Jaarverslag Informatiebeveiliging en Privacy

NEDERWEERT
NEDERWEERT-EIND
BUDSCHOP
OSPEL
OSPELDIJK
LEVEROY

Nederweert
samen groots, samen doen!

Jaarverslag informatieveiligheid en privacy

Inleiding
De gemeente Nederweert onderstreept het belang van informatieveiligheid en privacy. De grote hoeveelheid gegevens – vaak van burgers – die de gemeente gebruikt voor het uitvoeren van haar taken moeten op een veilige manier worden verwerkt met een zo klein mogelijk risico voor de betrokkenen. In 2013 heeft de gemeente, samen met alle andere gemeenten in Nederland, de resolutie “Informatieveiligheid, randvoorwaarde voor de professionele gemeente” getekend. Hiermee conformeert de gemeente zich aan de implementatie van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). De inwerkingtreding van de Algemene Verordening Gegevensbescherming op 25 mei 2018 vraagt extra inspanningen van de gemeente ten aanzien van het veilig verwerken van persoonsgegevens.

Het doel is om onze werkprocessen in overeenstemming te brengen met de wettelijke eisen (onder andere vanuit de BIG en ENSIA) zodat het de toets van verplichte beveiligingseisen, privacy normen en audits kan blijven doorstaan.

Dit verslag behandelt kort de ontwikkelingen op het gebied van informatieveiligheid en privacy en de ondernomen en te nemen stappen door de gemeente. Hiermee verantwoord het college van burgemeester en wethouders zich over informatieveiligheid en privacy aan de gemeenteraad.

1. Eenduidige Normatiek Single Information Audit (ENSIA)
Vanaf 2017 moet de gemeente horizontale (aan de gemeenteraad) en verticale (aan de toezichthouders) verantwoording afleggen over informatieveiligheid. Via de ENSIA-methodiek legt de gemeente deze verantwoording af over de BIG, Basisregistratie personen (BRP), Paspoorten en Nederlandse Identiteitskaarten (PNIK), SUWInet, DigiD en BAG/BGT (Basisregistratie adressen en gebouwen/grootschalige topografie). Aan de hand van een zeer uitgebreide vragenlijst wordt verantwoord over informatieveiligheid in het algemeen en de benoemde gebieden. Voor 2017 vindt die verantwoording plaats op de gebieden SUWInet en DigID. In 2018 zal dit op alle benoemde gebieden gebeuren.

Op de onderdelen SUWInet en DigiD wordt een audit uitgevoerd door een gecertificeerde auditor. Op basis van de ENSIA-verantwoording verklaart het college met een collegeverklaring (zie bijlage 1) over het voldoen aan de door de toezichthouders vastgestelde normen. Op deze verklaring van het college wordt door de auditor “assurance” afgegeven; dat wil zeggen dat de auditor verklaart dat de verklaring van het college op waarheid berust.

Uit de ENSIA-verantwoording blijkt dat de gemeente Nederweert zowel bij SUWInet als bij DigiD aan één norm niet voldeed. In het geval van SUWInet bleek het informatieveiligheidsbeleid van de gemeente niet meer actueel. Bij DigiD bleek de beveiligingsmaatregel DNSSEC niet ingevoerd, DNSSEC zorgt ervoor dat de 'bewegwijzering' van het internet veiliger en vertrouwder wordt. Deze tekortkomingen zijn opgenomen in een verbeterplan per norm (zie bijlagen 2 en 3) en inmiddels gerepareerd en wel:

- Het beleid is geactualiseerd en opnieuw vastgesteld.
- Met de overstap naar een nieuwe leverancier wordt de invoering van DNSSEC mogelijk en gerealiseerd.

