Rekenkamercommissie Meppel, Staphorst, Steenwijkerland en Westerveld

Onderzoek informatiebeveiliging gemeente Westerveld; eindrapport

Eindrapport februari 2019

Inhoudsopgave

'PwC' is het merk waaronder PricewaterhouseCoopers Accountants N.V. (KvK 34180285), PricewaterhouseCoopers Belastingadviseurs N.V. (KvK 34180284), PricewaterhouseCoopers Advisory N.V. (KvK 34180287), PricewaterhouseCoopers Compliance Services B.V. (KvK 51414406), PricewaterhouseCoopers Pensions, Actuarial & Insurance Services B.V. (KvK 54226368), PricewaterhouseCoopers B.V. (KvK 34180289) en andere vennootschappen handelen en diensten verlenen. Op deze diensten zijn algemene voorwaarden van toepassing, waarin onder meer aansprakelijkheidsvoorwaarden zijn opgenomen. Op leveringen aan deze vennootschappen zijn algemene inkoopvoorwaarden van toepassing. Op www.pwc.nl treft u meer informatie over deze vennootschappen, waaronder deze algemene (inkoop)voorwaarden die ook zijn gedeponeerd bij de Kamer van Koophandel te Amsterdam.

Lijst van veel gebruikte afkortingen

AVG	Algemene verordening gegevensbescherming
AP	Autoriteit Persoonsgegevens, de nationale instantie die toezicht houdt op de bescherming van persoonsgegevens
BIG	Baseline Informatiebeveiliging voor Gemeenten; bevat de basisvereisten voor gemeenten opgesteld door VNG/KING, in 2020 treedt naar verwachting de BIO in werking, een Baseline Informatiebeveiliging voor de Overheid
BRP	Basis Registratie Persoonsgegevens
CISO	Chief Information Security Officer, de centrale functionaris voor informatiebeveiliging
ENSIA	Eenduidige normatiek single information audit; bij deze verplichte jaarlijkse vragenlijst voor gemeenten zijn een aantal vragenlijsten gecombineerd tot één vragenlijst
FG	Functionaris Gegevensbescherming, belast met toepassing en naleving van de Algemene Verordening Gegevensbescherming
Patch Management	Een omgeving van management systemen wat zorgt voor het verwerven, testen en installeren van meerdere patches (wijzigingen in de code) op een computersysteem. (bron: MarQit)
RI&E	Risico-Inventarisatie en -Evaluatie
Suwinet	Afkorting komt van de Wet SUWI, dat is de Wet structuur uitvoeringsorganisatie werk en inkomen. Via Suwinet kunnen overheidsorganisaties gegevens van burgers en bedrijven digitaal bij elkaar opvragen en naar elkaar sturen.

1. Inleiding

De gemeenteraad in een inventariserende ronde van de rekenkamercommissie naar nieuwe mogelijke onderzoeksonderwerpen aan informatiebeveiliging een belangrijk en actueel onderwerp te vinden. De rekenkamercommissie vindt het ook van groot belang dat gegevens bij de gemeente in veilige handen zijn. Voor het functioneren en de dienstverlening aan hun inwoners gebruiken gemeenten steeds meer gegevens, wisselen ze steeds meer gegevens uit en bewerken ze die. Door de nieuwe taken van gemeenten in het sociaal domein is dit nog verder toegenomen. Veel van deze gegevens hebben een vertrouwelijk karakter. De grotere prioriteit aan informatieveiligheid heeft ook te maken met nieuwe wetgeving die zich specifiek hierop richt. Deze wetgeving leidt tot handreikingen, verplichtingen en nieuwe 'rollen' met betrekking tot die informatieveiligheid binnen de gemeentelijke overheid. Eerste onderzoeken bij andere gemeenten laten zien dat informatiebeveiliging bij gemeenten nog verder verbeterd kan worden, zoals de recente rekenkameronderzoeken in Rotterdam en Breda.

Dit onderzoek zal het eerste onderzoek zijn dat tegelijk in de vier gemeenten wordt uitgevoerd. Tijdens het onderzoek kan zo synergie ontstaan en kunnen de vier gemeenten ook van elkaar leren. Het onderzoek is, onder verantwoordelijkheid van de rekenkamercommissie, uitgevoerd door PwC.

2. Samenvatting, conclusies en aanbevelingen

2.1. Introductie

De gemeenteraad van Westerveld noemde tijdens een inventariserende ronde van de rekenkamercommissie het onderwerp “informatiebeveiliging” als relevant onderwerp om te onderzoeken. De rekenkamercommissie heeft besloten dit onderwerp op te pakken en een onderzoek te doen waarbij de vraag centraal staat of de informatiebeveiliging in de gemeenten Meppel, Staphorst, Steenwijkerland en Westerveld doeltreffend is. Het onderzoek is dus uitgevoerd in vier gemeenten tegelijk. In het onderzoek is naar drie deelaspecten gekeken:

- organisatie en beleid;
- mens en gedrag;
- techniek.

Na een startgesprek met de rekenkamercommissie en het onderzoeksbureau (PwC) is eerst een startbijeenkomst met de direct betrokkenen van de gemeente gehouden. Hierin is het doel, de aanpak en de planning toegelicht. Gestart is met het verzamelen van feitelijke informatie door documentonderzoek en enkele inventariserende gesprekken. Aan de hand van deze gegevens is een normenkader opgesteld. Vervolgens zijn gegevens verzameld om de praktijk te toetsen aan de normen. Daarvoor zijn interviews gehouden, is een vragenlijst onder medewerkers verspreid, is het beheer van enkele cruciale applicaties onderzocht en is voor Westerveld ook een penetratietest (methode van hack-pogingen) uitgevoerd.

2.2. Conclusies en aanbevelingen

Nu de rol van CISO (Chief Information Security Officer, lees: Hoofd informatiebeveiliging), in Westerveld is ingevuld, kan het informatiebeveiligingsbeleid goed worden geactualiseerd. Invulling van deze rol heeft niettemin te lang op zich laten wachten. Het nieuwe beleid zal naar het oordeel van de Rekenkamercommissie het startpunt moeten zijn van een nieuwe PDCA-cyclus of leercyclus. Het beleid moet vorm krijgen in een concreet jaarplan met uit te voeren maatregelen, gebaseerd op risicoanalyses. Met het vertrek van de CISO in 2015 is de bestuurlijke aandacht voor het vraagstuk van informatiebeveiliging/privacy achtergebleven. Met de komst van een CISO eind 2018 is deze lacune eindelijk ingevuld. Hiermee kan ook het beleid een impuls krijgen en is dit ook een prima moment voor meer bestuurlijke aandacht voor dit vraagstuk Door bestuurlijk meer aandacht te geven aan dit onderwerp kan ook de betrokkenheid van gehele organisatie een impuls krijgen. Deze is onontbeerlijk bij het implementeren en vervolgens het monitoren van noodzakelijke technische maatregelen. Voortdurende aandacht is nodig. De digitale wereld verandert razendsnel. Technieken veranderen en nieuwe risico’s kunnen ontstaan.

Organisatie en beleid

Het meest recente vastgestelde informatiebeveiligingsbeleid is van 2014 en in dat jaar is ook voor het laatst een jaarplan voor informatiebeveiliging opgesteld. In 2010 is voor het laatst een risicoanalyse uitgevoerd. De maatregelen worden nu vastgesteld op basis van een analyse van de Baseline Informatiebeveiliging voor Gemeenten. Inmiddels is er tijdens dit onderzoek een geactualiseerd informatiebeveiligingsbeleid gereedgekomen voor besluitvorming door het college. Met een regelmatig terugkerende integrale risicoanalyse kan de gemeente de maatregelen meer richten op de specifieke context van de gemeente en maatregelen beter prioriteren naar de belangrijkste risico’s die de gemeente loopt. Bescherming van gevoelige data verdient bij een dergelijke risicoanalyse extra aandacht.

Aanbeveling: Voer regelmatig een integrale risicoanalyse uit op het gebied van informatiebeveiliging als basis voor het informatiebeveiligingsbeleid en het bepalen en prioriteren van maatregelen in de jaarplannen.

De uitvoering van het jaarplan is met het vertrek van de CISO in 2015 niet meer consequent ter hand genomen en er zijn ook geen jaarlijkse plannen meer opgesteld in de jaren daarna. Vanaf september 2018 is de rol van de Chief Information Security Officer (CISO) weer volwaardig ingevuld. Daardoor is in de afgelopen maanden een impuls gegeven aan de uitwerking van procedures en maatregelen om informatiebeveiliging te versterken. Dit heeft ook tot gevolg gehad dat de jaarlijkse leercyclus van het plannen van maatregelen, de uitvoering daarvan en het evalueren en verbeteren niet expliciet doorlopen werd met direct betrokkenen. Met de komst van de CISO kan er weer regie gevoerd worden op dit proces.

Aanbeveling: Doorloop weer ieder jaar een leercyclus waarbij wordt teruggekeken op genomen maatregelen, lessen worden geleerd en op basis van het beleid nieuwe maatregelen voor het komende jaar worden opgenomen in een jaarplan.

Uit de enquête onder medewerkers van Westerveld blijkt dat zij even goed of iets beter dan in de andere onderzochte gemeenten op de hoogte zijn van de rollen en verantwoordelijkheden in de organisatie op het gebied van informatiebeveiliging. De raad wordt over informatiebeveiliging geïnformeerd door een paragraaf in het jaarverslag. De paragrafen in het jaarverslag worden in de loop van 2014 tot en met 2017 steeds korter.

Aanbeveling: Gebruik de prioriteiten uit het nieuwe informatiebeveiligingsbeleid als uitgangspunt voor de rapportage in het jaarverslag, vermeld de mate waarin geplande maatregelen uitgevoerd konden worden met de beschikbare capaciteit en middelen en vermeld kort de resultaten van het continu leren en verbeteren.

Er is geen specifiek collegelid verantwoordelijk voor informatiebeveiliging. In andere gemeenten zijn hiermee positieve ervaringen doordat zo een helder bestuurlijk aanspreekpunt ontstaat voor de raad en de ambtelijke organisatie op het gebied van informatiebeveiliging.

