rekenschap

Zwolle

Advies

Telefoon (038) 498 2240

Jaarverslag informatieveiligheid 2018

Opdrachtgever	College
Opdrachtnemer	A.P. Britstra, M. Hol
Versie	1
Datum	21 mei 2019

Datum 21 mei 2019
Titel Jaarverslag informatieveiligheid 2018

Inhoud

1	**Inleiding**	**3**
1.1	Leeswijzer	3
2	**Informatiebeveiliging**	**5**
2.1	ENSIA	5
2.1.1	Basisregistratie Ondergrond	5
2.1.2	Baseline Informatiebeveiliging Gemeenten (BIG)	6
2.2	Beleid	7
2.2.1	Hoofdpunten	7
2.2.2	Implementatie	8
2.3	Organisatie van informatiebeveiliging	8
2.3.1	Personele zaken	8
2.3.2	Architectuurboard	8
2.4	Samenwerking	9
2.4.1	Zwolle-Kampen	9
2.4.2	Via het shared service centrum ONS	9
2.4.3	GGI Veilig	9
3	**Privacy**	**10**
3.1	AVG	10
3.2	Datalekken	10
3.3	Training	11
3.4	Onderzoek BMC	11
3.5	Suwinet	12
4	**Bewustwording**	**13**
4.1	Trainingen	13
4.1.1	Voorbereiding	13
4.1.2	Workshops	13
4.1.3	Gevolgen	14
4.2	Communicatie	14
5	**Incidenten**	**15**
5.1	Beveiligingsincidenten	15
5.1.1	Overige incidenten	15

Datum 21 mei 2019
Titel Jaarverslag informatieveiligheid 2018

1 Inleiding

Voor u ligt het Jaarverslag Informatieveiligheid 2018 van de gemeente Zwolle. Dit beschrijft op hoofdlijnen wat in en voor deze gemeente aan activiteiten is ontplooid in 2018 op gebied van informatiebeveiliging en privacy. Op hoofdlijnen, want informatieveiligheid is een zo breed onderwerp dat het ondoenlijk is om alle activiteiten in één document te beschrijven.

In 2018 stond het woord 'bewustwording' centraal. Dat de Algemene Verordening Gegevensbescherming (AVG) per mei van het jaar in werking trad heeft veel aandacht gekregen. In de media, maar ook in onze organisatie. Niet alleen door de vele mails van leveranciers over privacy-tools en -diensten, maar ook door de vele bewustwordings-trainingen die binnen de organisatie zijn gegeven. Daarin was er veel aandacht voor de verandering door digitalisering. Want digitaal werken kent andere risico's dan analoog werken, zoals de kwetsbaarheid voor aanvallen door hackers. Cyberaanvallen zijn "profijtelijk, laagdrempelig en weinig riskant voor aanvallers" aldus het Nationaal Cyber Security Centrum[1]. Niet alle hackers zijn tegen te houden, maar een bewuste houding van medewerkers maakt onze gemeente zeker weerbaarder.

De verwachting is dat de komende jaren veel tijd en geld besteed moet worden om de Informatiebeveiliging op peil te houden. Technische ontwikkelingen om te kunnen hacken gaan razendsnel, dat vraagt continu om aanpassingen ter bescherming. Dit brengt de nodige investeringen met zich mee.

Gemeenten Kampen en Zwolle hebben eind 2018 een nieuw Strategisch Informatiebeveiligingsbeleid vastgesteld. Hierin is expliciet aandacht gegeven aan het beleggen van verantwoordelijkheden en aan een risicogerichte aanpak van informatiebeveiliging. Hiermee sluit de gemeente Zwolle aan bij de Baseline Informatiebeveiliging Overheid (BIO); van kracht per 2019 en vanaf 1 januari 2020 de verplichte baseline voor gemeenten en bij de constateringen die de VNG verwoord in het gemeentelijke dreigingsbeeld[2].

1.1 Leeswijzer

Dit jaarverslag beging in het tweede hoofdstuk met de verplichte verantwoording over informatiebeveiliging volgens de ENSIA-systematiek. Het benoemt specifiek enkele aandachtpunten vanuit het zelfassessment over de Baseline Informatiebeveiliging Gemeenten. Vervolgens schenkt het aandacht aan het nieuwe informatiebeveiligings-beleid en de organisatie van informatiebeveiliging. Het hoofdstuk eindigt met gemeentelijke samenwerking rond informatiebeveiliging.

[1] Zie het artikel op www.ncsc.nl over het Cybersecuritybeeld Nederland 2018.
[2] De inleiding van het 'Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2019/2020' (Informatiebeveiligingsdienst van de Vereniging Nederlandse Gemeenten, december 2018) begint met als kop 'Informatiebeveiliging = risicomanagement'. De VNG schrijft daarin: "Of de dreiging nu komt van een onbewuste medewerker, een criminele organisatie of een stroomstoring: de technische en organisatorische maatregelen om schade te voorkomen, te beperken en te vermijden zijn hetzelfde. Risicomanagement is de basis van een goede informatiebeveiliging" (blz. 3).

