Gemeente Oudewater

RAADSINFORMATIEBRIEF Oudewater
18R.00785

Van : College van burgemeester en wethouders
Datum : 4 december 2018
Portefeuillehouder(s) : Wethouder W.J.P. Kok
Portefeuille(s) : Informatieveiligheid en privacy
Contactpersoon : S. Nicolasen
Tel.nr. : 8450
E-mailadres : nicolasen.s@woerden.nl

Onderwerp:

Jaarverslagen Informatieveiligheid en Privacy 2017

Kennisnemen van:

de jaarverslagen Informatieveiligheid en Privacy 2017.

Inleiding:

Met ingang van 2017 is de Eenduidige Normatiek Single Information Audit (ENSIA) ingevoerd. Op de uitgangspunten, inhoud en werking van ENSIA wordt in bijgaand Jaarverslag Informatieveiligheid nader ingegaan. Dat jaarverslag vloeit voort uit de systematiek van de ENSIA.
Met ingang van 25 mei 2018 is de Algemene Verordening Gegevensbescherming ingevoerd. In 2017 is de voorbereiding van deze Europese regelgeving ter hand genomen. Het Jaarverslag Privacy legt verslag van hetgeen in 2017 aan voorbereidingen daarop is gerealiseerd.

Kernboodschap:

De gemeente heeft conform de systematiek van de ENSIA over 2017 een zelfevaluatie informatiebeveiliging uitgevoerd onder meer gericht op beveiligingsnormen van de BRP, PUN, BAG, BGT, DigiD en Suwinet. Het college van B&W heeft over de informatiebeveiliging gerapporteerd aan de gemeenteraad in een paragraaf in het jaarverslag. Deze paragraaf bevat een verwijzing naar de zogenoemde Collegeverklaring ENSIA over een aantal geselecteerde beveiligingsnormen. Een IT -auditor heeft de Collegeverklaring gecontroleerd en een Assurancerapport opgesteld. Daaruit blijkt dat de gemeente aan de gestelde eisen op het gebied van informatieveiligheid heeft voldaan. Aan de raad is

toegezegd in een afzonderlijk "Jaarverslag Informatieveiligheid 2017" nadere informatie te verstrekken. In 2017 zijn de voorbereidingen op de invoering van de AVG gestart. De organisatie heeft de noodzakelijke stappen gezet om per 25 mei 2018 aan de aanvullende eisen, zoals een eigen verwerkingsregister en de verantwoordingsplicht (accountability) te voldoen. Het jaarverslag geeft daarover nadere informatie.

Financiën

n.v.t.

Vervolg:

In het vervolg zullen geen afzonderlijke jaarverslagen Informatieveiligheid en Privacy worden opgesteld, maar zal over deze onderwerpen in het algemene jaarverslag worden gerapporteerd.

Bijlagen:

Jaarverslag Informatieveiligheid 2017 (18i.05837)
Jaarverslag Privacy 2017 (18i.05836)
Assuranceverklaring (18.012823)

Het college van burgemeester en wethouders,

De wnd. secretaris

ir. W.J. Tempel

De burgemeester

mr. drs. P. Verhoeve

Gemeente Oudewater

gemeente WOERDEN

Jaarverslag Informatieveiligheid 2017

Inhoudsopgave

1 Doel van het document

Dit voortgangsrapport is een periodieke rapportage van de Chief Information Security Officer (CISO) en levert het bestuur informatie over de voortgang en status van de werkzaamheden en de (tussen)resultaten op het gebied van de informatieveiligheid. Nadat het bestuur over 2016 zeer gedetailleerd is geïnformeerd, is nu gekozen voor een rapportage op hoofdlijnen. Gelet op de openbaarheid van dit document, wordt uiteraard niet ingegaan op de gebruikte toepassingen om de veiligheid van de systemen te borgen.

2 Conclusie en samenvatting

Ten aanzien van 'Informatieveiligheid' zijn voor 2017 de volgende **doelen geformuleerd**:

- Voorbereiden ENSIA[1], waaronder begrepen:
  - Voorbereiding DigiD audit.
  - Actualisering handboek BRP.
  - Actualiseren handboek PNIK.
  - Actualiseren handboek SUWI.
  - Actualiseren Handboek BAG.
- Uitvoeren van de wettelijke controles.
- Actualiseren documentatie.
- Uitvoeren bewustzijnsactie onder het personeel.
- Ontwikkeling eigen software 'Cumulus'.
- Uitvoeren Vulnerability Assessment

De **conclusie** is, dat de organisatie de geformuleerde **doelstellingen** over 2017 **deels** heeft **gerealiseerd**. In de volgende paragrafen volgt een uitleg van de planning versus de realisatie en een planning voor hetgeen in 2018 dient te gebeuren.

Hoewel de informatieveiligheid in de praktijk niet in het geding is geweest, zijn niet alle doelstellingen gehaald. De raad heeft in 2016 budget beschikbaar gesteld om een Information Security Officer aan te trekken, met als opdracht zorg te dragen voor o.m. het opsporen van verdacht netwerkverkeer met behulp van een Netwerk Intrusion Detection Systeem (NIDS) en het actualiseren en optimaliseren van de procedures rond informatieveiligheid. In 2017 zijn gesprekken gevoerd met een reeks aan sollicitanten, maar het bleek niet mogelijk een geschikte kandidaat aan onze organisatie te binden. De sterk gegroeide behoefte van het bedrijfsleven aan ICT'ers met kennis op het gebied van information security was daar voor een belangrijk deel debet aan. Daarop is met ingang van 1 december 2017 tijdelijk (tot 1 december 2018) in de vacature voorzien door inhuur van een deskundige.

Ondanks deze tegenvaller heeft de organisatie wel in voldoende mate voldaan aan het normenkader van de Baseline Informatieveiligheid Gemeenten, zoals blijkt uit het door een onafhankelijke auditor afgegeven 'assurance-rapport' met betrekking tot de Collegeverklaring in het kader van de Eenduidige Normatiek Single Information Audit (ENSIA). De auditor toetst daarbij of de collegeverklaring een waarheidsgetrouw beeld geeft.

Hieruit mag echter niet de conclusie worden getrokken dat de documentatie op orde is gebracht. Bij de ENSIA-audit wordt door de auditor conform de richtlijnen gekeken naar opzet en bestaan van procedures[2]. De werking behoorde over 2017 niet tot de scope van de auditor voor ENSIA. Op onderdelen lopen bestaande beschrijvingen achter op de realiteit, zeker gelet op de ingrijpende wijzigingen die het team ICT de afgelopen tijd heeft gerealiseerd in verband met verhuizing naar tijdelijke locatie, zoals het beschikbaar stellen van mobile devices aan alle medewerkers, de invoering van papierloos werken en het plaats- en tijdonafhankelijk werken. Ten aanzien van de documentatie resteert bijgevolg nog een uitdaging.

Ten aanzien van het gebruik van Suwi-net door het KCC voor adresonderzoek waren er enige op- en aanmerkingen, waaruit de opdracht om te komen tot een verbeterplan is voortgekomen.

[1] Een toelichting op ENSIA volgt in § 2.1.
[2] Zie hierover de bijlage in § 4.2.

2.1 Voorbereiden ENSIA

ENSIA (Eenduidige Normatiek Single Information Audit) heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatieveiligheid en kan het hier ook beter op sturen.

Horizontale verantwoording

Met de resolutie "Informatieveiligheid, randvoorwaarde voor de professionele gemeente" van 2013 hebben de gemeenten afgesproken de Baseline Informatieveiligheid Gemeenten (BIG) te implementeren. Deze baseline is de kern van de verantwoording over informatieveiligheid aan de gemeenteraad. De horizontale verantwoording bestaat uit de zelfevaluatie, een IT-audit, een verklaring van het College van B&W en een passage over informatieveiligheid in het jaarverslag.

Verticale verantwoording

Over de BRP, PUN, Suwinet, BAG, BGT, BRO en DigiD moeten gemeenten ook verantwoording afleggen. Dit noemen we de 'verticale verantwoording'. De horizontale verantwoording richting gemeenteraad vormt hiervoor de basis. De normen van de BIG en de specifieke normen van de BRP, PUN, Suwinet, BAG, BGT, BRO en DigiD zijn opgenomen in de zelfevaluatievragenlijst. Voor de zelfevaluatie Basisregistratie Ondergrond (BRO) geldt 2018 als een proefjaar. In deze vragenlijst zijn ook vragen opgenomen over niet-informatieveiligheidsaspecten van genoemde stelsels, zodat deze niet afzonderlijk hoeven te worden beantwoord.

