rekenschap

Zwolle

Advies

Stadskantoor
Lübeckplein 2
Postbus 538
8000 AM Zwolle
Telefoon (038) 498 2240
www.zwolle.nl

Jaarverslag informatiebeveiliging

Meer grip op informatieveiligheid en privacy

Opdrachtgever	College van B&W
Opdrachtnemer	Marrie Hol, CISO
Versie	0.9
Datum	4 april 2017

Datum 5 april 2017
Ons kenmerk Jaarverslag informatiebeveiliging

Inhoud

Datum 5 april 2017
Ons kenmerk Jaarverslag
informatiebeveiliging

1 Inleiding

Voor u ligt het Jaarverslag Informatiebeveiliging van de gemeente Zwolle. De titel “Meer grip op informatieveiligheid en privacy” duidt op het verbeteringsproces dat in 2016 in gang is gezet en in 2017 verder zal worden uitgebouwd. Informatieveiligheid en privacy zijn geen nieuwe begrippen voor gemeenten. Toch krijgen ze meer aandacht in de organisatie en in de media, omdat verdere digitalisering van werkprocessen en systemen andere uitdagingen met zich meebrengen.

Daarnaast werd en wordt wet- en regelgeving strikter. Naast invoering van de Baseline Informatiebeveiliging Gemeenten is in 2016 de Wet bescherming persoonsgegevens aangescherpt middels de Wet Datalekken. Hiermee loopt de Nederlandse overheid vooruit op de invoering van de Europese vervanger van de Wet bescherming Persoonsgegevens, de GDPR (General Data Protection Regulation) in 2018. Deze Europese privacywetgeving stelt striktere eisen aan persoonsregistraties en de organisaties die hiermee werken.

Deze verscherpingen zijn niet zonder reden. Meer en meer wordt informatie van burgers digitaal opgeslagen. Omdat de burger zelf vaak geen weet heeft waar welke data wordt opgeslagen, is het steeds lastiger een beeld te krijgen van die gegevens. Maar door het koppelen van al die digitale datasets kunnen bedrijven en overheden wel steeds meer informatie over burgers (en hun gedragingen) opslaan en gebruiken, maar soms ook voorspellen. Naast kansen brengt deze ontwikkeling ook risico’s met zich mee. De gedachte is dat strikte regelgeving deze risico’s beperkt en de burger een sterkere positie geeft richting overheden en bedrijven.

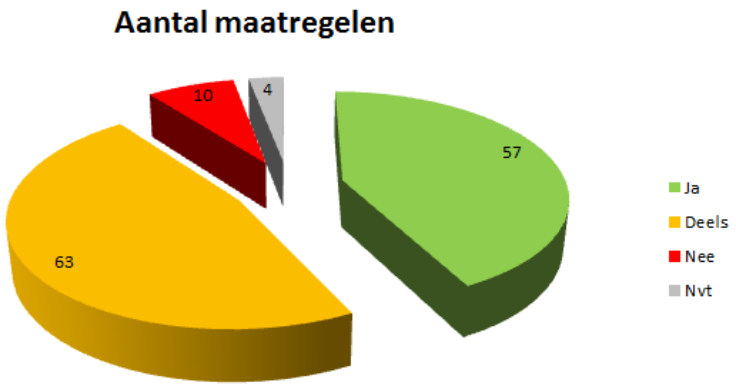
Ook de gemeente Zwolle heeft met deze ontwikkeling te maken. Hierom is in 2013 het informatiebeveiligingsbeleid aangescherpt en zijn in 2014 een FG (Functionaris Gegevensbescherming: interne privacy toezichthouder) en een CISO (Corporate/Chief Information Security Officer: interne toezichthouder op informatieveiligheid) aangesteld. Samen met andere spelers in de organisatie werken zij aan het verstevigen van informatiebeveiliging en privacy in het algemeen en specifiek binnen gemeentelijke processen waarin veel gebruik wordt gemaakt van (soms zeer gevoelige) persoonsgegevens.

In 2016 is een integraal Informatiebeveiligingsplan vastgesteld door het MTZ. Daarin staan diverse acties genoemd die de gemeente Zwolle aan zou pakken om informatieveiligheid en privacy nog beter te borgen. Als rapportage geeft voorliggend jaarverslag geeft – volgens eenzelfde hoofdstukindeling – een overzicht van de behaalde resultaten.

Marrie Hol,
Chief Information Security Officer

2 Implementatie BIG

De Baseline Informatiebeveiliging Gemeenten (BIG) omvat ruim 300 maatregelen, onderverdeeld in 134 hoofdgroepen, die er samen voor zorgen dat de informatiebeveiliging ‘in de basis’ op orde komt. Voor specifieke processen of systemen zijn bovenop deze basis nog aanvullende maatregelen nodig. Het implementeren van de BIG dient eind 2017 op orde te zijn, waarna conform de PDCA-cyclus de basis op orde gehouden moet worden.



