inzicht

Advies en Faciliteiten
AFI

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

Beveiliging Suwinet 2015

Jaarverslag

Opdrachtgever	Bernard Mencke
Opdrachtnemer	Allin Peter Britstra
Versie	0.3
Datum	14 januari 2016

Datum 14 januari 2016
Ons kenmerk Beveiliging Suwinet 2015

Inhoud

1	**Suwinet en de gemeente Zwolle**	**3**
1.1	Drie aansluitingen met samen ruim 100 gebruikers	3
1.2	Leeswijzer	3
1.3	Constatering	3
2	**Organiseren van veilig gebruik van Suwinet**	**4**
2.1	Rollen en positie	4
2.1.1	Security Officer	4
2.1.2	Interne Controller	4
3	**In 2015 uitgevoerde controles**	**6**
3.1	EDP-Audit	6
3.2	Onderzoek Inspectie SZW	7
3.3	Gebruiksrapportages	7
3.4	Steekproef	7
3.5	Verbeterpunten	7
4	**Vooruitblik**	**8**
4.1	Reorganiseren van (beveiligings)processen	8
4.1.1	Standaardisatie	8
4.2	ICT	8
4.3	Bewustwording	8
4.4	Controles	8
4.5	VNG verbeterprogramma	9
4.6	Integrale sturing van informatiebeveiliging	9

Datum 14 januari 2016
Ons kenmerk Beveiliging Suwinet 2015

1 Suwinet en de gemeente Zwolle

Het informatiesysteem ‘Suwinet’ is het voorbije jaar veel in het nieuws geweest. Vaak in één adem genoemd met disfunctionerende gemeenten, die geen oog zouden hebben voor de privacy van de burger.

Aandacht voor Suwinet is terecht, want via Suwinet delen overheidsorganisaties digitaal diverse gegevens (van burgers en bedrijven) die gaan over werk en inkomen. Om burgers snel en beter te helpen zit het systeem vol met veel en gevoelige informatie. Juist daarom moet die burger kunnen vertrouwen op een zorgvuldige manier van werken door de gebruikers van Suwinet.

1.1 Drie aansluitingen met samen ruim 100 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. Inmiddels 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’.

1.2 Leeswijzer

Dit jaarverslag belicht een aantal activiteiten die in 2015 zijn uitgevoerd om privacy van onze burgers te waarborgen via het veilig gebruiken van Suwinet. We lichten een aantal controles toe die zijn uitgevoerd en gaan in op de resultaten ervan. We merkten op dat een aantal processen en ICT-zaken beter kunnen. Die verbeterpunten pakken we dit jaar op. Daarom biedt het laatste hoofdstuk van dit rapport een vooruitblik op 2016.

1.3 Constatering

Wat nog rest voor dit eerste hoofdstuk is een opmerking over de manier waarop Suwinet daadwerkelijk gebruikt wordt. Op basis van de uitgevoerde controles constateren we dat het systeem in 2015 veilig en zorgvuldig is gebruikt door de medewerkers van de gemeente Zwolle.

2 Organiseren van veilig gebruik van Suwinet

Suwinet bevat veel (en gevoelige) informatie van alle Nederlandse burgers. Hierom heeft iedere gemeente de verplichting om de privacy van deze burgers te waarborgen. Hiervoor stelt zij beleid vast en richt zij een aantal processen in voor een veilig gebruik van Suwinet.

Wanneer we het nieuws volgen over hoe 'de gemeenten' hiermee omgaan, dan mogen we gerust stellen dat Zwolle de voorbije jaren een serieus en professioneel raamwerk heeft gebouwd rond Suwinet. Dit neemt niet weg dat de organisatie kritisch naar zichzelf moet blijven kijken en waar nodig mee moet bewegen.

Rond het veilig gebruiken van Suwinet heeft de gemeente Zwolle haar processen op orde. In de uitvoering ervan zagen we in 2015 een aantal verbetermogelijkheden. Een deel daarvan speelde in op wijzigingen binnen de organisatie en leidde tot een andere positionering van een aantal beveiligingstaken. Die veranderingen lichten we in dit hoofdstuk toe. Een aantal andere verbeterpunten zullen we in 2016 oppakken, daarover gaat hoofdstuk 4.

2.1 Rollen en positie

Binnen de werkprocessen zijn een aantal rollen benoemd. Door veranderingen in de organisatie zijn ook rollen verandert: van inhoud of van positie. Twee daarvan verdienen aandacht in dit jaarverslag.

2.1.1 Security Officer

Iedere organisatie kent een 'security officer'. Deze persoon is verantwoordelijk voor de beveiliging van Suwinet. In Zwolle waren dit drie personen, één voor iedere aansluiting. Op 18 november heeft het MTZ besloten de rol security officer centraal te beleggen bij de adviseur informatiebeveiliging van de afdeling Advies.