Hoofdstuk drie gaat specifiek in op privacy en bevat het verantwoordingsverslag van de Functionaris Gegevensbescherming (inclusief rapportage van datalekken) en van de Security Officer Suwinet.

Het vierde hoofdstuk draait om bewustwording. Het staat (beknopt) stil bij de verschillende activiteiten die in 2018 zijn uitgevoerd om medewerkers van de gemeente Zwolle bewuster te maken van informatiebeveiliging en privacy.

In het vijfde hoofdstuk wordt verslag gedaan van de beveiligingsincidenten die zich in 2018 hebben voorgedaan binnen de gemeente Zwolle.

2 Informatiebeveiliging

Dit hoofdstuk beschrijft in hoofdlijnen de zaken die in 2018 ten aanzien van informatiebeveiliging zijn uitgevoerd door de gemeente Zwolle.

2.1 ENSIA

Via de zogenaamde ENSIA[3] systematiek leggen alle Nederlandse gemeenten verantwoording af over de stand van de informatiebeveiliging. De Zwolse ENSIA-verantwoording is separaat van dit jaarverslag aangeboden aan het college en aan (toezichthouders namens) de betreffende ministeries.

ENSIA kent de volgende onderdelen:

- Zelfassessment over de Baseline Informatiebeveiliging Gemeenten (BIG)
- Zelfassessment over DigiD
- Zelfassessment over Suwinet
- Zelfassessment over de volgende basisregistraties:
    - Basisregistratie Adressen en Gebouwen
    - Basisregistratie Grootschalige Topografie
    - Basisregistratie Ondergrond[4]
    - Basisregistratie Personen

Naast de zelfassessments kent de ENSIA-verantwoording over 2018 twee audits die door een externe auditor worden uitgevoerd, namelijk over DigiD en Suwinet.

2.1.1 Basisregistratie Ondergrond

De status van de afzonderlijke basisregistraties wordt verantwoord via de binnen ENSIA vastgestelde procedure. Over 2018 geldt die verplichting nog niet voor de Basisregistratie Ondergrond.

Sinds 1 januari zijn gemeenten verplicht om bepaalde activiteiten in de ondergrond op te nemen in de Basisregistratie ondergrond (BRO). Ook Zwolle. De verschillende activiteiten zitten verspreid door de organisatie en worden gefaseerd ingevoerd. Zwolle is bronhouder geworden van de gegevens in de BRO en verantwoordelijk voor de kwaliteit van de gegevens en verantwoordelijk voor de actualiteit.

Een van de eerste stappen die gezet moeten worden door een bronhouder is het benoemen van een Coördinator ondergrond. Vanuit deze functie wordt de inbedding en vervolgens het beheer aangestuurd. Binnen Zwolle is een coördinator aangewezen. Vanuit zijn rol als Gebiedsbeheerder ondergrond (verantwoordelijk voor de kwaliteit van het grondwater onder Zwolle en de gebiedsgerichte aanpak van verontreinigingen) een logische keuze. Het zijn wel nieuwe activiteiten die moeten worden uitgevoerd waarvoor geen budget beschikbaar is en binnen de verschillende afdelingen moeten personen aangewezen gaan worden die de processen aanpassen zodat de activiteiten worden

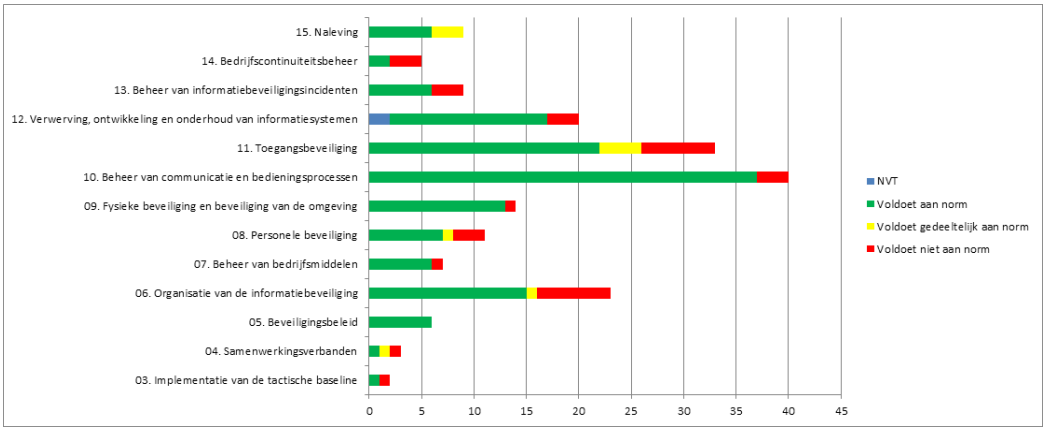
[3] Eenduidige Normatiek Single Information Audit, voor meer informatie ga naar www.ensia.nl
[4] Het zelfassessment over de BRO over 2018 was vrijwillig. Over 2019 wordt binnen ENSIA verplicht verantwoording afgelegd over de BRO.