Figuur: binnen Zwolle geïmplementeerde BIG-maatregelen eind 2016

De BIG beslaat een aantal terreinen. Het doorvoeren van maatregelen op het gebied van ICT is in 2016 niet zo vlot verlopen als vooraf verwacht. Bij de uitvoering van haar taken heeft het SSC-ONS vooral veel energie moeten steken in het verhelpen van verstoringen en het borgen van de dienstverlening. Niet alle gewenste wijzigingen en verbeteringen zijn hierom doorgevoerd. Anderzijds hebben de storingen wel extra risico’s opgeleverd ten aanzien van informatieveiligheid. Het is niet uit te sluiten dat medewerkers – om toch door te kunnen werken – extra gebruik hebben gemaakt van clouddiensten die volgens de richtlijnen van de Nederlandse overheid niet als veilig mogen worden beschouwd. Gelukkig zijn bij de gemeente Zwollen geen incidenten gemeld waaruit zou blijken dat hierdoor onzorgvuldig is omgegaan met vertrouwelijke (persoonsgegevens) van de gemeente Zwolle.

Een ander belangrijk aandachtpunt is het onderwerp personele beveiliging. Binnen dit onderwerp zijn vooral de thema’s screening, introductie en toegang van belang. In 2016 is gestart met een gemakkelijker wijze van aanvragen van Verklaring Omtrent Gedrag (VOG). Zorgen dat voor de juiste functies een VOG wordt aangevraagd (aanscherpen van het beleid rond vertrouwensfuncties) zal in 2017 plaatsvinden, evenals het creeren en borgen van bewustzijn rond informatieveiligheid bij nieuwe en bestaande medewerkers van de gemeente Zwolle.

In 2016 is een begin gemaakt met het uitvoeren van BIG-gerelateerde risicoanalyses. De resultaten hiervan hebben geresulteerd in strakkere afspraken met leveranciers rond

beschikbaarheid en/of beveiliging van webbased software. Helaas is het uitvoeren van risicoanalyses aan de start van nieuwe projecten nog geen gemeengoed, in 2017 zal meer aandacht geschonken worden aan ‘security by design’ en ‘privacy by design’. Vooraf goed nadenken over risico’s en bijbehorende maatregelen is namelijk effectiever (en minder tijdrovend) dan achteraf repareren van kwetsbaarheden.

2.1 Beleid

Diverse activiteiten rondom informatiebeveiliging zijn gebaseerd op het Informatiebeveiligingsbeleid van de gemeente Zwolle. Dit is een overkoepelend beleid voor een grote diversiteit aan activiteiten. Om praktische uitvoering te kunnen geven aan deelgebieden van dit beleid is in oktober 2016 een aantal besluiten genomen door het MTZ, gericht op digitaal veilig en duurzaam kunnen blijven werken. Belangrijke zijn het autorisatiebeleid en de aanpak voor dataclassificatie.

Met het vaststellen van het autorisatiebeleid en de aanpak voor dataclassificatie is een start gemaakt met een belangrijke stap voor de BIG, de Baseline Informatiebeveiliging Gemeenten. Voor beide is het van belang te weten wie de eigenaar is van een systeem, proces of set gegevens. En beide vragen om een goede classificatie van de inhoud door die eigenaar en daarop gebaseerde toegang tot systemen en informatie. Alleen op deze wijze kan de gemeente gestructureerd de toegang tot haar kroonjuwelen – gevoelige informatie – goed inrichten en beheersen.

2.2 Incidenten

Op het gebied van informatiebeveiliging zijn er in 2016 circa 140 incidenten gemeld bij de Servicedesk van de gemeente Zwolle. Voor een organisatie van onze omvang is dit een laag aantal. Dit heeft drie belangrijke oorzaken.

1. Nog niet iedere medewerker is zich ervan bewust dat incidenten gemeld moeten worden. En ook niet iedereen is ervan op de hoogte welke situaties als incident aangemerkt worden. We communiceren hierover via intranet, maar daarmee wordt nog niet iedere medewerker bereikt.
2. Het vergeten van wachtwoorden of het locken van een systeem door het te vaak intypen van een verkeerd wachtwoord wordt niet geregistreerd als beveiligingsincident. Maar beide situaties komen wel degelijk voor in onze organisatie. In 2016 is 1672 maal een wachtwoordreset uitgevoerd en 2685 maal was het nodig om een unlock uit te voeren.
3. Het SSC gebruikt een eigen incidentmanagementsysteem, waardoor de daar gemelde incidenten niet in beeld zijn in de Zwolse omgeving.

Het eerste punt wordt in 2017 meegenomen als we actief aan de slag gaan met bewustwording. Voor het tweede punt ligt er een verzoek bij het SSC-ONS. Gevraagd is een voorziening in te richten waarmee medewerkers zelf hun wachtwoord kunnen wijzigen, zoals dat ook op veel websites het geval is. Hiermee komt het beheer van wachtwoorden in handen van de medewerker zelf te liggen en wordt de Servicedesk

ontlast. De sterkte van wachtwoorden zal door het systeem afgedwongen worden. Het derde punt vraagt om afstemming tussen de partners.