Single Information Audit

Uitgangspunt van ENSIA is de single information audit. Dit betekent dat u maar één keer per jaar deze zelfevaluatielijst hoeft in te vullen. De informatie wordt gebruikt voor de horizontale verantwoording richting gemeenteraad en de diverse verticale verantwoordingslijnen richting departementen.

Initiatief

ENSIA is een gezamenlijk project van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, de VNG, gemeenten, het ministerie van Sociale Zaken & Werkgelegenheid en het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (DGBRW).

Het grootste deel van de gemeentelijke dienstverlening verloopt inmiddels digitaal. Dit brengt een grote verantwoordelijkheid voor een zorgvuldige omgang met informatieveiligheid en privacy met zich mee. Informatieveiligheid gaat om beschikbaarheid, vertrouwelijkheid en integriteit. Werkt het? Kan er iemand bij de informatie die daar niet bij mag? Zijn de gegevens juist en volledig? Privacy gaat over de zorgvuldige omgang met persoonlijke gegevens van inwoners en bedrijven. Het gaat daarbij ook om de bescherming van de persoonlijke levenssfeer van onze inwoners. In het jaarverslag over 2017 is verantwoording afgelegd aan de gemeenteraad over informatieveiligheid met behulp van een nieuwe systematiek: de **Eenduidige Normatiek Single Information Audit** (ENSIA). Deze nieuwe systematiek maakt de stand van zaken rondom informatieveiligheid meer inzichtelijk en uiteindelijk meer efficiënt. Met ENSIA toetsen wij de situatie van onze organisatie aan de normen uit de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

2.2 Uitvoeren wettelijke controles

ENSIA is bedoeld als effectief en efficiënt verantwoordingsstelsel voor informatieveiligheid, gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en helpt gemeenten verantwoording af te leggen over informatieveiligheid aan de raad. ENSIA sluit daarvoor aan op de planning- en controlecyclus van de gemeente. Hierdoor kan het bestuur beter sturen op informatieveiligheid en verantwoording afleggen aan de gemeenteraad.

ENSIA structureert echter ook de gemeentelijke verantwoording aan de verantwoordelijke agentschappen van de rijksoverheid over de Basisregistratie Personen (BRP), de Paspoortuitvoeringsregeling (PUN), de Digitale persoonsidentificatie (DigiD), en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet). 2017 was voor de de Basisregistratie Adressen en Gebouwen (BAG), de Basisregistratie Grootschalige Topografie (BGT) een proefjaar.

Zoals in het jaarverslag over 2017 aan de raad is gemeld, is over de collegeverklaring betreffende informatieveiligheid door de externe auditor een assurance-verklaring afgegeven. Het jaarverslag is tijdig ingezonden aan BZK.

2.3 Uitvoeren bewustzijnsactie onder het personeel

Medewerkers moeten voortdurend worden geïnformeerd over gevaren die dreigen vanuit het internet. Ontwikkelingen die zich voordoen, worden op het Personeel Informatie Systeem (PIM) gepubliceerd in begrijpelijke taal en met richtlijnen voor het handelen. Een voorbeeld van een dergelijk bericht is opgenomen in bijlage 4.1.

Via PIM worden medewerkers geïnformeerd, wanneer een update van het besturingssysteem van het mobiele device kan worden geïnstalleerd, nadat er eerst is getest of de update geen problemen veroorzaakt. Er wordt tevens controle uitgeoefend of medewerkers de update daadwerkelijk installeren. Mocht dat onverhoopt zijn verzuimd, dan worden die medewerkers daarop geattendeerd.

Informatieveiligheid en privacy zijn onlosmakelijk aan elkaar verbonden. Bij presentaties over de gevolgen van de Europese privacywetgeving, de Algemene Verordening Persoonsgegevens (AVG), is daarom ook gesproken over informatieveiligheid en risico's die zich voordoen of kunnen voordoen.

Zo is uitleg gegeven over begrippen als aangegeven op nevenstaande pagina uit één van de presentaties. Maar ook is aandacht besteed aan andere fenomenen, zoals Social Engineering.

2.4 Ontwikkeling eigen software 'Cumulus'

Binnen het Sociaal Domein wordt ter vervanging van de GWS-Suite de applicatie Cumulus ontwikkeld. Met het oog op toepassen van het beginsel 'privacy-by-design' is direct bij de start van dit proces een Privacy Impact Assessment (PIA) uitgevoerd. Een dergelijk onderzoek is voorgeschreven vanuit de Algemene Verordening Gegevensbescherming, die in 2017 weliswaar nog niet in werking was getreden. Op het moment van de verwachte ingebruikneming van Cumulus is de AVG echter wel van toepassing, zodat daarop bij de ontwikkeling van Cumulus is geanticipeerd. De resultaten van het onderzoek zijn meegenomen bij de ontwikkeling van deze nieuwe applicatie. In het bijzonder is er vanuit de CISO op toegezien, dat de ontwikkelde software voldoet aan de te stellen eisen op het gebied van informatieveiligheid. Uiteraard zal voor ontsluiting naar de inwoner opnieuw een dergelijk onderzoek worden uitgevoerd, mede ook om aan de eisen van Logius[3] voor de DigiD koppeling te voldoen.

In november 2017 is een PIA uitgevoerd ten aanzien van het proces 'Afvalverwerking'. De uitkomsten van dit onderzoek hebben o.m. geleid tot aanpassingen in het digitale proces van interne data uitwisseling, in die zin dat een mogelijke kwetsbaarheid is onderkend en verholpen.

2.5 Vulnerability Assessment

Begin 2018 is door een extern bedrijf in het kader van ENSIA (over 2017) een Vulnerability Assessment uitgevoerd. Daarbij maakten de volgende onderwerpen deel uit van het onderzoek:

- Hardening
- Patchmanagement
- Periodieke penetratietests
- Periodieke Vulnerability Assessments
- Verwijderen oude informatie
- Demilitarised Zone (DMZ)
- Scheiden beheer- en productieverkeer
- Netwerktoegang
- Beheermechanismen
- Versleutelde verbindingen (HTTPS)

Het vulnerability assessment is uitgevoerd op basis van zowel handmatige tests, alsmede geautomatiseerde tests, waarbij deze software in staat is een groot aantal controles in een korte tijd uit te voeren. Alle bevindingen komen voort uit handmatige tests, waarbij verificatie direct heeft plaats gevonden.

Het assessment heeft geleid tot de volgende aanbevelingen en conclusies:

- Evalueer configuraties van aanwezige netwerkcomponenten en -diensten en werk deze waar nodig bij.
- Inventariseer alle aanwezige software en werk deze regelmatig bij.
- Sluit onveilige beheermechanismen af en draag zorg voor een beleid waarin enkel veilige beheermechanismen beschikbaar zijn en toegepast worden.
- Controleer de implementaties van versleutelde verbindingen op bekenden zwakheden en pas configuraties aan zodat deze veilig zijn.

[3] Logius is een dienst van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en beheert generieke ICT-voorzieningen. Logius levert diensten aan andere overheidsorganisaties en organisaties met een publieke taak. Voorbeelden van diensten zijn DigiD, Digipoort, MijnOverheid en eHerkenning.

Aan deze aanbevelingen is in 2018 opvolging gegeven.

Ten aanzien van het verwijderen van oude informatie doet zich bij alle grotere organisaties een probleem voor. Dat probleem heeft geen betrekking op de duidelijk gestructureerde data in bijvoorbeeld het Document Management Systeem, maar wel op de opslag van bijvoorbeeld tijdelijke documenten in mappen en bestanden van teams. Concepten en oudere versies moeten handmatig worden verwijderd, wat vaak achterwege bleef en blijft. De aangeboden applicaties om dit probleem op te lossen bieden onvoldoende resultaat. In 2018 zullen de mogelijkheden om dit probleem te verhelpen worden onderzocht.

2.6 Incidenten

In 2017 hebben zich de volgende grotere incidenten voorgedaan:

- Bij graafwerkzaamheden voor het nieuwe stadhuis werden de kabels van zowel de hoofdstroom- als de noodstroomvoorziening beschadigd, waardoor de servers uitvielen. Om problemen met applicaties en verlies van data te voorkomen zijn de servers conform de procedure opnieuw opgestart. Binnen iets meer dan 24 uur kon de organisatie weer over de digitale omgeving beschikken.
- Gebleken is, dat bij slecht weer (hevige regenval) de straalverbinding met Oudewater in 2017 meerdere keren is uitgevallen. Daarnaast bleek de antenne niet bestand tegen de najaarsstormen. Om dit probleem optimaal te verhelpen is gekozen voor een glasvezelverbinding van het Stadhuis in Woerden naar het Stadskantoor in Oudewater. Hoewel een dergelijke end-to-end-verbinding in beginsel veilig is, moet ook worden voorkomen dat door het fysiek inbreken op de verbinding datadiefstal mogelijk zou zijn. Dit probleem is in 2018 verholpen.
- In 2017 werd onder meer gewaarschuwd voor een kwetsbaarheid op mobiele telefoons bij het gebruik van bluetooth. Daaraan is direct aandacht geschonken via PIM. Deze kwetsbaarheid bleek te verhelpen door installatie van een beveiligingsupdate. Door middel van ons Mobile Device Management System is gecontroleerd of alle medewerkers alle beveiligingsupdates hebben geïnstalleerd. Medewerkers die dat nog niet hadden gedaan, zijn daarop gewezen.

