dient de gemeente te voldoen aan de normen/eisen uit de BIO. Met betrekking de logische toegangsbeveiliging zijn in de BIO specifieke eisen benoemd die in dit beleid zijn opgenomen. Het 'Beleid logische toegangsbeveiliging gemeente Meppel' is opgesteld met inachtneming van de 'Handreiking logische toegangsbeveiliging' van de Informatie Beveiligingsdienst (IBD).

1.2. Het belang van logische toegangsbeveiliging

Informatie speelt een belangrijke rol in de gemeentelijke bedrijfsprocessen. Hierdoor krijgt de beveiliging van de informatie ook een steeds hogere prioriteit. Logische toegangsbeveiliging is een belangrijk onderdeel van de gemeentelijke informatiebeveiliging. Logische toegangsbeveiliging zorgt ervoor dat onbevoegden minder gemakkelijk toegang kunnen krijgen tot gemeentelijke informatiesystemen en informatie binnen deze gemeentelijke informatiesystemen.

Het ontbreken van een adequate logische toegangsbeveiliging kan ertoe leiden dat onbevoegden zich toegang kunnen verschaffen tot gemeentelijke informatiesystemen en informatie binnen deze informatiesystemen, waardoor ongewenste acties op de dienstverlening kunnen plaatsvinden en/of informatie kan worden ontvreemd of verminkt. Hiermee kan de vertrouwelijkheid, de integriteit maar ook het imago van de gemeente worden geschaad.

1.3. Logische versus fysieke toegangsbeveiliging.

De fysieke en logische toegangsbeveiliging van organisaties wordt vaak nog gescheiden uitgevoerd. De integratie van de fysieke en logische toegangsbeveiliging geeft een 'veiligere en efficiëntere situatie.
Daar waar de fysieke toegangsbeveiliging voornamelijk betrekking heeft op de toegang tot gebouwen heeft de logische toegangsbeveiliging betrekking op de toegang tot informatiesystemen. Door de integratie van het logische toegangsbeleid met het fysieke toegangsbeleid ontstaat er een veiligere en efficiëntere situatie en wordt het beheer van de totale toegangsbeveiliging gemakkelijker.

1.4. Doelstelling.

Doelstelling van logische toegangsbeveiliging is het vaststellen van de identiteit van een gebruiker die toegang krijgt tot gemeentelijke gegevens, informatiesystemen of diensten en het waarborgen van een gecontroleerde toegang (autorisatie) tot, en gebruik van, gemeentelijke gegevens, informatiesystemen of diensten door medewerkers van de gemeente en of medewerkers bij (keten) partners.

2. Beleid logische toegangsbeveiliging gemeente Meppel.

2.1. Algemeen.

Met de steeds toenemende automatisering en de toenemende nadruk op veiligheid en integriteit wordt de vraag 'wie is gemachtigd welke handelingen in een bepaald geautomatiseerd informatiesysteem te verrichten?' van steeds groter belang.

Uitgangspunten bij de logische toegangsbeveiliging is dat uitsluitend bevoegde personen toegang hebben en gebruik kunnen maken van informatiesystemen en/of gegevens. De bevoegdheid van een persoon moet worden afgeleid van de taak, functie of verantwoordelijkheid van de betreffende persoon. Dit ter beoordeling van de proces- en/of gegevenseigenaar en op aangeven van een autorisatiebevoegde medewerker. Afhankelijk van de dataclassificatie dienen medewerkers een geheimhoudingsverklaring te ondertekenen.

2.2. Definities.

In het beleid worden de volgende definities gehanteerd.

- **Beleid logische toegangsbeveiliging.**
  De uitgangspunten die de gemeente hanteert bij het regelen van een beheerste toegang tot, en gebruik van, een informatiesysteem.
- **Autoriseren in het kader van het beleid logische toegangsbeveiliging.**
  Iemand een bevoegdheid geven tot het wijzigen van het informatiesysteem zelf, of tot het wijzigen of raadplegen van de inhoud van het informatiesysteem.
- **Eigenaar.**
  De eigenaar is verantwoordelijk voor het goed functioneren van het informatiesysteem en van de processen die een wisselwerking hebben met het informatiesysteem.
- **Gegevenseigenaar.**
  De gegevenseigenaar is verantwoordelijk voor de juistheid van de gegevens in het informatiesysteem.

