Raadsvoorstel

Agendapunt:
Zaaknummer: 2016-014667

Onderwerp
Informatiebeveiliging

Datum voorstel	**Datum raadsvergadering**	**Bijlagen**	**Ter inzage**
20-12-2016	07-03-2017		

Aan de gemeenteraad,

0. Samenvatting
In 2017 moet conform afspraak met de VNG de implementatie van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) worden afgerond. Informatieveiligheid hoort aantoonbaar op procesniveau te worden geborgd. Om hier te komen dient te worden geïnvesteerd. De uitgaven genoemd in dit raadsvoorstel moeten er toe leiden dat de gemeente Goirle voor wat betreft informatiebeveiliging volledig in control is.

1. Wat is de aanleiding / wat is het probleem?
Informatie is één van de voornaamste bedrijfsmiddelen van de gemeente. Informatieveiligheid is daarom van groot belang. Informatiebeveiliging (IB) is het proces dat dit belang dient. Sinds medio 2016 is een chief information security officer (CISO) op ad interim basis gestart bij de gemeente Goirle. Om te kunnen voldoen aan de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) dienen financiële middelen te worden vrijgemaakt om daadwerkelijk in control te kunnen komen.

2. Wat willen we bereiken?
Bereikt moet worden dat de gemeente Goirle in dit kader passende technische en organisatorische maatregelen neemt om gemeentelijke informatie te beschermen en te waarborgen, zodat de gemeente voldoet aan relevante wet- en regelgeving. Goirle streeft ernaar om aantoonbaar ‘in control’ te zijn en daarover op professionele wijze verantwoording af te leggen, en zo uiteindelijk de BIG volledig te implementeren.

3. Wat gaan we daarvoor doen?
Informatieveiligheid en privacy zijn onderwerpen die steeds prominenter op de agenda staan bij de lokale overheden. Dit is niet zo vreemd, als je bedenkt dat de primaire bedrijfsprocessen van deze organisaties steeds meer lijken op die van een ‘informatiefabriek’ en de digitalisering steeds verder toeneemt. Keerzijde van de digitalisering is de kwetsbaarheid op dit vlak. Dagelijkse berichtgeving in de media over informatiebeveiligings- en privacy incidenten en niet in de laatste plaats de dwingende wet- en regelgeving (o.a. Wet Datalekken en Europese Privacyverordening) noopt lokale overheden tot het goed organiseren van informatieveiligheid.

Informatieveiligheid staat inmiddels prominent op de radar bij bestuurders en (lijn) management van de gemeente Goirle. Dit mede gezien de aanstelling (vooralsnog d.m.v. inhuur) en duidelijke positionering van de adviseur informatieveiligheid (CISO) binnen de afdeling bestuurs- en directie ondersteuning.

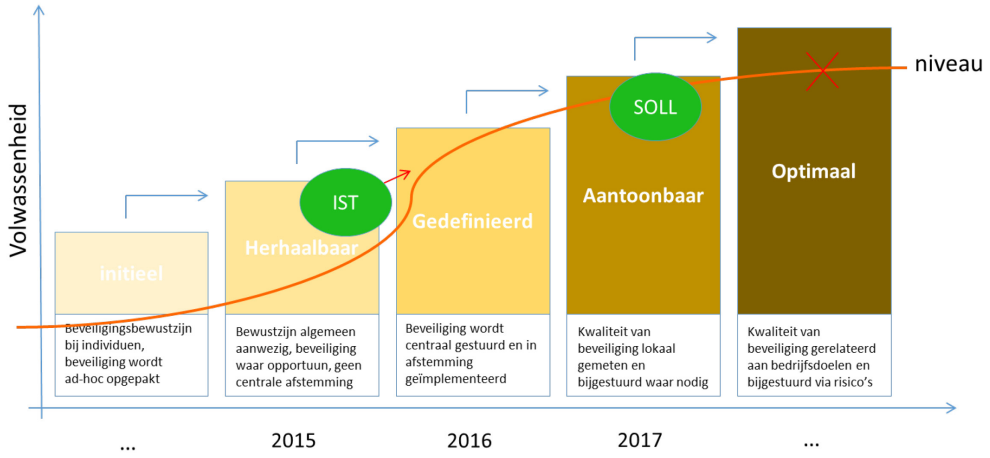
Het is zaak om met elkaar informatieveiligheid ook in een nog breder perspectief te plaatsen en organisatie breed te promoten, stimuleren, incorporeren in de bedrijfsvoering en adequaat te borgen in beleid, processen/procedures en werkinstructies. Dit vindt grotendeels stap-voor-stap plaats met de invoering van de baseline informatieveiligheid Nederlandse gemeenten (BIG) in 2017.