De overige 140 meldingen lopen uiteen van het niet afsluiten van containers voor vertrouwelijke papiervernietiging tot het verdwijnen van laptops en smartphones. Het is nog niet mogelijk deze meldingen in een goed overzicht te zetten, de huidige indeling in categorieën is hiervoor niet ingericht. Hierdoor is er voor het maken van een helder overzicht is teveel handwerk nodig. Om in de toekomst wel dit overzicht te hebben, schenkt de Servicedesk in 2017 aandacht aan de wijze van registreren.

In het overzicht zijn beveiligingsincidenten die gemeld worden bij het SSC-ONS niet meegenomen. De veranderende wijze van registreren van meldingen binnen het SSC-ONS voorziet niet in het verstrekken van overzichten van beveiligingsincidenten.

3 Visitatiecommissie Informatieveiligheid

De Visitatiecommissie Informatieveiligheid is opgericht naar aanleiding van de resolutie die in november 2013 op de Buitengewone Algemene Ledenvergadering van de VNG werd aangenomen. De Visitatiecommissie zou moeten toetsen of de 'verplichtende zelfregulering' voldoende werkt en of gemeenten voldoen aan de basisnormen die zijn vastgelegd in de BIG, de Baseline Informatiebeveiliging Gemeenten.

Op 21 september 2016 bezocht de visitatiecommissie de gemeente Zwolle en sprak met wethouder Jan Brink, MTZ-lid Bernard Mencke en de Informatiemanager en CISO Marrie Hol. Het verslag van dit bezoek is als bijlage gevoegd bij dit jaarverslag. Uit het verslag komen drie belangrijke zaken naar voren.

3.1 Houd oog voor de actuele ontwikkelingen en deel kennis

Zwolle werkt professioneel aan informatieveiligheid, terwijl de omgeving continue en snel verandert. Dit betekent onder meer het belang om te investeren op de benodigde (technische) kennis en applicaties. Daarbij kan gedacht worden aan het realtime monitoren en analyseren van het dataverkeer, zoals Zwolle dat op dit moment al doet. De Commissie raadt Zwolle aan om dergelijke initiatieven voort te zetten om technisch bij te kunnen blijven. Tegen de achtergrond dat informatieveiligheid een randvoorwaarde is om de privacy van haar inwoners te borgen, is het belang toenemend om cyberdreigingen te kunnen duiden, tegenmaatregelen te kunnen adviseren en inzicht te houden in actuele risico's. Desgewenst kan Zwolle samenwerking en aansluiting zoeken met andere gemeenten (bijvoorbeeld in de regio, in het geval van Zwolle bijvoorbeeld in het shared service center met Kampen en de Provincie Overijsel), overigens zonder dat dit haar van haar individuele verantwoordelijkheid onder de BIG ontslaat. De Commissie roept Zwolle op om haar analyses en inzichten op basis van realtime monitoring te delen in IBD-verband. Langs deze weg kan Zwolle een voortrekkersrol (blijven) vervullen op het gebied van informatieveiligheid.

3.2 Sluit tot en met stap 4 aan bij de IBD

Zwolle is tot en met stap 2 aangesloten bij de IBD. De Commissie benadrukt het belang om tot en met stap 4 aan te sluiten bij de IBD, hetgeen Zwolle onderschrijft. Aansluiting tot en met stap 4 stelt de IBD in staat om gericht te waarschuwen bij concrete incidenten/dreigingen. Gemeenten krijgen zo meer inzicht in incidenten die zich bij collega-gemeenten hebben voorgedaan. Dit kan bovendien het bewustzijn verder vergroten. Ten slotte benadrukt de Commissie dat, na aansluiting tot en met stap 4, de ICT-foto periodiek dient te worden geüpdatet, omdat de ICT omgeving bij de gemeente continue zal blijven veranderen. De Commissie raadt aan om het periodiek updaten van de ICT foto te borgen in de werkprocessen van de gemeente Zwolle.

3.3 Werk in nog sterkere mate op systematische wijze aan informatieveiligheid

Zwolle geeft aan dat zij het informatieveiligheidsbeleid op dit moment herziet en een hoog ambitieniveau heeft. De Commissie benadrukt om vanuit het beleid en haar ambitie de bijbehorende concrete acties en prioriteiten te benoemen. Door een structurele agenda en actieplannen kan Zwolle scherp voor ogen te houden wat zij in een bepaalde periode beoogt te realiseren. Het is bovendien van belang om het sturen op de realisatie/voortgang (door middel van Plan-Do-Check-Act) te verankeren in de organisatie door de verbinding te leggen tussen managementinformatie uit ISMS en de P&C cyclus. Dit is een belangrijke stap naar een verdere, nog meer systematische, manier van werken aan informatieveiligheid binnen de gemeente Zwolle. Dit voorkomt dat het werken van aan informatieveiligheid te veel ad hoc of op basis van concrete incidenten is georganiseerd.

