GEMEENTE BEEMSTER
WERELDERFGOED

INGEKOMEN 2 2 MEI 2017

Team Beleid en Projecten

Gemeenteraad van Beemster

uw brief van	*uw kenmerk*	*ons kenmerk*	*datum*
		1372344	15 mei 2017

onderwerp
Tweede halfjaarrapportage informatieveiligheid en privacy 2016

Geachte leden van de Raad,

Zoals eerder met u afgesproken bieden wij u hierbij de tweede halfjaarrapportage informatieveiligheid en privacy 2016 aan. In het kort noemen wij u daaruit de bevindingen:

1. De aandacht vanuit de buitenwereld voor onze informatiehuishouding neemt toe.
2. Het bewustzijn over informatieveiligheid en privacybescherming is groeiende.
3. In 2016 hebben we te maken gehad met 49 geregistreerde veiligheidsincidenten.
4. Van deze 49 incidenten zijn er 19 aan te merken als 'cybercrime'
5. In 30 van de 49 gevallen ging het om situaties waarin we in meer of mindere mate afhankelijk zijn van leveranciers of ketenpartners.
6. Veel van de incidenten zijn een gevolg van inrichting van systemen (19 van de 49).
7. Eveneens 19 van deze incidenten hebben betrekking op het werken met persoonsgegevens. Daarvan zijn er vier als datalek gemeld bij de Autoriteit Persoonsgegevens.

De komende tijd staan verschillend activiteiten op het programma. De belangrijkste daaruit zijn: de voorbereiding op het in werking treden van de Algemene Verordening Gegevensbescherming (AVG) en de invoering van de Eenduidige Normatiek Single Information Auidit (Ensia). Over dit laatste onderwerp zullen wij u binnenkort uitgebreider informeren.

Hoogachtend,
burgemeester en wethouders van Beemster.

A.J.M. van Beek
burgemeester

H.C.P. van Duivenvoorde
Gemeentesecretaris

bijlage(n): een

behandeld door:
H. Winkel

telefoonnummer
0299-452514

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

Bijlage. Tweede halfjaarrapportage Informatieveiligheid en privacy 2016

Bijlage. Tweede halfjaarrapportage Informatieveiligheid en privacy 2016

1. Inleiding

Met de Raad is afgesproken dat zij elk halfjaar een rapportage krijgt over de staat informatiebeveiliging en privacybescherming. De onderstaande casus is daar een treffende illustratie van.

Op 2 december 2016 bereikte ons de mededeling dat er was ingebroken op een router van Purmerend. Dit apparaat regelt de verbindingen tussen de gemeentelijke ICT en "het internet". Daarvan zijn er verschillende in gebruik. Het apparaat is meegenomen voor forensisch onderzoek en vervangen door een ander exemplaar. Hieruit bleek dat allerlei instellingen waren gewijzigd en ook dat er sporen waren aangetroffen die wezen op illegale activiteiten vanuit Rusland, India en Brazilië. Deze digitale voetsporen zijn gebruikt voor nader onderzoek op onze firewall. Daaruit is geconstateerd dat er mislukte pogingen zijn gedaan om verbindingen op te zetten.
Op advies van deze provider is meteen een melding gedaan bij de Autoriteit Persoonsgegevens. Aangezien daarna geen sporen zijn aangetroffen van een daadwerkelijke inbraak op de gemeentelijke systemen is de melding weer ingetrokken. De indruk op basis van de aangerichte schade in de router is dat het hier niet gaat om een gerichte aanval maar om een willekeurige poging om zoek naar zwakke plekken.

2. Bevindingen

Onze bevindingen komen voort uit allerlei bronnen. Externe meldingen van bijvoorbeeld de Informatiebeveiligingsdient (IBD), externe en interne netwerken en ervaringen opgedaan met incidenten. Daarop zijn de volgende bevindingen gebaseerd.

