Gemeente Beemster

Jaarverslag 2017 Privacy en Informatieveiligheid

Kenmerk: 1426030

Inhoud

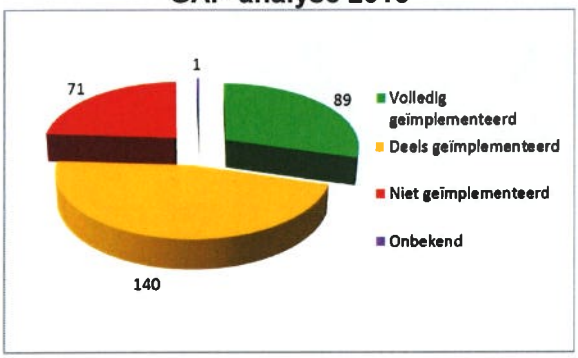
Samenvatting vooraf

Met dit jaarverslag legt het college verantwoording af aan de raad over de informatieveiligheid en privacy bescherming door de gemeente. Nieuw aan dit jaarverslag is dat voor informatieveiligheid gebruik is gemaakt van de ENSIA-methodiek. ENSIA staat voor Eenduidige Normatiek Single Information Audit die wordt toegepast door alle gemeenten in Nederland.

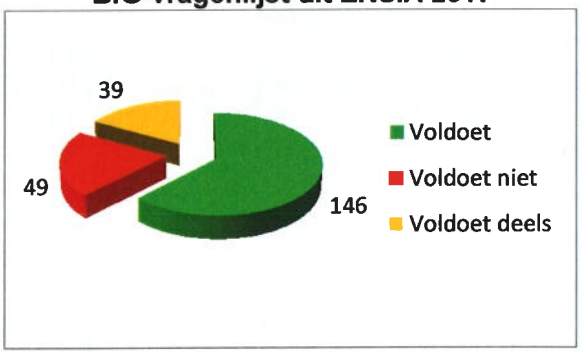
ENSIA omvat meer dan alleen informatiebeveiliging. Ook wordt verantwoording afgelegd over de Basisregistratie Personen (BRP), Paspoort Uitvoeringsregeling Nederland, Basisregistratie Adressen en Gebouwen (BAG) en Basisregistratie Grootschalige Topografie (BGT). Daarnaast specifiek de informatiebeveiliging DigiD en SUWI. Dit jaarverslag gaat alleen over de informatiebeveiliging in het algemeen. Het uitgangspunt daarvoor is de Baseline Informatiebeveiliging Gemeenten (BIG).

In 2015 is een interne analyse gemaakt hoe ver onze gemeente stond met de invoering van de BIG. Ter vergelijking laten we de resultaten uit ENSIA 2017 zien.

GAP-analyse 2015



BIG-vragenlijst uit ENSIA 2017



Er is vooruitgang geboekt, maar er zijn zeker verbeteringen noodzakelijk. Die worden benoemd in het Informatiebeveiligingsplan 2018 (Verbeterplan) dat gelijktijdig met dit jaarverslag door het college is vastgesteld.

1. Inleiding

Dit jaarverslag Informatieveiligheid en Privacy ziet er anders uit dan in de twee voorafgaande jaren. Anders dan afgesproken met de Raad is er na het eerste halfjaar van 2017 geen rapportage verschenen. Door allerlei onvoorziene omstandigheden liep een mogelijke verschijning uit tot oktober. Daar komt bij dat in medio het jaar de uitvoering van de nieuwe landelijke verantwoordingsmethodiek op gang is gekomen: de Eenduidige Normatiek Single Information Audit (ENSIA). Dit jaarverslag sluit qua inhoud en vorm daarop aan. Traditiegetrouw begint dit verslag met de verkenning van onze eigen omgeving.