Aanbeveling: Overweeg een portefeuillehouder voor informatiebeveiliging aan te stellen.

Mens en gedrag

Over de voorbeeldfunctie van het management bestaan wisselende beelden bij de medewerkers, maar Westerveld scoort op dit punt wel iets beter dan het gemiddelde van de vier onderzochte gemeenten. Er zijn diverse bewustwordingsactiviteiten voor medewerkers en uit de vragenlijst blijkt dat medewerkers van Westerveld gemiddeld wat beter op de hoogte zijn van informatiebeveiliging, hun eigen rol daarin, datalekken en het omgaan met gevoelige gegevens. Medewerkers missen wel samenhang en een zekere regelmaat in de bewustwordingsactiviteiten.

Aanbeveling: Besteed in de bewustwordingsactiviteiten aandacht aan het actief betrekken van het management, de samenhang tussen de activiteiten, regelmaat en het bereiken van nog niet goed geïnformeerde medewerkers.

Techniek

Hoewel in Westerveld een aantal technische beveiligingsmaatregelen zijn getroffen heeft de penetratietest een aantal belangrijke kwetsbaarheden laten zien. Gelet op de bevindingen was het volgens de onderzoekers te risicovol om hiermee te wachten en is vooruitlopend op de oplevering van het onderzoeksrapport al contact met de organisatie gehad om beheersmaatregelen te nemen op de geconstateerde kwetsbaarheden. Er worden telkens nieuwe methoden en technieken ontwikkeld en gebruikt door kwaadwillenden. Het is daarom goed om regelmatig, bijvoorbeeld jaarlijks, een vergelijkbare penetratietest uit te laten voeren.

Aanbeveling: Voer als onderdeel van het informatiebeveiligingsbeleid regelmatig een penetratietest uit.

De belangrijkste conclusie uit de penetratietest is dat patch management verder kan worden verfijnd, zodat systemen minder kwetsbaar zijn. Waar systemen niet bijgewerkt zouden kunnen worden, dienen aanvullende mitigerende maatregelen te worden bepaald.

Aanbeveling: Herzie het beleid ten aanzien van patch management en zorg dat systemen systematisch en periodiek worden bijgewerkt waar mogelijk.

Onderzoeksvragen en aanpak

2.3. Onderzoeksvragen

We stellen in het onderzoek de volgende vraag centraal:

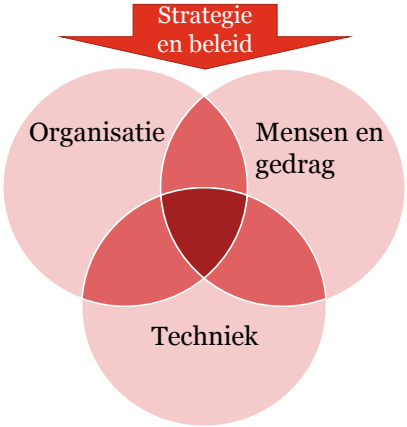
Is de informatiebeveiliging van de gemeenten Meppel, Staphorst, Steenwijkerland en Westerveld doeltreffend?

Met de vraag wordt bedoeld dat de gemeente gedaan heeft wat redelijkerwijs verwacht mag worden om te voorkomen dat informatie in verkeerde handen komt. Die doeltreffendheid kan alleen bereikt worden als drie elementen goed samenwerken, namelijk: de organisatie, het gedrag van mensen en de techniek. Er is strategie en beleid nodig om deze drie aspecten goed op elkaar af te stemmen. Voor deze aspecten zijn er vervolgens normen, wetten en regels die aangeven wat er verwacht mag worden. In ons onderzoek stellen we een normenkader op dat op deze wetten en handreikingen is gebaseerd.

De onderzoeksvraag gaat over beveiliging van informatie. We realiseren ons dat de meeste informatie tegenwoordig digitaal is, maar er is ook nog steeds informatie op papier. Ook deze informatie nemen we mee in het onderzoek.

Doel van dit onderzoek is te leren hoe we waar mogelijk kunnen bevorderen dat de gemeentelijke informatie in veilige handen is. Daarbij gaat het om de hoofdlijnen, om dat wat belangrijk is. De rekenkamercommissie wil met dit onderzoek de bewustwording voor dit onderwerp vergroten. Die bewustwording is overal belangrijk, bij de raad, het college en de ambtelijke organisatie.

Doeltreffende informatiebeveiliging gebaseerd op samenwerking van drie aspecten



Om de hoofdvraag verder uit te werken in deelvragen, stellen we daarom vragen over de organisatie, mensen en gedrag en de techniek. Hieronder presenteren we deze deelvragen in een tabel met daarnaast de normen die we bij die vragen hanteren.

Organisatie en beleid

Startpunt van het onderzoek vormt het gemeentelijke beleid en de wettelijke vereisten.

Informatiebeveiliging kan niet zonder systematische en actuele risicoanalyses. Bij de risico's horen maatregelen om die risico's te verminderen en plannen om met incidenten om te gaan. Daarbij kan gedacht worden aan een goed beheer van ICT-middelen, cryptografie, toegangsbeveiliging zodat niet iedereen toegang heeft tot data en systemen, fysieke beveiliging, goede afspraken met leveranciers, beheer van informatiebeveiligingsincidenten (datalekken) en back-up & disaster recovery.

De basis van het informatiebeveiligingsbeleid kan gevonden worden in diverse standaarden en regelingen (zoals de Baseline Informatiebeveiliging Gemeenten (BIG) en de Algemene Verordening Gegevensbescherming (AVG) en ISO2001:2013). De gemeente beheert daarbij een aantal gevoelige systemen (BRP, uitkeringen, DiGiD, Wmo). Het is belangrijk dat het informatiebeveiligingsbeleid juist met deze systemen rekening houdt.

Het beleid heeft vervolgens een vertaling nodig naar concrete activiteiten en daarvoor zijn voldoende middelen nodig, vaak vooral in de vorm van voldoende budget, kennis en capaciteit. Een ander aspect van deze concrete vertaling is het beleggen van rollen en verantwoordelijkheden voor informatiebeveiliging in de organisatie. Tenslotte dient de raad periodiek geïnformeerd te worden op hoofdlijnen over de status van de informatiebeveiliging.

Mens en gedrag

Het tweede element in het geheel van informatiebeveiliging is mens en gedrag. Het hogere management vervult een belangrijke voorbeeldfunctie, bijvoorbeeld door de wijze waarop invulling wordt gegeven aan de rollen en verantwoordelijkheden. Het management dient daarom actief betrokken te zijn bij (aspecten van) informatiebeveiliging. Verder is het belangrijk dat er een breder bewustzijn binnen de organisatie is van het belang van informatiebeveiliging en de wijze waarop medewerkers daarin een rol spelen en verantwoordelijkheid dragen.

Techniek

Technisch is het belangrijk dat het netwerk en bedrijfskritische systemen voldoende technisch beveiligd zijn om ongeautoriseerde toegang te voorkomen. Met een scan en eventueel een test door een specialist zal deze beveiliging getoetst worden, om zo de zwakke plekken aan te kunnen wijzen. Doel daarvan is deze zwakke plekken te verbeteren. Het onderzoek zal specifiek aandacht schenken aan processen met gevoelige informatie, zoals persoonlijke gegevens.

2.4. Deelvragen en normenkader

Per deelvraag zijn voor dit onderzoek een aantal normen geformuleerd.

Organisatie en beleid	**Normen**
1.1 Worden er systematische en actuele risicoanalyses gemaakt rond informatiebeveiliging uitgevoerd en worden er op basis daarvan passende beheersmaatregelen genomen?	• Er worden met voldoende frequentie risico analyses uitgevoerd. In de risicoanalyses zijn de belangrijkste risico's geïdentificeerd. De risicoanalyses geven ook inzicht in specifieke risico's m.b.t. het beheer van (bijzondere) persoonsgegevens. • Relevante beheersmaatregelen worden vastgesteld op basis van good practices, zoals de BIG. • Het totaal aan maatregelen geeft voldoende waarborgen voor een goede bescherming van de (bijzondere) persoonsgegevens die de gemeente in beheer heeft.

1.2 Biedt het informatiebeveiligingsbeleid voldoende basis voor de bescherming van gegevens?	• De gemeente beschikt over een actueel overkoepelend informatiebeveiligingsbeleid dat op onderdelen is uitgewerkt in specifieke procedures en/of richtlijnen. • De inhoud van het informatiebeveiligingsbeleid sluit aan op good practices, zoals de BIG en relevante wet- en regelgeving (zoals de AVG). • In het informatiebeveiligingsbeleid is beschreven hoe invulling wordt gegeven aan de PDCA-cyclus rond informatiebeveiliging. • Het informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld. • de gemeente classificeert de informatie die zij verwerkt naar mate van beschikbaarheid, integriteit en vertrouwelijkheid.
1.3 Is het informatiebeveiligingsbeleid vertaald naar concrete activiteiten en zijn hiervoor voldoende middelen beschikbaar gesteld?	• De gemeente beschikt over een actueel informatiebeveiligingsplan met concrete activiteiten om nader invulling te geven aan diverse onderdelen van het informatiebeveiligingsbeleid. Op basis van de activiteiten is er een urenraming en budget opgesteld. • De gemeente beschikt over procedures en of richtlijnen waarin diverse onderdelen van het informatiebeveiligingsbeleid nader invulling hebben gekregen. • De PDCA-cyclus krijgt in de praktijk uitvoering zoals beschreven in het beleid.
1.4 Zijn binnen de organisatie de rollen en verantwoordelijkheden voor informatiebeveiliging helder belegd?	• Taken en verantwoordelijkheden rond informatiebeveiliging en de bescherming van (bijzondere) persoonsgegevens zijn duidelijk belegd in de organisatie.
1.5 Wordt de Raad periodiek geïnformeerd over de status van informatiebeveiliging?	• Het college legt verantwoording af over het informatiebeveiligingsbeleid, de gemaakte afspraken en geplande activiteiten.

Mens en gedrag	**Normen**
2.1 Is het hogere management actief betrokken bij informatiebeveiliging en het uitdragen daarvan binnen de organisatie?	• De directie stelt zich duidelijk achter het informatiebeveiligingsbeleid, vervult een voorbeeldfunctie en informeert en motiveert medewerkers om het beleid actief gestalte te geven.