1. De **aandacht vanuit de buitenwereld** voor onze informatiehuishouding is groeiende. Deze aandacht komt van verschillende kanten:
    a. Kwaadwillenden pogen binnen te komen. Hun motieven zijn niet zozeer interessant, de effecten daarentegen wel. De belangrijkste risico's zijn dat persoonsgegevens worden gelekt en/of dat de bedrijfsprocessen worden verstoord. Een uur stilstand kost al gauw zo'n € 30.000 aan salariskosten.
    b. Rijksoverheid en de Autoriteit Persoonsgegevens verlangen van ons dat de informatiebeveiliging en privacybescherming aantoonbaar op orde is.
    c. Media hebben deze thema's ontdekt en houden nauwlettend de prestaties van gemeenten in de gaten.
    d. Steeds vaker uiten burgers hun bezorgdheid over de privacybescherming waardoor het vertrouwen in de overheid afneemt.
2. Het **bewustzijn** bij medewerkers, collegeleden en raadsleden hierover is groeiende. Er wordt vaker gesproken over deze thema's en zorgen worden geuit. Toch is er nog steeds een grote groep medewerkers die zich hieraan onttrekt.
3. In heel 2016 zijn 49 veiligheidsincidenten geregistreerd. Onderstaande tabel geeft daarvan een analyse.

	Waar?					
Incidenten	**Elders[1]; geen impact**	**Elders; wel impact**	**Externe hosting[2]**	**Hybride hosting[3]**	**Intern[4]**	**Eind totaal**
Beschikbaarheid (DDos aanval[5], sabotage)		1				1
Inbraak (poging tot)	1	2	2	3	4	12
Informatiebeveiliging (misbruik van kwetsbaarheid, inlogpogingen)	1				1	2
Verzamelen van informatie (Phishing)		1		2	1	4
Subtotaal Cybercriminaliteit	**2**	**4**	**2**	**5**	**6**	**19**
Softwarefouten					1	1
Stroomstoring					1	1
Systeeminrichting		3	4	5	7	19
Systeemstoring					2	2
Verkeerd gebruik		1	2	2	2	7
Subtotaal Overige incidenten	**0**	**4**	**6**	**7**	**13**	**30**
Eindtotaal	**2**	**8**	**8**	**12**	**19**	**49**

4. Deze zijn grofweg in te delen naar ***cybercrime*** (oorzaken van misdadige aard zoals de casus hierboven) en ***overige oorzaken*** (variërend van stroomstoringen tot menselijke fouten). Het grootste aantal incidenten (30 van de 49) zit in de categorie van overige oorzaken. Deze aantallen zeggen nog niet zoveel over de kans op daadwerkelijke verstoringen en de omvang van de schade. In deze casus bleef de schade beperkt tot uren werk voor ICT. Indien de beveiliging niet op orde was geweest dan was de schade heel groot geweest.
5. Het valt op dat 30 van de 49 incidenten geheel of gedeeltelijk betrekking heeft op situaties waarbij onze organisatie ***afhankelijk*** is van de digitale ketens met ***leveranciers en/of ketenpartners***. In 20 van deze situaties is onze organisatie wel degelijk verantwoordelijk. Dit betekent dat onze aandacht moet uitgaan naar informatieveiligheid en privacybescherming binnen onze eigen organisatie maar ook naar al die organisaties die onder onze verantwoordelijkheid gegevens verwerken en bewerken.
6. Bezien naar de oorzaak van de incidenten gaat het veelal om ***fouten in de inrichting van systemen***. Dus niet om fouten van apparaten of programmeerfouten, maar om menselijk falen. Denk bijvoorbeeld aan ontoereikende instellingen om de privacy te beschermen, aan het niet tijdig plaatsen van nieuwe versies van software of aan applicaties van leveranciers die niet tijdig hun producten aanpassen aan de geldende veiligheidseisen waardoor wij genoodzaakt zijn om verouderde systemen in de lucht te houden. Om dit soort oorzaken te elimineren spelen de beheerders van onze technische systemen, applicaties en gegevens een essentiële rol.
7. Uit de analyse van de incidenten blijkt hoe vaak veiligheidsincidenten direct ook betrekking hebben op **persoonsgegevens** (19 van de 49). Deze incidenten zijn niet

---

[1] Elders: bij andere organisaties dus buiten de verantwoordelijkheid van onze organisatie.
[2] Externe hosting: bij andere organisaties maar wel onder onze verantwoordelijkheid (bijv. toepassingen die volledige in de cloud draaien.
[3] Hybride hosting: toepassingen onder onze verantwoordelijkheid die gedeeltelijk buiten de deur en gedeeltelijk bij ons draaien.
[4] Intern: toepassingen die volledig bij ons draaien.
[5] DDos aanval: een aanval waarbij gepoogd wordt van buitenaf een toepassing "plat" te leggen door een "bombardement" van signalen (bijv. e-mails).