2. Algemene Verordening Gegevensbescherming

Op 25 mei 2018 treedt de Algemene Verordening Gegevensbescherming (AVG) in werking. Deze Europese wetgeving vervangt de huidige Wet bescherming persoonsgegevens (Wbp). De AVG schrijft voor hoe en op welke gronden persoonsgegevens worden verwerkt en dat deze adequaat moeten worden beschermd. De AVG verscherpt de wetgeving hieromtrent. De AVG verplicht de gemeente onder andere tot het aanstellen van een interne toezichthouder – de Functionaris Gegevensbescherming (FG) – en het vastleggen van alle verwerkingen van persoonsgegevens in een verwerkingenregister.

Ook de rechten van betrokkenen (burgers) zijn in de AVG aangescherpt; een burger mag de gemeente Nederweert vragen inzage te bieden waar en op welke gronden zijn of haar gegevens worden verwerkt. Na een dergelijk verzoek moet de gemeente op korte termijn inzage bieden. De Autoriteit Persoonsgegevens (AP) houdt in Nederland toezicht op de naleving van de AVG en mag onder meer boetes uitdelen. De gemeente Nederweert heeft ruim op tijd een FG aangesteld en aangemeld bij de AP. Tevens is een verwerkingenregister opgesteld en wordt het bestaande privacybeleid en verband houdende protocollen herzien.

3. Baseline Informatiebeveiliging Nederlandse Gemeenten

In 2013 is de gemeente Nederweert gestart met de implementatie van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Dit is een basisnormenkader waarin de minimaal te treffen maatregelen voor informatieveiligheid zijn vastgelegd. Om dit normenkader, bestaande uit 300 maatregelen, stapsgewijs te implementeren wordt ieder jaar een informatieveiligheidsanalyse gedaan. Op basis van deze analyse en een risicoanalyse zijn maatregelen geprioriteerd en vastgelegd in een jaarlijks actieplan. Uit de analyse van mei 2017 bleek dat ongeveer 70% van alle maatregelen zijn geïmplementeerd. Dit is, landelijk gezien, een goede score voor de fase waarin Nederweert zich nu bevindt.

Met het huidige actieplan 2017-2018 wordt een stijging naar 90% beoogd en naar verwachting gerealiseerd in 2019. Er wordt in 2018 een nieuwe analyse uitgevoerd en een actieplan voor 2019 opgesteld. Dit is maatwerk. Via een prioritering wordt een selectie gemaakt van verbetermaatregelen die in het actieplan worden opgenomen. Centraal staat hierbij de maat van Nederweert. Als Nederweertse criteria geldt dat aan wettelijke verplichtingen te allen tijde wordt voldaan en dat technische en procedurele acties m.b.t ICT-NML, privacy taken, ENSIA taken en bewustwording centraal staan. Dit betekent dat acties die hierop betrekking hebben als prioriteit worden gezien. Zo blijft de basis op orde en kan de gemeente voldoen aan wettelijke verplichtingen.

4. Implementatie van de AVG

De gemeente Nederweert is in 2017 begonnen met de voorbereidingen op de implementatie van de nieuwe Algemene Verordening Gegevensbescherming. Hiervoor zijn de verwerkingen van persoonsgegevens binnen de gemeente vastgelegd in een verwerkingenregister. Daarnaast wordt privacybeleid herzien en is een procedure voor het melden van datalekken vastgesteld. Aan de hand van een plan van aanpak privacy 2018-2019 worden activiteiten uitgevoerd om een privacyproof basisniveau te realiseren en een veilige verwerking van persoonsgegevens te waarborgen.

5. Verantwoordelijkheid in de lijn

Het lijnmanagement van de gemeente Nederweert is integraal verantwoordelijk voor informatieveiligheid en privacy in de bedrijfsvoering. Het Managementteam heeft eind 2017 aangegeven nadrukkelijker invulling te willen geven aan deze verantwoordelijkheden. Er is frequent een MT-plusoverleg gevoerd waar informatieveiligheid en privacy op de agenda staat.

Daarnaast toont het lijnmanagement betrokkenheid door het aansturen en aanwijzen van de beveiligingsorganisatie. Ook geeft het lijnmanagement invulling aan haar verantwoordelijkheid door periodiek interne controles te laten uitvoeren en hierover aan hun te laten rapporteren. Dit heeft ertoe geleid dat in 2018 informatieveiligheid en privacy sterker zijn geborgd in de organisatie.