2. Datalekken, incidenten en dreigingen

Wereldwijd gezien ging in het jaar 2017 veel aandacht uit naar allerlei vormen van cybercriminaliteit (bijv. het Nonpetya-incident); op landelijk vlak ging het daarbij ook over datalekken. Deze lekken deden zich met name voor in de gezondheidszorg, banken en bij overheden. Van cybercrime hebben de meeste van onze gebruikers in hun werk weinig gemerkt maar van de tweede categorie des te meer. Voor de meeste burgers geldt dat zij bij onze gemeente niets of maar heel weinig gemerkt hebben van datalekken en incidenten

Op 20 juli publiceerde Het Parool over een datalek bij de gemeente Purmerend (hoewel niet met name genoemd ging het ook over de gemeente Beemster). Dit datalek betrof circa 150 jeugdige GGZ-cliënten waarvan NAW-gegevens, BSN en gedeclareerde bedragen gedurende enkele maanden zichtbaar waren geweest voor alle ruim 900 gebruikers van het interne netwerk. Het bericht werd door andere media overgenomen. Dit datalek kwam in de media nadat de gemeente GGZ-instellingen waar deze cliënten in behandeling waren op de hoogte had gesteld. Deze aandacht in de media moet gezien worden in de context van de maatschappelijke discussies over de overdracht van de taken in het kader van de Jeugdwet naar gemeenten.

Het ontstaan en de communicatie van dit datalek is 9 augustus 2017 geëvalueerd met interne betrokkenen.

Stijging van het aantal incidenten en datalekken.
Enkele voorbeelden van veiligheidsincidenten zijn: de ongecontroleerde en spontane verzending van e-mail waarvoor e-mailboxen moesten worden geopend en het tonen van gegevens van personeelsleden aan alle gebruikers binnen Youforce. Sinds 2016 wordt op gestandaardiseerde wijze bijgehouden welke datalekken, incidenten en dreigingen zich hebben voorgedaan. Figuur 1 hieronder illustreert onze ervaringen. Uit de cijfers vallen meteen twee verschijnselen op: het aantal geregistreerde meldingen is gestegen maar de onderlinge verhouding tussen cybercrime en overige oorzaken is ongeveer gelijk gebleven. Het valt ook op dat de stijging van het aantal "overige oorzaken" veel groter is dan cybercrime. Wat is de verklaring van deze stijging? Ons vermoeden is dat de hoofdoorzaak een groter bewustzijn van de medewerkers is, waardoor zij eerder een verschijnsel niet vertrouwen en dan ook melden. Dit vermoeden wordt ondersteund door de lichtere stijging van cybercrime. Onlangs heeft de Informatiebeveiligingsdienst (IBD) het "*Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten*" gepubliceerd. Wat daarin staat is onverkort van belang voor onze gemeente.

Figuur 1. Incidenten en datalekken	2016		2017	
Categorie	**Aantal**	**%**	**Aantal**	**%**
Cybercrime	**19**	**39**	**22**	**35**
Overige oorzaken	**30**	**61**	**41**	**65**
Eindtotaal	49	100	63	100

Waardoor en waar doet het zich voor? Binnen? Buiten?
Waar gaat het eigenlijk over; wat is de wereld achter de cijfers? Dat laat het volgende figuur 2 zien. Per rij staat een uitsplitsing van de categorie oorzaken. De kolommen geven aan waar de voorvallen zich hebben voorgedaan. "*Elders*" wil zeggen buiten de verantwoordelijkheid van onze gemeente, "*externe hosting*" gaat over uitbestede werkzaamheden onder onze verantwoordelijkheid en "*Intern*" wil zeggen: volledig in eigen beheer. De term "*Hybride hosting*" duidt op de combinatie van deels uitbesteding en deels eigen beheer. Ter vergelijking zijn weer de totaalcijfers over 2016 toegevoegd. De belangrijkste conclusie is wel dat ongeacht de categorie (cybercrime of overig oorzaken) onze gemeente op verschillende borden moet schaken: zowel in eigen huis beheer in de hand houden als buiten de deur allerlei externe partijen in de gaten houden.

Figuur 2. Oorzaken van datalekken, dreigingen en incidenten.	2016 Totaal	Plaats van de hosting en/of het beheer in 2017					
		Elders; geen impact	Elders; wel impact	Externe hosting	Hybride hosting	Intern	Totaal
Cybercrime	**19**	**4**	**2**	**7**	**5**	**4**	**22**
Beschikbaarheid	1						
Fraude						1	1
Inbraak (poging tot)	12	3		3	3	1	10
Informatiebeveiliging	2						
Kwalijke inhoud			2	4			6
Malware		1				1	2
Verzamelen van informatie	4				2	1	3
Overige oorzaken	**30**	**2**	**2**	**6**	**4**	**27**	**41**
Overige					1	1	2
Softwarefouten	1	1		4	1	3	9
Stroomstoring	1					2	2
Systeeminrichting	19	1		1	1	2	5
Systeemstoring	2		1			9	10
Verkeerd gebruik	7		1	1	1	10	13
Eindtotaal	**49**	**6**	**4**	**13**	**9**	**31**	**63**

Wat zijn onze kwetsbaarheden?
Naast de oorzaken is het ook van belang te weten wat onze kwetsbaarheden zijn. Dat toont het volgende figuur 3 waarin de onderdelen van de informatievoorziening ook zijn uitgesplitst naar de betreffende gemeente.