2.2 Zijn medewerkers bewust van informatiebeveiligingsrisico's en is voor medewerkers duidelijk wat van hun verwacht wordt ten aanzien van informatiebeveiliging?	• Alle medewerkers gaan bewust en veilig om met vertrouwelijke informatie. De regels wat betreft vertrouwelijkheid, integriteit, beschikbaarheid en privacybescherming worden nageleefd. De gemeente zorgt ervoor dat iedere medewerker goed op de hoogte is van de regels, de risico's en de plicht om incidenten en datalekken te melden.

Techniek	**Normen**
3.1 Zijn het netwerk en bedrijfskritische systemen voldoende technisch beveiligd om ongeautoriseerde toegang te voorkomen? 3.2 Is er extra aandacht voor de technische beveiliging van gevoelige informatie, zoals persoonlijke gegevens?	• Er is een up-to-date overzicht van systemen, applicaties en dergelijke, waarin de gemeente informatie verwerkt. • De gemeente heeft afdoende technische maatregelen getroffen om ongeautoriseerde interne en externe toegang te voorkomen. • De gemeente heeft voldoende aanvullende technische beheersmaatregelen genomen om risico's ten aanzien van de bescherming van gevoelige informatie (waaronder persoonsgegevens) te waarborgen.

2.5. *Aanpak van het onderzoek*

In deze paragraaf geven we kort aan welke stappen zijn doorlopen bij dit onderzoek. We zijn het onderzoek begonnen met een startgesprek met de direct betrokkenen van de ambtelijke organisatie om doel, aanpak en planning van het onderzoek toe te lichten. Na het startgesprek verzamelden we de feitelijke informatie, we voerden een kort dossieronderzoek uit aan de hand van documenten en we voerden enkele inventariserende gesprekken. Met de resultaten daarvan stelden we een normenkader op. Vervolgens zijn we praktijkgegevens verzameld om de praktijk te toetsen aan deze normen. De bevindingen zijn vastgelegd in deze rapportage. Zo hebben we het onderzoek opgedeeld in vijf stappen, die in het onderstaande schema zijn aangegeven. De paragraaf hieronder geeft een meer gedetailleerde toelichting per stap.

Aanpak in vijf stappen

Activiteit	Toelichting	Resultaat
1. Start	• Startbijeenkomst met rekenkamercommissie: definitieve aanpak, wensen en verwachtingen, werkafspraken • Startbijeenkomst met betrokken ambtenaren	• Helder en gedragen plan van aanpak, goede werkafspraken
2. Inventarisatie	• Documentenanalyse, eventueel enkele inventariserende gesprekken	• Eerste beeld van beveiligingsbeleid en rapportages
3. Normenkader	• Opstellen normenkader, overleg met rekenkamercommissie, vaststellen normenkader	• Heldere normen voor alle onderzoeksvragen
4. Data verzamelen	• Interviews betrokken ambtenaren, diverse tests, online vragenlijst medewerkers, groepsgesprek raadsleden, leer- en werksessie gemeenten,	• Bevindingenrapport met bevindingen per deelvraag
5. Rapportage	• Afstemming rekenkamercommissie, ambtelijke wederhoor, eventuele aanpassingen en aanvullen met aanbevelingen, bestuurlijk wederhoor, ondersteuning bij presentatie rapportage	• Rapportage per gemeente en koepelnotitie

Stap 1: Start
Bij de start van het onderzoek zijn alle relevante documenten opgevraagd, is overlegd over de te houden interviews en is een contactpersoon voor het onderzoek per gemeente afgesproken om verdere werkafspraken te maken. Door de onderzoeksvragen en de aanpak toe te lichten werkte de rekenkamercommissie aan het vergroten van het draagvlak voor de uiteindelijke conclusies en aanbevelingen.

Stap 2: Inventarisatie
We hebben bewust eerst een globale inventarisatie uitgevoerd op basis van enkele sleuteldocumenten en gesprekken. Op basis van dat eerste resultaat is gekozen voor een verdieping (in stap 4) die past bij de gemeente.

Stap 3: Normenkader
Het onderzoek is gebaseerd op een normenkader per deelvraag. Dit normenkader is gelijk voor de vier gemeenten. Er waren geen inhoudelijke redenen om verschillende normen te hanteren. Bovendien maakte eenzelfde normenkader het leren en vergelijken tussen de vier gemeenten beter mogelijk.

Stap 4: Data verzamelen
In iedere gemeente zijn een aantal interviews gehouden met de direct betrokkenen bij informatiebeveiliging. Daarnaast is in iedere gemeente een vragenlijst uitgezet onder de medewerkers om de kennis en de mate waarin medewerkers bewust omgaan met informatiebeveiliging in beeld te krijgen. Verder zijn in iedere gemeente enkele applicaties en het beheer daarvan bekeken en is er in iedere gemeente een veiligheidsscan uitgevoerd.

Naast deze werkzaamheden is op basis van de inventarisatie door de rekenkamer besloten het onderzoek deels van maatwerk te voorzien en aan te passen aan de behoefte per gemeente. Alle vier de gemeenten vonden het een goed idee om de resultaten van het onderzoek uit te wisselen en zo van elkaar te leren. De rekenkamercommissie heeft daarom besloten direct na het verzamelen van alle bevindingen en de ambtelijke wederhoor een werksessie te organiseren met de ambtelijk betrokkenen van de vier gemeenten en het onderzoeksbureau, met als doel ervaringen uit te wisselen en te leren van elkaar.

In Westerveld bleek voor het laatst in 2016 in samenwerking met de gemeente Meppel een penetratietest te zijn uitgevoerd (dit is te zien als een meer uitvoerige kwetsbaarheidsscan die we in iedere gemeente gehouden hebben). Voor Westerveld is een interne en externe penetratietest uitgevoerd. De kwetsbaarheidsscan beoogt

kwetsbaarheden in het netwerk vast te stellen en te bezien of het mogelijk is om ongeautoriseerde toegang te verkrijgen tot één specifiek kritisch systeem. De scan levert ook op welke maatregelen kunnen helpen om de beveiliging waar mogelijk te verbeteren. De penetratietest is uitgebreider dan de kwetsbaarheidsscans die we in Meppel en Steenwijkerland hebben uitgevoerd. Bij de interne test wordt er gewerkt vanuit het perspectief van een interne aanvaller, bij een externe test wordt er gewerkt vanuit het perspectief van een hacker. Dat betekent concreet dat er bij een penetratietest meer kwetsbaarheden aan het licht komen. De resultaten tussen de vier gemeenten op dit vlak zijn daarom niet goed onderling te vergelijken.

De (technische) kwetsbaarheden die we gevonden hebben bij de penetratietest hebben we direct op een veilige manier verstuurd aan de CISO van de betrokken gemeente. Zo kon de CISO direct aan de slag om deze zaken op te lossen. We doen van deze bevindingen niet in detail verslag in deze openbare rapportage. Dat zou de gemeente immers kunnen schaden. In het kader van de ambtelijke en bestuurlijke wederhoor vragen we als rekenkamer echter wel of de gevonden kwetsbaarheden zijn verholpen, zodat u daar als raad van op de hoogte bent. In deze rapportage vindt u een kort verslag op hoofdlijnen op dit punt.

Stap 5: Rapportage

Tenslotte is na ambtelijk en bestuurlijk hoor- en wederhoor deze rapportage opgesteld.

3. Bevindingen

In dit hoofdstuk zijn de bevindingen per onderzoeksvraag en per norm aangegeven. Bij de bevindingen is telkens aangegeven op basis waarvan de bevinding is opgenomen, dat kunnen documenten, interviews, vragenlijsten, tests of andere bronnen zijn.

3.1. Organisatie en beleid

Onderzoeksvraag 1.1: Worden er systematische en actuele risicoanalyses gemaakt rond informatiebeveiliging en worden er op basis daarvan passende beheersmaatregelen genomen?

Norm: Er worden met voldoende frequentie risicoanalyses uitgevoerd. In de risicoanalyses zijn de belangrijkste risico's geïdentificeerd. De risicoanalyses geven ook inzicht in specifieke risico's m.b.t. het beheer van (bijzondere) persoonsgegevens.

Het informatiebeveiligingsbeleid van de gemeente Westerveld beschrijft dat risicoanalyse(s) uitgevoerd worden, maar RI&E-documentatie is niet beschikbaar. Uit verdere navraag is gebleken dat in 2010 de laatste risicoanalyse is uitgevoerd.

In latere jaren is geen RI&E meer uitgevoerd. Beheersmaatregelen worden vastgesteld op basis een analyse van de Baseline Informatiebeveiliging voor Gemeenten, daarbij wordt gekeken in welke mate de maatregelen zijn uitgevoerd. Dit wordt een GAP-analyse op de BIG genoemd. Prioriteit bij het oppakken van ontbrekende maatregelen is gesteld op basis van het risico dat het ontbreken van een maatregel in zich draagt.

Norm: Relevante beheersmaatregelen worden vastgesteld op basis van good practices, zoals de BIG.

De gemeente Westerveld heeft een gap-analyse uitgevoerd op basis van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). De laatste gap-analyse is uitgevoerd in 2018.

In het GAP-analyse document geeft de gemeente Westerveld per BIG-maatregel aan wat de status is:
- Geaccepteerd risico;
- Direct implementeren;
- Later implementeren;
- Onbekend;
- Niet van toepassing;
- Reeds geïmplementeerd.

Uit interviews blijkt dat er een werkgroep informatiebeveiliging is. Deze groep komt eenmaal per zes weken bij elkaar. De agenda wordt bepaald door de gap-analyse op de BIG.

Norm: Het totaal aan maatregelen geeft voldoende waarborgen voor een goede bescherming van de (bijzondere) persoonsgegevens die de gemeente in beheer heeft.