6. Intern controleplan

Uit toetsing van het normenkader (BIG) bleek eerder dat de risico's liggen op het bestaan en werking van bestaande procedures. Dit wil zeggen dat in de praktijk en in werkprocessen ook door de interne organisatie gewerkt moet worden conform standaardprocedures, afspraken en dat hierover periodiek wordt gerapporteerd.

Om de effectiviteit en het bestaan van maatregelen ten aanzien van informatieveiligheid en privacy structureel te borgen en te toetsen, is in 2018 een intern controleplan opgesteld. Hierin is per kwartaal vastgelegd welke interne controles plaatsvinden, op welke wijze, door wie en aan wie wordt gerapporteerd. Verschillende medewerkers voeren de interne controles uit onder verantwoordelijkheid van het lijnmanagement. De controller informatieveiligheid (concern control), de CISO en de Functionaris Gegevensbescherming verrichten het verbijzonderde toezicht op dit controleplan. In kwartaalrapportages wordt generiek aan het MT verantwoording afgelegd over deze controles. Hiermee toont de gemeente Nederweert aan in control te zijn.

7. Externe ondersteuning

Om informatieveiligheid en privacy goed te borgen in de gemeentelijke processen is externe ondersteuning ingeschakeld van BMC. Met deze ondersteuning zijn uitvoerende acties opgepakt en zijn beveiligingsbeheerders opgeleid voor hun rol en taken binnen de organisatie. Deze ondersteuning is dusdanig ingericht dat de gemeente zelfstandig in staat is om privacy en informatiebeveiliging structureel te borgen in de organisatie en de benodigde taken efficiënt en doelmatig uit te voeren. Hierdoor ontstaat een adequaat kennisniveau in de organisatie en kan worden voldaan aan wettelijke verplichtingen, normen en audits. Er zijn voldoende financiële middelen aanwezig om de komende jaren, daar waar nodig, gebruik te maken van de expertise en advisering van BMC.

8. Vooruitblik

Er wordt continu gewerkt aan het verbeteren en duurzaam borgen van informatieveiligheid en privacy in de gemeentelijke processen. Op basis van een informatieveiligheidsanalyse en risicoanalyse wordt halverwege 2018 een nieuw actieplan vastgesteld voor de verdere implementatie van de BIG. Ook activiteiten uit het actieplan privacy lopen door zodat de gemeente voldoet aan de nieuwe privacy wetgeving. Eind 2018 moet de gemeente zich wederom verantwoorden over informatieveiligheid volgens de ENSIA-methodiek. In mei 2019 wordt dit verantwoordingsproces afgerond.

Bijlage 1 – Collegeverklaring ENSIA SUWInet en DigiD

Collegeverklaring ENSIA 2017 DigiD en SUWInet

Het college van burgemeester en wethouders van de gemeente Nederweert legt met deze verklaring verantwoording af over geselecteerde informatiebeveiligingsnormen inzake DigiD en Suwinet op basis van de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek.

Het doel van ENSIA is om verantwoording over informatieveiligheid af te leggen aan de gemeenteraad. ENSIA sluit aan op de gemeentelijke planning en controlcyclus voor informatiebeveiliging, neemt de Baseline Informatiebeveiliging Gemeenten (BIG) als uitgangspunt en maakt gebruik van een daarop ingerichte zelfevaluatie. Hierdoor heeft het gemeentebestuur meer overzicht over de informatiebeveiliging van de gemeente en kan het bestuur beter sturen en verantwoording afleggen aan de gemeenteraad en andere belanghebbenden.

