Gemeente
Haarlem

Verbeterplan
n.a.v. ENSIA 2018

1 maart 2019
E. Hotting
Concerncontrol

1. Aanleiding

Voor de tweede keer verantwoorden wij ons over de kwaliteit van de informatieveiligheid van diverse informatiesystemen met behulp van de Eenduidige Normatiek Single Information Audit (ENSIA). ENSIA is gebaseerd op de Baseline Informatieveiligheid Gemeenten (BIG). Of we voldoen aan deze Baseline is getoetst door middel van een zelfevaluatie. Voor het jaar 2018 geldt (net als voor het jaar 2017) dat de verantwoording Suwinet (aan Ministerie van SZW) en DigiD (aan Logius) wordt verantwoord door middel van een Collegeverklaring.

Uit deze zelfevaluatie blijkt dat de Gemeente Haarlem op peildatum 31 december 2018 de interne beheersingsmaatregelen in opzet en bestaan voldoen aan de geselecteerde normen inzake DigiD en Suwinet, met uitzondering van de in dit verbeterplan geadresseerde normen. Dit verbeterplan beschrijft welke opvolging (correctieve maatregelen) er door Gemeente Haarlem worden getroffen en welke verbetertermijn wordt gehanteerd.

2. Context

De toezichthouder hanteert generieke principes waaraan volgens de toezichthouder voldaan moet zijn bij de bescherming van gegevens. Die principes ondersteunen de oordeelsvorming. Normen kunnen het vertrekpunt zijn van die oordeelsvorming, maar niet het eindpunt. Te vaak is gebleken dat het voldoen aan normen een losse koppeling onderhoudt met de daadwerkelijke veiligheid. Naast het adresseren van de afwijkingen van de normen, wordt er middels het jaarverslag aan de raad over het totaalbeeld en de status van informatieveiligheid van de gemeente verantwoording afgelegd. Middels deze separate rapportage krijgt het gemeentebestuur meer zicht op de informatieveiligheid en is ze beter in staat om keuzes te maken in het informatieveiligheidsbeleid van de gemeente. Hiermee wordt aangesloten bij de gemeentelijke P&C-cyclus en wordt het leervermogen van de organisatie vergroot.

Dit verbeterplan adresseert de bevindingen uit de zelfevaluatie waarover het College verantwoording aflegt middels de Collegeverklaring, en de opvolging ervan. Hierbij wordt aangegeven wat de planning is voor uitvoering van de maatregelen.

De classificatie “voldoet niet” wordt meegegeven zodra aan een norm niet voor de volle 100% wordt voldaan.

3. Maatregelen

3.1 DigiD

3.1.1 Algemeen

In onderstaande wordt expliciet ingegaan op elke norm welke ten tijde van de zelfevaluatie niet voldoet, welke maatregel wordt genomen om dit te corrigeren en welke planning daarvoor geldt.

3.1.2 Norm U/NW.06

Beschrijving van de norm: Voor het configureren van netwerken is een handeling richtlijn beschikbaar.

Bevinding: Er zijn meerdere documenten die worden gehanteerd als baseline, maar de samenhang tussen deze documenten is niet voldoende. Ook wordt niet voldoende beschreven waarom bepaalde keuzes worden gemaakt.

Maatregel: Een nieuwe, complete baseline wordt opgesteld of overgenomen, waarbij duidelijk wordt beschreven waarom bepaalde keuzes worden gemaakt.
Planning: Dit wordt in 2019 kwartaal 2 afgerond.

3.1.3 Norm C.09

Beschrijving van de norm: Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.

Bevinding: Er is een oude jQeury library aangetroffen welke niet was gepatcht, en welke de gemeente Haarlem niet zelf kan patchen. Dit betrof een applicatie die relevant is voor de DigiD verwerking. Feitelijke dreiging leek niet aanwezig, maar de patch behoort uitgevoerd te zijn.

Maatregel: In overleg met de leverancier de betreffende library alsnog patchen.
Planning: Dit is reeds uitgevoerd. Het verbeterplan beschrijft de werkelijkheid van 31 december 2018.

