Gemeente Heerlen

GEMEENTEBLAD

Officiële uitgave van de gemeente Heerlen

Nr. 132497

29 april

2021

Gemeente Heerlen - Informatiebeveiligingsplan DigiD gemeente Heerlen

Het college van burgemeester en wethouders van de gemeente Heerlen
VOORSTEL
Gelezen het voorstel Zelfevaluatie 2020 inzake DigiD, Suwinet, BAG, BGT en BRO van 20 april2021 en met registratienummer BWV-21001098

OVERWEGING
gelet op het bepaalde in Besluit verwerking persoonsgegevens generieke digitale infrastructuur;
mede gelet op het bepaalde in de Regeling voorzieningen GDI (Generieke Digitale Infrastructuur);
mede gelet op het bepaalde in de Baseline Informatiebeveiliging Overheid;
mede gelet op de beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum (NCSC);
mede gelet op de Algemene verordening gegevensbescherming (AVG);
mede gelet op de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG);

BESLUIT
vast te stellen het navolgende: Informatiebeveiligingsplan DigiD gemeente Heerlen

Beleidsinhoud
De gemeente Heerlen gebruikt op basis van DigiD-identificatie persoonlijke informatie van inwoners. Het gaat om informatie over NAW-gegevens maar ook over BSN-nummer. Het is natuurlijk heel belangrijk dat het beheer van deze informatie én het beheer van de DigiD-toegang zorgvuldig gebeurt. Daarvoor past de gemeente Heerlen de Baseline Informatieveiligheid Overheid (BIO) toe. De actuele stand van zaken wordt getoetst tijdens de jaarlijkse ENSIA-audit. Maar binnen de ENSIA-audit is de DigiD een voornamelijk technische audit op een webapplicatie. Hierbij wordt gewerkt met een eigen vooral technisch normenkader, gebaseerd op de NCSC beveiligingsrichtlijnen voor webapplicaties, dat afwijkt van de BIO. Daarbij zijn pentesten een belangrijk onderdeel en mogelijk daarmee voor bestuurders technisch lastig leesbaar. Dit plan bevat de vertaling van de technische bevindingen naar meer bestuurlijke onderwerpen.

Verbetervoorstellen DigiD

Bijwerken technische infrastructuur DigiD
Het NCSC heeft diverse beveiligingsrichtlijnen voor webapplicaties aangescherpt. Onze technische infrastructuur voor DigiD voldoet op dit moment niet aan al deze eisen. Om te voldoen aan alle richtlijnen worden een aantal wijzingen doorgevoerd. De uitvoering van deze wijzingen liggen bij drie partijen: de interne functionele beheerder, bij Parkstad-IT en/of leverancier(s). Technische details zijn wel opgenomen in het risico-register van de CISO, maar bewust niet hier.
De CISO monitort de uitvoering van de noodzakelijke wijzigingen.
Afronding is voorzien in het tweede kwartaal van 2021 maar is mede afhankelijk van het technische onderzoek dat momenteel loopt.

Monitoren en uitvoering nieuwe technische eisen tav DigiD
Het NCSC verscherpt geregeld en gedurende de loop van het jaar de eisen die worden gesteld aan de technische infrastructuur voor oa de DigiD-aansluitingen. Deze aanscherpingen dienen tijdig te worden vertaald in wijzingen. De uitvoering van deze wijzingen kunnen bij drie partijen liggen: de interne functionele beheerder, bij Parkstad-IT en/of de leverancier(s).
Sommige nieuwe eisen kunnen zorgen voor extra drempels voor burgers bij het gebruik, zeker als deze burgers ‘oude’ apparatuur en software gebruikt. In zo’n geval zal dit worden besproken met de portefeuillehouder.
De CISO monitort de eisen die worden gesteld vanuit NCSC én voert regie op de uitvoering van eventuele wijzigingen.
Dit wordt ingevoerd vanaf 2021.

Tweede DigiD-aansluiting voor Parkeervergunningen
Op verzoek van het college wordt het gehele proces rondom parkeervergunningen verder gedigitaliseerd. Daarbij is het streven dat de burger via selfservice digitaal een parkeervergunning kan aanvragen. Voor de identificatie van die burger wordt dan gebruik gemaakt van DigiD.
Technisch bezien is hiervoor een tweede DigiD-aansluiting nodig voor de gemeente Heerlen.
De teamleider Vergunningen voert regie op de digitalisering van het werkproces. De CISO monitort de eisen die worden gesteld vanuit NCSC én voert regie op de uitvoering van de tweede DigiD-aansluiting.
Dit wordt ingevoerd in 2021.