2.7 Voorkomen incidenten

De Informatiebeveiligingsdienst van de VNG (IBD) wordt door het National Cyber Security Centrum (NCSC) in Den Haag gewezen op kwetsbaarheden in systemen. De IBD informeert vervolgens de aangesloten gemeenten. In 2017 zijn ruim 70 waarschuwingen ontvangen van mogelijke kwetsbaarheden in systemen, applicaties en andere bedreigingen. Alle berichten zijn onderzocht op feitelijke risico's voor onze systemen. Niet alle gemelde kwetsbaarheden (vulnerabilities) hadden betrekking op onze digitale omgeving, maar waar nodig zijn gepaste maatregelen genomen. Niet alle bedreigingen kunnen echter softwarematig worden geëlimineerd. In 2017 was de ransomsoftware BadRabbit lange tijd in het nieuws. Maar minder bekend zijn de talloze andere bedreigingen die het NCSC signaleert. Nieuw waren bijvoorbeeld ook Hidden Cobra en de Bleichenbacher-kwetsbaarheid.

Maar ook oudere technieken zoals E-mail spoofing werd nieuw leven ingeblazen. Spoofing gebeurt als iemand een e-mail verstuurt op naam van iemand anders. In 2017 was o.m. de burgemeester van Rotterdam daarvan het slachtoffer.

Naast de publieke kwetsbaarheden doen de beveiligingssystemen van de gemeente dagelijks hun werk. Zo werden er maandelijks ongeveer 150.000 e-mails verwerkt, waarvan 60.000 zijn tegengehouden als spam berichten en 0,1% in verband met de aanwezigheid van een virus. Ook houden de firewalls dagelijks kwaadwillend of onderzoekend verkeer tegen.

2.8 Actualiteit van het beleid

Het beleid is in 2017 beoordeeld of dat nog in lijn is met:

- de feitelijke situatie in de organisatie;
- de huidige wet en regelgeving;
- de maatschappelijke eisen; en:
- de stand van de techniek.

Op grond van de jaarlijkse controle komen we tot oordeel dat de feitelijke situatie als gevolg van de tijdelijke huisvesting op onderdelen afwijkt van hetgeen is beschreven. Het beleid zal worden geëvalueerd op het moment dat de organisatie is verhuisd naar de nieuwe locatie.

2.9 Actualiteit van procedures en documentatie

Door veranderingen in de organisatie (o.m. huisvesting en werkwijze), wet en regelgeving en de stand van de techniek is het van belang om de uitwerking van het beleid in procedures en documentatie actueel te houden. Op grond van de jaarlijkse controle komen we tot het oordeel dat de documentatie tekort schiet en procedures niet altijd strikt worden gevolgd.

2.10 Planning 2018

Om de kwaliteit van informatiebeveiliging verder te verbeteren zijn voor 2018 de volgende activiteiten gepland.

- Bewustwordingsacties onder het personeel.
- Bijscholing van medewerkers.
- Actualisering van de risico- en GAP-analyse.
- Segmentatie van het netwerk.
- Verhogen netwerk veiligheid nevenlocaties, zoals het Stadserf Woerden en het Oudewater Stadskantoor.
- Actualiseren beleid en documentatie.

3 Ontwikkelingen

Kernbevindingen

- Beroepscriminelen en statelijke actoren vormen nog altijd de grootste dreiging en richten de meeste schade aan
- Digitale aanvallen worden gebruikt om democratische processen te beïnvloeden
- De kwetsbaarheid van het internet of things heeft tot verstorende aanvallen geleid die de noodzaak tot het versterken van de digitale weerbaarheid onderschrijven
- Veel organisaties zijn afhankelijk van een beperkt aantal buitenlandse aanbieders van digitale infrastructuurdiensten waardoor de maatschappelijke impact bij verstoring groot is
- Weerbaarheid van individuen en organisaties blijft achter bij de groei van de dreiging

3.1 IBD Jaaroverzicht 2017:

Verhogen digitale weerbaarheid

Hoewel gemeenten zonder uitzondering grote stappen hebben gezet, moet blijvend worden gewerkt aan de digitale weerbaarheid. Om de volgende stap naar meer monitoring, response en detectie mogelijk te maken, ondersteunt de IBD gemeenten in 2018 extra om de basis op een gemeenschappelijk niveau te krijgen. Dat vereist een gestandaardiseerde aanpak waar alle gemeenten hun eigen elementen kunnen kiezen. Tegelijkertijd ondersteunt de IBD ook de koplopergemeenten met kennis(deling) en expertise op de doorontwikkeling van monitoring en detectie.

Het NCSC geeft in het Cybersecuritybeeld Nederland 2017 een vijftal Kernbevindingen aan, die hiernaast zijn weergegeven.

Aanvullend daarop:

- Bij statelijke actoren vallen vaak de namen van Rusland, China en Noord-Korea.
- Voor beïnvloeding van het democratische proces is in 2017 o.m. gebruik gemaakt van informatie afkomstig van Facebook, die is verwerkt door Cambridge Analytics. In het bijzonder Rusland wordt genoemd, als het gaat om beïnvloeding.
- Het Internet of Things (IoT) is de ontwikkeling dat steeds meer ‘dingen’ (machines, objecten, producten, apparaten, systemen) digitaal met elkaar en met de mens communiceren. Dit is mogelijk door ze met – vaak al eenvoudige – elektronica ‘slim’ te maken. Met sensoren krijgen producten als het ware zintuigen die waardevolle informatie verzamelen over hun toestand en hun omgeving. Met draadloze connectiviteit en via het internet wisselen zij deze informatie uit. Machines en producten zijn zo op afstand, bijvoorbeeld via een smartphone, te bedienen. Op deze manier raken de fysieke en de virtuele wereld steeds meer met elkaar verbonden. Onvoldoende beveiliging op slimme apparaten (Internet of Things) maakt het onder meer mogelijk die apparaten op te nemen in Botnets[4], die worden gebruikt om DDos-aanvallen uit te voeren. Daarnaast sturen veel slimme apparaten informatie naar de fabrikant, terwijl voor de consument niet duidelijk is welke informatie, hoe lang en waar die data worden bewaard en met wie de gegevens worden gedeeld.
- Buitenlandse aanbieders zijn bijvoorbeeld Microsoft, Google (Android) en Apple (iOS).
- Voor veel consumenten is het vrijwel onmogelijk weerstand te bieden aan de dreigingen die zich vanuit het internet aandienen, maar ook voor organisaties vergt adequate informatiebeveiliging steeds meer investeringen en capaciteit.

[4] De term "botnet" wordt vooral gebruikt voor een collectie van aan elkaar gekoppelde computers die software gebruiken die meestal is geïnstalleerd door een computerworm, Trojaans paard of achterdeurtje. De meeste computers die door deze software worden geïnfecteerd draaien onder Microsoft Windows, maar andere besturingssystemen kunnen ook worden aangetast. De geïnfecteerde computers heten ook wel zombies, het botnet heet ook wel zombienetwerk.
Een botnet heeft altijd een beheerder genaamd een "bot herder". Deze beheerder kan de groep op afstand besturen, vaak via middelen als IRC, meestal met slechte bedoelingen. Een bot van een botnet draait op een computer meestal op de achtergrond zodat hij niet opvalt. Vaak heeft de beheerder van een botnet de beschikking over een aantal hulpmiddelen om firewalls en buffers op andere computers te omzeilen. Nieuwere bots kunnen vaak zelf zwakke punten in een computer opzoeken.
Botnets zijn een significant onderdeel geworden van het internet. Veel internetservers blokkeren botnets. Er zijn al verschillende botnets opgespoord en verwijderd. Zo vond de Nederlandse politie in Sneek een botnet opgezet door een 19-jarige hacker.

4 Bijlage

4.1 Nieuwsbericht op PIM (Intranet)

PAS OP VOOR BAD RABBITS…

Door Saskia van Driel op dinsdag, 05-12-2017 12:17

Van de zomer zorgde het Petyavirus wereldwijd voor veel ellende. Netwerken van bedrijven werden platgelegd. Maersk leed een kwart miljard euro schade. En inmiddels is er alweer een nieuw virus, Bad Rabbit, dat vooral actief is in Rusland en Oekraïne.