2.3. Beleidsuitgangspunten.

1. Het beleid logische toegangsbeveiliging gemeente Meppel is van toepassing op informatiesystemen die de gemeente gebruikt om haar processen uit te voeren. Ook als informatiesystemen niet binnen de gemeente draaien is het beleid logische toegangsbeveiliging van toepassing. (zoals bij het gebruik van SaaS-oplossingen)
2. De gemeente maakt, waar mogelijk, gebruik van bestaande (landelijke) standaarden voor authenticatie en autorisatie.
3. Voor elk bedrijfsproces, informatiesysteem, gegevensverzameling is een verantwoordelijke eigenaar benoemd.
4. Iedere eigenaar voert een baselinetoets BIO uit en, afhankelijk van de uitkomsten van deze baselinetoets BIO, ook nog voor een diepgaande risicoanalyse voor de informatiesystemen waarvan hij eigenaar is.
5. Een eigenaar is eindverantwoordelijk voor autorisaties binnen elk informatiesysteem. Hiertoe wordt een autorisatiematrix opgesteld.
6. Er is een autorisatieprocedure opgesteld waarvoor een eigenaar is benoemd. De autorisatieprocedure regelt de toegang tot informatiesystemen en het opstellen van een autorisatiematrix binnen het systeem. Daar waar niet kan worden aangesloten bij een generieke autorisatieprocedure maakt iedere eigenaar een specifieke autorisatieprocedure voor elk informatiesysteem waarvan hij eigenaar is.
7. Iedere eigenaar past de generieke autorisatieprocedures toe voor de informatiesystemen waarvan hij eigenaar is.
8. De eigenaar hanteert bij het opstellen en uitvoeren van een generieke dan wel specifieke autorisatieprocedure de volgende uitgangspunten:
    - De autorisatiestructuur van een informatiesysteem is uniform voor de gehele gemeente.
    - De autorisatiestructuur van een informatiesysteem sluit aan bij de goedgekeurde procesbeschrijvingen.
    - Er mogen geen 'algemene' (ongepersonaliseerde) identiteiten worden gebruikt. Voor de herleidbaarheid en transparantie is het noodzakelijk te weten wie een bepaalde actie heeft uitgevoerd
    - Gegevens worden alleen gemuteerd door de eigenaar of de daartoe, door de eigenaar, gemachtigde medewerkers.
    - De eigenaar laat de autorisatieprocedure toetsen door de CISO.
8. De eigenaar houd bij het opstellen van een autorisatieprocedure rekening met mogelijk van toepassing zijnde wet- en regelgeving.
9. De eigenaar geeft bij het maken van een proces- of systeem specifieke autorisatieprocedure aan welke detailnormen hij wel of niet van toepassing wil laten zijn. Bij detailnormen geeft hij in het bijzonder gedacht aan de volgende normen:
    - De leidraad bij het opschonen van gegevens.
    - De checklist voor het borgen van de betrouwbaarheid van gegevens.

Functiescheiding

10. De beschikkende, technische, bewarende en controlerende taken worden in beginsel nooit in één functionaris tezamen gebracht. Indien dit toch noodzakelijk is dan wordt door de eigenaar apart toezicht georganiseerd op de betreffende medewerker.

Inhuur externen

11. De door de gemeente ingehuurde externen vallen onverkort onder het beleid logische toegangsbeveiliging en dienen conform deze regels te handelen.

12. Aan de hand van hun taken/functie zal hun toegang verleend worden tot de gegevens en informatiesystemen.

Uitbesteding aan een ICT-dienstverlener

13. De ICT-dienstverlener zal een beveiligingsbeleid moeten hebben en geëffectueerd maatregelen volgens de NEN/ISO 27001 of vergelijkbare algemeen erkende overheidsnorm.

Beoordeling van de uitvoering van het beleid

14. De eigenaar is eindverantwoordelijk voor de uitvoering van de autorisatieprocedure en legt de uitvoering hiervan in handen van de beheerder. De beheerder neemt interne beheersmaatregelen die in overeenstemming zijn met de eisen die uit de baselinetoets BIO of risicoanalyse voortvloeien.
15. De uitvoering van het beleid Logische Toegangsbeveiliging wordt periodiek beoordeeld door de interne controle. Het initiatief voor de uitvoering van de controles ligt bij de CISO of de eigenaren.