Deze rol is om twee reden 'verplaatst':

1. het verdwijnen van eenheden was aanleiding om de positionering te herijken;
2. daarnaast draagt deze keuze bij aan de binnen het systeem gewenste functiescheiding. De huidige security officer is onafhankelijk: hij is geen Suwinet gebruiker en hoort ook niet bij een afdeling die Suwinet gebruikt.

2.1.2 Interne Controller

Aandachtspunt bij het gebruik van Suwinet is het toekennen van de juiste autorisatie aan een medewerker. Hierbij is een belangrijke rol weggelegd voor de interne controller, die de medewerkers een gebruikersverklaring laat ondertekenen en zorgt voor een akkoord op de juiste autorisatie van de betreffende leidinggevende.

Tot voor kort vervulden de interne controllers deze rol alleen voor de Suwinet aansluiting van de eenheid Sociale Zaken en Werkgelegenheid. Vanwege een functieverschuiving naar de afdeling Advies, kunnen sinds het laatste kwartaal ook de

andere aansluitingen gebruik maken van de interne controllers en zo het autorisatieproces professionaliseren. De hiervoor benodigde verandering van procesbeschrijvingen vindt in 2016 plaats.

3 In 2015 uitgevoerde controles

In 2015 zijn verschillende controles uitgevoerd op het gebruik van Suwinet. In dit jaarverslag staan we kort stil bij de resultaten van deze controles.

3.1 EDP-Audit

Gemeenten met een groot aantal Suwinet gebruikers moeten hun proces laten auditen. In 2015 heeft Zwolle een EDP-auditor[1] gevraagd deze controle uit te voeren over het jaar 2014. Als leidraad gelden de normen uit het Normenkader Gezamenlijke elektronische Voorzieningen SUWI (GeVS). De audit is jaarlijks terugkerend binnen 3 maanden na afloop van elk kalenderjaar.

Wat betreft het testen van software scoort de gemeente Zwolle onvoldoende. Suwinet wordt aangeboden door het BKWI, onderdeel van het UWV. Deze organisatie test de software alvorens haar beschikbaar te stellen aan gebruikers. Toch verwacht de auditor dat de gemeente zelf ook een gebruikerstest uitvoert en dan de keuze maakt een nieuwe release van Suwinet wel of niet te gebruiken.

Per aansluiting verschilt op dit moment de autorisatieprocedure. Uit de audit kwam naar voren dat niet alle autorisatieprocedures even helder beschreven zijn. De auditor acht het mogelijke risico dat de gemeente Zwolle hierdoor loopt ‘aanvaardbaar’. Een aantal stappen in het proces zijn al verbeterd, waarmee de meest kritische opmerkingen zijn weggenomen. Verdere verbetering van het gehele proces wordt in gang gezet.

Voor iedere Suwinet aansluiting vraagt de security officer minimaal twee keer per jaar een gebruiksrapportage op. De auditor heeft geconstateerd dat niet iedere security officer in 2014 voldoende rapportages opvroeg. De onder 2.1 genoemde wijziging van de invulling van de rol security officer leidt ertoe dat er nu nog maar één security officer is voor heel Zwolle die meerdere keren per jaar gebruiksrapportages zal opvragen en daar zo nodig op zal anticiperen.

De auditor constateerde tevens dat een aantal ICT-zaken niet voldoen aan de gestelde normen. Er zijn bijvoorbeeld opmerkingen gemaakt over het kunnen uitwijken van processen in geval van een calamiteit. Dit gaat verder dan alleen het gebruik van Suwinet en raakt ook aanverwante systemen en processen.

Alhoewel er een aantal kritiekpunten zijn geconstateerd, 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 audit rapportage.

[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.

3.2 Onderzoek Inspectie SZW

Aan de hand van zeven essentiële beveiligingsnormen uit het Normenkader GeVS heeft de Inspectie SZW bij alle gemeenten getoetst of de beveiliging rondom Suwinet op orde is. Vier van deze normen toetsen of de verantwoordelijkheden goed zijn verdeeld. Drie normen kijken of de verantwoordelijkheid goed is geborgd in de organisatie.

Het toetsen vond plaats door het beantwoorden van een vragenlijst en het toesturen van bewijsstukken. November 2015 zijn door de Inspectie SZW aanvullende vragen gesteld en door de gemeente beantwoord. Op 30 december 2015 ontving het college van burgemeester en wethouders van de gemeente Zwolle het bericht dat de gemeente Zwolle voldoet aan de zeven essentiële normen.

De resultaten van dit onderzoek zijn voor de gemeente Zwolle van groter belang dan de audit, aangezien de scores hiervan bepalend zijn voor de rapportage aan de minister. Die consequenties wil verbinden aan slechte rapporten, want voor de minister is het veilig gebruik van Suwinet een speerpunt.

3.3 Gebruiksrapportages

Minimaal twee keer per jaar vraagt de ‘security officer’ voor iedere gemeentelijke aansluiting een gebruiksrapport op bij het BKWI. Het BKWI beheert Suwinet en is onderdeel van het UWV (UWV is eigenaar van Suwinet). Deze rapportages worden maandelijks opgesteld over de zes maanden eraan voorafgaand. Ze zijn samengesteld in overleg met de VNG en bedoeld om onrechtmatig gebruik van Suwinet in beeld te brengen. In 2015 brachten de Zwolse gebruiksrapportages geen onrechtmatig gebruik aan het licht.