Zo structureert ENSIA ook de verticale verantwoording van gemeenten richting de rijksoverheid over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Reikwijdte verklaring

Deze verklaring betreft de onderdelen van de ENSIA systematiek waarover assurance wordt gevraagd van een onafhankelijke IT auditor. Voor het jaar 2017 betreft dit DigID (aansluitnummer 1002221, aansluitnaam Gemeente Nederweert) en Suwinet. De verklaring omvat het op 31 december 2017 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen inzake DigiD (Norm ICT-beveiligingsassessments DigiD versie 2.0, op het openbare deel van de websites van het ministerie van BZK) en Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.01 op website BKWI en bijlage 1 van de notitie Verantwoordingsstelsel op website ENSIA voor de selectie van normen). De normen vinden hun basis in internationale standaarden en zijn geschikt voor het doel van deze Collegeverklaring. De Collegeverklaring omvat niet de werking van de maatregelen over 2017.

De beheersingsmaatregelen inzake DigiD die zijn uitbesteed vallen buiten de reikwijdte van deze collegeverklaring. Uit de bijlage bij de collegeverklaring “bijlage 1 DigiD” blijkt over welke beheersmaatregelen en DigiD-normen door de dienstverlener aan wie de beheersmaatregelen zijn uitbesteed verantwoording wordt afgelegd. Deze collegeverklaring en de verantwoording van de dienstverlener dekken tezamen de geselecteerde normen inzake DigiD af.

Deze Collegeverklaring is opgesteld voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet. De gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet zijn via bij deze collegeverklaring behorende afzonderlijke bijlagen voor DigiD (bijlage 1 Rapportage DigiD Assessment - ENSIA 2017) en Suwinet (bijlage 2 SUWI) geïnformeerd over de afwijkingen van de normen.

Verklaring college

Het college verklaart dat bij gemeente Nederweert op 31 december 2017 de interne beheersingsmaatregelen in opzet en bestaan voldoen aan de geselecteerde normen inzake DigiD en Suwinet, uitgezonderd de Suwinetnorm B.01 en de DigiD-norm U/NW.06.

De op de uitzonderingen gerichte beheersmaatregelen zijn in verbeterplannen opgenomen, zijn belegd en worden gemonitord.

Bijlage 2 – Verbeterplan SUWInet

Verbeterplan ENSIA audit SUWI 2018
De gemeente Nederweert heeft in 2017 voor het eerst verantwoording over informatieveiligheid afgelegd met de ENSIA-systematiek (Eenduidige Normatiek Single Information Audit). Met deze systematiek wordt integraal over de verschillende vakgebieden en stelsels verantwoording afgelegd aan de toezichthouders (verticaal; departementen) en de gemeenteraad (horizontaal). Onderdeel van deze verantwoording betreft een collegeverklaring inzake de beveiliging van DigiD en SUWInet, waarmee het college aangeeft in hoeverre aan de verplichte normen voor SUWI en DigiD te voldoen. Op deze verklaring wordt na uitvoering van een IT-audit assurrance afgegeven door een hiertoe bevoegde auditor (RE).
In de collegeverklaring heeft het college van Burgemeester en Wethouders van de gemeente Nederweert verklaart aan een SUWI-norm niet te voldoen. Ook is hierbij verklaard dat een verbeterplan is opgesteld om binnen redelijke termijn alsnog aan deze norm te gaan voldoen. Voorliggend document betreft het verbeterplan van de gemeente Nederweert om alsnog te voldoen aan de SUWI-norm **B.01**.

Verbeterplan SUWI-norm B.01

Beschrijving van de norm

De Afnemer heeft voor de aansluiting op Suwinet expliciet aandacht besteed aan het stelsel van beveiligingsmaatregelen in zijn informatiebeveiligingsbeleid, of hiervoor een apart aansluitingsbeleid ontwikkeld.

Bijbehorende ENSIA-vragen

5.1.1.a Is er een actueel informatiebeveiligingsbeleid?
5.1.2.a Wordt het informatiebeveiligingsbeleid **minimaal één keer per drie jaar** of bij grote wijzigingen binnen de organisatie opnieuw beoordeeld en indien nodig aangepast?