De gemeente Westerveld heeft in het beleidsplan (hoofdstuk 6 – governance) beschreven welk soort maatregelen noodzakelijk zijn om te voldoen aan de AVG. Het beschrijft dat op bestuurlijk en ambtelijk niveau een aantal organisatorische maatregelen noodzakelijk zijn. Hoofdstuk 6.2 van dat document beschrijft dat teamleiders primair verantwoordelijk zijn om passende technische en organisatorische maatregelen te treffen.

Verder beschrijft het document dat op het gebied van mens, proces en techniek maatregelen getroffen moeten worden.

Hoofdstuk II.II van het informatiebeveiligingsbeleid van de gemeente Westerveld beschrijft de informatieveiligheidspiramide. Deze piramide beschrijft de opzet van informatiebeveiliging in stappen, waarbij stap 1 het (opstellen van) beleid is. Stap 2 is de informatieveiligheidsanalyse. In die stap wordt een risico-inventarisatie en evaluatie uitgevoerd (RI&E). Stap 3 is het opstellen van een actieplan en stap 4 is het uitwerken van het beleid en de maatregelen naar de verschillende deelgebieden van de gemeente.

Met de opzet zoals beschreven is in 2014 gestart, maar met het vertrek van de CISO in 2015 zijn deze stappen niet meer consequent uitgevoerd. Zoals eerder gesteld is een RI&E destijds niet uitgevoerd. Uit de interviews bleek dat, hoewel er een werkgroep informatiebeveiliging is, deze werkgroep niet heeft gefunctioneerd zoals bedoeld. Het ontbrak aan tijd en prioriteit. De werkgroep miste een aanjager door het ontbreken van voldoende invulling van de rol van de CISO (chief information officer). Inmiddels is de capaciteit versterkt, zoals verderop in dit rapport wordt aangegeven.

In relatie tot dit onderwerp zijn in de enquête die gehouden is onder de medewerkers van de gemeente Westerveld een aantal vragen gesteld. Op de onderstaande onderdelen scoort Westerveld dicht bij het gemiddelde van de vier onderzochte gemeenten. De vragen en de reacties staan hieronder:

De gemeente doet de juiste dingen op het gebied van informatiebeveiliging:

Keuze:	**Aantal antwoorden:**	**Percentage:**	**Percentage gemiddelde van de vier onderzochte gemeenten:**
Helemaal eens	0	0%	5%
Eens	13	43%	40%
Neutraal	15	50%	48%
Oneens	2	7%	6%
Helemaal oneens	0	0%	0%

De gemeente doet de juiste dingen om de gegevens van eigen medewerkers te beschermen:

Keuze:	**Aantal antwoorden:**	**Percentage:**	**Percentage gemiddelde van de vier onderzochte gemeenten:**
Helemaal eens	1	3%	6%
Eens	13	43%	37%
Neutraal	13	43%	51%
Oneens	2	7%	4%
Helemaal oneens	1	3%	1%

De gemeente doet de juiste dingen om de gegevens van haar inwoners te beschermen:

Keuze:	**Aantal antwoorden:**	**Percentage:**	**Percentage gemiddelde van de vier onderzochte gemeenten:**
Helemaal eens	1	3%	7%
Eens	15	50%	46%
Neutraal	13	43%	42%
Oneens	1	3%	4%
Helemaal oneens	0	0%	0%

Onderzoeksvraag 1.2: Biedt het informatiebeveiligingsbeleid voldoende basis voor de bescherming van gegevens?

Norm: De gemeente beschikt over een actueel overkoepelend informatiebeveiligingsbeleid dat op onderdelen is uitgewerkt in specifieke procedures en/of richtlijnen.

De gemeente Westerveld heeft een informatiebeveiligingsbeleid dat stamt uit 2014. Ten tijde van het onderzoek lag een nieuw concept gereed voor vaststelling door het college. De nieuwe CISO heeft sinds zijn aantreden in september 2018 werk gemaakt van het finaliseren van dit beleid. De opzet van dit document is een doorontwikkeling van het informatiebeveiligingsbeleid van 21 november 2013. Daarnaast zijn er voorbeelden van een aantal procedures, bijvoorbeeld met betrekking tot de afvoer van (oude) computers, autorisatie tot gemeentelijke voorziening en/of het lokale gemeentelijke netwerk, back-up en restore, de rapportage van incidenten, enzovoorts.

In de praktijk worden maatregelen beperkt doorgevoerd. Zo is er bijvoorbeeld wel nagedacht over het afschermen van gegevens: een afdeling heeft een gescheiden omgeving in het DMS-systeem en een eigen omgeving op de netwerk share. De informatie daar is dan alleen voor de afdeling zelf inzichtelijk. Ook binnen die omgeving kunnen stukken aangeduid worden als vertrouwelijk.

Anderzijds is in interviews aangegeven dat een aantal procedures nog niet zijn uitgewerkt. Als oorzaak wordt gewezen op het ontbreken van een volwaardige invulling van de CISO-rol. Met de komst van de nieuwe fulltime CISO is de mogelijkheid ontstaan om procedures en processen verder uit te laten werken en aan te laten scherpen.

Norm: De inhoud van het informatiebeveiligingsbeleid sluit aan op good practices, zoals de BIG en relevante wet- en regelgeving (zoals de AVG).

De Gemeente Westerveld beschrijft in haar informatiebeveiligingsbeleid zich te baseren op de ISO 27001 en ISO 27002 normering en daarbij is ook aangegeven dat het beleid gebaseerd is op de BIG én rekening is gehouden met wettelijke kaders.

Uit de interviews blijkt ook dat de gemeente zich baseert op de wereldwijd geaccepteerde standaarden. Zoals eerder ook beschreven wordt de agenda van de werkgroep informatiebeveiliging met name bepaald door de resultaten van de gap-analyse op de BIG.

Norm: In het informatiebeveiligingsbeleid is beschreven hoe invulling wordt gegeven aan de PDCA-cyclus rond informatiebeveiliging.

Het informatiebeveiligingsbeleid van de gemeente Westerveld beschrijft in hoofdstuk 1.5:

"Om borging van het informatieveiligheidsbeleid en de daarvan afgeleide plannen te realiseren, wordt naast een toebedeling van rollen (zie hoofdstuk 2), onderstaande Plan, Do, Check, Act (PDCA) cyclus doorlopen. Alhoewel altijd tussentijds documenten kunnen worden bijgesteld, worden onderstaande uitgangspunten gehanteerd voor het doorlopen van de PDCA-cyclus (zie figuur 2):

1. ***Informatieveiligheidsbeleid**: bevat het informatieveiligheidsbeleid en de visie op informatieveiligheid. Bijstelling van het informatieveiligheidsbeleid vindt plaats in een cyclus van 3 jaar. Indien zich grote wijzigingen voordoen vindt actualisatie eerder plaats.*
2. ***Informatieveiligheidsanalyse**: bevat de risicoanalyse (de toets aan de praktijk) op basis van informatieveiligheidsbeleid en de normen die hierin zijn vermeld of de normen waar in het beleid naar wordt gerefereerd. Bijstelling van de informatieveiligheidsanalyse vindt plaats na 1 tot 2 jaar;*
3. ***Actieplan Informatieveiligheid**: bevat de concrete, geprioriteerde acties volgend uit de informatieveiligheidsanalyse. Bijstelling (hieronder valt ook de voortgang op de realisatie van de afgesproken acties en maatregelen) van het actieplan Informatieveiligheid vindt (conform de bespreking in het informatieveiligheidsoverleg zie paragraaf 2.3) twee- tot viermaal per jaar plaats."*

Norm: Het informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld.

Het informatiebeveiligingsbeleid van de gemeente Westerveld beschrijft in hoofdstuk 1.5 dat het informatieveiligheidsbeleid eenmaal per 3 jaar wordt bijgesteld, of eerder in geval van grote wijzigingen (zie ook het voorgaande norm). Het formele beleid stamt uit 2014. Het concept beleid is van maart 2018 en het is belangrijk dat dit beleid wordt bijgesteld, gevalideerd en gefinaliseerd.

Uit interviews blijkt dat de nieuwe CISO dit beleid als actiepunt heeft opgepakt. Het beleid wordt op zeer korte termijn opnieuw vastgesteld.

Norm: De gemeente classificeert de informatie die zij verwerkt naar mate van beschikbaarheid, integriteit en vertrouwelijkheid.

Hoofdstuk 3 van het informatiebeveiligingsbeleid beschrijft de classificatie en het beheer van informatie en bedrijfsmiddelen. Op pagina 29 staat het classificatietabel:

Niveau	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Geen / 0	**Niet nodig** gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn *(bv: ondersteunende tools als routeplanner)*	**Niet zeker** informatie mag worden veranderd *(bv: templates en sjablonen)*	**Openbaar** informatie mag door iedereen worden ingezien *(bv: algemene informatie op de externe website van de gemeente*
Laag / I	**Belangrijk** informatie mag incidenteel niet beschikbaar zijn *(bv: administratieve gegevens)*	**Beschermd** het bedrijfsproces staat enkele (integriteits-) fouten toe *(bv: interne rapportages)*	**Bedrijfsvertrouwelijk** informatie is toegankelijk voor alle medewerkers van de organisatie *(bv: informatie op het intranet en concept college/raad voorstellen)*
Midden / II	**Noodzakelijk** informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk *(bv: voorwaardelijke primaire proces informatie)*	**Hoog** het bedrijfsproces staat zeer weinig fouten toe *(bv: bedrijfsvoeringinformatie en primaire procesinformatie zoals vergunningen)*	**Vertrouwelijk** informatie is alleen toegankelijk voor een beperkte groep gebruikers *(bv: persoonsgegevens, bijzondere financiële gegevens, zoals aanbestedingscalculaties)*
Hoog / III	**Essentieel** informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten *(bv: basisregistratie BRP)*	**Absoluut** het bedrijfsproces staat geen fouten toe *(bv: specifieke gemeentelijke informatie waaraan rechten zijn te ontlenen in b.v in basisregistratie of op de website)*	**Geheim** informatie is alleen toegankelijk voor direct aan de taak toegewezen persoon *(bv: zorggegevens, strafrechtelijke informatie)*

Uit interviews blijkt dat in de praktijk met bepaalde stukken vertrouwelijk wordt omgegaan. Bijvoorbeeld als het gaat om disciplinaire maatregelen. Het stuk krijgt het label ‘Vertrouwelijk’ en is daardoor niet zichtbaar in de agenda of in publieke stukken.