4 Veilige gegevensuitwisseling Suwinet

Dit hoofdstuk van het jaarverslag is een bijdrage onder verantwoordelijkheid van de Security Officer Suwinet.

4.1 Drie aansluitingen met samen ruim 130 gebruikers

De gemeente Zwolle beschikt over drie verschillende aansluitingen op Suwinet, met in totaal meer dan honderd gebruikers. Het systeem is primair bedoeld voor UWV, SVB en gemeentelijke sociale diensten. Daarnaast gebruiken ook andere overheidsorganisaties Suwinet. Binnen de gemeente Zwolle behoren de adresonderzoekers van Burgerzaken en de belastingdeurwaarders tot die ‘andere’ overheidsorganisaties. Beide gebruikersgroepen hebben een eigen aansluiting op Suwinet. Ook RMC-medewerkers (leerplicht) gebruiken Suwinet, zij liften mee op de aansluiting ‘gemeentelijke sociale dienst’.

Naast de drie intern gebruikte aansluiting is er formeel een vierde aansluiting van de gemeente Zwolle op Suwinet. Deze betreft de informatie-uitwisseling tussen het UWV en het incassobureau Cannock Chase. Deze firma voert voor de gemeente specifieke incassodiensten uit, waarvoor zij inzage nodig heeft in gegevens van betreffende burgers. Hoewel Cannock Chase hierom formeel gebruik maakt van een aansluiting van de gemeente, valt zij niet onder het toezicht van de gemeentelijke Security Officer Suwinet, aangezien Cannock Chase werkzaamheden uitvoert voor meerdere gemeenten. Deze firma heeft een auditverplichting en legt zelfstandig verantwoording af aan het UWV.

4.2 Verdwijnen eenheden

Vanwege het verdwijnen van de eenheden en vanwege verschuiving van functies zijn een aantal procesbeschrijvingen en werkinstructies voor het gebruik van Suwinet aangepast. Bij het vormgeven van processen is gekeken naar de zaken die tijdens de audits als goed zijn bestempeld. Deze zijn als basis gebruikt bij het inrichten van de definitieve processen. November 2016 heeft het MTZ alle voorstellen bekrachtigd.

4.3 Controles

Toegang tot Suwinet verloopt volgens een door het MTZ vastgesteld protocol en volgens een door het MTZ vastgestelde autorisatiematrix. Een Interne Controle Functionaris ziet toe of deze procedure gevolgd wordt. Hierover wordt eens per kwartaal gerapporteerd aan de Security Officer Suwinet.

Iedere handeling in het systeem Suwinet wordt vastgelegd. Op basis van dit gebruik stelt het BKWI (beheerder van Suwinet en onderdeel van het UWV) een rapport op over het gebruik per gemeente. In 2016 heeft de Security Officer Suwinet per aansluiting tweemaal zo’n rapport opgevraagd. Uit de rapportages is geen onrechtmatig gebruik gebleken.

Ook is er een data analyse uitgevoerd. Meer hierover staat beschreven onder het programma ‘Borging veilige gegevensuitwisseling Suwinet’.

4.3.1 EDP-audit

Jaarlijks laat de gemeente Zwolle het gebruik van Suwinet beoordelen door een EDP-auditor[1]. Ook in 2016 is zo’n audit uitgevoerd, waarbij gekeken worde naar het Suwinet gebruik in 2015. Als leidraad gelden de normen uit het Normenkader Gezamenlijke elektronische Voorzieningen SUWI (GeVS).

Hoewel er door de auditor een aantal opmerkingen zijn geplaatst, is de algemene conclusie dat wij voldoende scoren op de volledige reeks van ruim 100 normen. Er is geen verplichting tot verbetering opgelegd naar aanleiding van de auditrapportage.

4.4 Borging veilige gegevensuitwisseling Suwinet

UWV, SVB en VNG zijn samen gestart met het programma ‘Borging veilige gegevens-uitwisseling Suwinet’. Via VNG/KING zijn alle Nederlandse gemeenten hierbij betrokken. Vanuit dit programma worden diverse maatregelen uitgerold, zoals het aanbieden van een autorisatiematrix, het opstellen van een nieuw normenkader (ingaande per 2017) en het invoeren van een whitelist.

4.4.1 Whitelist en data analyse

De whitelist houdt in dat medewerkers van een gemeente alleen BSN’s mogen raadplegen van burgers die reeds als cliënt in de gemeentelijke administratie voorkomen. Voor een aantal taken is dit echter lastig, omdat deze betrekking kunnen hebben op burgers die nog niet als cliënt staan geregistreerd. Denk aan intake aan de poort of taken van de Sociale Recherche. Aangezien een deel van deze taken voor de regio worden uitgevoerd, kan deze maatregel voor medewerkers van de gemeente Zwolle veel impact hebben.