Derde DigiD-aansluiting voor toegang tot dossiers
Op verzoek van het college wordt het gehele proces rondom de dienstverlening verder gedigitaliseerd. Daarbij is het streven dat de burger via selfservice digitaal toegang krijgt tot zijn dossiers en aanvragen. Voor de identificatie van die burger wordt dan gebruik gemaakt van DigiD.
Technisch bezien is hiervoor een derde DigiD-aansluiting nodig voor de gemeente Heerlen.
De projectleider Slim Digitaal Samenwerken voert regie op de digitalisering van de technische infrastructuur. De CISO monitort de eisen die worden gesteld vanuit NCSC én voert regie op de uitvoering van de derde DigiD-aansluiting.
Dit wordt ingevoerd in 2021 / 2022.
ENSIA 2021
Jaarlijks wordt de gemeente Heerlen geaudit vanuit de ENSIA. Ook in de ENSIA 2021 zal een verscherping van de audit-regels worden opgenomen, ook aangaande DigiD. Wij zullen hier tijdig op dienen te anticiperen.
De ENSIA-coördinator voert regie hierop.
Interne audit DigiD
Door middel van een jaarlijkse selfassessment (interne audit) stelt de gemeente Heerlen vast in hoeverre zij aan de eisen voldoet en daarmee welk volwassenheidsniveau van informatieveiligheid op dat moment geldt. Het selfassessment omvat ook de uitbestede diensten, dus de gehele keten. Voor wat betreft de uitbestede diensten bundelen gemeenten hun verzoeken om assurance (TPM) richting de leveranciers waar zij gezamenlijk gebruik van maken. Verplicht onderdeel van de selfassessment is een jaarlijkse penetratietest op de kroonjuwelen (waaronder DigiD) van de gemeente. Bij deze penetratietest wordt de feitelijke veiligheid getoetst bij gemeenten. In deze jaarlijkse interne audit zal DigiD een prominente rol krijgen.
Vooruitlopend op deze jaarlijkse penetratietest en selfassessment zullen periodiek ook extra interne controles plaatsvinden van de technische stand van zaken van in ieder geval de DigiD-infrastructuur.
De CISO voert regie op de uitvoering van deze extra interne controles en rapportage aan directie en portefeuillehouder.
Dit wordt per direct ingevoerd.
Verzelfstandiging Parkstad-IT
Zoals het er nu naar uitziet zal de lichte GR Parkstad-IT worden verzelfstandigd. Dit maakt dat bestaande (vaak impliciete) werkafspraken expliciet moeten worden vastgelegd in een SLA (service level agreement). In deze SLA zal ook expliciet moeten worden opgenomen hoe wordt omgegaan met geconstateerde afwijkingen ten opzichte van de ENSIA-normen, en specifiek de DigiD-normen.
De CISO voert regie op de verwerking van deze aanvullende eisen in de SLA.
Dit wordt uitgevoerd in aanloop naar de verzelfstandiging van Parkstad-IT, te starten in 2021.
Ketenbeheer DigiD – onderzoek aanvullende verklaring leverancier
Bij het beheer van de technische DigiD-infrastructuur zijn nu diverse partijen actief. Deze partijen voldoen aan de BIO-normen (of aan de ISO-normen). Maar de jaarlijkse DigiD-audit is een voornamelijk technische audit op een webapplicatie. Hierbij wordt gewerkt met een eigen vooral technisch normenkader, gebaseerd op de NCSC beveiligingsrichtlijnen voor webapplicaties, dat afwijkt van de BIO-normring (en de ISO-normering).
Onderzocht wordt of het mogelijk is of onze leveranciers, bovenop de ISO- of BIO-verklaring, een verklaring kunnen afgeven dat hun omgeving voldoet aan de ENSIA-normering inzake DigiD.
De CISO voert regie op dit onderzoek.
Dit wordt ingevoerd in 2021.

Inwerkingtreding

1. Dit uitwerkingsbesluit treedt in werking na publicatie.
2. Dit uitwerkingsbesluit wordt minimaal één keer per jaar, of zodra zich belangrijke wijzigingen voordoen, geëvalueerd, beoordeeld en zo nodig bijgesteld en vastgesteld.
3. De algemeen directeur/gemeente secretaris is gemandateerd tot het aanbrengen van kleine wijzingen in dit uitwerkingsbesluit, en wordt hierbij ondersteund door de CISO en/of de ENSIA-coördinator.
4. Aanpassingen van dit uitwerkingsbesluit worden bekendgemaakt, de meest actuele versie is te vinden op www.overheid.nl.

Aldus besloten in de vergadering van het college der gemeente Heerlen op 20 april 2021
de burgemeester,
drs. R. Wever
de secretaris,
L. Schouterden