Figuur 3. Kwetsbaarheden	2016 Totaal	Uitsplitsing per gemeente 2017			
		Beide	Beemster	Purmerend	Totaal
Applicaties	3	5	3	4	12
Elders	5	5		1	6
Email	6	1		1	2
Gebruikers	6			14	14
Imago gemeenten		1			1
IT-infrastructuur	12	9		4	13
Internet + email	6				
Leveranciers	4	1			1
Mobiel apparaat	3				
SMS				1	1
Social media				2	2
Stroomvoorziening	1	1			1
Website	3	3		7	10
Eindtotaal	49	26	3	34	63

Datalekken in het bijzonder
Tot slot zoomen we in op datalekken (incidenten waarbij persoonsgegevens onder ogen van onbevoegden zijn gekomen). Voor het categoriseren van de gemelde datalekken gebruiken we in figuur 4 de indeling die Autoriteit Persoonsgegevens pas in 2017 heeft ingevoerd. Conclusie hieruit is dat de meeste datalekken veroorzaakt worden door mensenwerk en niet door cybercrime.

Figuur 4.Categorieën datalekken	2016	Uitsplitsing per gemeente in 2017			
		Beide	Beemster	Purmerend	Totaal
Brief of postpakket met persoonsgegevens kwijtgeraakt of geopend retour ontvangen				2	2
Overig		2			2
Persoonsgegevens per ongeluk gepubliceerd				2	2
Persoonsgegevens van verkeerde klant getoond in klantportaal		1		1	2
Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger			1	5	6
Onbekend	4				
Eindtotaal	4	3	1	10	14

Hoe merkbaar voor de burgers, omgeving en medewerkers?
Alle incidenten en datalekken overziend blijft het de vraag wat de invloed daarvan is op de betrokkenen (burgers, medewerkers, maatschappelijke organisaties en bedrijven), ketenpartners en de eigen organisatie. Voor zover bekend hebben we geen tijd verloren door storingen. Daarnaast bestaan geen harde cijfers al blijkt uit media en eigen ervaring dat meer mensen zich zorgen maken over hun privacy dan vroeger. Het afhandelen van incidenten en datalekken kost echter veel tijd. Illustratief voor de impact van een datalek is dat de afhandelen en melden bij de Autoriteit Persoonsgegevens voor de ambtelijke organisatie uiteenloopt van vier tot meer dan honderdvijftig uur per geval.

3. Beleid, doelstellingen en afspraken

Het geldend GIBB dateert uit 2015 en was vastgesteld voor een periode van vier jaar. Daarin zijn de volgende doelstellingen vastgesteld voor de informatiebeveiliging:

Verantwoord	De verantwoording ligt bij de betrokken proces- & gegevenseigenaren. Zij maken keuzes over: - Risico's - Beveiligingsniveaus Zij zijn daarop aanspreekbaar.	Veiligheid	Bestaat uit: - Beschikbaarheid - Integriteit - Vertrouwelijkheid - Privacy
Omgevings-bewust	- Oog voor externe en interne kansen en dreigingen. - Afweging van de voordelen en de risico's. - Bepalen voor wie de informatie toegankelijk is.	Open	De primaire gerichtheid is: - Open - Transparant tenzij ....
Slim	- Gebruik van oplossingen die hun dienst bewezen hebben. - Leren van ervaringen van anderen en onszelf	Slank	Oplossingen die bijdragen aan: - Continuïteit - Efficiency - Flexibiliteit van de organisatie.

Figuur 5. Beeld van het informatiebeveiligingsbeleid in 2015.

