GEMEENTE BEEMSTER
WERELDERFGOED

INGEKOMEN 18 MAART 2019

Team Beleid en Projecten

Gemeenteraad van Beemster

uw brief van	*uw kenmerk*	*ons kenmerk*	*datum*
		043938724	12 maart 2019

onderwerp
Jaarverslag privacy en informatieveiligheid 2018

Geachte heer, mevrouw ,

In 2018 heeft de invoering van de Algemene Verordening Gegevensbescherming (AVG) - bijgedragen aan een grotere belangstelling voor zowel de bescherming van de persoonsgegevens als het onderwerp informatiebeveiliging. Informatiebeveiliging gaat over het waarborgen van de beschikbaarheid, integriteit (= betrouwbaarheid) en vertrouwelijkheid van alle soorten gegevens. Gezien de grote onderlinge verwevenheid ontvangt u van het college één rapportage over beide onderwerpen.

Hoe staan we ervoor?
Sinds 2017 maken alle gemeenten de balans op hoe het staat met hun informatieveiligheid. Dat doen zij door middel van de Eenduidige Normatiek Single Information Audit (ENSIA). Door vergelijking van de resultaten van 2017 met 2018 kunnen we zien dat er vooruitgang is geboekt. Het volgende figuur laat dat zien op basis van aantal vragen en percentages:

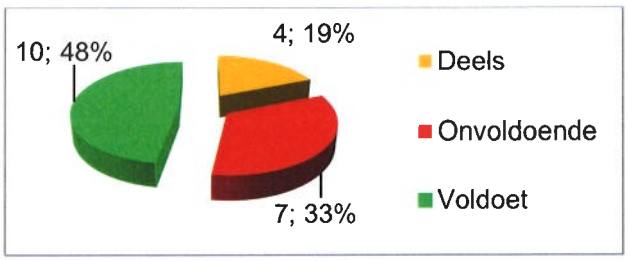
Aangezien de resultaten uit ENSIA niet openbaar worden gemaakt, is het onmogelijk om een vergelijking te maken met andere gemeenten. Wel is over informatieveiligheid vergelijkingsmateriaal over gemeenten beschikbaar op:
https://www.waarstaatjegemeente.nl/dashboard/Dienstverlening-en-digitalisering/
(Merk op: momenteel zijn de gegevens over 2018 nog niet gepubliceerd)

bijlage(n): Geen

behandeld door:	telefoonnummer
H. Winkel	0299-452514

Postadres: Postbus 7, 1462 ZG Middenbeemster
Telefoon: 0299 452 452
Website: www.beemster.net

In ENSIA 2018 zijn voor het eerst specifieke vragen opgenomen over de invoering van de AVG. De volgend figuur laat zien hoe "AVG-proof" wij zijn. Ook hier worden weer aantallen en percentages genoemd.



Wat deed zich voor in onze omgeving?
In de afgelopen paar jaar werd privacy vooral in verband gebracht met datalekken. Dit zijn informatiebeveiligingsincidenten waarin persoonsgegevens worden gelekt. Ook onze gemeente ontkomt daar niet aan. Sinds 2016 houden we alle incidenten nauwlettend in de gaten. Onderstaande overzichten geven daarvan een beeld voor de samenwerkende gemeenten Beemster en Purmerend. Allereerst valt de afname van het aantal geregistreerde incidenten op waarmee we afwijken van de landelijke stijging van het aantal gemelde datalekken zoals door de Autoriteit Persoonsgegevens wordt gesignaleerd. (Bron: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-ontvangt-bijna-21000-datalekken-2018)

Tabel 1. Op welke gemeente hadden de incidenten betrekking?	**2016**	**2017**	**2018**	**Totaal**
Beide gemeenten samen	37	26	25	88
Specifiek Beemster		3	1	4
Specifiek Purmerend	12	34	28	74
Eindtotaal	**49**	**63**	**54**	**166**

Als we inzoomen op de datalekken zien we dat de meeste veroorzaakt worden door menselijk handelen.

Tabel 2. Informatieveiligheidsincidenten	**2016**	**2017**	**2018**	**Totaal**
Datalekken	**12**	**22**	**20**	**54**
• Brief of postpakket met persoonsgegevens kwijtgeraakt of geopend retour ontvangen		3		3
• Hacking, malware e/of phishing	1		1	2
• Overig	3	4	1	8
• Persoonsgegevens bij oud papier gezet			1	1
• Persoonsgegevens nog aanwezig op afgedankt apparaat.	2			2
• Persoonsgegevens per ongeluk gepubliceerd	5	3	10	18
• Persoonsgegevens van verkeerde klant getoond in klantportaal		2	2	4
• Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger	1	10	5	16
Geen datalek: *overige incidenten*	**37**	**41**	**34**	**112**
Eindtotaal	**49**	**63**	**54**	**166**

Naast de datalekken is cybercrime een onderwerp dat in 2018 veel ter sprake kwam. In de volgende tabel maken we voor alle incidenten (waaronder de datalekken) een onderscheid tussen cybercrime en overige problemen.