opgenomen en de kwaliteit bewaken. Sturen zonder budget blijft lastig. Zijn taak was bewustwording creëren van de verplichtingen, inbedding van de eerste activiteiten en inzichtelijk maken welke effecten de invoering van de BRO op de organisatie heeft.

In 2018 zijn nog geen activiteiten ingevoerd in de BRO en nog geen processen aangepast. Wel is er bij de verschillende afdelingen een stukje bewustwording ontstaan maar ook zorg wat er op de afdelingen aan extra werkzaamheden afkomt. De bijgevoegde Ensia-enquête (in 2018 nog niet verplicht) is ingevuld en daar scoorde Zwolle 0 punten.

2.1.2 Baseline Informatiebeveiliging Gemeenten (BIG)

Deze paragraaf geeft een korte toelichting op de status van de BIG, omdat over DigiD en Suwinet apart verantwoording wordt afgelegd (ENSIA stukken). Ook voor de basisregistraties kent ENSIA eigen verantwoording.



Figuur 1: resultaat van het zelfassessment over de BIG

Over het algemeen mag gesteld worden dat de BIG op hoofdlijnen is ingevoerd binnen de gemeente Zwolle. Er zijn enkele zaken waarop de gemeente Zwolle eind 2018 te laag scoorde. Deze worden hieronder beknopt toegelicht, verbeterpunten zijn beschreven in het Jaarplan Informatiebeveiliging voor 2019.

Organisatie van de informatiebeveiliging

In beleid staat de organisatie van informatiebeveiliging goed beschreven (de theorie klopt). Echter, in de praktijk blijkt dit in onze organisatie nog niet goed geborgd te zijn. Een goed voorbeeld hiervan is ‘eigenaarschap’. In het nieuwe Strategisch informatiebeveiligingsbeleid wordt hieraan extra aandacht geschonken.

Een ander onderwerp waarop de gemeente Zwolle nog niet voldoende scoort is de omgang met Externe Partijen. Wat betreft (IT-)leveranciers is er in 2018 een grote stap voorwaarts gezet. Maar er zijn slechts mondjesmaat afspraken over informatiebeveiliging en privacy met de diverse Verbonden Partijen zoals bijvoorbeeld GBLT.

Personele beveiliging
In het BIG hoofdstuk dat gaat over personele beveiliging staan twee onderwerpen waar veel gemeenten mee worstelen. Allereerst het screenen van personeel, alvorens het in dienst te nemen. Tweede onderdeel is het in-, door- en uitstroomproces (IDU-proces) van medewerkers. Hierin moet geborgd zijn dat autorisaties zo worden ingericht dat fraude (met bijvoorbeeld geld of persoonsgegevens) voorkomen wordt. In 2018 is door het team Verbijzonderde Interne Controle onderzoek gedaan naar dit proces, waarbij substantiële tekortkomingen zijn geconstateerd. Dit rapport is een goed uitgangspunt voor verbetering van het proces.

Toegangsbeveiliging
Dat het IDU-proces niet op orde is (zie voorgaande) leidt automatisch tot een slechte score op toegangsbeveiliging. Pas als dit proces goed verloopt kan de gemeente Zwolle aantonen dat medewerkers beschikken over de juiste autorisaties tot systemen en gegevens (ook wel logische toegang genoemd).

De huidige regelingen van de gemeente Zwolle ten aanzien van BYOD en thuiswerken zijn voornamelijk gericht op het faciliteren van flexibel werken. De BIG eist dat een organisatie borgt dat dit veilig gebeurt en hiervoor instructies en richtlijnen opstelt.

Bedrijfscontinuïteit
Gemeente Zwolle heeft geen bedrijfscontinuïteitsplan. Vanwege toenemende ICT-perikelen is in 2017 een inventarisatie uitgevoerd, bedoeld om kritische processen in beeld te brengen. Vervolgens is geen verantwoordelijke voor dit proces aangewezen en zijn geen acties ondernomen om bedrijfscontinuïteit in te richten. Ontbreken van beleid en procedures kan leiden tot uitval van dienstverlening, wanneer zich een verstorende calamiteit voordoet. Voorts voldoet de gemeente Zwolle niet aan de eisen die gesteld worden in wetgeving vanuit de verschillende basisregistraties.