Daarnaast heeft de gemeente de mogelijkheid om informatie te beveiligen en het gebruik daarvan te beperken tot bepaalde personen.

In de enquête die als onderdeel van het onderzoek is uitgezet onder de medewerkers van de gemeente Westerveld, is ook een vraag gesteld over dataclassificatie. Westerveld scoort daarbij gemiddeld. Hieronder de vraag en de reactie daarop:

Zou u kunnen beoordelen wat de gevoeligheid is van de gegevens waarmee u dagelijks werkt, als dat u zou worden gevraagd? (Denk in termen van openbaar, vertrouwelijk en geheim)

Keuze:	Aantal antwoorden:	Percentage:	Percentage gemiddelde van de vier onderzochte gemeenten:
Zeer goed	8	27%	32%
Redelijk goed	18	60%	55%
Matig	3	10%	10%
Zeer beperkt	1	3%	4%
Helemaal niet	0	0%	0%

Onderzoeksvraag 1.3: Is het informatiebeveiligingsbeleid vertaald naar concrete activiteiten en zijn hiervoor voldoende middelen beschikbaar gesteld?

Norm: De gemeente beschikt over een actueel informatiebeveiligingsplan met concrete activiteiten om nader invulling te geven aan diverse onderdelen van het informatiebeveiligingsbeleid. Op basis van de activiteiten is er een urenraming en budget opgesteld.

De gemeente Westerveld heeft het beleidsplan van 2014 dit is in 2014 vertaald naar actieplan of jaarplan voor 2014. In de jaren daarna is er gaan jaarplan meer opgesteld.

Norm: De gemeente beschikt over procedures en of richtlijnen waarin diverse onderdelen van het informatiebeveiligingsbeleid nader invulling hebben gekregen.

Een aantal procedures zijn beschreven, zoals de afvoer van (oude) computers, autorisatie tot gemeentelijke voorziening en/of het lokale gemeentelijke netwerk, back-up en restore, de rapportage van incidenten, enzovoorts.

Uit interviews blijkt dat in de praktijk een aantal richtlijnen ten aanzien van informatiebeveiliging worden gehanteerd. Hierbij valt bijvoorbeeld te denken aan autorisaties: het bepalen van de vertrouwelijkheid van bepaalde stukken, het afschermen van gegevens, fysieke toegang. De relatie tussen de richtlijnen en de procedures en het informatiebeveiligingsbeleid is echter onduidelijk.

Norm: De PDCA-cyclus krijgt in de praktijk uitvoering zoals beschreven in het beleid.

In het beveiligingsbeleid in hoofdstuk 1.5 is beschreven hoe de PDCA-cyclus vorm krijgt. In hoofdstuk 2.3 is beschreven dat de CISO-voorzitter is van het overleg informatieveiligheid. Dat overleg vindt 2 tot 4 maal per jaar plaats.

Uit zowel documentatie als interviews blijkt dat bovenstaande PDCA-cyclus in de praktijk niet als zodanig wordt gevolgd. Een risicoanalyse in de zin van een RI&E is het laatst in 2010 uitgevoerd. Wel is er een gap-analyse op de BIG uitgevoerd. Deze resultaten en de daaruit voortvloeiende actiepunten worden besproken in de werkgroep informatiebeveiliging. Een actieplan c.q. jaarplan informatieveiligheid ontbreekt. De nieuwe CISO heeft dit als onderwerp op de agenda staan.

Onderzoeksvraag 1.4: Zijn binnen de organisatie de rollen en verantwoordelijkheden voor informatiebeveiliging helder belegd?

Norm: Taken en verantwoordelijkheden rond informatiebeveiliging en de bescherming van (bijzondere) persoonsgegevens zijn duidelijk belegd in de organisatie.

In het informatiebeveiligingsbeleid in hoofdstuk 2 is de organisatie van informatieveiligheid beschreven. In een ander document, het beleidsplan, is in hoofdstuk 6 de governance beschreven met betrekking tot de AVG. Het informatiebeveiligingsbeleid van de gemeente Westerveld beschrijft een aantal rollen en verantwoordelijkheden die breed worden belegd in de organisatie.

In het beleid zijn de rollen en verantwoordelijkheden duidelijk belegd. Uit de interviews blijkt dat de rol van CISO tot aan september 2018 werd ingevuld voor 4 uur per week. Daardoor ontbrak het 'aanjagen' van informatiebeveiliging, bijvoorbeeld in de werkgroep informatiebeveiliging. Met de komst van de nieuwe fulltime CISO kan dit een nieuwe impuls krijgen.

In de enquête die PwC heeft uitgezet onder de medewerkers van Westerveld zijn twee vragen gesteld met betrekking tot dit onderwerp. Uit de resultaten blijkt dat medewerkers even goed of iets beter op de hoogte zijn van rollen en verantwoordelijkheden in de organisatie in vergelijking met de andere drie onderzochte gemeenten.

Weet u wie op het gebied van informatiebeveiliging de belangrijkste functies vervullen in uw organisatie?

Keuze:	Aantal antwoorden:	Percentage:	Percentage gemiddelde van de vier onderzochte gemeenten:
Zeer goed	7	23%	24%
Redelijk goed	16	53%	44%
Matig	3	10%	21%
Zeer beperkt	1	3%	7%
Helemaal niet	1	3%	3%

Het is u bekend bij wie u terecht kunt als u een vraag zou hebben over het informatiebeveiligingsbeleid:

Keuze:	Aantal antwoorden:	Percentage:	Percentage gemiddelde van de vier onderzochte gemeenten:
Helemaal eens	10	33%	25%
Eens	16	53%	51%
Neutraal	2	7%	13%
Oneens	1	3%	8%
Helemaal oneens	1	3%	1%

Onderzoeksvraag 1.5: Wordt de raad periodiek geïnformeerd over de status van de informatiebeveiliging?

Norm: Het college legt verantwoording af over het informatiebeveiligingsbeleid, de gemaakte afspraken en geplande activiteiten.

In hoofdstuk II.IV van het informatiebeveiligingsbeleid is beschreven dat het college van burgemeester en wethouders op bestuurlijk niveau de verantwoordelijkheid heeft voor controle en toetsing op informatieveiligheid.

Informatiebeveiliging wordt als paragraaf opgenomen in het jaarverslag. Via deze paragraaf wordt de raad geïnformeerd over informatiebeveiliging. De medewerker Interne Controller van de gemeente Westerveld verzorgt deze rapportage. Bij de geïnterviewden was dit proces niet altijd bekend. Er is geen specifiek collegelid verantwoordelijk voor informatiebeveiliging.

De paragraaf bedrijfsvoering van de jaarrekening bevat een aparte kop informatiebeveiliging. De paragrafen in de jaarrekening worden in de loop van 2014 tot en met 2017 een stuk korter. In het verslag van 2014 is de

totstandkoming en het doel van het informatiebeveiligingsbeleid kort weergegeven. In 2015 is in kortere bewoordingen het informatiebeveiligingsbeleid weer toegelicht en is aangegeven dat niet alle geplande activiteiten zijn uitgevoerd. In de jaarrekening van 2016 wordt o.a. vermeld dat er een onderzoek is gedaan naar de beveiliging van het netwerk en dat de daaruit voortgekomen bevindingen zijn opgelost. In 2017 is de invoering van de ENSIA toegelicht (eenduidige vragenlijst die diverse zelfevaluaties vervangt) en wordt de invoering van de AVG genoemd.

3.2. Mens en gedrag

Het tweede element in het geheel van informatiebeveiliging is mens en gedrag.

Onderzoeksvraag 2.1: Is het hogere management actief betrokken bij informatiebeveiliging en het uitdragen daarvan binnen de organisatie?

Norm: De directie stelt zich duidelijk achter het informatiebeveiligingsbeleid, vervult een voorbeeldfunctie en informeert en motiveert medewerkers om het beleid actief gestalte te geven.

Het beleid van de gemeente Westerveld beschrijft de rollen en verantwoordelijkheden voor informatiebeveiliging.

Uit interviews blijkt dat de gemeente Westerveld geen strikt hiërarchische organisatie is. Verantwoordelijkheid voor informatiebeveiliging ligt zowel in het beleid (voor een deel) als in de praktijk bij iedereen. Het management moet er wel bij betrokken worden. Het management, het college en de raad worden nu nog zeer beperkt betrokken bij informatiebeveiliging.

De meningen liepen uiteen als het ging of het management informatiebeveiliging bespreekbaar maakt. De een gaf aan dat binnen de verschillende teams van de gemeente informatiebeveiliging als onderwerp wel bespreekbaar werd gemaakt, de ander gaf aan daar niets van te merken.

De rol van CISO is sinds de komst van de nieuwe CISO in september bewust losgekoppeld van de afdeling IT. Gecombineerd met het feit dat het een fulltime functie is geworden, veronderstelt dit dat de gemeente Westerveld op bestuurlijk niveau informatiebeveiliging belangrijk vindt.

In de enquête die is gehouden onder de medewerkers van de gemeente Westerveld is een stelling voorgelegd over actieve betrokkenheid van het management bij informatiebeveiliging. Westerveld scoort daarbij iets positiever dan het gemiddelde van de vier onderzochte gemeenten.

Het management is actief betrokken bij informatiebeveiliging en het uitdragen daarvan binnen (uw afdeling van) de organisatie:

Keuze:	Aantal antwoorden:	Percentage:	Percentage gemiddelde van de vier onderzochte gemeenten:
Helemaal eens	2	7%	6%
Eens	12	40%	32%
Neutraal	12	40%	46%
Oneens	3	10%	13%
Helemaal oneens	1	3%	3%

Onderzoeksvraag 2.2: Zijn medewerkers zich bewust van informatiebeveiligingsrisico's en is voor medewerkers duidelijk wat van hen verwacht wordt ten aanzien van informatiebeveiliging?

Norm: Alle medewerkers gaan bewust en veilig om met vertrouwelijke informatie. De regels wat betreft vertrouwelijkheid, integriteit, beschikbaarheid en privacybescherming worden nageleefd. De gemeente zorgt ervoor dat iedere medewerker goed op de hoogte is van de regels, de risico's en de plicht om incidenten en datalekken te melden.