Om deze impact in beeld te brengen is opdracht gegeven tot een data analyse. Hiervoor vergelijken we BSN’s van klanten met BSN’s die in Suwinet geraadpleegd zijn (over een periode van een half jaar). Op basis van deze vergelijking kan de impact van de invoering van de whitelist bepaald worden.

De analyse zal naar verwachting in beeld brengen hoe we de informatie voor de whitelist moeten aanleveren en duidelijk maken voor welke medewerkers het noodzakelijk is om ook niet-cliënten te raadplegen. Deze analyse is eind 2016 in gang gezet en zal naar verwachting in het eerste kwartaal van 2017 afgrond worden.

[1] Een EDP-auditor (= auditor van Electronic Data Processing, ook IT-auditor genoemd) beoordeelt de betrouwbaarheid, beveiliging, effectiviteit van geautomatiseerde informatiesystemen en de organisatie van de ICT het proces dat met die ICT-middelen werkt. Doel is het beoordelen of de verantwoordelijke ‘in control’ is.

4.5 Bewustwording

De Security Officer Suwinet is eind 2015 gestart met kennismaken met de verschillende afdelingen/teams die gebruik maken van Suwinet. In 2016 is dit voortgezet. Aanvullend hierop is op verzoek van de afdelingen in 2016 een start gemaakt met bewustwordingsbijeenkomsten medewerkers die in dienst treden of van functie veranderen en gebruik gaan maken van Suwinet. Zij worden gewezen op de gevoeligheid van de gegevens in het systeem en de richtlijnen die gelden voor het gebruik van het systeem. Hierbij wordt onder meer gebruik gemaakt van filmpjes die de VNG beschikbaar stelt vanuit het programma ‘Borging veilige gegevensuitwisseling Suwinet’.

5 Veilig gebruik van persoonsgegevens

Dit hoofdstuk van het jaarverslag is een bijdrage onder verantwoordelijkheid van de Functionaris Gegevensbescherming.

Met ingang van 1 januari 2016 heeft de Wet bescherming persoonsgegevens een aantal belangrijke wijzigingen ondergaan. Deze veranderingen dwingen organisaties om aantoonbaar zorgvuldig om te gaan met persoonsgegevens. Zo is er steeds meer aandacht voor de bewerkersovereenkomsten en is de meldplicht datalekken ingevoerd.

5.1 Bewustwording

In 2016 hebben we geïnvesteerd in het vergroten van het bewustzijn van medewerkers ten aanzien van het zorgvuldig omgaan met persoonsgegevens. Dit hebben we gedaan door middel van berichten op intranet, presentaties bij afdelingsoverleggen en een lunchbijeenkomst. Hierin werd de basis van de Wet bescherming persoonsgegevens uitgelegd en aangegeven hoe medewerkers op een zorgvuldige manier met persoonsgegevens om kunnen gaan.

5.2 Meldplicht datalekken

Om aan de meldplicht datalekken te voldoen hebben we binnen de organisatie diverse kanalen opgezet voor het doen van een melding van een datalek. Zo is het emailadres datalek@zwolle.nl aangemaakt en is het mogelijk een melding in Topdesk te doen. Medewerkers hebben we op bovenstaande wijze geïnformeerd over het herkennen en voorkomen van datalekken. Onder meer door het geven van voorbeelden van datalekken en de oproep aan medewerkers om een dergelijk incident zo snel mogelijk te melden.

5.3 Bewerkersovereenkomsten

Wanneer een leverancier van software, applicaties of systemen persoonsgegevens verwerkt en of toegang heeft tot onze persoonsgegevens dient er, naast de hoofdovereenkomst, een bewerkersovereenkomst te worden gesloten met de leverancier. Hierin wordt onder andere vastgelegd dat de leverancier, oftewel de bewerker, geen zelfstandige zeggenschap heeft over de gegevens en worden er eisen gesteld aan de beveiliging van de gegevens. In 2016 hebben we een standaard bewerkersovereenkomst gemaakt, deze fungeert als uitgangspunt bij nieuw af te sluiten bewerkersovereenkomsten. Het doel is om in 2017 het afsluiten van bewerkersovereenkomsten bij nieuwe contracten te continueren, maar ook om voor bestaande hoofdovereenkomsten bewerkersovereenkomsten af te sluiten.

6 Audits en zelftesten

Jaarlijks laat de gemeente Zwolle diverse audits uitvoeren. Daarnaast zijn er diverse verplichte zelftesten om te bepalen of de informatiehuishouding op orde is. Dit hoofdstuk vat kort samen welke taken er in 2016 op dit gebied zijn uitgevoerd.