Op basis van deze uitgangspunten zou tweejaarlijks een uitvoeringsplan worden vastgesteld door de Algemeen Directeur op basis van advies door het Tactisch Overleg Privacy en Informatieveiligheid. Als gevolg van de veranderingen in het management van de organisatie is er geen Uitvoeringsplan voor de periode 2017-2018 gekomen. Ook in het Tactisch Overleg dat bedoeld was om organisatie breed de Algemeen Directeur te adviseren over beleid is het zwaartepunt naar de operationele uitvoering van privacy en informatiebeveiliging verschoven. De doelstellingen voor 2017 waren dan ook verwoord in een document ("Vooruitblik 2017") dat vastgesteld is door het Tactisch overleg van november 2016. Omwille van de leesbaarheid zijn de voorgenomen activiteiten hieronder niet chronologisch maar thematisch gerangschikt:

Nr	Wat
1.	Informatielandschap in samenhang in beeld brengen: - Data ('kroonjuwelen') - Applicaties - Infrastructuur - Processen - Ketenpartners, leveranciers, bewerkers.
2.	Bewustwording a. Privacycampagne b. Phishingmail test c. e-learning phishingmail d. Alert Online: Veiligheidsbewustzijn
3.	Testen van de IT en veiligheid in het gebouw:

Nr	Wat
	a. Pentesten[1] op eigen IT b. Pentest op systemen rioolgemalen en verkeerslichten c. Pentest op extern gehoste systemen d. Fysiek binnendringen in gebouwen door een mystery guest
4.	Verantwoording: a. Keuze voor een ISMS. Bij voorkeur een combinatie met "privacyboekhouding" b. Invoering normen en beveiligingsmaatregelen in een ISMS; voorbereiding op ENSIA c. Selfassessment o.b.v. BIG ivm ENSIA
5.	Opstellen nieuwe PDCA-planning voor 2 jaar

Hieronder volgt een verantwoording in hoeverre die plan is gerealiseerd.

4. Algemeen beeld en resultaten afgelopen periode

In het algemeen gesteld: het jaar 2017 is héél anders gelopen dan voorzien was. Daar zijn verschillende oorzaken voor: aan het begin van het jaar werd het Tactisch Overleg versterkt door twee nieuwe leden: de directeur Bedrijfsvoering en de nieuwe concerncontroller. Op hun verzoek is veel energie gestoken in het opstellen van een inventarisatie van de risico's van de gemeente: de Risicokaart 2017 (zie § 5 hieronder). Daarnaast zijn er heel veel datalekken en incidenten informatieveiligheid geweest (zie § 2). In de derde plaats heeft het ENSIA-traject veel energie gekost. Wat is er dan wel gerealiseerd van de voorgenomen activiteiten? Onderstaande opsomming geeft daarvan een beeld:

- Het **informatielandschap** en de onderlinge relaties tussen de verschillende componenten (gegevens, applicaties, processen en IT-systemen) is nog niet in kaart gebracht. Wel is er met het oog op de verplichtingen vanuit de AVG een start gemaakt met het inventariseren van verwerkingen van persoonsgegevens.
- Er is heel veel energie gestoken in de **bewustmaking** van medewerkers van het belang van het veilig omgaan met persoonsgegevens. Gelijktijdig met de open dagen van het stadhuis Purmerend (8 en 9 september) is de Mirror Room aanwezig geweest. Hierin konden bezoekers ervaren wat er zo al gedaan kan worden met hun persoonsgegevens. Kort daarna is een presentatie gegeven door Maurits Martijn over "*Ik heb wel iets te verbergen*". Aansluitend daarop is de e-learning "*Omgaan met persoonsgegevens*" **beschikbaar gesteld aan alle gebruikers van het netwerk. De** deelname daaraan was gemeentebreed ongeveer net zo groot als aan de e-elearning phishingmail uit 2016: circa 30 %. Opgemerkt moet worden dat de deelname per team uiteenliep van 10 tot 90 %. Omdat deze beide activiteiten in het najaar plaatsvonden is er niet meegedaan aan de landelijke campagne Alert online.
- Er zijn dit jaar twee **pentesten** uitgevoerd: een op onze computers waarmee de verkeerslichten en rioolgemalen door externe leveranciers worden beheerd. Daarna een algemene test van onze eigen IT-infrastructuur. Uit deze test zijn verscheidene punten ter verbetering gekomen. Niet alle daarvan konden gerealiseerd worden. Het belangrijkste obstakel daarvoor is de afhankelijkheid van applicatieleveranciers. Niet alleen hun producten maar ook hun installatiewerkzaamheden voldoen niet altijd aan geldende standaards. Dit heeft mede aanleiding gegeven tot het opstarten van gesprekken met deze leveranciers. De pentest van het informatiesysteem van de Purmaryn is niet doorgegaan omdat er vroeger dan verwacht is besloten tot invoering van een nieuw systeem en leverancier. De geplande test van de gemeentelijke

[1] Pentest = penetratietest door ethisch hackers.

