Vragen aan het college n.a.v. agendapunt 13, Implementatie Wmebv

Inbreng D66

We hebben de volgende vragen rondom de implementatie van de Wmebv

1. Hoe wordt gewaarborgd dat de berichten die worden verstuurd vanuit de burger naar de gemeente toe veilig zijn? In de bijlage wordt als elektronisch pad nu vaak bijvoorbeeld een webformulier genoemd dat de burger dient te gebruiken. Hierop is slechts in enkele gevallen DigID of eHerkenning als authenticatiemiddel toegepast.
   REACTIE college
   Wij erkennen dat standaard email en onversleutelde webformulieren niet voldoen aan de uitgangspunten van de gewenste beveiligingsnormering. Daarom werken wij conform BIO 2.0 (Baseline Informatiebeveiliging Overheid) en de Cyberbeveiligingswet (implementatie Europese richtlijn NIS2) structureel aan het verbeteren van de digitale communicatie. De invoering van de Wmebv, met aansluiting op het huidige informatiebeleid en de verdere opbouw van de informatiearchitectuur, zijn gericht op het vergroten van de veiligheid van digitale communicatie. Dit is een permanent bedrijfsproces, met als voorbeelden:
   - Versterken authenticatie en autorisatie; bij formulieren met DigiD of E-herkenning. Waar niet mogelijk of toegestaan streven we naar veilige alternatieven;
   - Versleuteling; voor zover nog niet aanwezig alle communicatiekanalen voorzien van end-to-end encryptie (TLS 1.3 of hoger)
   - Jaarlijkse risicobeoordeling van formulieren en portals.

   Planning is dat eind 2026 alle pdf-formulierenzijn vervangen door E-formulieren met veilige authenticatie. Voor processen waar authenticatie niet verplicht is, wordt minimaal HTTPS en aanvullende maatregelen zoals CAPTCHA en logging toegepast. Dit sluit aan bij de Wet digitale overheid, de Nationale Cybersecurity Strategie en de uitgangspunten van de Wmebv.

2. Niet alle uitgaande berichten vanuit de gemeente naar de burger gaan via de berichtenbox mijnoverheid.nl. Deze berichtenbox is gegarandeerd veilig. Kan de gemeente aangeven wanneer alle uitgaande stromen via de berichtenbox beschikbaar zijn?
   REACTIE college
   Wij verwachten in 2027 een volledige aansluiting te realiseren op de berichtenbox voor het formele berichtenverkeer. Vanuit de normering uit de Wet digitale overheid en BIO 2.0 is het realiseren van dit hogere beveiligingsniveau voor inwoners, organisaties en ondernemers wenselijk. Het realiseren van dit uitgangspunt is o.a. afhankelijk van:
   - Zaaksysteem-integratie: De al lopende migratie van ons huidige zaaksysteem dat de berichtenbox-functionaliteit ondersteunt.
   - Architectuur & Compliance: Het voldoen aan archiverings- en integratie-eisen uit de Wmebv en NIS2.

3. Hoe wil de gemeente zich in de toekomst zich op gaan voorbereiden op het garanderen van meer veiligheid bij het gebruik van elektronische communicatie vanuit de burger naar de gemeente toe en wat is de ambitie van de gemeente qua veiligheid hierin?

   REACTIE college

   Digitale veiligheid is al een permanent bedrijfsproces. Ons doel hierbij is om in 2027 zo volledig als mogelijk is aan te sluiten bij de normeringen BIO 2.0 en de Cyberbeveiligingswet. Onderwerpen die in uitvoering zijn, zijn BIO 2.0 normen voor informatiebeveiliging, Cyberbeveiligingswet (NIS2) voor kritieke processen, leveranciersketenbeveiliging, risicobeheer, incidentenopvolging en rapportage. Concrete maatregelen zijn:

   - jaarlijkse testen en security audits;
   - Security Awareness-trainingen voor medewerkers;
   - een beveiligingsaanpak met als uitgangspunt dat niemand automatisch betrouwbaar is, maar altijd controleren op wie toegang krijgt;
   - incidentresponsplan conform NIS2.