6.1 Basisregistratie Personen (BRP) en Register Niet-Ingezetenen (RNI)

De jaarlijkse zelfevaluaties voor de BRP en het RNI zijn tijdig voor 1 oktober 2016 uitgevoerd. Op het onderdeel RNI heeft de gemeente het resultaat “goed” gescoord. De twee aanbevelingen worden meegenomen door de afdeling Inwonerszaken.

De inhoudelijke kwaliteit van de gegevens in de BRP is goed. Op het totale gebied van beleid en processen scoort Zwolle met een totaal van 89% iets minder dan de norm van 90% en daarmee on*voldoende.*

De aanbevelingen die voor dit onderdeel gedaan worden betreffen het ontbreken van:

- actueel beveiligingsbeleid voor de BRP;
- een rapportage over dit beleid;
- een beveiligingsplan met te nemen maatregelen; (inmiddels gerealiseerd)
- een draaiboek voor uitwijk van de dienstverlening en jaarlijkse toetsing hiervan.

Op dit moment klopt het dat dit beleid niet helemaal actueel is. In 2013 is het beleid voor de BRP het laatst geactualiseerd en vastgesteld. In 2016 is een gemeente brede informatiebeveiligingsgroep ingesteld die bezig is met de ontwikkeling van nieuw beveiligingsbeleid waarvoor de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) de basis is. Deze BIG hanteert het Ministerie van Binnenlandse Zaken ook bij de jaarlijkse zelfevaluatie BRP. Het doel van de informatiebeveiligingsgroep is een integrale aanpak van beveiligingsaspecten, waar nodig aangescherpt voor kritieke bedrijfsprocessen zoals BRP en Suwinet.

De aanbeveling dat de gemeente Zwolle uitwijkplan moet maken om bij calamiteiten op het stadskantoor de dienstverlening beperkt te kunnen voortzetten op een andere locatie wordt ook breed opgepakt. Vanuit de gemeente brede informatiebeveiligingsgroep is een voorstel geformuleerd voor het MT Zwolle om te komen tot een gemeentelijk bedrijfscontinuïteitsplan. Deze maatregel betreft immers niet alleen de dienstverlening van Publiekszaken, maar bijvoorbeeld ook van Sociale Zaken. Daarom is gekozen voor een integraal plan en niet alleen een plan voor de BRP.

6.2 Zelfevaluatie Paspoorten en Nederlandse Identiteitskaarten (PNIK)

In 2016 heeft Zwolle de resultaten van de Zelfevaluatie PNIK aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) gerapporteerd. Zwolle heeft daarin de uitslag goed behaald, wat betekent dat zij > 95% van de maximaal te behalen score heeft bereikt. Het exacte percentage dat Zwolle heeft gescoord is 98%.

De Zelfevaluatie PNIK is opgedeeld in thema's. Per onderdeel kan men goed, voldoende of onvoldoende scoren. Naar aanleiding van de scores van Zwolle, hieronder in de tabel weergegeven, wordt uitgelicht wat goed en minder goed gaat in Zwolle.

Thema	*Wettelijke norm*	*Aanbe-velingen*	*Totaal*	*Totaal Perc.*	*Totaal Norm-perc.*	*Totaal Resultaat*
Beleid en Regelgeving	105 (108)	5 (5)	110 (113)	97%	90%	Goed
Processen	259 (262)	24 (24)	283 (286)	99%	90%	Goed
Gegevens	54 (54)	2 (6)	56 (60)	93%	90%	Voldoende
Personeel	201 (206)	0 (0)	201 (206)	98%	90%	Goed
Fysieke Beveiliging	162 (162)	14 (18)	176 (180)	98%	90%	Goed
Calamiteiten	54 (54)	6 (6)	60 (60)	100%	90%	Goed
Architectuur	12 (12)	0 (0)	12 (12)	100%	90%	Goed
Naleving	12 (12)	0 (0)	12 (12)	100%	90%	Goed

6.2.1 Beleid en Regelgeving

Naast dat de score goed is (97% bereikt) zijn er twee aanbevelingen (vraag 5 en 6 van de zelfevaluatie). Het betreft het opnemen van de onderwerpen: 'Het gebruik van het mobiele vingerafdrukopname-apparaat in de beveiligingsprocedure'. Hetzelfde geldt voor het vaststellen van de identiteit en de nationaliteit van de aanvragen, ook dit onderwerp moet opgenomen worden in de beveiligingsprocedure reisdocumenten. Momenteel wordt de beveiligingsprocedure (als onderdeel de incidentenprocedure) integraal opgesteld voor Gemeente Zwolle. De incidentenprocedure wordt een onderdeel van de beveiligingsprocedure. Bij het herzien van de incidentenprocedure worden er onderdelen m.b.t. de aanbevelingen opgenomen.