Tabel 3. Aandeel cybercrime in alle incidenten	**2016**	**2017**	**2018**	**Totaal**
Cybercrime	**19**	**22**	**16**	**57**
1. Beschikbaarheid	**1**			**1**
2. Fraude		**1**	**3**	**4**
3. Inbraak (poging tot)	**12**	**10**	**4**	**26**
4. Informatiebeveiliging	**2**		**1**	**3**
5. Kwalijke inhoud (bijv. dreigmail)		**6**	**2**	**8**
6. Malware		**2**	**3**	**5**
7. Verzamelen van informatie	**4**	**3**	**3**	**10**
Niet-cybercrime	**30**	**41**	**38**	**109**
8. Overige		**2**	**5**	**7**
9. Softwarefouten	**1**	**9**	**3**	**13**
10. Stroomstoring	**1**	**2**	**1**	**4**
11. Systeeminrichting	**19**	**5**	**7**	**31**
12. Systeemstoring	**2**	**10**	**5**	**17**
13. Verkeerd gebruik	**7**	**13**	**17**	**37**
Eindtotaal	**49**	**63**	**54**	**166**

Het aandeel meldingen dat te bestempelen is als cybercrime is dus aanzienlijk kleiner dan het aantal overige incidenten. Opvallend is dat de meeste overige incidenten te maken hebben met menselijk gedrag of fouten. Gelukkig is de schade die we in 2018 geleden hebben door al deze incidenten gering te noemen.

Wat hebben we er aan gedaan?
De mens is dus de zwakste schakel. Regelmatig laten we daarom het bewustzijn van onze medewerkers m.b.t. informatieveiligheid en de techniek testen door externe partijen. Op grond van de uitkomst van de technische test van 2017 hebben zo'n 60 ICT-collega's en andere belangstellenden een workshop Cybersecurity gedaan om te leren denken als een hacker. In het najaar van 2018 heeft een derde deel van de medewerkers een phishingmail gekregen om hun wachtwoorden te ontfutselen. De resultaten daarvan en het bezoek van mystery guests aan drie gebouwen laten zien dat er nog heel wat gedaan moet worden om het veiligheidsbewustzijn te verhogen. Ook bleek uit die tests dat hackers gemakkelijk zouden kunnen binnendringen door misbruik te maken van de zwakheden van de gebruikers.

Eind van het jaar is de aanbesteding afgerond om het IT-netwerk te voorzien van nieuwere apparatuur die het indringers veel lastiger maakt om binnen te komen. Steeds vaker starten ICT-projecten voor nieuwe applicaties met een analyse van de veiligheidsrisico's om te bepalen welke veiligheidsmaatregelen nodig zijn. Veel energie is gaan zitten in het sluiten van passende overeenkomsten met leveranciers. Daarbij maken we gebruik van de Gemeentelijke Inkoopvoorwaarden Bij IT-overeenkomsten. Als er sprake is van de verwerking van persoonsgegevens bij dienstverleners dan zijn we ook verplicht om zogeheten verwerkersovereenkomsten te sluiten. Zowel bij ons als in den lande blijkt dit een lastig proces te zijn.

Wat is het vooruitzicht voor 2019?
Informatieveiligheid is en blijft een uitdaging voor onze gemeente. Gelukkig weten overheden elkaar op dat terrein steeds meer te vinden. Met ingang van dit jaar geldt voor de gehele overheid nog maar één normenkader: de Baseline Informatiebeveiliging Overheid (BIO). Dit bevordert de samenwerking in de digitale ketens. Eén van de belangrijkste onderdelen daaruit is dat alle overheden verplicht zijn om voor elk informatiesysteem vast te leggen welk Basisbeveiligingsniveau van toepassing is. In het vernieuwde Gemeentelijk Informatiebeveiligingsbeleid 2019-2021 hebben we de ambitie uitgesproken om de gehele BIO voor eind 2021 ingevoerd te hebben. Een van de kernpunten daarin is dat we voor alle informatiesystemen het Basisbeveiligingsniveau hebben bepaald. In dit proces spelen de lijnmanagers in hun rol van intern gegevenseigenaar een cruciale rol omdat zij het gewenste niveau vast stellen. Dat vraagt om toepassing van het veiligheidsdenken in de concrete werkprocessen. Hopelijk draagt dat ertoe bij dat de dalende tendens in het aantal informatiebeveiligingsincidenten en datalekken zich doorzet.

Hoogachtend,
burgemeester en wethouders van Beemster.

A.J.M. van Beek
burgemeester

b.a. AG Dehé

H.C.P. van Duivenvoorde
gemeentesecretaris