Moeten wij ons zorgen maken? Kunnen wij ook getroffen worden door zo'n virus? En hoe erg is dat?

Hoe groot is de kans dat je op een verkeerde link klikt in een onschuldig ogend mailtje? Die kans wordt steeds groter. De hoeveelheid 'malware' neemt toe. En de effecten zijn niet te verwaarlozen. Maersk moest alle hard- en software vervangen, schepen werden niet gelost en goederen waren bedorven. Allemaal door één muisklik.

Daarnaast is er nog een ander risico. Een virus kan ervoor zorgen dat anderen makkelijk bij onze gegevens kunnen. Zo ook hackers. Er kunnen datalekken ontstaan en het boetebedrag daarvoor kan nu al oplopen tot € 900.000, maar vanaf 25 mei 2018 worden de boetes nog veel hoger!

Kortom: het voorkomen van virussen is belangrijk. Dat begint bij alert zijn op informatieveiligheid. Vertrouw je een mailtje niet? Open het niet, maar delete het en doe een melding bij de Servicedesk.

Werken phishingmail

Wat een phishingmail precies is en hoe je deze kunt herkennen lees je op de pagina over veilig mailverkeer.

Ben je op je werk slachtoffer geworden van internetcriminelen? Meld dit dan bij de Servicedesk (8899), maar ook zo snel mogelijk via het mailadres !Informatieveiligheid en Privacy en naar je teammanager. Dit in verband met de Meldplicht datalekken.

4.2 Procesaudit

Een procesgerichte organisatie steunt op processen. Daartoe is het nodig om ook de procesontwikkeling zelf te besturen. De besturing van de procesontwikkeling is ook een regelkring bestaande uit een voortdurende cyclus van toetsen en bijstellen van processen. Het toetsen van processen wordt auditten genoemd.

Wat is een audit?

Het toetsen van processen is onlosmakelijk aan procesmanagement verbonden. Een procestoets of audit is een onafhankelijk onderzoek naar het functioneren van een proces. Onderzocht wordt of de processen daadwerkelijk worden gevolgd en of ze nog voldoen (dienen ze nog het doel?).

Een audit kan zowel intern als extern worden uitgevoerd. Interne audits worden door de organisatie zelf uitgevoerd. De externe audit heeft betrekking op de toetsing die de certificerende instantie uitvoert om te bepalen of de organisatie aan de gestelde normen voldoet. Vaak wordt daarbij gebruik gemaakt van een set van normen en criteria van buiten (bijvoorbeeld ISO).

Het effect van interne audits gaat verder dan de procestoets. Zij vormen de basis om de processen actueel te houden, 'tussen de oren' van de mensen te krijgen en om verbeteringen te realiseren. Een goed opgezet en transparant intern auditsysteem vormt bovendien de basis voor een externe audit. De externe audit kan zich beperken tot een marginale toets van de interne audit resultaten.

Een audit bestaat uit de volgende stappen:

Procesaudit (aan de hand van een norm)

De auditors bestuderen eerst de procesbeschrijvingen en relevante documenten. Vervolgens interviewen zij de medewerkers van het proces. Vastgesteld wordt of de processen bekend zijn bij relevante betrokkenen.

Signalering afwijkingen van de norm

Aan de hand van een interne of externe norm (toetsingskader) worden afwijkingen gesignaleerd. Hoe goed is het proces ontworpen?

Afwijking wordt verbeterpunt

Elke afwijking wordt vervolgens samen met de procesmedewerker omgezet in een verbeterpunt.

Verbeteringen implementeren

Dit vindt plaats door de procesmedewerker zelf. In de volgende audit wordt op de voortgang ingegaan.

Voorbeelden van externe normen of toetsingskaders zijn NEN–ISO 9000 (algemene norm kwaliteitssystemen) en de BIG (Baseline Informatieveiligheid Gemeenten).

`Waarop wordt geaudit?

Bij een audit staat aantoonbaarheid voorop. De gebruikelijke norm is:

- Opzet: is er een ontwerp?
- Bestaan: zijn de processen er? en
- Werking: werken ze zoals bedoeld?

Voor cyber security bestaan veiligheidsnormen. Allereerst wordt de opzet en het bestaan van het informatieveiligheidsbeleid getoetst. Daarna wordt bekeken of dit in de praktijk werkt. Dit gebeurt fasegewijs:

Fase 1: opzet en bestaan

Fase 2: werking.

Gemeente Oudewater

gemeente WOERDEN

Jaarverslag Privacy 2017

Inhoudsopgave

1 Doel van het document

Dit voortgangsrapport is een periodieke rapportage van de Functionaris Gegevensbescherming en levert het bestuur informatie op over de voortgang en status van de werkzaamheden en de (tussen)resultaten op het gebied van de privacybescherming. Nadat het bestuur over 2016 zeer gedetailleerd is geïnformeerd, is nu gekozen voor een rapportage op hoofdlijnen.

2 Conclusie en samenvatting

Ten aanzien van 'Privacy' zijn voor 2017 de volgende **doelen geformuleerd**:

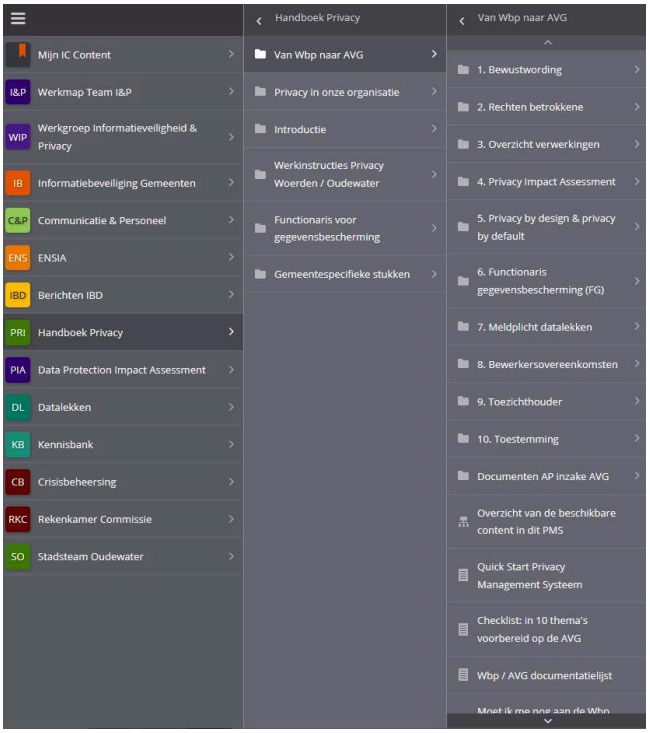
- Het actualiseren van het privacy managementsysteem (PMS).
- Het correct afdoen en voorkomen van datalekken.
- Het bevorderen van het bewustzijn (awareness) onder het personeel.
- Het uitvoeren van wettelijke controles.
- Het uitvoeren van privacy impact assessments (PIA's) in het geval van nieuwe processen of applicaties.
- Het voorbereiden van de invoering van de Algemene Verordening Persoonsgegevens (AVG) per 25 mei 2018.

In het bijzonder is veel tijd en aandacht geschonken aan de laatste doelstelling. De nieuwe Europese Algemene Verordening Gegevensbescherming (AVG) is de opvolger van een Europese richtlijn uit 1995, die in Nederland omgezet werd in de Wet bescherming persoonsgegevens (Wbp) uit 2001. De Wbp komt te vervallen; de AVG wordt vanaf 25 mei de énige privacywet.

> Inhoudelijk is de AVG vooral een kwestie van de touwtjes stevig aantrekken. De belangrijkste vernieuwingen zijn:
>
> - Veel meer gegevens vallen onder het begrip 'persoonsgegevens'.
> - De regels om toestemming te vragen worden strenger.
> - Iedere verwerking moet in een register zijn uitgewerkt.
> - Bij potentieel risicovolle verwerkingen moet een voorafgaande risicoanalyse zijn uitgevoerd en maatregelen zijn genomen om die risico's te beperken.
> - Iedere organisatie moet procedures hebben om mensen inzage in hun persoonsgegevens te verschaffen, om fouten te corrigeren en om verouderde gegevens te wissen.
> - Wie leveranciers of partners toegang geeft tot persoonsgegevens, moet dat geborgd hebben middels een verwerkersovereenkomst.
> - Er moet concreet beleid rond datalekken en beveiliging zijn.
>
> Strenger toezicht gaat samen met de nieuwe sanctiemogelijkheden van de Autoriteit Persoonsgegevens. Daarvoor bestaat ook een zekere angst. Niet geheel ten onrechte: de boetebedragen zijn aanzienlijk verhoogd. De AVG kent twee boetecategorieën: een lage categorie bij overtreding van administratieve bepalingen en een hoge categorie voor meer fundamentele overtredingen. Dat 'laag' is relatief: maximaal tien miljoen euro, of als dat meer is 2% van de wereldwijde jaaromzet. De hoge categorie is maar liefst twintig miljoen of 4%. Deze enorme bedragen zijn met name bedoeld voor de technologie-reuzen zoals Facebook, Google en Amazon die miljarden winst maken met de verwerking van persoonsgegevens. Een overzicht van de overtredingen en de daaraan toe te kennen boete is nevenstaand opgenomen.