2.2 Beleid

Eén van de hoofdpunten van de BIG is informatiebeveiligingsbeleid. Dat is nodig om sturing te geven aan een veilige inrichting van de organisatie en haar informatievoorziening. Het informatiebeveiligingsbeleid van de gemeente Zwolle was verouderd. In 2018 is in samenwerking met Gemeente Kampen nieuw beleid tot stand gekomen.

2.2.1 Hoofdpunten

Waar het oude informatiebeveiligingsbeleid een weerslag was van het geldende normenkader, geeft het nieuwe beleid meer de visie weer waarom de gemeente Zwolle haar informatie wil beveiligen. Waarbij de nadruk ligt op toenemende aandacht voor het beschermen van persoonsgegevens. Gemeente Zwolle beschikt over veel persoonsgegevens, die door toenemende digitalisering steeds gemakkelijker benaderbaar zijn door veel medewerkers. Een goede inrichting van processen en systemen is daarom noodzakelijk om privacy van burgers te beschermen.

De BIG is gericht op het implementeren van maatregelen. Hiermee kunnen gemeenten de basis van hun informatiebeveiliging op orde brengen. Ons nieuwe beleid is gericht op de Baseline Informatiebeveiliging Overheid (BIO), die uitgaat van risicomanagement. Voor ieder proces en project geldt dat aan de basis moet worden voldaan, maar ook dat een risicoanalyse wordt uitgevoerd. Op basis van de uitkomst van die analyse wordt vervolgens besloten welke maatregelen worden ingericht om informatie te beveiligen.

Deze aanpak vraagt om een grotere verantwoordelijkheid van lijnmanagers. Zij geven opdracht tot het vernieuwen of wijzigen van processen of systemen. Dat maakt hen verantwoordelijk voor genoemde risicoanalyse. En zij dienen te bepalen welke risico's zij wel of juist niet wensen te verkleinen of te voorkomen.

2.2.2 Implementatie

December 2018 is het Strategisch informatiebeveiligingsbeleid vastgesteld door het college. Vanaf begin 2019 zal dit worden uitgedragen, onder andere door het onderwerp informatiebeveiliging te bespreken met alle managers van de gemeente Zwolle tijdens de zogenaamde Management Dialoog[5].

2.3 Organisatie van informatiebeveiliging

2.3.1 Personele zaken

In 2018 is de aandacht vooral uitgegaan naar het vergroten van bewustwording voor informatieveiligheid van de medewerkers.er is minder inzet geweest voor het uitvoeren van risicoanalyses.

2.3.2 Architectuurboard

Ter voorbereiding op de reorganisatie van de IV-kolom zijn enkele functionarissen in 2018 onder leiding van de informatie architect gestart met een zogenaamde Architectuurboard. Voordat nieuwe projecten op het gebied van informatievoorziening starten, dient een zogenaamde project startarchitectuur[6] opgeleverd te worden. Pas na bespreking in en goedkeuring door de Architectuurboard kan het project daadwerkelijk in gang worden gezet.

De eerste ervaringen in 2018 waren positief. De gestructureerde aanpak helpt het project bij het in kaart brengen van alle belangrijke aandachtspunten. De bespreking binnen de Architectuurboard vergroot de integrale aanpak van afzonderlijke disciplines binnen en project en de samenhang tussen projecten. Omdat de Architectuurboard nog geen formele status kent, bleek het lastig acteren wanneer binnen een project werd besloten af te wijken van het advies van de Architectuurboard.

[5] Deze en andere acties zijn opgenomen in het Jaarplan Informatiebeveiliging 2019.
[6] Een Project StartArchitectuur (PSA) is een projectdocument dat als hulpmiddel bij een project wordt ingezet om veranderingen te faciliteren. De PSA richt zich daarbij op kaders die op een project van toepassing zijn en de impact van deze kaders op de beoogde verandering. Bron: www.noraonline.nl.

2.4 Samenwerking

2.4.1 Zwolle-Kampen

De samenwerking tussen de gemeenten Kampen en Zwolle is in 2018 met succes geïntensiveerd. De beide gemeenten hebben gezamenlijk een nieuw Strategisch Informatiebeveiligingsbeleid vastgesteld. Ook rond het concreet implementeren van het beleid in praktische zaken was er in 2018 een toename waarneembaar van overleg over en invulling van een gezamenlijke aanpak.

2.4.2 Via het shared service centrum ONS

Eén van de zaken waarin de gemeenten Kampen en Zwolle steeds intensiever optrekken is de deelname aan het Breed Tactisch Overleg Securityboard van het SSC-ONS. In dat overleg worden de security aandachtspunten besproken die voor het SSC en haar partners van belang zijn.