3.2 Suwinet

3.2.1 Algemeen

Voor Suwinet geldt dat de nieuwe ENSIA een uitbreiding van scope tot gevolg heeft gehad, welke pas duidelijk werd tijdens de zelfevaluatie eind 2017. Waar in voorgaande jaren keer op keer werd voldaan aan de zeven normen waarop de toezichthouder toezag, blijkt dat met de huidige scope niet langer het geval.

Daarnaast is het, net als rond DigiD, in het algemeen noodzakelijk dat de verantwoording over de informatieveiligheid een zaak wordt van de betrokken lijnmanagers en deze verantwoordelijkheid ook zo gevoeld wordt. Dit betekent onder meer dat de bijbehorende werkzaamheden niet kunnen worden

uitbesteed aan adviseurs, en verantwoordelijkheid niet gedelegeerd. Vanaf 2018 krijgt dit punt de nodige aandacht onder regie van de Concerncontroller, FG en CISO.

3.2.2 Norm B.01

Beschrijving van de norm: De Afnemer heeft voor de aansluiting op Suwinet expliciet aandacht besteed aan het stelsel van beveiligingsmaatregelen in zijn informatiebeveiligingsbeleid, of hiervoor een apart aansluitingsbeleid ontwikkeld.

Bevinding: Er is naar aanleiding van de aanbevelingen van de Rekenkamercommissie versneld nieuw Strategisch beleid vastgesteld op basis van de BIO. Dit is daarmee up-to-date. Specifiek aansluitbeleid en de uitwerking voor SUWI loopt echter achter.

Maatregel: Het aansluitbeleid voor SUWI wordt bijgewerkt zodat het past bij de nieuwe aansluitnormen. Ook wordt het passend gemaakt op de nieuwe afdelingsnamen en functies. Alle onderliggende procedures (de uitwerking) ligt in principe klaar, daarop zal nog een check worden gedaan en waar nodig bijstelling plaatsvinden nadat het aansluitbeleid is aangepast.

Planning: Dit wordt in 2019 afgerond.

3.2.3 Norm U.03

Beschrijving van de norm: Elke gebruiker/beheerder behoort over een unieke identificatiecode te beschikken (User-ID) voor uitsluitend persoonlijk gebruik, ook behoort een geschikte authenticatie techniek te worden gekozen.

Bevinding: Het bleek mogelijk de applicatie MensCentraal te gebruiken vanaf het Wifi-netwerk voor gasten. Daarmee waren andere ingestelde maatregelen niet langer effectief.

Maatregel: Toegang via gastnetwerk wordt onmogelijk gemaakt.
Planning: Dit is reeds uitgevoerd. Het verbeterplan beschrijft de werkelijkheid van 31 december 2018.

3.2.4 Norm C.01

Beschrijving van de norm: (De implementatie van) het aansluitbeleid wordt periodiek beoordeeld op veranderingen in de wetgeving, wijziging van functionaliteit en uit te wisselen gegevens en veranderde technologiën.

Bevinding: Zelfde bevinding als bij Norm B.01, maar dan specifiek voor het aansluitbeleid. Het aansluitbeleid is nog niet bijgewerkt waardoor het ook niet voldoet aan norm C.01. In het verouderde beleid wordt wel aandacht besteed aan awareness.

Maatregel: Zelfde maatregel als bij Norm B.01. Het aansluitbeleid voor SUWI wordt bijgewerkt zodat het past bij de nieuwe aansluitnormen. Ook wordt het passend gemaakt op de nieuwe afdelingsnamen en functies. Alle onderliggende procedures (de uitwerking) ligt in principe klaar, daarop zal nog een check worden gedaan en waar nodig bijstelling plaatsvinden nadat het aansluitbeleid is aangepast.

Planning: Dit wordt in 2019 afgerond.

3.2.5 Norm C.06

Beschrijving van de norm: De log-informatie wordt regelmatig gemonitord (signaleren, analyseren rapporteren en bijsturen)

Bevinding: De applicatie MensCentraal biedt niet de benodigde functionaliteit voor het volgens de norm analyseren van logs. Dit is dan ook onvoldoende uitgevoerd.

Maatregel: De applicatie MensCentraal wordt uitgefaseerd, de processen worden daarna ondersteund met een nieuwe applicatie. De verwerving daarvan is reeds uitgevoerd, momenteel wordt gewerkt aan de inrichting en ingebruikname.

Planning: Vervanging en uitfasering van MensCentraal is gepland voor eind 2019.