Geconstateerde afwijking

Het informatiebeveiligingsbeleid van de gemeente is in 2013 vastgesteld. **Hiermee wordt niet voldaan aan het hebben van een actueel beleid** (jonger dan 3 jaar). Om aan de gestelde norm te voldoen had het beleid uiterlijk eind 2016 moeten worden herzien en opnieuw vastgesteld.

Verbeterplan

Inmiddels is het informatieveiligheidsbeleid geactualiseerd en in routering gebracht ter vaststelling door het college.

Maatregel	Actiehouder	Uitvoering	Planning
Actualiseren van het informatieveiligheidsbeleid	Pascalle Mommers en Lex Smit	Dave Giesbertsen	Q1 2018

Bijlage 3 -- Verbeterplan DigiD

Verbeterplan ENSIA audit DigiD 2018

De gemeente Nederweert heeft in 2017 voor het eerst verantwoording over informatieveiligheid afgelegd met de ENSIA-systematiek (Eenduidige Normatiek Single Information Audit). Met deze systematiek wordt integraal over de verschillende vakgebieden en stelsels verantwoording afgelegd aan de toezichthouders (verticaal; departementen) en de gemeenteraad (horizontaal). Onderdeel van deze verantwoording betreft een collegeverklaring inzake de beveiliging van DigiD en SUWInet, waarmee het college aangeeft in hoeverre aan de verplichte normen voor SUWI en DigiD te voldoen. Op deze verklaring wordt na uitvoering van een IT-audit assurrance afgegeven door een hiertoe bevoegde auditor (RE).

In de collegeverklaring heeft het college van Burgemeester en Wethouders van de gemeente Nederweert verklaart aan een DigiD-norm niet te voldoen. Ook is hierbij verklaard dat een verbeterplan is opgesteld om binnen redelijke termijn alsnog aan deze norm te gaan voldoen. Voorliggend document betreft het verbeterplan van de gemeente Nederweert om alsnog te voldoen aan de DigiD-norm **U/NW.06**.

Verbeterplan DigiD-norm U/NW.06

Beschrijving van de norm

Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.

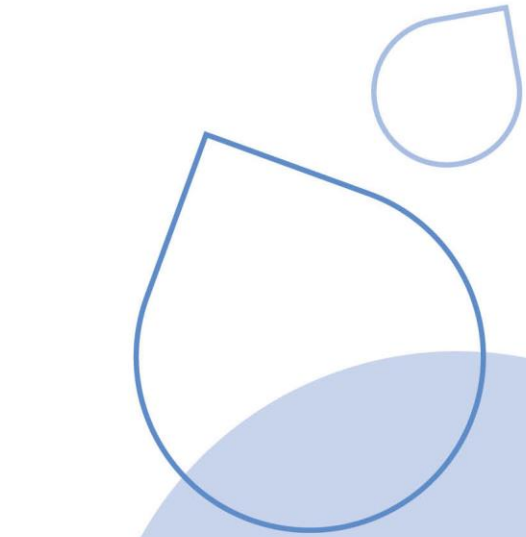
Geconstateerde afwijking

De leverancier/provider van het platform van de gemeente Nederweert (Ziggo) biedt niet de mogelijkheid om DNSSEC in te schakelen. Dit is wel een vereiste.

Verbeterplan

Inmiddels is overeenstemming bereikt met een nieuwe leverancier. Deze aanbieder maakt DNSSEC wel mogelijk. De implementatie hiervan vindt waarschijnlijk eind maart 2018 plaats.

Maatregel	Actiehouder	Uitvoering	Planning
Overschakelen naar andere leverancier; inschakelen DNSSEC.	Joop Beris (ICT NML)	Joop Beris (ICT NML)	Q1/Q2 2018



Nederweert
samen groots, samen doen!

Raadhuisplein 1
Nederweert
Postbus 2728
6030 AA Nederweert

T 0495 677 111 en 14 0495
F 0495 633 245
E info@nederweert.nl

www.nederweert.nl