Niet geldig toestemming vragen	Hoge categorie
Het burgerservicenummer gebruiken als dat niet verplicht is	Hoge categorie
Een onduidelijke privacyverklaring publiceren	Hoge categorie
Een datalek veroorzaken door slechte beveiliging	Lage categorie
Een datalek niet melden (ongeacht de kwaliteit van de beveiliging)	Lage categorie
Weigeren een kopie van iemands dossier te geven	Hoge categorie
Geen verwerkingsregister hebben	Lage categorie
Gegevens niet wissen als ze verouderd zijn	Hoge categorie

De **conclusie** is, dat de organisatie de geformuleerde **doelstellingen** over 2017 heeft **gerealiseerd**. Hierna wordt nader ingegaan op hetgeen daartoe is gerealiseerd en een planning voor hetgeen in 2018 gaat gebeuren.



2.1 Actualiseren van het privacy management systeem (PMS).

Voor de onderwerpen Privacy en Informatieveiligheid wordt gebruik gemaakt van de applicaties IC Content en (sinds kort) IC Control. Binnen de applicatie IC Content krijgt het PMS vorm in het ***Handboek Privacy***.

Het handboek biedt structuur en relevante content op gebied van de AVG en laat zien hoe en waarom bepaalde regels moeten worden toegepast. Het handboek wordt benut als centraal platform voor het privacybeleid en alle documenten die daarbij horen. Het wordt voortdurend verbeterd en aangevuld, onder andere met documenten van de Autoriteit Persoonsgegevens (AP), het Europees Comité voor gegevensbescherming en met best practices van implementaties. Het handboek is een integraal privacy beheersysteem waarmee de organisatie kan worden betrokken bij privacy management en de daaraan verbonden informatiebeveiliging.

Ten aanzien van vrijwel alle onderwerpen van het handboek zijn in 2017 activiteiten ontplooid. Een gedetailleerde beschrijving van alle acties voert in het kader van dit jaarverslag te ver. Enige onderwerpen die in 2017 bijzondere aandacht hebben gekregen zijn hierna genoemd. Uiteraard is de invoering van de AVG per 25 mei 2018 leidend geweest voor de keuze van onderwerpen waaraan met voorrang aandacht is geschonken.

Naast de benoeming van een Functionaris Gegevensbescherming en het opzetten van bovengenoemd PMS is in 2017 bijzondere aandacht uitgegaan naar:

- werkinstructies op het gebied van het sociaal domein,
- privacy-by-design bij de ontwikkeling van Cumulus,
- privacy Impact assessment (PIA) op het proces afvalverwerking,
- bewustwording medewerkers,
- voorbereiding van de overgang van Wbp naar AVG, en
- het werkproces datalekken.

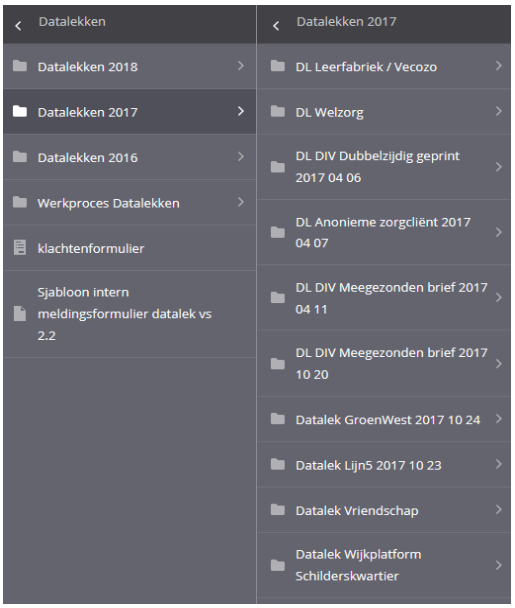
In § 5.1 is een schematische weergave van het PMS als bijlage opgenomen.

2.2 Datalekken correct afdoen, voorkomen en awareness

Sinds 1 januari 2016 bestaat op grond van de Wbp de plicht datalekken te melden bij de toezichthouder, de Autoriteit Persoonsgegevens (AP). Deze meldingsplicht is ook onder het regime van de AVG gehandhaafd. Naast deze meldingsplicht is verantwoording (accountability) expliciet benoemd in de AVG. Om te kunnen verantwoorden dat datalekken correct zijn afgewikkeld, is er een interne registratie opgezet. Daarin zijn alle gemelde tien 'beveiligingsincidenten' geregistreerd. Niet elk gemeld incident bleek een (formeel) datalek. Alle datalekken zijn afgehandeld overeenkomstig het werkproces datalekken, dat eerder (bij het jaarverslag over 2016) aan uw raad ter kennisname is toegezonden.

Belangrijk in dat proces is de evaluatie. Daarbij wordt niet alleen gekeken naar het doorlopen meldproces, maar vooral ook naar de oorzaak van het datalek, opdat voor de toekomst (zo mogelijk) maatregelen kunnen worden genomen ter voorkoming.

De datalekken die het moeilijkst zijn te voorkomen worden veroorzaakt door simpele menselijke fouten. Over deze fouten wordt onderling gesproken (bijv. in werkoverleg situaties) waardoor de bewustwording (awareness) privacy wordt vergroot. Daarnaast wordt daaraan via intranet (PIM) aandacht geschonken en zijn er presentaties gegeven voor management en medewerkers.



2.3 Het uitvoeren van bewustzijnsacties onder het personeel

In presentaties voor college, management en medewerkers is o.m. aandacht geschonken aan de wijzigingen die zich als gevolg van de invoering van de AVG voordoen. Dat de bewustwording ook daadwerkelijk is vergroot blijkt uit het aantal adviesverzoeken aan de FG: in 2017 zijn er 50 adviezen gevraagd, over 2018 zullen dat er naar verwachting 90 worden.

Verder mocht ook de nieuwe systematiek van de Eenduidige Normatiek Single Information Audit (ENSIA) niet ontbreken. Zowel onder de oude wetgeving (Wbp) als in de nieuwe wetgeving (AVG) zijn organisaties die persoonsgegeven verwerken, verplicht technische en organische maatregelen te treffen om de bescherming van die persoonsgegevens te waarborgen. Daarop werd controle uitgeoefend door meerdere toezichthouders. Vanaf 2017 is dat gestroomlijnd door middel van ENSIA.

2.4 Het uitvoeren van de wettelijke controles.

De wettelijke controles op het goed functioneren van o.m. beveiligingsmaatregelen op het gebied van DigiD, SuwiNet en de Basisregistratie Personen (BRP) zijn, zoals hiervoor al aangegeven, ondergebracht in de nieuwe systematiek van ***ENSIA***. Het doel daarvan is om de auditlast voor gemeenten te beperken. Hierop wordt nader ingegaan in het Jaarverslag Informatieveiligheid.

Op het gebied van privacy bestaan er (nog) geen wettelijke controles. De toezichthouder (AP) heeft nog niet concreet benoemd op welke wijze het toezicht op naleving van de AVG zal worden geëffectueerd, maar heeft daarover het volgende gepubliceerd:

"Om vast te stellen of aan de verantwoordingsplichten van de AVG is voldaan, wordt in verschillende sectoren de naleving van één van de plichten uit de AVG gecontroleerd. Daarbij is de verwachting dat informatie over de uitkomsten van de controles het lerend vermogen van organisaties ten aanzien van de naleving van de AVG zal vergroten."

Tot het opstellen van dit jaarverslag is het toezicht van de AVG voor onze organisatie beperkt gebleven tot controle op de aanwezigheid van een Functionaris Gegevensbescherming bij alle overheidsinstellingen.

2.5 Het uitvoeren van Privacy impact assessments (PIA's) op nieuwe processen of applicaties

Binnen het Sociaal Domein wordt ter vervanging van de GWS-Suite de applicatie Cumulus ontwikkeld. Met het oog op toepassen van het beginsel 'privacy-by-design' is direct bij de start van dit proces een Privacy Impact Assessment uitgevoerd. De resultaten van dat onderzoek zijn meegenomen bij de ontwikkeling van deze nieuwe applicatie. Uiteraard zal voor ontsluiting naar de inwoner opnieuw een dergelijk onderzoek worden uitgevoerd.