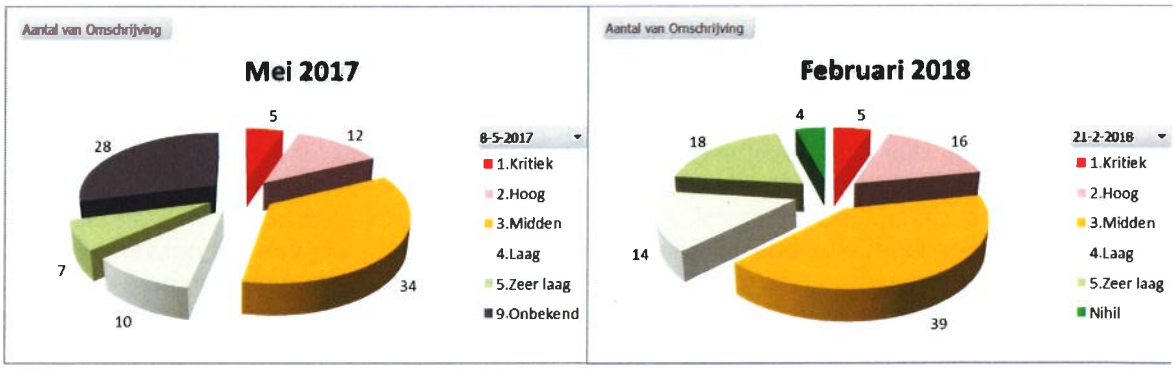
websites is opgeschoven naar en uitgevoerd in januari 2018. De test met de mysteryguest om het fysieke binnendringen uit te proberen is nog niet geweest.

- In dit jaar is nog niet gekozen voor de invoering van een ISMS (= Information Security Management System). Daar zijn verschillende redenen voor. Met het oog op de in werking treding van de AVG (Algemene Verordening Gegevensbescherming) leeft de voorkeur om een informatiesysteem in te voeren dat zowel inzetbaar is voor informatiebeveiliging als voor de eisen vanuit de AVG. Hoewel er nogal veel nieuw aanbod is in de markt hebben we nog niet een product gezien dat volledig voldoet aan onze eisen en wensen. Daarboven geldt dat de invoering van ENSIA (de nieuwe verantwoordingsmethodiek voor informatiebeveiliging) heel veel tijd heeft gekost. Maar onze gemeente heeft wel binnen de gestelde termijnen voldaan aan het inleveren van alle gegevens van het selfassessment: 1 oktober voor Basisregistratie Personen en voor 31 december Baseline Informatiebeveiliging Gemeenten.
- De nieuwe planning voor informatiebeveiliging is nog niet gereed. Het is ook logischer om deze op te stellen aan de hand van de resultaten van het assessment.

5. Beheersmaatregelen privacy en informatieveiligheid

Het bovenstaande overzicht geeft (gelukkig) geen volledig beeld van de werkzaamheden om de privacy en informatieveiligheid op een hoger peil te brengen. Er zijn namelijk heel wat meer activiteiten uitgevoerd. In het volgende overzicht bespreken we deze maatregelen vanuit een aantal thema's.

- **Risicokaart 2017**: vanaf begin van het jaar is een inventarisatie gemaakt van risicovolle situaties en objecten. Hierover heeft het college in oktober een besluit genomen om de topprioriteiten aan te pakken. Door tijdgebrek (ENSIA-traject en aanpak van incidenten en datalekken) zijn daar nog geen grote acties opgevolgd. Wel zijn er in de loop van het jaar meer risico's geïdentificeerd. De verbeteringen zoals getoond in figuur 6 rechts zijn vooral het gevolg van het treffen van technische maatregelen die zijn gesignaleerd door de uitgevoerde pentesten.



Figuur 6. De risico-ontwikkeling bezien vanuit de Risicokaart 2017.