De gap-analyse laat zien dat er geen bewustwordingscursus is, maar dat dat direct geïmplementeerd moet worden (zie punt 7.1.3.2 van de gap-analyse).

In de interviews werd unaniem aangegeven dat informatiebeveiliging wel onder de aandacht wordt gebracht, maar dat dit geen vaste regelmaat heeft. Er zijn geen vaste campagnes, maar er wordt geïnformeerd via bijvoorbeeld het personeelsoverleg, via mededelingen van de schermbeveiligingen, via het intranet zijn er

instructies beschikbaar bijvoorbeeld voor hoe om te gaan met USB-sticks en e-mail en ook Technisch Beheer plaatst berichten op het intranet wanneer er informatiebeveiligingsrisico's zijn. De Functionaris Gegevensbescherming heeft extra aandacht gevraagd voor privacy en het goed omgaan met gevoelige gegevens, wat nauw verbonden is met informatiebeveiliging.

Ook de komst van de AVG heeft geholpen bij de bewustwording van mensen. Volgens geïnterviewden is het management zich niet meer of minder bewust van informatiebeveiliging dan de 'gewone' medewerker.

In de enquête die als onderdeel van dit onderzoek is uitgezet onder de medewerkers van de gemeente Westerveld zijn een aantal vragen gesteld met betrekking tot dit onderwerp. De score is hier in de buurt of iets positiever dan het gemiddelde van de vier gemeenten. Ook is gevraagd welk cijfer de medewerkers de gemeente zouden geven. Dit zijn de resultaten:

Als u uw organisatie een cijfer zou mogen geven voor informatiebeveiliging (op een schaal van 1 tot 10) welk cijfer zou dat dan zijn?
Antwoord (gemiddelde van 30 cijfers): **6,5**

In hoeverre bent u bekend met het informatiebeveiligingsbeleid van de gemeente en de inhoud ervan?

Keuze:	**Aantal antwoorden:**	**Percentage:**	**Percentage gemiddelde van de vier onderzochte gemeenten:**
Zeer goed	3	10%	8%
Redelijk goed	14	47%	47%
Matig	8	27%	31%
Zeer beperkt	4	13%	10%
Helemaal niet	1	3%	5%

Is voor u duidelijk wat van u verwacht wordt ten aanzien van informatiebeveiliging?

Keuze:	**Aantal antwoorden:**	**Percentage:**	**Percentage gemiddelde van de vier onderzochte gemeenten:**
Zeer goed	4	13%	13%
Redelijk goed	18	60%	58%
Matig	7	23%	20%
Zeer beperkt	0	0%	5%
Helemaal niet	1	3%	3%

Zou u een situatie kunnen herkennen waarin sprake is van een datalek?

Keuze:	**Aantal antwoorden:**	**Percentage:**	**Percentage gemiddelde van de vier onderzochte gemeenten:**
Zeer goed	3	10%	14%
Redelijk goed	13	43%	50%
Matig	10	33%	24%
Zeer beperkt	2	7%	6%
Helemaal niet	2	7%	7%

U wordt regelmatig en goed geïnformeerd over informatiebeveiliging:

Keuze:	Aantal antwoorden:	Percentage:	Percentage gemiddelde van de vier onderzochte gemeenten:
Helemaal eens	1	3%	8%
Eens	13	43%	38%
Neutraal	11	37%	36%
Oneens	5	17%	17%
Helemaal oneens	0	0%	1%

U weet wat u moet doen als u een datalek zou hebben ontdekt of als u daarop attent zou zijn gemaakt:

Keuze:	Aantal antwoorden:	Percentage:	Percentage gemiddelde van de vier onderzochte gemeenten:
Helemaal eens	4	13%	17%
Eens	18	60%	51%
Neutraal	4	13%	18%
Oneens	3	10%	12%
Helemaal oneens	1	3%	2%

U bent op de hoogte van regels en risico's omtrent de omgang met gevoelige gegevens:

Keuze:	Aantal antwoorden:	Percentage:	Percentage gemiddelde van de vier onderzochte gemeenten:
Helemaal eens	5	17%	17%
Eens	18	60%	51%
Neutraal	6	20%	23%
Oneens	1	3%	6%
Helemaal oneens	0	0%	1%

3.3. Techniek

Het derde element van informatiebeveiliging is de techniek.

Onderzoeksvraag: 3.1 Zijn het netwerk en de bedrijfskritische systemen voldoende technisch beveiligd om ongeautoriseerde toegang te voorkomen?

Norm: Er is een up-to-date overzicht van systemen, applicaties en dergelijke, waarin de gemeente informatie verwerkt.

De Gemeente Westerveld heeft in een Excel sheet een overzicht van Leveranciers, Pakket namen, Referentiecomponenten binnen de gemeente, de Status (in productie of anders), Gebruikte technologieën en ten laatste welke organisatie gebruik maakt van het pakket (Westerveld of RUD Drenthe).

Norm: De gemeente heeft afdoende technische maatregelen getroffen om ongeautoriseerde interne en externe toegang te voorkomen.

Normaliter zou naar aanleiding van een risicoanalyse en/of een informatiebeveiligings(jaar)plan een overzicht van getroffen en te treffen maatregelen zijn gedocumenteerd. Deze documentatie is bij de gemeente Westerveld het laatst in het jaarplan voor 2014 aanwezig. Wat de samenhang is tussen de getroffen maatregelen kan niet worden geduid vanwege het ontbreken van een jaarplan in latere jaren.

Uiteraard zijn er wel een reeks van technische maatregelen getroffen om ongeautoriseerde interne en externe toegang te voorkomen. Hierbij kan gedacht worden aan firewalls, antivirus, veilig e-mailen, een applicatie voor veilige bestandsuitwisseling, beheer van mobiele apparaten (mobieltjes) en een pasjessysteem voor fysieke toegang.

Als onderdeel van het Rekenkameronderzoek Informatiebeveiliging heeft PwC bij de gemeente Westerveld een penetratietest onderzoek uitgevoerd. Het doel van dit onderzoek is om inzicht te verschaffen in de veiligheid van het interne netwerk van de gemeente en mogelijke verbeterpunten te identificeren. Een penetratietest wordt vaak gebruikt om de technische beveiliging te controleren.

Het belangrijkste resultaat van ons onderzoek is dat het verouderd netwerkprotocol, het gebruik van lokale administratieve accounts met eenzelfde wachtwoord op alle devices en missende beveiligingsupdates ongeautoriseerde toegang mogelijk maken tot het interne netwerk van de gemeente Westerveld. Zonder enige vorm van rechten op de infrastructuur van gemeente Westerveld was het mogelijk om de hoogst mogelijke rechten en daarmee volledige administratieve controle te verkrijgen op het interne netwerk. Daarmee kan een kwaadwillende toegang krijgen tot persoonsgegevens van inwoners van de gemeente Westerveld.

Onveilige configuratie maakt het mogelijk om rechten te verkrijgen en te verhogen op het interne netwerk

Er zijn kwetsbare netwerkprotocollen ingeschakeld op systemen van gemeente Westerveld. Het technische gevolg is dat zoekopdrachten voor onbekende, niet meer bestaande systemen op het netwerk worden omgeroepen. Een aanvaller kan van deze oproepen misbruik maken en zo kan een kwaadwillende betrekkelijk eenvoudig inzage kan krijgen in data op de server.

Een aanvaller moet zich eerst toegang verschaffen tot het netwerk van de gemeente om misbruik te kunnen maken van deze kwetsbaarheid. Daarna is de aanval zoals boven beschreven relatief eenvoudig uit te voeren. Het benodigde kennisniveau voor deze aanval ligt tussen beginner en gevorderde.

Lokale administratieve accounts met eenzelfde wachtwoord

Het wachtwoord van lokale administratieve accounts (beheeraccounts) is op meerdere servers identiek. Als een aanvaller zich toegang heeft verschaft tot het lokale administratieve account, kan hij diezelfde rechten op meerdere andere servers direct inzetten. Op die manier kan hij eenvoudig zijn toegang binnen het netwerk uitbreiden en met behulp van de informatie van andere systemen zijn toegangsrechten vermeerderen.

Om hier misbruik van te kunnen maken, moet een aanvaller zich eerst toegang hebben verschaft tot 1 systeem. De moeilijkheidsgraad voor die stap is verschillend. De drempel voor toegang tot andere systemen daarna is erg laag en dat is waar deze kwetsbaarheid om draait.

Missende kritieke updates maken gemeente Westerveld kwetsbaar voor ransomware aanvallen
Uit onze werkzaamheden bleek dat vijf systemen op het netwerk van gemeente Westerveld specifieke beveiligingsupdates missen, die nodig zijn om een ransomware aanval te stoppen. De kwetsbaarheid die het hier betreft, heeft destijds elders de *Wannacry ransomware* aanval gefaciliteerd.

Bij deze aanval zijn diverse organisaties getroffen door malafide programmatuur die alle gegevens op een systeem versleutelt en zichzelf door het hele netwerk verspreidt. Hierbij kunnen gegevens verloren raken en systemen voor lange tijd niet beschikbaar zijn. Deze zelfde kwetsbaarheid kan misbruikt worden om administratieve controle te verkrijgen op het interne netwerk. Het verhelpen van deze kwetsbaarheid door de betreffende update te installeren is dus zeer belangrijk omdat het risico van misbruik substantieel is.

Onderzoeksvraag: 3.2 Is er extra aandacht voor de technische beveiliging van gevoelige informatie, zoals persoonlijke gegevens?

Norm: De gemeente heeft voldoende aanvullende technische beheersmaatregelen genomen om risico's ten aanzien van de bescherming van gevoelige informatie (waaronder persoonsgegevens) te waarborgen.

Hoofdstuk 1.4 van het informatiebeveiligingsbeleid beschrijft dat als uit de risicoanalyse blijkt dat voor bepaalde gegevensverwerkingen een hoger beveiligingsniveau is vereist dan de BIG, dat een daarvoor verantwoordelijk persoon aanvullende maatregelen moet treffen.