2.4.3 GGI Veilig

Vanuit de VNG zou in 2018 een Europese aanbesteding voor IT-beveiligingsproducten worden gedaan. Dit biedt een aantal voordelen voor gemeenten. Allereerst vraagt deze aanbesteding om specifieke kennis en kunde. Door gezamenlijk op te trekken, zijn gemeenten in staat deze kennis en kunde zelf op te brengen. Een ander voordeel is de schaalgrootte. De verwachting is dat het gezamenlijke volume van veel gemeenten en gemeentelijke samenwerkingsverbanden een aanzienlijk prijsvoordeel oplevert.

Vanuit de gemeente Zwolle is een bijdrage geleverd aan de expertgroep die de aanbesteding en de bijbehorende documentatie en procedures voorbereid. Omdat de VNG tijdens de procedure juridische obstakels ontdekte, is de aanbesteding teruggetrokken om in 2019 opnieuw in de markt gezet te worden.

3 Privacy

3.1 AVG

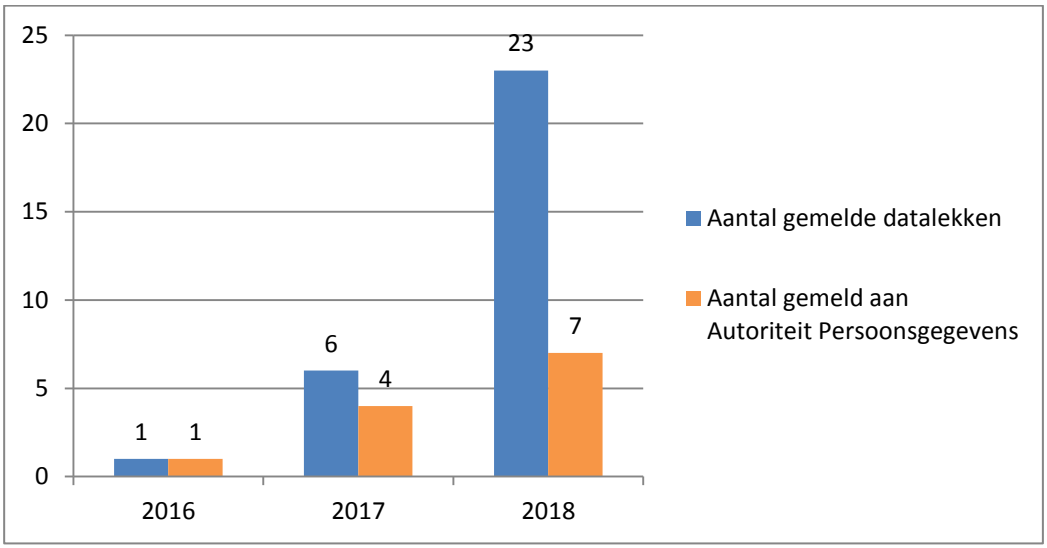
Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) als opvolger van de Wet bescherming persoonsgegevens (Wbp) van kracht geworden. De AVG is veelal niet nieuw, maar wel een aanscherping van de Wbp. Ook de mogelijkheid van de Autoriteit Persoonsgegevens als toezichthouder om (aanzienlijke) boetes op te leggen is vergroot. Als gevolg van de invoering van de AVG is de aandacht voor het onderwerp bescherming van persoonsgegevens sterk vergroot. Dit geldt met name voor de aandacht voor datalekken.

3.2 Datalekken

Ten aanzien van datalekken kan een onderscheid gemaakt worden tussen drie categorieën incidenten, te weten beveiligingsincidenten, datalekken en datalekken die gemeld moeten worden bij de Autoriteit Persoonsgegevens. Beveiligingsincidenten zijn gebeurtenissen waarbij de mogelijkheid bestaat op een inbreuk op de bescherming van persoonsgegevens. Voorbeelden hiervan zijn een virus, pogingen tot hacken of te ruime autorisaties. Van een datalek is sprake als er daadwerkelijk onrechtmatige toegang, verlies, wijziging, verstrekking of vernietiging van persoonsgegevens heeft plaatsgevonden.

Er is in 2018 een toename in de geregistreerde en gemelde datalekken. Deze is vooral te verklaren door de bewustwordingstrainingen die aan de medewerkers zijn gegeven. Medewerkers worden gestimuleerd om melding te maken van beveiligingsincidenten en datalekken zodat er op de juiste wijze gehandeld kan worden. Dit betreft bijvoorbeeld het tijdig doen van meldingen, maar ook het treffen van snelle technische maatregelen om verdere inbreuken te beperken. De geregistreerde datalekken zijn geëvalueerd en er is waar mogelijk vastgelegd met welke maatregelen ze een volgende keer voorkomen kunnen worden.