De grootste uitdaging zit echter niet in de techniek zoals vaak verondersteld wordt, maar in de factor mens. Het zodanig beïnvloeden van houding & gedrag dat informatieveiligheid een integraal onderdeel van het DNA van de medewerkers wordt vergt een lange adem.

Vanaf 2017 dient in de jaarrekening verplicht een collegeverklaring te worden opgenomen, waarin het college zich expliciet verantwoord over de mate waarin zij aantoonbaar in control is ten aanzien van het taakveld informatieveiligheid. De collegeverklaring maakt onderdeel uit van de verplichte audit. De ingevulde vragenlijsten (240 + vragen, de getekende collegeverklaring en de assurance-verklaring van de externe auditor moeten voor 31 december van elk jaar worden geüpload ten behoeve van de externe toezichthouders (Ministerie van binnenlandse zaken en koninkrijksrelaties, Ministerie van infra & milieu, rijksdienst voor identiteitsgegevens, autoriteit persoonsgegevens, BKWI (Suwinet) en Logius (DigiD). Het beschikbaar stellen van de benodigde middelen is ook om deze reden van belang; het niveau van informatieveiligheid is niet vrijblijvend.

Gecontroleerd van IST naar SOLL
De CISO coördineert en regisseert centraal de uitvoering van alle activiteiten op strategisch, tactisch en indien nodig ook op operationeel niveau binnen het taakveld informatieveiligheid. Over de voortgang, uitdagingen en bevindingen rapporteert de CISO rechtstreeks aan hoofd BDO (generiek) op dagdagelijkse basis. Daarnaast rapporteert de CISO (generiek en specifiek) aan het college van B&W door tussenkomst van de gemeentesecretaris en/of de burgemeester als portefeuillehouder informatieveiligheid.

Met de uitvoering van het *jaarplan informatiebeveiliging 2016-2017* geeft de CISO richting, vorm en inhoud aan de implementatie van de baseline informatieveiligheid Nederlandse gemeenten (BIG). De GAP-analyse (2016) vormt hiervoor de basis. Doel is dat de gemeente Goirle eind 2017 aantoonbaar voldoet aan de BIG (opzet, bestaan en werking), en hierop objectief ge-audit kan worden.



Bevoegdheid CISO/rechtvaardiging
De belangrijkste bevoegdheid is om op elke plek binnen de organisatie gevraagd en ongevraagd onderzoek te kunnen (laten) doen en zo nodig zaken voor te schrijven. Bij informatiebeveiliging is het echter noodzakelijk om centraal keuzes te maken. Bij (grote) beveiligingsincidenten/-risico's heeft de CISO de bevoegdheid, zo nodig, direct in te grijpen (met verantwoording achteraf richting het management). Voorwaarde om de functie CISO volledig te kunnen vormgeven, is de bevoegdheid om gevraagd en ongevraagd te mogen rapporteren aan het college van B&W of de raad.

ISMS (Information security management system)
Aangezien informatiebeveiliging een complex proces is waarbij stap-voor-stap de kwaliteit op een hoger niveau moet worden gebracht èn worden geborgd wordt aanbevolen om hiervoor een information security management system (ISMS) in te zetten ter ondersteuning.
Het betreft een softwareoplossing die werkt conform het principe van plan-do-check-act (Deming Cycle) en die daarmee de 'stap-voor-stap verbeteren' aanpak ondersteunt, waarbij de verantwoordelijkheid nadrukkelijk bij de proces-eigenaren ligt en de CISO coördineert. De proceseigenaren rapporteren in het MT onder leiding van de gemeentesecretaris.

Een ISMS draagt ook bij aan het op juiste en correcte wijze verantwoording af te leggen over het gebruik van de systemen die gebruikt worden om informatie op te slaan, uit te wisselen etc. Dit gebeurt door middel van audits door externe onafhankelijke toezichthouders. Een audit is een onderzoek naar de organisatie van de informatiebeveiliging betreffende de webapplicaties van de gemeente.
Vanaf 2017 start de landelijke uitrol van ENSIA (Eenduidige Normatiek Single Information Audit). ENSIA ondersteunt gemeenten om horizontaal toezicht op de taakvelden informatieveiligheid en privacy te organiseren. De verticale toezichthouders Logius, RvIG, AP, I&M en BKWI kunnen via ENSIA toezicht houden op de eisen die gesteld worden aan het gebruik van BRP (Basisregistratie personen), PUN (Wet Paspoortuitvoeringsregeling), BAG (Basisregistratie adressen en gebouwen), DIGID, SUWINET (Wet Structuur Uitvoeringsorganisatie Werk en Inkomen), BGT. De vragen worden beantwoord vanuit het ISMS, waardoor dubbele werkzaamheden via ENSIA worden uitgesloten en de kans op fouten verkleind wordt. De aanschaf van een ISMS draagt derhalve bij aan verlagen van de auditlast voor gemeenten.