zonder meer meldingsplichtig. In het tweede halfjaar 2016 is slechts één ernstig veiligheidsincident als dreigend datalek bij de Autoriteit Persoonsgegevens gemeld (de bovenstaande casus). Bij nadere analyse van de impact bleek dat er geen persoonsgegevens waren gelekt en kon de melding worden ingetrokken. Het aantal gemelde datalekken voor 2016 bleef daardoor staan op vier.

8. De organisatie is op gang gekomen met het uitvoeren van de huidige en toekomstige verplichtingen op het gebied van privacybescherming. Voldaan wordt aan het melden van datalekken maar zoals zoveel organisaties zijn we nog niet gereed voor de inwerkingtreding van de **Algemene verordening gegevensbescherming** (AVG) in mei 2018.

3. Wat hebben we er mee gedaan?

In dit halfjaar is uitvoering gegeven aan verschillende activiteiten:

- **Incidentmanagement** is verder ingericht. Naast een Meldpunt Datalekken bestaat er nu een Computer Incident Response Team dat coördinerend optreedt bij incidenten en de schakel vormt tussen onze organisatie en de Informatiebeveiligingsdiensten Gemeenten (IBD). Door betrokken medewerkers, het Meldpunt Datalekken en enkele anderen is een incidenttraining gehouden. De belangrijkste les hoe elkaar te vinden in het eerste uur na het optreden van het incident.
- We zijn enorm afhankelijk van **leveranciers en ketenpartners**. Dit noodzaakt tot het maken van goede afspraken. In VNG/KING verband is daarom meegewerkt aan de ontwikkeling van de Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT). Daarnaast is van groot belang dat de organisatie het IT-contractmanagement gaat oppakken. Verder zijn de (wettelijk verplichte!) bewerkersovereenkomsten van belang. Het sluiten daarvan gaat langzamer dan verwacht omdat verschillende leveranciers moeite hebben hun wettelijke aansprakelijkheid te accepteren. Hierbij zijn de diverse netwerken van gemeentelijke juristen, ICT-ers en beveiligingsfunctionarissen van groot belang om het gemeentelijk belang veilig te stellen.
- Vanuit de media is grote aandacht voor het **onveilig e-mailverkeer en onveilige websites** bij gemeenten. Inmiddels voldoen onze e-mailfaciliteiten aan alle geldende technische standaards. (Zie bijvoorbeeld: www.internet.nl) Daarnaast beschikken de gebruikers binnen ons netwerk over de mogelijkheid om e-mail versleuteld te versturen. In januari starten de instructies daarvoor. In dit halfjaar is gestart met de migratie van de hoofdwebsites naar een nieuwe vormgeving en naar nieuwe servers. Als deze operatie afgerond is (februari 2017) voldoen ook onze sites aan de geldende veiligheidsnormen.
- Aan de **interne ICT-infrastructuur** wordt voortdurend gewerkt om de veiligheid op peil te houden en te verbeteren. In het tweede halfjaar is het aantal systeembeheerders uitgebreid en daardoor is er meer tijd voor monitoring en het bijhouden van updates. In aanvulling daarop is eind 2016 opdracht gegeven tot de levering van een systeem dat in het bijzonder de beveiliging gaat regelen van de geautomatiseerde gegevensuitwisseling met de systemen van ketenpartners. Ook zijn de meeste problemen opgelost die bij de penetratietest in het voorjaar aan het licht waren gekomen.
- In de periode van 3 tot met 14 oktober heeft de gemeente meegedaan aan de landelijke **campagne Alert Online**. De nadruk lag er op wat mensen zelf kunnen doen aan hun digitale veiligheid. De reacties hierop waren uiteenlopend. Er kwamen veel positieve reacties op de tips ("ook handig voor jezelf") en er waren reacties dat men zich overladen voelde door de e-mailberichten. Voor het eerst is in deze campagne ook aandacht gegeven aan de burgers en bedrijven van onze gemeente door publicatie van campagnemateriaal in de gemeentelijke nieuwsbrieven en websites.
- Aansluitend op deze campagne is een digitale training in het **herkennen van phishingmail** aangeboden. Ook hierop waren de reacties zeer uiteenlopend: van zeer positief tot negatief. Uiteindelijk heeft 32% van de aangeschreven gebruikers er aan mee gedaan. Dit is een resultaat dat tot nadenken stemt.