In 2018 hebben we 23 datalekken geregistreerd. In 2017 waren dit er 6 en in 2016 was dit er 1. Een datalek moet binnen 72 uur na ontdekking gemeld worden bij de Autoriteit Persoonsgegevens als er sprake is van een aannemelijk risico op een inbreuk op de rechten en vrijheden van natuurlijke personen. In 2018 hebben we 7 datalekken gemeld. In 2017 waren dit er 4 en in 2016 1.



Figuur 2: aantal gemelde datalekken

3.3 Training

Gemeentebreed is een bewustwordingstraining opgezet om bij medewerkers aandacht te vragen voor het op een juiste manier omgaan met persoonsgegevens en veilig werken. In het voorjaar van 2018 hebben vier medewerkers (twee adviseurs op het gebied van privacy en twee adviseurs op het gebied van informatiebeveiliging) de bewustwordingstraining “Werk Veilig & (Gast)Vrij” ontwikkelt en zijn ze gestart met het geven van deze training aan alle medewerkers in de organisatie. Dat verloopt met enthousiasme en naar volle tevredenheid. De reacties op de training zijn erg positief. Inmiddels worden de laatste groepen gepland. In de trainingen wordt door medewerkers echter ook regelmatig aangegeven dat wat in de training qua gedrag van medewerkers gevraagd wordt, niet gefaciliteerd wordt door de organisatie. Issues die daarbij naar voren komen zijn bijvoorbeeld de inrichting van de kantoren en de (on-)mogelijkheid om vertrouwelijke gesprekken en telefoongesprekken te voeren en de inrichting van autorisaties. Om ervoor te zorgen dat bewust en veilig werken in overeenstemming met de AVG blijvend wordt nageleefd, is het van belang dat de geconstateerde knelpunten worden aangepakt.

3.4 Onderzoek BMC

In augustus 2018 is door BMC een onderzoek uitgevoerd naar de implementatie van de AVG. BMC heeft het rapport ‘Persoonsinformatie en Privacy’ opgeleverd. De conclusie van het rapport is dat we op weg zijn naar een adequaat uitvoeringsniveau van de AVG, maar dat er nog het nodige te doen valt om dat te bereiken. We zijn nog niet ‘compliant’, maar we hebben de risico’s in beeld en we werken eraan om deze uit te schakelen / zo klein mogelijk te maken.

De belangrijkste constateringen uit het rapport worden onderschreven. Organisatie brede bewustwording ten aanzien van privacy moet groeien, dat is niet een traject wat we binnen een jaar voor elkaar hebben. Bescherming van persoonsgegevens is ieders

verantwoordelijkheid en dat bewustzijn moet groeien. We herkennen ook dat we als afdeling Juridische Zaken keuzes moeten maken - het rapport bevat 45 aanbevelingen - hoe intensief we de implementatie en het structureel inbedden en toetsen van privacy aspecten op gaan pakken. Juridische Zaken komt niet aan de door BMC minimaal geadviseerde capaciteit om de prioriteiten te gaan coördineren en (laten) uitvoeren. Dit heeft consequenties voor de looptijd van de implementatie en de volledigheid van de daarna in te voeren ‘plan-do-check-act’ cyclus.

Vanuit BMC hebben we 45 aanbevelingen gekregen waar actiehouders (overwegend Privacy Officer of Functionaris Gegevensbescherming) aan zijn gekoppeld. Van de 45 aanbevelingen zijn er inmiddels 14 afgehandeld. Een groot aantal andere aanbevelingen is in gang gezet of er is de keuze gemaakt om, gelet op de beperkte capaciteit, deze vooralsnog niet op te pakken. Pas na invoering of uitvoering van deze acties en aanbevelingen kunnen we overschakelen naar de ‘plan-do-check-act-fase’ in haar volle omvang.

3.5 Suwinet

In 2018 is er geen controle geweest op het gebruik van Suwinet door ambtenaren van de gemeente Zwolle. Verantwoording hierover heeft plaatsgevonden binnen het ENSIA-proces.

4 Bewustwording

De AVG, het normenkader Suwinet, diverse baselines – elk stuk wet- en regelgeving op gebied van informatiebeveiliging en privacy eist van organisaties dat zij werken aan bewustwording. Duidelijk maken wat de kaders zijn, maar ook handreikingen geven hoe medewerkers binnen die kaders hun taken uit kunnen en mogen voeren. In 2018 kreeg dit onderwerp op verschillende manieren vorm.

4.1 Trainingen

Belangrijkste onderdeel vormde de training Informatiebeveiliging en Privacy onder de paraplu ‘Werk veilig en (gast)vrij’. Deze training is door het MTZ in de zomer van 2017 verplicht gesteld voor alle medewerkers.