In datzelfde hoofdstuk is ook beschreven dat afhankelijk van de klassenindeling van de AVG aanvullende maatregelen vereist kunnen zijn bij de verwerking van persoonsgegevens.

Een RI&E is niet uitgevoerd. Van daaruit is derhalve niet gedocumenteerd welke aanvullende maatregelen –ten opzichte van de BIG en waar nodig- zijn getroffen. Ook andere documentatie van aanvullende maatregelen vanwege een verhoogd risico is niet aanwezig.

Uit de interviews blijkt dat in de praktijk wel specifieke maatregelen zijn getroffen waar nodig. Een voorbeeld daarvan is dat het pasjessysteem (voor fysieke toegang) is losgekoppeld van het gemeentelijke netwerk.

Applicatieonderzoeken
In het kader van deze norm zijn bij de gemeente Westerveld een tweetal applicaties/applicatiesets onderzocht, te weten het Green Valley Zaaksysteem en het Sociaal Domein bestaande uit Aeolus, JVS en Veilig Opgroeien. De belangrijkste resultaten worden hieronder geschetst. Per onderwerp wordt gestart met een korte omschrijving, gevolgd door de bevindingen per applicatie. Voor meer context verwijzen wij u naar Annex A.

- *Autorisatiebeheer*

Het is belangrijk om alleen die personen toegang te geven tot een applicatie en/of delen van een applicatie die de toegang nodig hebben in het kader van hun functie. Op die manier wordt ongeautoriseerde toegang tot een minimum beperkt, evenals de kans op datalekken.

Het beheer van accounts verloopt voor Green Valley en voor het Sociaal Domein op een procesmatige wijze.

Periodieke controle op autorisaties wordt echter niet uitgevoerd. Dit kan in theorie betekenen dat er accounts aanwezig zijn die niet meer aan een persoon gelinkt kunnen worden of dat er accounts zijn met een teveel aan rechten. Wel is in verband tot het Sociaal Domein aangegeven dat het om een dermate kleine hoeveelheid gebruikers gaat, dat er hierdoor vanzelf wel overzicht is.

- *Beschikbaarheid*

Beschikbaarheid is van oudsher een belangrijk aspect. Als een applicatie niet beschikbaar is kan er ook niet gewerkt worden. Daarnaast is het van belang om goede backups te maken en te testen, zodat een applicatie binnen afzienbare tijd hersteld kan worden na een calamiteit.

Green Valley is een applicatie in de cloud, daardoor ligt beschikbaarheid als verantwoordelijkheid bij de leverancier. Dit blijkt in de praktijk goed geborgd te zijn.

- *Change management*

Het aanbrengen van veranderingen aan applicaties dient op een verantwoorde manier te gebeuren. Een historie van wijzigingen dient te worden bijgehouden en nieuwe wijzigingen dienen niet lichtvoetig te worden doorgevoerd. Daarom moeten nieuwe updates eerst goed worden getest. Dit om de stabiliteit en functionaliteit van de omgeving niet in gevaar te brengen. Maar hier moet ook nagedacht worden over welke medewerkers toegang hebben tot de gegevens.

Het doorvoeren van nieuwe updates voor Green Valley geschiedt door de nieuwe updates en functionaliteit eerst in een testomgeving te testen. Na goedkeuring van de gemeente wordt een update doorgevoerd in productie.

Voor het Sociaal Domein zijn ook twee omgevingen, Test en Productie. Er zijn echter wel minder personen die toegang hebben tot de testomgeving

In Green Valley is per zaaktype terug te herleiden tot aan het begin van de zaak hoe de instellingen zijn geweest. Hierdoor kan integriteit van de data bewaakt worden, doordat foutieve wijzigingen opgespoord kunnen worden.

Voor het Sociaal Domein wordt een historie van updates of configuratiewijzigingen niet specifiek bijgehouden. Alleen als een nieuwe update nieuwe functionaliteit heeft, dan wordt aan de afdeling gevraagd of ze die functionaliteit willen en zo ja, om dan een melding te openen in TOPdesk.

- *Risico op databeveiligingsincidenten*

Het risico op incidenten waardoor een datalek optreedt wordt beperkt door de inname, het gebruik van en toegang tot persoonsgegevens tot een minimum te beperken. Toegang tot extra gevoelige gegevens moet extra gereguleerd of beperkt worden.

Voor Green Vally is alle data in de testomgeving fictief. Dit betekent dat gevoelige gegevens niet via de testomgeving gelekt kunnen worden. Verder is er strenge toegangsregeling tot zaaktypen. Medewerkers hebben niet alleen wel of niet toegang tot een bepaalde zaak, maar kunnen indien noodzakelijk ook bepaalde onderdelen niet zien, zoals het BSN.

Voor Aeolus is er een anonimiseringsscript om de database in de Testomgeving te anonimiseren. Dat is dan in eerste instantie een backup vanuit Productie, maar wordt dus geanonimiseerd. Veilig Opgroeien Test bevat geen productiedata. In JVS staat in test een oude versie van de productiedatabase.

De gemeente heeft de thuiswerkplek zodanig ingesteld dat het niet mogelijk is om bestanden vanuit huis te uploaden naar danwel te downloaden van de werkplekomgeving. Dit verkleint de kans op datalekken.

- *AVG - Logging en Monitoring*

In het kader van de AVG is het van belang om aan te kunnen tonen dat data niet ongeautoriseerd benaderd is. Tevens ondersteunt dit bij enkele rechten van betrokkenen, zoals het recht om te weten wat er met persoonsgegevens gebeurd is.

Bij de gemeente Westerveld is voor Green Vally indien gewenst zeer gedetailleerd logging op te vragen, die aantoont wat er met persoonsgegevens is gebeurd.

Elke activiteit die iemand doet bij Veilig Opgroeien wordt gelogd, zoals het aanmaken. In Aeolus kan alles worden opgevraagd wat een gebruiker heeft gedaan. Ook activiteiten van beheerders worden vastgelegd. De

techlogs (onder andere storingen in de applicatie) van Aeolus gaan tot 8 weken terug in het verleden, de gebeurtenissen logs tot 1 maand.

- *Leveranciersmanagement*

Onder leveranciersmanagement verstaan we in het kader van dit onderzoek dat er goede afspraken zijn gemaakt over support (ondersteuning) en beschikbaarheid. Maar vooral dat dit goed functioneert in de praktijk.

Er zijn twee leveranciers. Ieder jaar is er van beide leveranciers een klantendag. De leverancier Horlings en Eerbeek organiseert iedere 2 maanden bijeenkomsten voor de noordelijke gemeenten, zodat zaken op het gebied van ondersteuning en beschikbaarheid regelmatig besproken kunnen worden. Er zijn tevens afspraken gemaakt met de leverancier van het zaaksysteem.

Er zijn wel afspraken vastgelegd met de leverancier over bijvoorbeeld de snelheid van het oppakken van support calls, maar de afspraken zijn nooit opgezocht, omdat de beheerder tevreden is over hoe de leveranciers de problemen oppakken.

- *Logische toegangsbeveiliging*

Naast autorisatiebeheer, wat het beheer van gebruikersaccounts behelst, is logische toegangsbeveiliging een maatregelen om ongeautoriseerde toegang tot persoonsgegevens te beperken. Bijvoorbeeld door 2-factor authenticatie in te zetten of door de applicatie alleen vanuit (een deel van) het gemeentenetwerk beschikbaar te stellen.

Bij de gemeente Westerveld is toegang tot Green Valley en het Sociaal Domein geregeld door middel van een gebruikersnaam en wachtwoord. Alleen voor Aeolus is dit gekoppeld aan het account wat iemand heeft voor de werkplekomgeving. Wachtwoorden moeten periodiek gewijzigd worden en er zitten (beperkte) complexiteitseisen aan.

Hoewel we dit niet konden vaststellen, wijze we erop dat het uitwisselen van deze authenticatiegegevens voor Green Valley niet onbeveiligd via de telefoon mag verlopen. Voor Sociaal Domein geldt dat een gebruiker een door Functioneel Beheer ingesteld wachtwoord altijd direct moet wijzigen bij de eerstvolgende keer dat hij/zij inlogt.

Toegang voor thuiswerken wordt door de gemeente Westerveld geregeld op basis van 2-factor authenticatie (gebruikersnaam, wachtwoord en code). Dat is een sterke manier van authenticatie.

A. Applicatieonderzoeken

A.1. Green Valley Zaaksysteem

Autorisatiebeheer
Nieuwe gebruikers worden aangemaakt door Functioneel Beheer. Personeelszaken vult een formulier in en geeft daarbij een referentieprofiel aan op basis waarvan het nieuwe account aangemaakt moet worden. Het referentieprofiel bepaalt de rollen en rechten van het nieuwe account. Wanneer een medewerker van functie verandert, dan moet de teamleider via TOPdesk een aanvraag doen om de rechten van de betreffende persoon te veranderen/verwijderen. Het uitdienstproces wordt geïnitieerd door Personeelszaken en verloopt via TOPdesk.

Standaard periodieke controles op autorisaties zijn er niet.

Naast de Productieomgeving is er ook een Testomgeving. In de testomgeving wordt gebruik gemaakt van fictieve useraccounts.

Om van buitenaf in te loggen moet een token worden gebruikt, het zogenaamde 2-factor authenticatie.

Beschikbaarheid
Green Valley is een applicatie in de cloud. Daardoor is beschikbaarheid met name een verantwoordelijkheid van de leverancier.

In het verleden kon de applicatie erg langzaam zijn en 'hangen'. Tegenwoordig is het stabieler, maar de applicatie kan nog steeds 'hikjes' vertonen.

Change management
Bij een nieuwe release van de applicatie controleert de gemeente Westerveld eerst de release notes. Vervolgens testen de beheerders de nieuwe release in de Testomgeving door dezelfde stappen te doorlopen die gebruikers ook zouden doorlopen. Als laatste stap wordt gecontroleerd of de in de release notes benoemde bug fixes ook daadwerkelijk zijn opgelost zoals beschreven. Als dat niet het geval is wordt daar melding van gemaakt bij de leverancier.