4. Externe en interne beoordeling

In het tweede halfjaar zijn er verschillende onderzoeken naar de staat van onze beveiliging uitgevoerd. In chronologische volgorde:

- **Zelfevaluatie Basisregistratie Personen**. Het resultaat is "goed" conform de geldende normen. Ten aanzien van de gemeente Beemster staat er nog wel een actie open om documenten die te vroeg zijn overgedragen aan het Waterlands Archief terug te halen.
- **Zelfevaluatie Paspoorten en Nationale Identiteitskaarten**. Het resultaat is "goed" conform de geldende normen.
- **SUWINET**: in het eerste halfjaar bleek dat onze organisatie niet volledig voldeed aan de zeven gestelde normen. Hierop zijn maatregelen ter verbetering genomen en 20 oktober kwam het bericht binnen van het ministerie van Sociale Zaken en Werkgelegenheid dat daar nu wel aan wordt voldaan.
- **DigiD audit 2016**: in het najaar zijn twee nieuwe DigiD-aansluitingen bij het bedrijf GouwIT in gebruik genomen voor de afhandeling van bezwaren belastingen en heffingen. Binnen twee maanden na ingebruikname moet het assessment zijn doorlopen. Vlak voor kerst is dit afgerond. Inmiddels heeft Logius het rapport van de auditor goedgekeurd. In het eerste kwartaal van 2017 wordt het assessment van de twee oudere DigiD-aansluitingen bij een andere leverancier afgerond.

In 2016 is er geen verplichting geweest tot het uitvoeren van een **BAG-audit**. Ook de voorgenomen tweede **penetratietest** van onze IT-infrastructuur is niet uitgevoerd. Besloten is deze voortaan eenmaal per jaar uit te voeren. Wel zijn de voorbereidingen getroffen voor een pentest in begin 2017 op de systemen voor de rioolgemalen en verkeerslichten. Steeds meer niet-administratieve systemen staan in verbinding met het internet en zijn potentiele doelwitten van cybercriminelen.

5. Vooruitzichten 2017

Het prille begin van 2017 heeft laten zien dat de gesignaleerde trends zich voortzetten: problemen met verkiezingssystemen in verband met "statelijke" aandacht voor onze verkiezingen en een flinke stroomstoring in de regio.

- Begin 2017 starten we met een nieuwe inventarisatie en inschatting van onze risico's. De vorige dateerde uit 2015.
- Op basis van die afweging nemen we maatregelen of accepteren we onze risico's. Medio dit jaar treedt de Eenduidige Normatiek Single Information Audit (ENSIA) in werking die gebaseerd is op de Baseline Informatiebeveiliging Gemeenten. Dit is geen vrijblijvende zaak meer; voor de BIG geldt het principe "***pas toe of leg uit***".
- In mei 2018 zullen we moeten voldoen aan de AVG. Hier geldt het principe: van ***"tell me***" naar "***prove to me***" M.a.w.: we moeten richting burgers en de toezichthouder kunnen aantonen dat we persoonsgegevens verwerken in overeenstemming met de privacywetgeving. Om dit te realiseren zal o.a. in de loop van 2017 de verplichte Functionaris Gegevensbescherming benoemd moeten zijn. We kunnen het op tijd redden als we er nu aan werken.
- Het borgen van de informatieveiligheid en privacy zijn in de praktijk geen op zichzelf staande werkzaamheden maar cruciaal onderdeel van veel functies. De uitbreiding van het aantal systeembeheerders is een goede eerste stap. Andere sleutelfuncties om de kwetsbaarheden te verminderen zijn: functioneel beheerders, inkopers contractmanagers en gegevenseigenaren en -beheerders en projectleiders.
- Daar komt bovenop dat elke medewerker er mee te maken in zijn of haar werkzaamheden van alledag. De promotie van het privacy- en veiligheidsbewustzijn blijft belangrijk.