4.1.1 Voorbereiding

De functionaris gegevensbescherming, de privacy officer, de adviseur informatiebeveiliging en de adviseur informatisering hebben de trainingen goed voorbereid en uitgevoerd. De basis hiervoor is wet- en regelgeving, maar ook is er uitgebreid aandacht besteed aan de dagelijkse praktijk (zie ook hoofdstuk 5 Incidenten) en zijn de resultaten van testen gebruikt.

Eind 2017 zijn er enkele proeftrainingen/workshops gehouden. Op basis daarvan is besloten de workshops door eigen personeel te laten geven. De aansluiting tussen de groep en de trainers die hierdoor ontstaat had namelijk een sterk positief effect op het uiteindelijke resultaat.

Gaandeweg het traject was er veelvuldig samenwerking met HR. Dit heeft ertoe geleid dat diverse workshops onder één paraplu zijn gehangen. Omdat alle workshops gericht zijn op gedrag van medewerkers; informatiebeveiliging en privacy evengoed als feedback geven en het nieuwe werken. Dit leidde ertoe dat begin 2018 de trainers van al deze afzonderlijke workshops een door HR georganiseerde cursus ‘train de trainer’ hebben gevolgd. De kennis en ervaring die hierdoor werd opgedaan kon direct worden vertaald naar een nog betere workshop informatiebeveiliging en privacy.

4.1.2 Workshops

De workshops zelf zijn voor een groot deel in 2018 georganiseerd. Daarmee zijn zo’n 650 medewerkers bereikt. In 2019 volgt het overige deel van het personeel, inclusief de medewerkers voor wie het niet mogelijk was om samen met hun team deel te nemen en medewerkers die later bij de gemeente Zwolle zijn komen werken.

Aandachtspunt is het plannen en organiseren van de trainingen. Het praktische deel hiervan is belegd bij het SSC-ONS. Zodat aan de hand van de personeelsadministratie kan worden vastgelegd of deze heeft deelgenomen. Het afstemmen van de wensen van trainers vergde meer aandacht dan vooraf ingeschat. Voordeel is dat een review onderdeel is van het instrumentarium van ONS. Daaruit bleek dat de trainingen over het algemeen goed worden gewaardeerd door de medewerkers van de gemeente Zwolle.

4.1.3 Gevolgen

Gevolg van de workshops is een toename van vragen aan de adviseurs, omdat medewerkers in hun dagelijks werk zorgvuldig willen omgaan met persoonsgegevens of andere vertrouwelijke gegevens. Ook zien we een toenamen van incidentmeldingen. Niet omdat het aantal incidenten toeneemt, maar omdat medewerkers sinds de training weten wanneer een gebeurtenis een incident is en waar zij dit kunnen en moeten melden.

Uiteraard leveren de workshops ook input op voor de organisatie. Een deel kan door de trainers meegenomen worden in het dagelijkse werk. Een ander deel komt in 2019 aan de orde, als de trainers een evaluatie willen bespreken met het MTZ.

Enkele maanden na afloop van de workshops krijgen medewerkers de uitnodiging om vrijwillig twee maanden mee te spelen met Knowingo. Dit is een quiz app die door de gemeente Zwolle wordt ingezet om de aangeboden onderwerpen nogmaals onder de aandacht te brengen. Gedachte hierachter is dat de onderwerpen dankzij het spelen van korte quizzen beter beklijven. Doordat medewerkers enkele keren per dag of week even kort na moeten denken over informatiebeveiliging en privacy. Knowingo is november 2018 uitgerold en wordt tot en met oktober 2019 ingezet.

4.2 Communicatie

Op intranet van de gemeente Zwolle is in 2018 verschillende keren aandacht gevraagd voor informatiebeveiliging en privacy. Soms vanwege een incident, andere keren om nieuwe ontwikkelingen onder het voetlicht te brengen. Een deel verscheen in de vorm van een blog, andere als tip of als artikel.