iBewustzijn
Bewustwording is van essentieel belang wanneer het gaat om informatiebeveiliging. Een gemeente kan nog zo veel technische maatregelen nemen, wanneer medewerkers er niet naar handelen hebben deze maatregelen uiteindelijk aanzienlijk minder effect. De gebruiker ziet niet altijd het belang in van informatiebeveiliging. Zo worden wachtwoorden vergeten of op een Post-it onder het toetsenbord geplakt, computers en/of laptops onbeheerd achtergelaten en bezoekers niet begeleid door het pand. Bewustwording heeft als doel om alle gemeentelijke medewerkers bewust te maken van de informatiebeveiligingsrisico's die de gemeente loopt en ook van de wijze waarop zij zich hiertegen kunnen beschermen.
Informatieveiligheid is dus (ook) sterk afhankelijk van de menselijke kant van de organisatie. Hoe goed de techniek ook is georganiseerd en de fysieke beveiliging mogelijk ook is geregeld, als medewerkers de deuren open houden voor vreemden, niet alert zijn op onbevoegden, phishing mail niet herkennen, etc, dan is de organisatie nog steeds erg kwetsbaar. Om die reden is het van belang dat bestuur, management en de medewerkers ondersteund worden bij het iBewustzijn ter bevordering van het veilig werken.
iBewustzijn zijn niet-bedrijfsspecifieke kennis en vaardigheden. De zwakste schakel binnen het taakveld informatieveiligheid is de factor mens. Er wordt een security awareness programma opgezet en stap-voor-stap uitgevoerd gedurende 2017, waarbij alle personeelsleden in hun respectievelijke rollen en verantwoordelijkheden (verplicht) worden betrokken. Doel is om aandacht voor informatieveiligheid langzaam, maar zeker in het DNA van de medewerkers te krijgen èn te houden. Het betreft hier een samengesteld programma ontwikkeld waarbij de medewerkers zich bewust worden van de risico's en handvatten krijgen rondom (informatie) veilig handelen. Onderdelen hierbinnen zijn:

- Nulmeting en een intakegesprek met CISO en opdrachtgever over welke beveiligingsissues er zijn, actualiteit, keuze in vormen van leren)
- Begeleiden van de organisatie, Bestuur en Management naar iBewustzijn
- Begeleiding inrichting en borging leercyclus: organiseren, uitnodigen, voortgang bewaken, rapportages, analyseren, toetsen van de leercyclus
- Bespreken resultaten en bijstellen van de leercyclus in het iBewustzijnplan met CISO, opdrachtgever en HRM.

Externe expertise
Het kan noodzakelijk of gewenst zijn om tijdelijk externe expertise in te schakelen, bijvoorbeeld na een security incident zoals een (groot) datalek. Hiertoe moet de CISO over voldoende middelen kunnen beschikken om indien nodig snel te kunnen schakelen, uiteraard met verantwoording achteraf. Daarnaast is het soms noodzakelijk om steekproefsgewijs de organisatie te "testen" (door security audits/mystery guests) en om specialistische kennis in te schakelen (bv. tegen hackers).

4. Wat mag het kosten?
Informatieveiligheid hoort aantoonbaar op procesniveau te worden geborgd, waarbij de proceseigenaar eindverantwoordelijk is. Coördinatie, regie en betrokkenheid is essentieel voor het welslagen van de implementatie. Hier horen uiteraard middelen bij.
Aangezien de rol van CISO nieuw is binnen Goirle en concrete ervaringscijfers ontbreken, is voor 2016 nog geen budget vastgesteld. Over 2016 zijn de volgende kengetallen bekend:
Tot 31 december 2016 zijn de volgende kosten gemaakt in overleg met hoofd BDO:

- Kwetsbaarheid scans website(s), € 1.000,00

- Interne audit technische infrastructuur en datacenter, € 500,00
- Aanschaf versleutelde USB-sticks, € 120,00

Voor 2017 wordt gevraagd om middelen vrij te maken voor drie zaken:

- Aanschaf ISMS
- iBewustzijnsprogramma
- Externe expertise

ISMS

Een ISMS-implementatie vergt een "investering" in software (SaaS) en eenmalig tijdelijke ondersteuning bij de inrichting. Het betreft in eerste aanleg een 3-jarig ISMS2.0 abonnement:

Jaar 1:	Jaarlijkse abonnementskosten incl. eenmalige implementatie	€ 7.450,00 (i + s)
Jaar 2 en 3:	Jaarlijkse abonnementskosten	€ 4.100,00 + (s)
Totale investering 3-jarig ISMS2.0 abonnement		€ 15.650,00

Er wordt een 3-jarig abonnement afgesloten. Na afloop van deze periode blijft een vervolg nodig, waardoor de kosten een structureel karakter hebben, ook na de periode van 3 jaar.

iBewustzijnsprogramma

Het bewustzijnsprogramma omvat een totale kostenpost van € 20.500,00 (i)

NB: het iBewustzijnsprogramma is tot een maximum van € 10.000,00 subsidiabel. De werkelijke kosten kunnen daardoor lager uitvallen. Het actueel houden van iBewustzijn onder het personeel blijft ook na 2017 aan de orde. Denk hierbij aan opleiden nieuwe medewerkers of opfrissen van kennis. Deze lasten zullen flink lager zijn en hiervoor wordt het opleidingsbudget ingezet.

Externe expertise

Voor de inhuur van externe expertise dienen onderstaande structurele kosten worden gemaakt:

Security audits	€ 7.000,00
Specialistische ondersteuning	€ 10.000,00
Onvoorzien	€ 5.000,00 +
Totaal	€ 22.000,00 (s)

	2017	**2018 en verder**
Incidentele lasten	€ 23.850,00	€ 0,00
Structurele lasten	€ 26.100,00	€ 26.100,00
Totaal	**€ 49.950,00**	**€ 26.100,00**

In de begroting 2017 zijn geen middelen gereserveerd voor het implementeren van de BIG. Het is echter wel een verplichting waar we als gemeente aan moeten voldoen. Daarom wordt voorgesteld om de financiële middelen voor 2017 van in totaal € 49.950,00, ondanks het deels structurele karakter van de lasten, als volgt te dekken:

Totaal kosten 2017	€ 49.950,00
Opleidingsbudget	€ 10.500,00 -/- (max. € 20.500,00 afhankelijk van subsidie)
Subsidie iBewustzijnsprogramma	€ 10.000,00 -/-
Restant	€ 29.450,00

Voorgesteld wordt om het restant van € 29.450,00 te dekken door een onttrekking uit de Algemene Weerstandsreserve (AWR).
Vanaf 2018 worden de structurele lasten van € 26.100,00 meegenomen in de (meerjaren)begroting en wordt naar een structurele dekking voor deze lasten gezocht.

Het is niet uitgesloten dat er nog aanvullend budget nodig is voor de uitvoering van het informatiebeveiligingsplan vóór 01-01-2018. Dit heeft naar waarschijnlijkheid een incidenteel karakter en valt op dit moment niet te becijferen.

5. Communicatie en participatie / inspraak

6. Vervolgtraject besluitvorming
Uw raad wordt verzocht de benodigde budgetten beschikbaar te stellen

7. Fatale beslisdatum
De gemeenteraad kan een besluit nemen in haar raadsvergadering van 7 maart 2017.

8. Voorstel

1. Het college een budget beschikbaar te stellen van € 29.450,00 ten behoeve van de incidentele lasten van de implementatie van de Baseline Informatiebeveiliging Nederlandse Gemeenten en dekking te laten plaatsvinden uit de Algemene Weerstandsreserve.
2. De structurele lasten van € 26.100,00 voor informatiebeveiliging op te nemen in de meerjarenbegroting vanaf het begrotingsjaar 2018.

burgemeester en wethouders van Goirle

Mark van Stappershoef, burgemeester
Michel Tromp, secretaris

De raad van de gemeente Goirle;

gelezen het voorstel van burgemeester en wethouders d.d. 20-12-2016;

gelezen het advies van de commissie Algemene Zaken, d.d. 15-02-2017 ;

gelet op de Gemeentewet;

b e s l u i t :

1. Het college een budget beschikbaar te stellen van € 29.450,00 ten behoeve van de incidentele lasten van de implementatie van de Baseline Informatiebeveiliging Nederlandse Gemeenten en dekking te laten plaatsvinden uit de Algemene Weerstandsreserve.
2. De structurele lasten van € 26.100,00 voor informatiebeveiliging op te nemen in de meerjarenbegroting vanaf het begrotingsjaar 2018.

Aldus besloten door de raad van de gemeente Goirle in zijn vergadering van 07-03-2017.

, de voorzitter

, de griffier