In november 2017 is een PIA uitgevoerd ten aanzien van het proces 'Afvalverwerking'. De uitkomsten van dit onderzoek hebben o.m. geleid tot aanpassingen in het proces van interne data uitwisseling, in die zin dat een mogelijke kwetsbaarheid is onderkend en verholpen.

2.6 Voorbereiding AVG

Ter voorbereiding van de invoering van de AVG is in 2017 een overzicht opgesteld van alle bekende verwerkingen van persoonsgegevens binnen onze organisatie. Dit ter reaisatie van het onder de AVG verplichte ***register van verwerkingen***. Dit register wordt in de loop van 2018 en 2019 nader gedetailleerd en geprofessionaliseerd in de applicatie IC Control. In hoofdstuk 4 wordt daarop een preview gegeven en in het jaarverslag over 2018 zal over de voortgang worden gerapporteerd.

Veel tijd is besteed aan bestaande, nieuw af te sluiten en ontbrekende ***bewerkersovereenkomsten***. Onder de AVG is de naam gewijzigd in verwerkingsovereenkomsten die moeten worden aangegaan door verwerkingsverantwoordelijken en de verwerkers. Om andere partijen persoonsgegevens te laten verwerken, moeten met die andere partijen afspraken worden gemaakt over tal van onderwerpen, zoals het eigendom van de data, de plaats waar de gegevens mogen worden opgeslagen (gehost), welke actie van wie is vereist in het geval van een onverhoopt datalek en afspraken over aansprakelijkheid. Omdat de eerder gesloten bewerkersovereenkomsten verwijzen naar de Wbp, moeten alle bestaande bewerkersovereenkomsten worden herzien. Daarvoor is een standaard verwerkingsovereenkomst opgesteld, die aan verwerkers wordt voorgelegd.

3 Kwaliteitsonderzoek

De functionaris voor gegevensbescherming voert jaarlijks een kwaliteitsonderzoek uit naar o.m. de volgende zaken:

- De kwaliteit van naleving van privacywetgeving en het privacybeleid volgens de FG
- (Aankomende) wijzigingen in het privacybeleid en de consequenties hiervan voor de organisatie
- Toezicht, incidenten en controles op de naleving van genomen maatregelen
- Ondernomen acties en adviezen ten aanzien van PIA's
- Ondernomen activiteiten ten aanzien van opleidingen en awareness van medewerkers

Op grond van bovenstaande onderzoeken hebben geleid tot de volgende constateringen:

3.1.1 De kwaliteit van naleving van privacywetgeving en het privacybeleid volgens de FG

Gelet op de groei van het aantal adviesverzoeken mag worden geconstateerd dat de naleving van privacywetgeving en –beleid steeds meer aandacht krijgt in de organisatie. Er bestaat – voor zover bekend –geen terughoudendheid om incidenten te melden en op correcte wijze af te doen. Een aandachtspunt is echter, of bij het uitvragen van gegevens van inwoners de noodzaak aanwezig is om die gegevens voor het gestelde doel te verwerken. Dat het 'wel handig' is om over bepaalde gegevens te beschikken, is immers geen criterium. Daaraan zal bij verdere detaillering van het register van verwerkingen aandacht worden geschonken.

3.1.2 (Aankomende) wijzigingen in het privacybeleid en de consequenties hiervan voor de organisatie

De invoering van de Algemene Verordening Persoonsgegevens in 2018 heeft geleid tot hernieuwde aandacht voor alle verwerkingen van persoonsgegevens in de organisatie. Sinds de invoering van de Wet bescherming persoonsgegevens in 2001 zijn alle verwerkingen van persoonsgegevens gemeld bij het College bescherming persoonsgegevens (Cbp), thans de Autoriteit Persoonsgegevens. Alle meldingen die in het register van de AP voorkwamen zijn gedeeld met het verantwoordelijke lijnmanagement. Als gevolg van reorganisaties over de afgelopen jaren, was het niet altijd duidelijk welk team thans verantwoordelijk is voor enige verwerkingen. Dat vergde nader onderzoek en met een groot deel van de teammanagers hebben aanvullend gesprekken plaatsgevonden. Daarbij is naar voren gekomen, dat enige teammanagers hun eigen rol voor wat betreft privacy onderschatten en een belangrijke rol op dat gebied toekenden aan de FG. De FG heeft echter een adviserende en toeziende taak en kan zich daarom niet bezighouden met uitvoerende taken op het gebied van de privacy.

Daarnaast is gebleken dat intern gerichte verwerkingen ontbraken. In de voorbereidingen van het eigen register van verwerkingen (zoals verplicht per 25 mei 2018) zijn die verwerkingen zoveel mogelijk meegenomen.

3.1.3 Toezicht, incidenten en controles op de naleving van genomen maatregelen

Teneinde het toezicht, de afhandeling van incidenten en de controle op naleving van maatregelen maximaal vorm te geven heeft de FG ogen en oren in de organisatie nodig. Daartoe is er een werkgroep met vertegenwoordigers uit de organisatie gevormd, die maandelijks bijeenkomt en relevante zaken bespreekt. In 2017 behoorden tot deze werkgroep de privacy-officer van het sociaal domein, een juridisch consulent, een communicatiedeskundige, medewerkers van systeembeheer en helpdesk van het team ICT, de plaatsvervangend FG, de kwaliteitsmedewerkers Documentaire Informatievoorziening en Gegevensbeheer en de applicatiebeheerder Basis Registratie Personen.

Op basis van signalen zijn er – naast de vele gevraagde adviezen – ook ongevraagd adviezen gegeven. De verantwoordelijkheid voor het naleven van de wet- en regelgeving berust bij het lijnmanagement. In 2017 zijn echter alle gegeven adviezen door het management gevolgd.

Verder is veel aandacht uitgegaan naar zowel bestaande als ontbrekende bewerkersovereenkomsten, zoals hiervoor in §2.6 is vermeld. Gebleken is, dat door juristen verschillend wordt gekeken naar de verhouding verantwoordelijke versus bewerker. In enige gevallen bleken bewerkers feitelijk eigenstandige verantwoordelijke voor de verwerking van persoonsgegevens. Daarop zijn correcties uitgevoerd. Daarnaast is onderzocht in welke gevallen een bewerkersovereenkomst ontbrak. In die gevallen zijn de verantwoordelijke lijnmanagers aangesproken alsnog voor de totstandkoming zorg te dragen.

3.1.4 Ondernomen acties en adviezen ten aanzien van PIA's

Zoals eerder gemeld zijn er Privacy Impact Assessments gehouden ten aanzien van de ontwikkeling van Cumulus en de registraties bij afvalverwerking. De daaruit voortgekomen adviezen zijn opgevolgd.

3.1.5 Ondernomen activiteiten ten aanzien van opleidingen en awareness van medewerkers

In 2017 hebben de FG en de kwaliteitsmedewerkers van de teams Documentaire Informatievoorziening (DIV) en Gegevensbeheer opleidingen gevolgd op het gebied van privacy. Er zijn presentaties gehouden betreffende de overgang van Wbp naar AVG aan het college van B&W van Woerden, het lijnmanagement en (op verzoek) in het werkoverleg van enige teams.

4 Planning 2018

Om de kwaliteit van de privacybescherming op peil te houden en verder te verbeteren zijn voor 2018 de volgende activiteiten gepland.

- Bewustwordingsacties onder het personeel.
- Bijscholing van medewerkers.
- Actualisering van het register van de verwerkingsactiviteiten

4.1 Bewustwordingsacties onder het personeel

Ook in 2018 zullen presentaties worden gehouden voor medewerkers. Daarnaast zal via intranet (PIM) relevante informatie worden gedeeld. In 2018 zal ook worden onderzocht of er een voor onze organisatie geschikte en betaalbare e-learning beschikbaar is in de markt, om de bewustwording van de gevaren op internet en de daarmee verbonden risico's voor privacy verder te vergroten.

Hoewel datalekken niet juichend worden ontvangen, dragen die vaak wel bij aan de bewustwording. Niemand wil de oorzaak zijn van een datalek en wellicht vormt dat gegeven de basis voor de sterke toename van het aantal adviesverzoeken uit de organisatie.

4.2 Bijscholing van medewerkers

Gepland voor 2018 zijn een uitgebreide opleiding van de FG en een basisopleiding voor de plaatsvervangend FG op het gebied van de privacy in het algemeen en de AVG in het bijzonder.

In 2018 zullen opnieuw presentaties worden gegeven aan medewerkers met betrekking tot de komende wetswijziging, maar ook zoveel mogelijk worden ingegaan op praktische vragen die zich voordoen bij de uitvoering van individuele of groepstaken. Het uiteindelijke doel is, dat iedere medewerker zich afvraagt of er een noodzaak is om persoonsgegevens te verwerken, welke dat zijn (dataminimalisatie), of de verwerking in verhouding staat tot het te realiseren doel en er een juridische grondslag voor de gewenste verwerking bestaat.