- **Voorbereiding op de Algemene Verordening Gegevensbescherming**: op 25 mei 2018 moeten alle organisaties die persoonsgegevens verwerken aan deze Europese verordening voldoen. In het verslagjaar heeft de voorbereiding zich vooral gericht op drie activiteiten. In de eerste plaats het creëren van de functie van Functionaris Gegevensbescherming. Met allerlei gremia is daarover overleg geweest. Een extern juridische deskundige heeft het college uitleg gegeven over de AVG en met de OR is uitvoerig overleg geweest over deze nieuwe functie. Resultaat is dat de werving begin 2018 is gestart. De tweede hoofdactiviteit is het aangaan van verwerkersovereenkomsten met organisaties die in opdracht van de gemeente persoonsgegevens verwerken. Dit is tijdrovende taak omdat veel verwerkers niet

bekend zijn en/of moeite hebben met de wettelijke verplichtingen die voor hen gelden. De derde activiteit is het opstellen van een register van verwerkingen. Dit is een overzicht van alle verzamelingen waarin de gemeente persoonsgegevens verwerkt. Hiervoor is een start gemaakt met een inventarisatie bij alle teams.

- **Lerende organisatie:** onder deze noemer vatten we alle activiteiten die gericht zijn op het omgaan met datalekken, incidenten en dreigingen. Het jaar 2017 was met al zijn wisselvalligheden ook een enorme leerschool. Naar aanleiding van het bovengenoemde datalek dat Het Parool heeft gehaald is het proces rondom het melden van datalekken geëvalueerd. Daarnaast is het proces afhandelen van informatiebeveiligingsincidenten opnieuw besproken. De grootste verandering daaraan is tweeërlei: meer aandacht voor een bewuste inschatting van de veiligheidsrisico's en het formeren van een "Computer Security Incident Response Team"(= CSIRT) waarvan de leden tevens Vertrouwenscontactpersonen voor de Informatiebeveiligingsdienst (IBD) zijn. Tot slot is van belang te melden dat enkele collega's een training "Incidentmanagement" van de IBD hebben gevolgd.
- **Technische maatregelen:** op allerlei vlak zijn deze getroffen. Een belangrijke bron daarvoor zijn de hiervoor genoemde pentesten. Onderstaand figuur 7 laat de voortgang in de aanpak van de kwetsbaarheden zien. Vaak is het onmogelijk om alle kwetsbaarheden meteen op te lossen, omdat we nog niet afscheid kunnen nemen van verouderde systemen.

Figuur 7. Resultaten Penetratietest IT-infrastructuur

Risico categorie	Nog niet aangepakt	Gereed	Deels gereed	Geaccepteerd Risico	Ingepland	Eind-totaal
1. Kritiek						0
2. Hoog		1	4		2	7
3. Midden	3	3	5	1	1	13
4. Laag	1	1	1			3
5. Informatief		1				1
Eindtotaal	**4**	**6**	**10**	**1**	**3**	**24**

Een andere belangrijke aanleiding is de zogeheten Faalkaart waarop gemeentelijke websites staan vermeld (zie: www.faalkaart.nl) . Hoewel niet direct zichtbaar zijn er bij de meeste gemeentelijke sites veel verbeteringen doorgevoerd. Hierboven is al aangegeven dat de gemeente erg afhankelijk is van de medewerking van haar IT-leveranciers. In november is een start gemaakt met periodiek gesprek daarover met de grootste leverancier. Een punt van aanhoudende zorg is het onveilig e-mailverkeer (vooral in het sociaal domein). De gemeente zet daarvoor Sharefile is. Het probleem van deze tool en zijn concurrenten is dan lang niet alle ontvangers daarmee kunnen, willen en/of mogen werken. Vanuit de IBD en het NCSC (Nationaal Cybersecurity center) wordt gepropageerd dat men zich gaat houden veiligheidsstandaards (zie: www.internet.nl) Onze gemeente voldoet inmiddels aan bijna alle standaards voor veilig e-mailen.