6.2.2 Processen

De processen op het gebied van reisdocumenten zijn vastgelegd in duidelijke procedures en voldoen in goede mate aan de eisen die over het werkproces in wet- en regelgeving zijn vastgelegd. Er is 99% van de maximaal te behalen score bereikt. Aanbeveling: voorheen werden reisdocumenten die in Zwolle werden gevonden bewaard en werd desbetreffende gemeente hiervan op de hoogte gesteld. Dit deed Zwolle vooral als gastheer van de regio, gezien er zoveel forenzen en studenten in Zwolle verkeren. Inmiddels is de wetgeving aangepast en onttrekt ook Zwolle een reisdocument definitief aan het verkeer wanneer een reisdocumenten als gevonden is ontvangen en de houder niet in de gemeente woonachtig is.

6.2.3 Gegevens

Op dit onderdeel is voldoende gescoord, er is 93% van de maximaal te behalen score bereikt. De toegang tot en het gebruik van gegevens rondom het reisdocumentenproces is in Zwolle voldoende geregeld. Zwolle waarborgt de kwalitiet van gegevens voldoende, net als de bescherming van de vertrouwelijkheid. Er zijn enkele verbeteringen wenselijk om tot een beter resultaat te komen, namelijk:
De houder iedere 60 dagen de pincode van de identificatiekaart laten wijzigen. Dit willen wij in Zwolle graag doorvoeren. Helaas maakt de software het ons niet mogelijk om dit automatisch in te stellen. Dat betekent dat wij dit handmatig moeten invoeren. Helaas is er bij handmatige invoering geen controle mogelijk. Daarom hebben wij deze bevinding geëscaleerd naar het Rijksdienst voor Identiteitsgegevens (RvIG). Omdat meer gemeenten tegen dit probleem aanlopen verwachten wij actie van het RvIG.

6.2.4 Personeel

Op dit onderdeel scoort Zwolle goed, namelijk 98% van de totaal te behalen score. Er is echter één actiepunt, namelijk ‘Bij het aanstellen van vast en tijdelijk personeel de opgegeven gegevens van de medewerkers verifiëren’. Dit onderdeel is voor Zwolle niet van toepassing, gezien er geen vaste medewerkers meer in dienst worden genomen. Het kan alleen gelden voor tijdelijke medewerkers, maar gezien dit veelal stagiaires zijn worden er geen gegevens gecontroleerd. Gegevens zijn in deze zin CV en diploma’s. Stagiaires hebben over het algemeen nog geen diploma, of dit is niet relevant. Uiteraard moeten alle medewerkers werkzaam aan het reisdocumentenproces een VOG ondertekenen. Dit is dan ook een risico waar we ons bewust van zijn, maar ook bewust geen actie op ondernemen.

6.2.5 Fysieke beveiliging

Op dit onderdeel scoort Zwolle 98% van de maximaal te behalen score. De fysieke beveiliging in Zwolle is goed. De fysieke bescherming en daarmee de veiligheid van reisdocumenten en medewerkers is in dit proces in goede mate geregeld.

6.2.6 Calamiteiten

Op dit onderdeel wordt 100% gescoord. Calamiteitenbeheersing bij reisdocumenten in Zwolle is goed geregeld. Zwolle is een goed voorbereid op een eventuele gebeurtenis die de normale bedrijfsvoering ernstig of langdurig zou kunnen verstoren.

6.2.7 Architectuur

Zwolle scoort ook op dit onderdeel 100%. De informatiesystemen rondom het reisdocumentenproces zijn is Zwolle op goede wijze ingericht.

6.2.8 Naleving

Ook op dit onderdeel scoort Zwolle goed, weer 100%. Dit betekent dat wij als Zwolle goed omgaan met de uitkomsten van de zelfevaluatie en continue willen verbeteren.

6.3 Interne controle

De interne controlerol is aan het veranderen aangezien meer en meer wordt vastgelegd in verschillende systemen. Belangrijk is dat de beoordeelde informatie betrouwbaar is. Daarnaast is het van belang dat alleen bevoegde personen toegang hebben (zowel fysiek als digitaal).

De interne controle voert daarom de volgende werkzaamheden uit:

- Check of personen die uit dienst zijn toegang hebben tot het netwerk middels controle op last login;
- Controle op algemene accounts.

Daarnaast wordt tussentijds gemonitord wat de opvolging is van de bevindingen van de accountant.

Om eerder in het proces eventuele tekortkomingen te constateren heeft afstemming plaatsgevonden met de functioneel beheerders van One World om bepaalde controles in bedden in het reguliere beheerproces.

Maandelijks vindt informeel overleg plaats met de adviseur informatiebeveiliging. Aan bod komen bevindingen, mogelijk uit te voeren controles en ontwikkelingen binnen de informatieveiligheid.

6.4 Informatieveiligheid en de accountant

Jaarlijks voert de accountant een IT-audit uit op de voor de accountant belangrijkste systemen (One World, GWS4ALL, TOP Regie en Financieel en You Force). Gelet op het belang van informatieveiligheid worden deze controles meer uitgebreid.