4.3 Actualisering van het register van de verwerkingsactiviteiten

In 2017 is een begin gemaakt met het ingevolge de AVG verplichte verwerkingsregister. Sinds de invoering van de Wbp zijn alle bekende verwerkingen gemeld bij het College bescherming persoonsgegevens. Dit openbare register houdt per 25 mei 2018 op te bestaan. De in dat register ingevoerde verwerkingen van onze organisatie vormden de basis voor het nieuw op te zetten register. Gebleken is, dat een aantal – meest interne verwerkingen – niet eerder als verwerking zijn onderkend en gemeld. Zo zijn ook de abonnementenlijst van nieuwsbrieven, de backups van onze netwerkservers, de statistieken van onze websites en zelfs de interne autorisatietabel voor toegang tot netwerk en applicaties verwerkingen die in het register moesten worden opgenomen.

Een vervolgstap voor 2018 betreft de nadere detaillering van het verwerkingsregister in de applicatie IC Control. Daarin worden de verwerkingen met alle relevante informatie (gebruikte applicaties, bewaartermijnen, soort gegevens, uitgevoerde PIA, aanwezigheid verwerkers en verwerkersovereenkomsten) opgenomen. Zoals de naam van de applicatie al aangeeft, is het vooral ook een gereedschap om in control te komen. Met behulp van de aanwezige rapportages kan bijvoorbeeld een overzicht worden gegenereerd van applicaties waarvan een contract afloopt. Om een indruk te geven onderstaand een tweetal previews.

Per proces worden de verwerkingen opgenomen, met vervolgens informatie over de gebruikte persoonsgegevens, de wettelijke bewaartermijnen, welke systemen en/of diensten worden gebruikt en welke beveiligingsmaatregelen moeten worden genomen.

Het programma biedt tevens de mogelijkheid een totaaloverzicht te generen van alle verwerkingen van persoonsgegevens die binnen onze organisatie plaatsvinden. Uiteraard gaat het in de volgende afbeelding slechts om een beperkt voorbeeld daarvan.

TOTAALOVERZICHT VAN VERWERKINGEN

PROCESNAAM	PROCESDOEL	VERANTWOORDELIJKE VOOR PROCES	NAAM VERWERKING	VERWERKINGSDOEL	GRONDSLAG	VERANTWOORDELIJKE VOOR VERWERKING	AANTEKENINGEN OVER DE VERWERKING
Duurzaam opslaan en ontsluiten informatieobjecten	Functionaliteit voor het duurzaam opslaan, in stand en toegankelijk houden van informatieobjecten.		GISviewer	Op geografische wijze ontsluiten van informatie die gebruikers nodig hebben in het kader van de uitvoering van Publiek- en privaatrechtelijke taken	Taak algemeen belang of openbaar gezag (Art 6.1.e AVG)	College van BenW	Diverse wetgeving publiek- en privaatrechtelijke taken
Afvalverwerking	Het periodiek inzamelen van (huishoudelijk) afval huis-aan-huis of via vaste of mobiele inzamelpunten.		Afvalstoffen	Containerregistratie	Taak algemeen belang of openbaar gezag (Art 6.1.e AVG)	College van BenW	Milieuwetgeving
Afvalverwerking	Het periodiek inzamelen van (huishoudelijk) afval huis-aan-huis of via vaste of mobiele inzamelpunten.		Afvalpas	Behandelen aanvragen vervangende passen	Taak algemeen belang of openbaar gezag (Art 6.1.e AVG)	College van BenW	Milieuwetgeving
Interne dienstverlening (bestuurs- en managementondersteuning)	Bestuurs- en managementondersteuning		Koninklijke en gemeentelijke onderscheidingen	Behandeling van voordrachten voor Koninklijke en gemeentelijke onderscheiding	Taak algemeen belang of openbaar gezag (Art 6.1.e AVG)	College van BenW	Kapittel Civiele orden
Interne dienstverlening (bestuurs- en managementondersteuning)	Bestuurs- en managementondersteuning		Jubileaoverzichten (50- 60 jarige en > 60 jarige huwelijke en honderjarigen	Felicitatie van burgemeester	Taak algemeen belang of openbaar gezag (Art 6.1.e AVG)	College van BenW	
Beheren archief en informatie	Het opslaan van informatieobjecten en het beheren van wat zich in de opslag bevindt zodanig dat deze duurzaam toegankelijk blijft		Zakenmagazijn	1. Bestand met af te handelen dossiers van burgers en bedrijven 2. Voor daartoe geautoriseerde medewerkers digitaal toegankelijk maken te behandelen zaken 3. Voortgangsmonitoring	Taak algemeen belang of openbaar gezag (Art 6.1.e AVG)	College van BenW	
Beheren archief en informatie	Het opslaan van informatieobjecten en het beheren van wat zich in de opslag bevindt zodanig dat deze duurzaam toegankelijk blijft		Postregistratie/Documentenbeh... zowel schriftelijke als digitale post (via stadhuis@woerden.nl en	Registratie van de ontvangst, behandeling en afdoening van documenten, zowel papier als elektronisch	Taak algemeen belang of openbaar gezag (Art 6.1.e AVG)	College van BenW	AWB, Archiefwet, Verordening documentaire informatievoorziening (DIV), Besluit DIV
Griffie taken	ondersteunen van raadsleden bij het opstellen van initiatiefvoorstellen, amendementen, moties en schriftelijke raadsvragen en zorgen voor de communicatie van de gemeenteraad zodat de positie en de handelingen van de raad alom bekend zijn bij de lokale samenleving.		Overzicht nevenfuncties raadsleden	Openbaar maken nevenfuncties	Taak algemeen belang of openbaar gezag (Art 6.1.e AVG)	Raad	art 36 VWbp

Het opzetten van deze registratie heeft de FG voor zijn verantwoordelijkheid genomen. Voor wat betreft de bijhouding vervult de FG een coördinerende en toezichthoudende taak. Het lijnmanagement is daarvoor verantwoordelijk. De verwachting is, dat in 2019 de verantwoordelijkheid voor het bijhouden kan worden overgedragen aan het lijnmanagement. Daartoe zullen per organisatieonderdeel medewerkers moeten worden aangewezen, die de verwerkingen die binnen het eigen team plaatsvinden zo nodig actualiseren, aanvullen of verbeteren.

5 Ontwikkelingen

5.1 Privacy in het nieuws

In 2017 was er herhaaldelijk aandacht voor de invoering van de AVG. De indruk werd gewekt, dat er erg veel ging veranderen, niet zelden aangezwengeld door commerciële partijen die hierin een verdienmodel zagen en wezen op de sterk verhoogde boetemogelijkheden van de Autoriteit Persoonsgegevens. In feite is het aantal wijzigingen ten opzichte van de Wet bescherming persoonsgegevens (Wbp) beperkt en zijn veel bepalingen nauwelijks gewijzigd. De belangrijkste wijzigingen en de consequenties daarvan voor onze organisatie zijn in hoofdstuk 2 beschreven.

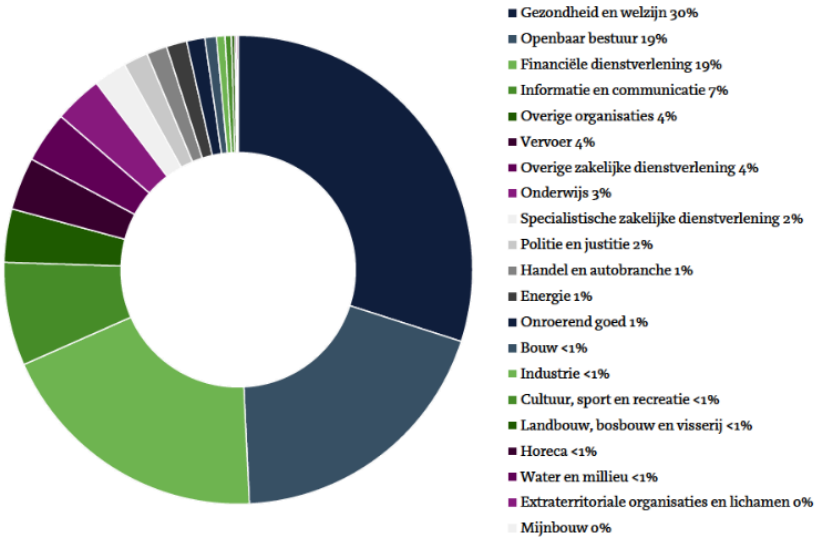
Veel aandacht ging ook uit naar Facebook en in het bijzonder de activiteiten van Cambridge Analytica met betrekking tot de Amerikaanse verkiezingen, maar ook de Nederlandse 'Stemwijzer' voor de Tweede Kamerverkiezingen werd argwanend bekeken.