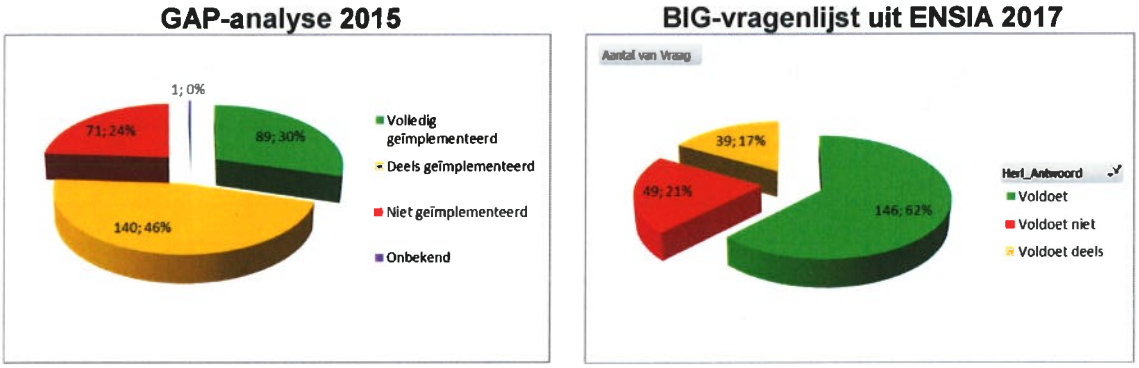
- **Samenwerking:** ook op het gebied van bescherming persoonsgegevens en informatieveiligheid zoeken we de samenwerking. Dat doet onze gemeente door een actieve rol spelen in de regio en daarnaast door gebruik te maken van de middelen die in het verband van de IBD worden beschikbaar gesteld. Een goed voorbeeld is de deelname aan het ENSIA-traject.

6. Disclaimer

Veiligheid is een toestand die nooit voor 100% gerealiseerd wordt. Alle inspanningen ten spijt blijft de kans aanwezig dat een kwaadwillend iemand binnendringt. Een nog groter risico is dat iemand in alle onschuld een vergissing maakt waardoor gevoelige gegevens in verkeerde handen komen. Het doel van privacybescherming en informatiebeveiliging is en blijft het verkleinen van de kansen daarop.

7. Realisatie doelstellingen IB-beleid (effectiviteit beheersmaatregelen en risico's)

In 2013 hebben de gemeenten in VNG-verband afgesproken informatieveiligheid via zelfregulering tot stand te brengen. Daarbij is afgesproken dat de Baseline Informatiebeveiliging als referentiekader zou dienen en met ingang van het jaar 2017 zou daarop een jaarlijks assessment worden uitgevoerd. In 2015 hebben we een zogeheten GAP-analyse uitgevoerd op de BIG. De resultaten daaruit hebben we in figuur 8 vergeleken met de zelfevaluatie op basis van de ENSIA-vragenlijst. Hierbij moet de opmerking worden gemaakt dat het aantal vragen van beide analyses verschilt. Om die reden geven we hier aantal gevolgd door percentage.



Figuur 8. Vergelijking GAP-analyse 2015 met ENSIA 2017

Betekent dit dat we er slecht voor staan? Geenzins. Allereerst hebben we beter in beeld waar de risico's zitten en wat er aan gedaan moet worden. In de tweede plaats hebben we onze ervaringen met datalekken en incidenten. Zoals het er nu voor staat hebben we indruk dat we niet geraakt zijn door grotere en kleinere dreigingen van buiten af. Wat echter veel duidelijker is geworden dat zijn onze eigen zwakke plekken. Die zitten in de eigen gemeente (mensen, organisatie en techniek) maar zeker ook bij externe partijen (leveranciers en verwerkers) waar we van afhankelijk zijn.

8. Meerjarenperspectief

De komende jaren moeten we rekening blijven houden met de interne zwaktes en externe dreigingen. Kort voor het verschijnen van dit verslag heeft de IBD het zogeheten "*Dreigingsbeeld informatiebeveiliging Nederlandse Gemeenten 2018*" uitgebracht. Dit dreigingsbeeld is zonder meer van toepassing op onze gemeenten.

De Baseline Informatiebeveiliging Gemeenten (en andere normenkaders zoals de Algemene Verordening Gegevensbescherming) bieden voldoende aanknopingspunten om het perspectief voor de komende jaren te duiden. Dat is simpelweg: het realiseren van alle maatregelen die nu nog niet tot uitvoering zijn gekomen.. Daarnaast is het noodzakelijk er voor te zorgen dat we straks blijven voldoen aan de normen waar we nu al aan voldoen. Apart van dit jaarverslag is een verbeterplan voor het jaar 2018 opgesteld: het Informatiebeveiligingsplan 2018. Daarin staan de prioriteiten voor het lopend jaar. Door uitvoering van de volgende ENSIA-ronde (2018) weten we hoever we zijn gekomen en welke nieuwe prioriteiten we moeten stellen.