

Raadsinformatiememo

Datum woensdag 4 februari 2015
Ons kenmerk 15.002096
Aan De Gemeenteraad en de Commissie Samenleving
Kopie aan
Van College van burgemeester en wethouders
Onderwerp Stand van zaken implementatie Baseline Informatiebeveiliging Nederlandse Gemeenten en de uitgevoerde GAP analyse

Geachte dames en heren,

Wat is informatiebeveiliging?

Informatiebeveiliging staat voor het vooraf treffen van maatregelen ter voorkoming, beperking, herstel en opsporing van verstoringen in de informatievoorziening. Om informatie adequaat te beschermen, moet een samenhangend stelsel van organisatorische, ICT, fysieke en menselijke maatregelen worden genomen.

Wat is privacy?

Privacy is het recht om vergeten te worden. De grondslag van de privacy wordt onder andere gevonden in de grondwet, EVRM (Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden) en de Wet bescherming persoonsgegevens. Uit artikel 13 van de Wet bescherming persoonsgegevens blijkt de samenhang tussen de privacy en informatiebeveiliging, namelijk om de bescherming van persoonsgegevens te waarborgen hebben wij passende organisatorische en technische maatregelen nodig. Door de decentralisatie krijgt de gemeente vanaf 1 januari 2015 meer persoonsgegevens onder haar hoede.

Resolutie en de Baseline informatiebeveiliging Nederlandse Gemeenten

De leden van de Vereniging Nederlandse Gemeenten (VNG) hebben tijdens de Bijzondere Algemene Ledenvergadering op 29 november 2013 de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' aangenomen. In deze resolutie is aangegeven dat het college de gemeenteraad informeert over informatieveiligheid. In deze resolutie is tevens ingestemd met de Baseline Informatiebeveiliging Gemeenten (hierna: BIG) die voortaan als hét gemeentelijke basishoofdkader geldt.

Gemeente Schagen onderschrijft het belang van informatieveiligheid en de implementatie van de BIG als basishoofdkader. De BIG is de basis van ons eigen informatiebeveiligingsbeleid 2014-2018. De baseline bevat een set van ruim 150 beveiligingsmaatregelen. Aan de hand van de uitgevoerde GAP analyse (vergelijking gewenste en huidige situatie) is prioritering aangebracht in de implementatie.

Aansluiting Informatiebeveiligingsdienst

Vanuit de hierboven genoemde resolutie is gemeente Schagen aangesloten bij de Informatiebeveiligingsdienst (IBD). De IBD is een gezamenlijk initiatief van de VNG en het Kwaliteitsinstituut Nederlandse Gemeenten (KING). De IBD is er voor alle gemeenten en richt zich op bewustwording en concrete (incident)ondersteuning aangaande informatiebeveiliging. Door het aansluiten bij de IBD worden wij ook op de hoogte gesteld wanneer er mogelijke dreigingen zijn.

Visie en strategische aanpak

Visie op informatiebeveiliging: Zoals in het informatiebeveiligingsbeleid 2014-2018 benoemd, wil gemeente Schagen conform de Meerjarenvisie in 2018 in control zijn en hier op professionele wijze verantwoording over afleggen.

Strategische aanpak informatiebeveiliging: "Van onbewust risico's lopen, naar bewust risico's nemen".

Gemeente Schagen kiest voor een gedifferentieerde risiconeutrale strategische aanpak voor informatiebeveiliging middels preventieve, detectieve en repressieve maatregelen.

Met risiconeutraal bedoelen wij dat de dreiging niet meer manifest is, óf als de dreiging wel manifest is geworden, de gevolgschade geminimaliseerd wordt.

Met gedifferentieerde beveiliging bedoelen wij dat de gekozen aanpak een doorlopende afweging is tussen het te lopen risico en de eventuele schade.

Activiteiten i.h.k.v. informatiebeveiliging en privacy

In 2013 hebben wij onder andere

- een gemeentebreed informatiebeveiligingsbeleid 2014-2018 opgesteld
- extra ICT maatregelen op het gebied van technische toegangsbeveiliging, zoals wachtwoordenbeleid en stringente schermbeveiliging, ingevoerd
- een autorisatiebeleid rondom toegang tot gemeentelijke gebouwen geïmplementeerd
- diverse audits, zoals de zelfevaluatie waardedocumenten en de DigiD-audit, uitgevoerd.