Er worden controlewerkzaamheden uitgevoerd op onder andere de volgende onderdelen en worden als onderdeel in de Managementletter opgenomen (en uiteindelijk het jaarlijkse accountantsverslag). Enkele bevindingen zijn:

- Afwezigheid actuele, formele changemanagement procedure en uitgevoerde controlemaatregelen changemanagement proces GWS en TOP Regie en TOP Financieel worden niet zichtbaar vastgelegd;
- Formele autorisatieprocedure niet aanwezig en uitdienstprocedure verloopt niet adequaat;
- Afwezigheid Business Continuity Plan en geen formele back-up en restore procedure.

6.4.1 Functioneel Beheer OneWorld

Een van de systemen waar de accountant op toeziet is OneWorld. In 2016 beschikte Zwolle over een door de systeemeigenaar getekend informatiebeveiligingsplan voor OneWorld.

Ook is gestart met het acief aanschrijven van medewerkers die langer dan 3 maand niet ingelogd hebben in OneWorld en met het periodiek controleren van de rechten en bevoegdheden van kritieke functies van medewerkers in OneWorld (afdeling AFF).

Het doorvoeren van systeemwijzigingen is verbeterd, zodat het proces voldoet aan gestelde eisen, onder andere op het gebied van testen. Sinds najaar 2016 is één van de functioneel beheerders van de applicatie OneWorld gecertificeerd tester. Ook het contact met functioneel beheerders van andere applicaties intensiveert, mede rond het onderwerp informatieveiligheid.

Onderzoek is gestart naar het kunnen toepassen van data-analyse door de accountant. Dit is alleen mogelijk als aan alle eisen omtrent bijvoorbeeld beveiliging wordt voldaan. Dit onderzoek is nog niet afgerond en loopt door in 2017.

6.5 Penetratietesten

Een penetratietest (pentest of binnendringingstest) is een toets van een of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden ook werkelijk gebruikt worden om in deze systemen in te breken. Periodiek moeten deze testen worden uitgevoerd op de ICT omgevingen om er voor te zorgen dat eventuele kwetsbaarheden tijdig worden ontdekt en kunnen worden hersteld. Vaak wordt dit ook afgedwongen om te kunnen slagen voor een audit.

Voor de digid audit is dit onder andere het geval. In 2016 zijn een aantal van deze penetratietesten uitgevoerd. De resultaten zijn afgestemd met de eigenaar van de betreffende toepassing en zijn voor een deel inmiddels hersteld.

6.6 Blik vooruit: ENSIA

Elk jaar moeten gemeenten zich verantwoorden over de kwaliteit van de informatieveiligheid van diverse informatiesystemen. In 2017 zal dit voor het eerst gebeuren met een nieuwe audit systematiek: de Eenduidige Normatiek Single Information Audit (ENSIA). Met ENSIA wordt de verantwoordingssystematiek over BRP, PUN, Suwi, BAG, BGT en DigiD gebundeld. Bovendien sluit hiermee de horizontale verantwoording over informatieveiligheid aan op de gemeentelijke planning en control-cyclus. Hierdoor krijgt het gemeentebestuur meer overzicht over de informatieveiligheid van hun gemeente en kan het bestuur beter sturen en verantwoording afleggen aan de gemeenteraad.

Voorheen waren er aparte audits voor de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet).

7 Zwolle 'in control'

De gemeente Zwolle wil informatiebeveiliging en privacy op een gecontroleerde manier borgen binnen haar processen. Hierom is in 2016, op basis van een meervoudig onderhandse aanbesteding, een ‘Information Security Management System’ ondersteunende tool (ISMS-tool) aangeschaft. Hierin worden de maatregelen vanuit de diverse normenkaders ingevoerd. Dit betreft de maatregelen vanwege de Baseline Informatiebeveiliging Gemeenten, maar ook die vanwege de Wet BRP, Wet PUN, Suwinet en DigiD.

Het voordeel van deze functionaliteit is niet alleen het houden van een helder overzicht van maatregelen. Het is hiermee ook mogelijk aan maatregelen de nodige acties en actiehouders te koppelen, taken uit te zetten, voortgang te monitoren en over het resultaat te rapporteren.

7.1 Integrale aanpak

Door de maatregelen vanuit de diverse normenkaders in één functionaliteit in te voeren ontstaat een compleet overzicht. Op basis van dit ene overzicht is het beter mogelijk te sturen op informatiebeveiliging, dan wanneer er sprake is van afzonderlijke lijsten. Bijkomend voordeel is dat een koppeling gelegd kan worden tussen de normenkaders, zodat een zelfde of vergelijkbare maatregel niet meerdere keren, maar slechts één keer wordt opgepakt.

In het laatste kwartaal van 2016 is de software op hoofdlijnen ingericht voor de BIG. Begin 2017 zal verdere implementatie plaatsvinden en zal de software breder worden ingezet binnen de gemeente Zwolle.

Datum 5 april 2017
Ons kenmerk Jaarverslag informatiebeveiliging

Bijlage: verslag visitatiecommissie