Over 2017 werden bij de Autoriteit Persoonsgegevens ruim 10.000 meldingen gedaan van datalekken, waarbij het in 47% ging om persoonsgegevens verstuurd of ontvangen aan de verkeerde ontvanger. Meestal ging het om NAW-gegevens, geboortedatum c.q. leeftijd en het Burger Service Nummer. Ten opzichte van 2016 is dit een toename van ca. 40% en de verwachting is, dat ook 2018 een verdere stijging te zien zal geven. Uit onderstaand overzicht blijkt dat 19% van de datalekken zijn gemeld vanuit het openbaar bestuur.

Bij bijna 8500 van de 10.000 meldingen was er voor de AP aanleiding die meldingen te controleren en in 635 gevallen is onderzoek gedaan naar de beveiliging en naar mogelijke datalekken bij organisaties. De datalekken die vanuit onze organisatie bij de AP zijn gemeld, hebben niet geleid tot nadere controle en/of onderzoek.

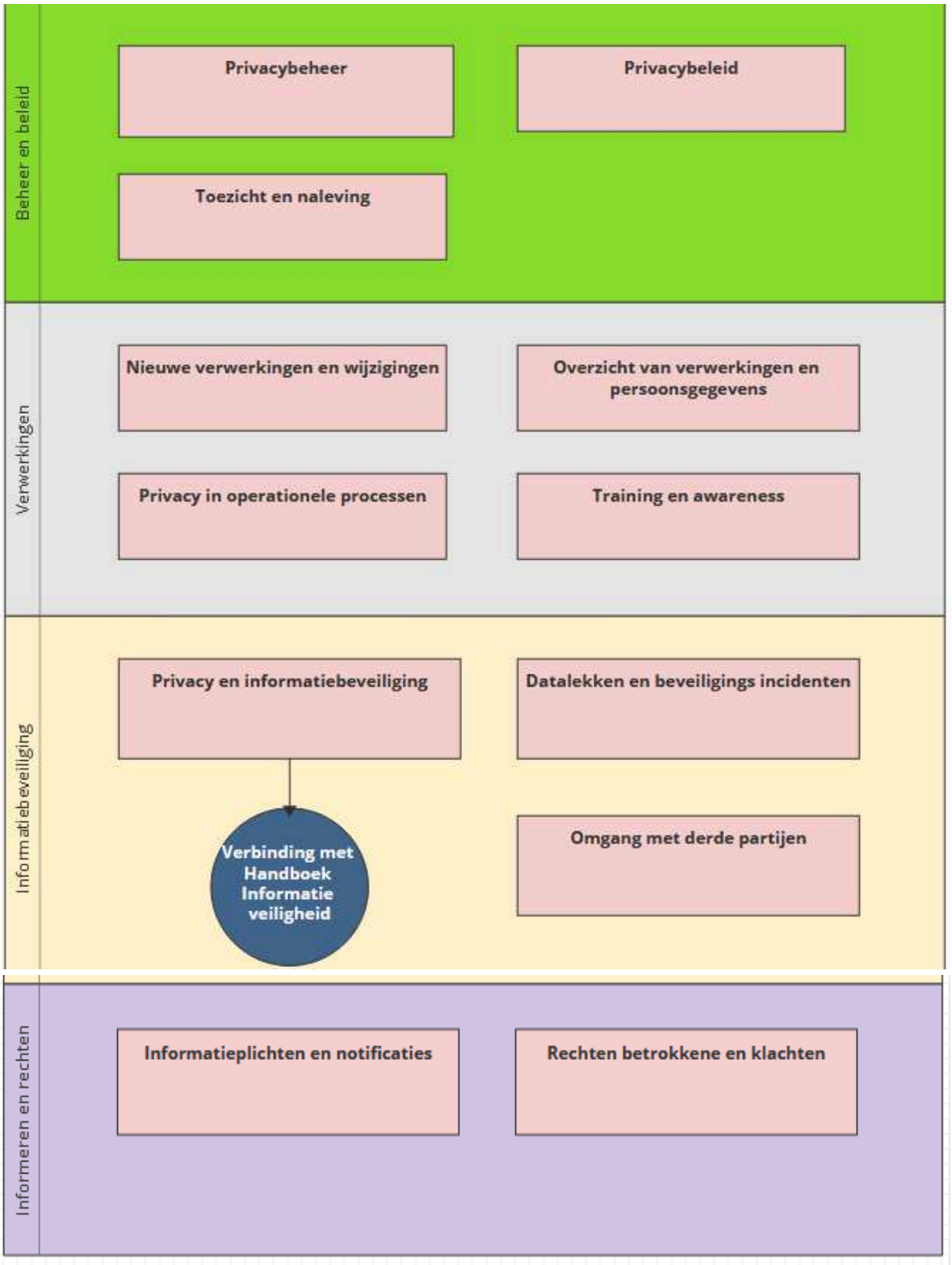
In dit kader mag de ontwikkeling van Big Data niet onvermeld blijven. Niet alleen het bedrijfsleven, ook de overheid wil graag gebruik maken van big data. Statistisch onderzoek is toegestaan, maar als de uitkomsten worden gebruikt om mensen dingen te verplichten of te verbieden ontstaat strijd met de regels omtrent profiling. Dit creëert een buitengewoon lastig dilemma. De AVG geeft hier vooralsnog geen antwoord op. (Zie § 5.2 inzake Big Data).

Meldingen datalekken per sector



6 Bijlagen

6.1 Privacy Management Systeem



6.2 De AVG versus big data

De term big data wordt gebruikt om te verwijzen naar verzamelingen data die zo groot zijn dat ze met traditionele databasesystemen niet goed meer te verwerken zijn. De snelle groei van verwerkings- en opslagcapaciteit van ICT-systemen maken het mogelijk dat hoeveelheden data worden verwerkt waar vroeger alleen van kon worden gedroomd. En bij zulke grote hoeveelheden data speelt ook nog eens het probleem dat de data zelden netjes gestructureerd of gelabeld is, zodat zoeken, combineren en analyseren van die data minstens zo'n uitdaging is als ze bij elkaar krijgen.

Met big data kan worden gezocht naar combinaties of trends die in kleinere hoeveelheden data onzichtbaar zouden zijn gebleven. Met statistische analyses door krachtige computers kunnen dan verbanden worden gevonden die handmatig onderzoek nooit had kunnen vinden. Correleer tienduizend factoren over een periode van vijfjaar en je zult opmerkelijke dingen vinden: een patroon van frauduleuze transacties in de boekhouding, de kans dat een ontslagen patiënt op korte termijn terugkomt in het ziekenhuis of het tijdstip waarop een machine op de productievloer het beste vervangen kan worden.

Veel big data bevat persoonlijke informatie: aankoopgedrag, bezoekgegevens en ga zo maar door. En dat maakt werken met big data lastig: het verwerken van persoonsgegevens is aan strenge regels onderworpen. Het begint al bij de eenvoudige vraag hoe je toestemming moet vragen aan alle betrokkenen. Waar dat bij een aanmelding op een website nog wel lukt, is het bij 4.5 miljard 'Vind-ik-leuks' per dag al een stuk moeilijker om per geval op een zinvolle manier toestemming te vragen. Ook de eis van doelbinding zit in de weg: bij big data onderzoek weet je vooraf vaak niet wat je gaat doen, terwijl deze eis met zich meebrengt dat je vooraf zegt wat je gaat doen.

De grote weerstand tegen de AVG kwam vooral vanuit Amerikaanse techbedrijven, en precies om deze reden. Het grote geld wordt verdiend met het commercieel verwerken van die miljarden gegevens. Iedereen voorlichten en toestemming vragen legt een bom onder dat model: zonder werkbare toestemming geen gerichte advertenties, en zonder gerichte advertenties geen inkomsten. Uit vele onderzoeken blijkt namelijk dat 'gewone' advertenties veel minder succesvol zijn dan gerichte, op bezoekersprofielen afgestemde advertenties. Ook een beroep op een eigen belang is erg ingewikkeld, vanwege de complexe belangenafweging en vooral de opt-out die dan moet worden geboden.

Dit creëert een buitengewoon lastig dilemma. Big data verbieden zal internetondernemers zwaar raken in hun commerciële mogelijkheden, en gezien de belangstelling voor hun diensten bij het publiek is een verbod moeilijk uit te leggen. De AVG geeft hier vooralsnog geen antwoord op.

Bron: Handboek AVG, Compliance in de praktijk van A. Engelfriet c.s.