In 2014 hebben wij de volgende acties uitgevoerd:

- Inbedden en inzichtelijk maken van beveiligingsmaatregelen op het gebied van waardedocumenten en SUWI-net.
- Inrichten van de continuïteitsorganisatie en –proces t.b.v. COWWI. Hiermee hebben we een proces opgezet waardoor de organisatie voldoende voorbereid moet zijn op incidenten en mogelijke disrupties (ernstige ontwrichting) om de kwaliteit van die dienstverlening op een vooraf gedefinieerd niveau te waarborgen. Het verzekert op hoofdlijnen de continue beschikbaarheid van de gedefinieerde kritieke activiteiten en bronnen die benodigd zijn om te allen tijde de kritieke producten en diensten te leveren.
- Analyseren privacyaspecten op de vijf hoofdprocessen van het sociaal domein (i.c.m. interactieve workshops t.b.v. bewustwording privacy medewerkers)
- Opstellen diverse bewerkersovereenkomsten t.b.v. bescherming persoonsgegevens
- Uitvoeren diverse audits, zoals de zelfevaluatie waardedocumenten, Brp en de DigiD-audit.

Wat gaan wij in 2015 uitvoeren?

- Implementatie diverse maatregelen op het gebied van fysieke beveiliging, personele beveiliging en mobiele beveiliging
- Inrichting en implementatie van de continuïteitsorganisatie en –proces voor de gehele organisatie
- Uitvoering geven aan het plan van aanpak organisatiebrede privacybeleid
- Uitvoering geven aan een bewustwordingsprogramma voor medewerkers op het gebied van informatiebeveiliging en privacy

Audit informatiebeveiliging/ DigiD

Sinds 2013 is elke gemeente met een DigiD-aansluiting verplicht om op 28 voorgeschreven normen zicht te laten auditen door een onafhankelijk IT-auditor. Van deze normenset worden 22 normen bij de websiteleverancier geaudit.

De overige zes normen zijn:

- Toegangsbeveiliging/toegangsbeheer;
- Niet (meer) gebruikte websites en/of informatie moet worden verwijderd;
- Overeenkomst met leverancier;
- Veilig beheermechanismen;
- Versleutelen van gevoelige gegevens;
- Governance, organisatie, rollen en bevoegdheden inzake preventie, detectie en respons inzake informatiebeveiliging

Bovenstaande normen geven een goede weergave hoe binnen de gemeente informatiebeveiliging is georganiseerd en geborgd.

Audit 2013

Zoals u in het jaarverslag van de accountant in 2013 heeft kunnen lezen, waren wij in eerste

instantie niet geslaagd op dit normenkader. Dit heeft **nooit** geïmpliceerd dat wij geen veilige DigiD omgeving hebben. Door het korte bestaan van de gemeente Schagen waren sommige onderdelen nog niet optimaal ingericht.

Her-audit 2013

Direct na uitslag van de audit 2013 hebben wij een verbeteringsplan opgesteld. Medio juli 2014 heeft een her-audit 2013 plaatsgevonden en zijn wij geslaagd op alle zes normen van het normenkader.

Audit 2014

Ook voor het normenkader voor het auditjaar 2014 zijn wij op alle zes normen geslaagd.

Samengevat

Gemeente Schagen onderschrijft het belang van informatieveiligheid en de implementatie van de BIG als basishorvenkader. Wij prioriteren de implementatie van de maatregelen door een jaarlijkse uit te voeren GAP analyse, zodat alle maatregelen geïmplementeerd zijn en wij in 2018 in control zijn op dit onderwerp, aansluitend bij de Meerjarenvisie 2014-2018.

Onze werkzaamheden zijn er op gericht om de risico's voor zo ver mogelijk af te dekken. "Voor zo ver mogelijk" omdat het met een onderwerp als informatiebeveiliging in de digitale wereld waarin wij leven, moeilijk te voorspellen hoe deze wereld er morgen uit ziet. Indien er mogelijke reële dreigingen zijn, spelen wij hier uiteraard direct op in. Aansluiten bij de IBD heeft hier met de signalerende rol van de IBD voor wat betreft dreigingen bij geholpen.

Verklarend afkortingenlijst

BIG	Baseline Informatiebeveiliging Nederlandse Gemeenten
Brp	Basisregistratie Personen
COWWI	Centrale Ondersteuning Wijkteams, Werk en Inkomen
EVRM	Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden
GAP analyse	Analyse tussen de gewenste situatie en huidige situatie
KING	Kwaliteitsinstituut Nederlandse Gemeenten
IBD	Informatiebeveiligingsdienst
SUWI	Structuur Uitvoeringsorganisatie Werk en Inkomen
VNG	Vereniging Nederlandse Gemeenten