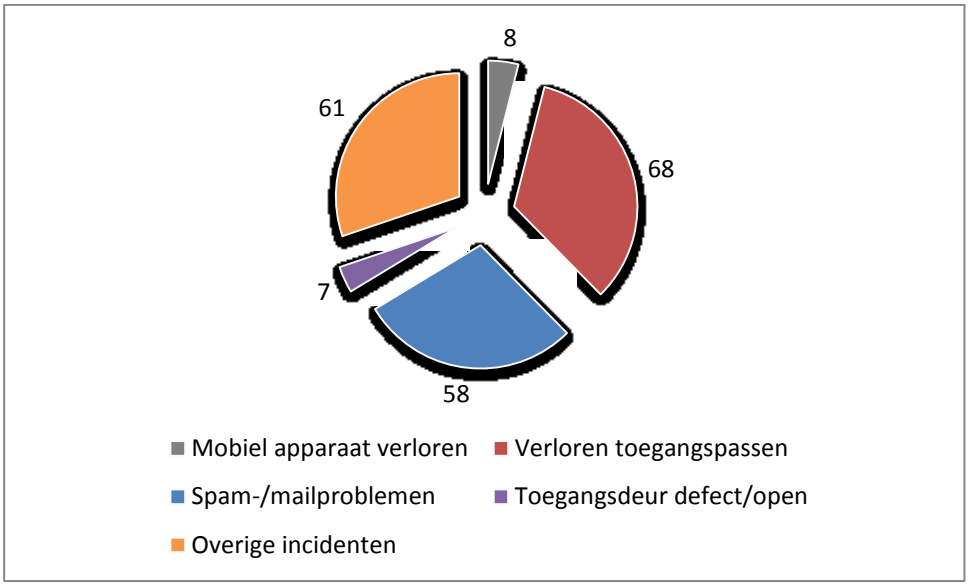
5 Incidenten

Ook bij de gemeente Zwolle gaan wel eens dingen mis. In een aantal gevallen is er sprake van een incident. Dit hoofdstuk gaat kort in op de beveiligingsincidenten die in 2018 hebben plaatsgevonden.

5.1 Beveiligingsincidenten

Van de incidenten die in 2018 zijn gemeld zijn 202 aangemerkt als informatie-beveiligingsincident. De tabel hieronder toont de verdeling naar categorieën. Sommige beveiligingsincidenten hebben geleid tot een datalek. Deze zijn in hoofdstuk 3 Privacy toegelicht.

Wat niet in het overzicht staat zijn meldingen ‘ vergeten wachtwoord’ of een ‘gelocket account’ (door te vaak onjuist wachtwoord intypen). In 2018 zijn over deze beide soorten incidenten 4015 meldingen gedaan. Formeel zijn dit informatiebeveiligings-incidenten, omdat een medewerker op zo’n moment geen toegang meer heeft tot het eigen account.



Figuur 3: aantal informatiebeveiligingsincidenten naar categorie

5.1.1 Overige incidenten

De kop ‘overige incidenten’ bevat een breed scala van gebeurtenissen. Een aantal ervan lichten we hier toe.

Wat helaas nog steeds voorkomt is het delen van persoonlijke accountgegevens (inlognaam en wachtwoord) met collega's. Soms gebeurt dit zelfs op verzoek van een leidinggevende. Door de toename van digitaal werken neemt het risico op misbruik van accountgegevens toe. Dit onderwerp heeft daarom specifieke aandacht gekregen binnen de verplichte training over veilig werken.

In een aantal gevallen is het nodig geweest om bij ziekte toegang te verschaffen tot een mailbox om een afwezigheidsassistent te activeren. Dit vraagt om aanscherping van onze digitale hygiëne. Het is fijner wanneer een collega zelf het initiatief neemt een andere collega te machtigen tot een mailbox. Dit voorkomt dat bij plotselinge, langdurige afwezigheid met toestemming van de gemeentesecretaris moet worden 'ingebroken' op het account van de medewerker om zakelijke mails te kunnen lezen en/of een afwezigheidsassistent in te stellen. Ook dit wordt besproken tijdens de eerder genoemde training.

Ook de gemeente Zwolle was in 2018 slachtoffer van een zogenaamde Microsoft scam. Dit incident maakte duidelijk dat ons netwerk goed is beveiligd tegen het installeren van illegale software door malafide derden. Uit voorzorg heeft dit geleid tot acute aanscherping van externe toegang door het SSC. De wijze waarop dit is doorgevoerd en de communicatie hierover tussen SSC-ONS en Zwolle kan beter.

In 2018 was CEO-fraude regelmatig in het nieuws, mede vanwege berichten over een bedrijf dat voor 19 miljoen euro schade leed. Aan de hand van dit voorbeeld is extra gecommuniceerd binnen de organisatie. Mede hierom is een CEO-fraudemail die de gemeente Zwolle in 2018 ontving tijdig herkent, waardoor de gemeente Zwolle geen financiële schade heeft geleden. In overleg met de Informatiebeveiligingsdienst van de VNG is besloten dit incident te melden bij de Fraudehelpdesk en de Politie.

Medewerkers melden het verlies van zakelijke telefoons en van toestellen die via de BYOD-regeling zijn aangeschaft. Omdat gebruiker anders geen nieuw toestel of nieuwe SIM-kaart ontvangen. Echter, wanneer een privé telefoon of tablet kwijtraakt, waarmee men toegang had tot e-mail en/of agenda met het gemeentelijk account, kan er ook sprake zijn van een datalek. Het is de vraag of in zo’n geval het verlies van privételefoons wordt gemeld. Om gemeentelijke data beter te kunnen beschermen wordt met het SSC-ONS gesproken over betere databescherming voor mobiele apparaten.