3.4 Steekproef

Naast de reguliere gebruiksrapportages kan de security officer specifieke rapportages opvragen. December 2015 is aan het BKWI een lijst verstrekt met de BSN’s van 33 ‘bekende Zwollenaren’. Een deel betrof Zwolse burgers die nationale bekendheid genieten. Een ander deel betrof mensen van binnen en buiten Zwolle, die vanwege hun rol in de Zwolse samenleving bekend zijn bij het publiek.

Aan het BKWI is gevraagd of gegevens van deze mensen vanuit de gemeente Zwolle zijn geraadpleegd via Suwinet. Op basis van het resultaat van deze steekproef bleek geen onrechtmatig gebruik van Suwinet door medewerkers van de gemeente Zwolle.

3.5 Verbeterpunten

De resultaten van de audit worden begin 2016 gedeeld met betrokken leidinggevenden. Een aantal verbeteringen is direct geïmplementeerd. Over verdere verbetering van processen en systemen kunt u lezen in het volgende hoofdstuk. Dat blikt vooruit op het jaar 2016.

4 Vooruitblik

Dit rapport blikt in hoofdzaak terug op het jaar 2015. Dit neemt niet weg dat ook in 2016 gewerkt zal worden aan een veilig gebruik van Suwinet. Daarbij borduurt de gemeente Zwolle voort op de stappen die de afgelopen jaren zijn gezet.

4.1 Reorganiseren van (beveiligings)processen

Vanwege het verdwijnen van de eenheden en vanwege verschuiving van functies moeten alle procesbeschrijvingen en werkinstructies voor het gebruik van Suwinet worden aangepast. Bij die aanpassing nemen we de opmerkingen mee die tijdens de EDP-audit op deze onderdelen naar voren zijn gekomen. November 2015 is het MTZ ermee akkoord gegaan dat deze aanpassing in het eerste kwartaal van 2016 zal plaatsvinden. Dit biedt ruimte om van alle controles de verbeterpunten mee te nemen.

4.1.1 Standaardisatie

Bij het vormgeven van processen, zoals de autorisatieprocedure, worden de werkwijzen van de drie afzonderlijke aansluitingen zoveel mogelijk gestandaardiseerd om bij één Zwolse procedure uit te komen. Uitgangspunt hierbij zijn de procesbeschrijvingen die bij uitgevoerde controles het predikaat ‘goed’ ontvingen. Grotendeels zijn deze afkomstig van de eenheid Sociale Zaken en Werkgelegenheid, waar de vroegere security officer met veel aandacht en energie heeft gewerkt aan het borgen van veilig werken met Suwinet.

4.2 ICT

De opmerkingen van de EDP-auditor op het gebied van ICT worden opgenomen in een verbeterplan van het Shared Service Centrum Zwolle en worden in 2016 uitgevoerd. Een deel hiervan in samenhang met andere verbeterpunten, vanwege de implementatie van de Baseline Informatiebeveiliging Gemeenten (BIG).

4.3 Bewustwording

Een onderwerp dat steeds meer aandacht krijgt is het bewust omgaan met de privacy van burgers. Dit vereist dat medewerkers van de gemeente Zwolle bewust omgaan met gegevens van burgers. Hierom zal in 2016 meer aandacht besteed worden aan bewust gebruik van Suwinet. Dit onderwerp komt aan de orde bij de rondgang die de nieuwe security officer maakt langs de teams. Verdere activiteiten worden uitgevoerd in samenhang met bewustwordingsactiviteiten vanwege de implementatie van de BIG.

4.4 Controles

Heel frequent zullen de reguliere gebruiksrapportages worden gemaakt door de security officer.
Jaarlijks terugkerend is de verplichte audit aan het einde van elk kalenderjaar.
De resultaten worden opgenomen in een verbeterplan.

4.5 VNG verbeterprogramma

UWV, SVB en VNG zijn samen gestart met het programma ‘Borging veilige gegevens-uitwisseling Suwinet’. De VNG neemt binnen dit programma een actieve rol in en betrekt gemeenten hierbij. De gemeente Zwolle is ook in 2016 aangehaakt en zal actief acteren op aanbevelingen vanuit dit programma.

4.6 Integrale sturing van informatiebeveiliging

Voor de gemeente Zwolle staat het beveiligen van Suwinet niet op zichzelf. Om privacy en beveiliging integraal te borgen krijgt Suwinet een plaats in het gemeentebrede informatiebeveiligingsbeleid. Daaruit volgt dat concrete acties een plek krijgen in het gemeentebrede informatiebeveiligingsplan. Dit voorkomt dubbele acties en versterkt de regie op informatieveiligheid binnen de gemeente Zwolle.