Pas na goedkeuring wordt een nieuwe release vrijgegeven voor Productie. De gemeente Westerveld heeft in het verleden een landelijke update geblokkeerd doordat in de nieuwe release een aantal essentiële issues werden ontdekt.

Voor wat betreft de configuratie is in een zaak (zaaktype) terug te herleiden tot aan het begin van de zaak hoe de settings ingesteld zijn geweest.

Risico op Databeveiligingsincidenten
De Testomgeving bevat geen productiedata. Alle data in de testomgeving is fictief.

Vanuit het gemeentenetwerk kan worden ingelogd met een gebruikersnaam en wachtwoord. Het is voor de gebruikers die rechten hebben op de applicatie mogelijk om gegevens te exporteren en lokaal op te slaan. Hiermee ontstaat er een risico op een datalek, als het gegevens uit productie betreft. De gegevens kunnen bijvoorbeeld op een USB-stick terecht komen die wordt verloren, of gemaild worden naar een verkeerd mailadres, of op een laptop worden opgeslagen waarna de laptop wordt gestolen of wordt verloren.

Van buiten het gemeentenetwerk moet eerst op het gemeentenetwerk ingelogd worden met een token. Het is daarna niet mogelijk om data uit de applicatie te exporteren en lokaal op een thuis-pc op te slaan.

Sommige zaaktypen zijn qua toegang strenger afgesteld, zodat alleen enkele mensen toegang hebben. Het BSN-nummer kan ook worden afgeschermd voor bepaalde gebruikers. Gebruikers die wel toegang hebben tot de

'Zaak', maar niet het BSN mogen zien, kunnen het BSN dan ook op geen enkele manier doorsturen of exporteren vanuit de applicatie.

AVG – Logging en Monitoring
Green Valley kent 2 vormen van audit logging:
- Zaak audit log. Deze blijft net zo lang bestaan als de levensduur (vernietigingstermijn) van een zaak (wordt mee vernietigd).
- Personen audit log (overzicht opvragingen): deze wordt 2 jaar bewaard.

Daarnaast kent Green Valley zogenaamde server logging om de toestand van de software te kunnen monitoren/analyseren. Deze logging wordt 2 maanden bewaard.

In de persoon audit logging staan geen gevoelige gegevens anders dan een BSN van een persoon die wordt opgevraagd. Andere persoonsgegevens worden niet gelogd.

In de zaak audit log staan wel mutaties over zaken en mogelijk personen. Deze worden via de software afgeschermd. Daarnaast is er een extra beveiliging die waarborgt dat records niet buiten de software om gemuteerd worden.

In de praktijk worden 'audit log' rapporten niet op een standaard periodieke basis opgevraagd. Daarmee wordt niet standaard gemonitord op ongeautoriseerde toegang. De audit log informatie wordt ad hoc opgevraagd wanneer er een situatie ontstaat waarin deze informatie nodig is.

Daarnaast is er een standaard "Historie" tabblad (audit log), waarin te zien is wat er in het verleden is gebeurd met een zaak. Zelfs is terug te zien wat er voorheen stond en waarin dat is gewijzigd (en door wie).

Leveranciersmanagement
Afspraken zijn vastgelegd in de overeenkomst technisch beheer & hosting Green Valley Suite en de overeenkomst applicatiebeheer en –onderhoud Green Valley Suite. Daarnaast is er een bewerkersovereenkomst met Green Valley afgesloten.

Jaarlijks worden TPM-verklaringen van Green Valley (applicatie) en Denit (de hosting partij) opgevraagd en gecontroleerd of de scope van zowel de TPM en interne verbeterpunten (vanuit ENSIA) de volledige norm omvatten. Green Valley is bezig met ISO27001 certificering en verwacht dit in februari 2019 rond te hebben. Ze gaan vanaf dan jaarlijks audits uit laten voeren door externe partij.

In de SNO (Service Niveau Overeenkomst) met Green Valley is de escalatieprocedure vastgelegd. Maandelijks is overleg tussen de gemeente en de accountmanager van Green Valley over lopende meldingen.

Logische toegangsbeveiliging
Gebruikers loggen in op de applicatie met een gebruikersnaam en wachtwoord. Het wachtwoord dient iedere 60 dagen vernieuwd te worden. De complexiteitseisen van het wachtwoord zijn beperkt: het aantal karakters kan opgegeven worden en ook dat het wachtwoord cijfers moet bevatten. Maar leestekens zijn niet te gebruiken in het wachtwoord. Dat ondersteunt de applicatie niet.

Wanneer een gebruiker driemaal zijn wachtwoord verkeerd invult, dan wordt het account vergrendeld, waarna het account handmatig door Functioneel Beheer weer moet worden vrijgegeven. Bij een succesvolle login wordt echter niet de datum en tijdstip weergegeven van de vorige/laatste succesvolle login.

Er is geen formeel beleid om gebruikers bij de eerste keer dat ze de applicatie gebruiken het wachtwoord te laten wijzigen. Het wachtwoord wordt gemaild. Soms kan de gebruiker zijn wachtwoord direct komen invullen bij de beheerder in de management console 'iManager'. Dit is geen vastomlijnd proces.

Actieve gebruikerssessies kunnen niet door de beheerders worden afgesloten.

De gebruikersinterface van de applicatie is web based, wat betekent dat gebruikers met een browser naar de juiste pagina moeten surfen. Het uitwisselen van gegevens tussen gebruiker en applicatie loopt via het beveiligde gemnet netwerk en het verkeer is op zichzelf ook nog een keer versleuteld.

A.2. Sociaal Domein

Sociaal Domein wordt bij de gemeente Westerveld ingevuld met de applicaties Aeolus (Backoffice Wmo en Jeugd), JVS (Leerplicht) en Veilig Opgroeien (Veilig Opgroeien wet voor de jeugd). Van deze drie is Aeolus de meest gebruikte en belangrijkste applicatie.

Autorisatiebeheer
Via HR komt in TOPdesk een formulier voor indienst of uitdienst. Bij nieuwe medewerkers staat aangegeven tot welke applicaties zij toegang moeten hebben en er wordt een referentieprofiel aangegeven (de naam van een collega).

In Aeolus zijn de volgende rollen ingericht: technisch beheer voor het upgraden van de applicatie (3 personen), administratie (4 personen), beheer overig (2 personen), of raadpleeg- rechten (1 persoon).

Er is nog wel nog wel een standaard door de leverancier ingebouwd “admin” account, maar die wordt alleen gebruikt wanneer nodig (wanneer de leverancier erbij moet kunnen). De leverancier krijgt op dat moment alleen tijdelijk toegang, het admin account wordt tijdelijk opengezet en toegang verloopt via TeamViewer en dus via tussenkomst van een medewerker van de gemeente.

Er is een dermate beperkt aantal medewerkers met een account in deze applicaties, dat te allen tijde automatisch het overzicht bestaat over de accounts die toegang hebben. Soms hebben nieuwe releases van de applicaties wijzigingen op (bestaande) rechten, waardoor de rollen en rechten-structuur en ook de accounts weer worden gecontroleerd.

Beschikbaarheid
Aeolus staat lokaal (dwz in eigen rekencentrum en in eigen beheer) en JVS en Veilig Opgroeien zijn SaaS oplossingen. Van de SaaS-oplossingen ligt de verantwoordelijkheid voor backups en beschikbaarheid bij de leverancier en niet bij de gemeente. Voor Aeolus ligt de verantwoordelijkheid wel bij de gemeente (dat geldt namelijk voor alle lokale applicaties/data).

Er worden dagelijks backups gemaakt naar een uitwijkcentrum in Almere. Van de data wordt dagelijks een backup gemaakt online. Een backup van de programmatuur vindt plaats 1 x per week (op tape).

Er zijn restore procedures en deze worden ook getest en alleen daarvoor geautoriseerd personeel heeft toegang tot de backups.

Er is een Gemeentebreed uitwijkplan. Hierin wordt ook Aeolus (lokale applicaties) getest. Externe verbindingen (voor toegang tot de SaaS applicaties) kunnen niet op de uitwijklocatie worden getest, omdat vanaf die locatie geen toegang wordt verleend. Bij noodzakelijke uitwijk maak je met de leverancier afspraken over een nieuw toe te staan IP-adres, maar dat kun je tijdens een uitwijktest niet doen.

Change management
Ten behoeve van het bijwerken van applicaties in het sociale domein is er een Testomgeving en een Productieomgeving.

- Voor JVS geldt dat de medewerkers die in de Productieomgeving werken ook kunnen inloggen in de Testomgeving.
- De Testomgeving van Veilig Opgroeien is alleen beschikbaar voor de Functioneel Beheerder en niet voor de overige medewerkers.
- De Testomgeving van Aeolus is beschikbaar voor de leverancier door middel van het standaard admin account (maar zoals eerder aangegeven enkel door tussenkomst van een medewerker van de gemeente

Westerveld). Daarnaast kunnen ook Technisch Beheer en Functioneel Beheer in de Testomgeving van Aeolus inloggen.

Nieuwe versies van de applicaties staan meestal binnen een week (vanuit Test) in Productie. Aeolus updates bevatten vaak een upgrade van standaarden en daar is de gemeente van afhankelijk. Grote wijzigingen worden via TOPdesk vastgelegd, kleine wijzigingen kunnen ook ad-hoc/mondeling worden afgestemd. Op het moment dat een update een grote wijziging betreft (veel impact en veel tijd), zal dit opgenomen worden binnen het programma Westerveld 2020 en aan een deelproject gekoppeld worden.

Een historie van updates of configuratiewijzigingen wordt niet specifiek bijgehouden. Alleen als een nieuwe update nieuwe functionaliteit heeft, dan wordt aan de afdeling gevraagd of ze die functionaliteit willen en zo ja, om dan een melding te openen in TOPdesk.

In de gebeurtenissen logs van Aeolus is te zien welke wijzigingen een beheerder heeft doorgevoerd. Dit is terug te halen tot een maand terug.

Risico op Databeveiligingsincidenten
Gebruikers van de applicatie Aeolus kunnen de overzichten genereren die standaard in het pakket aanwezig zijn. Ze kunnen het bestand dan lokaal opslaan in hun werkplek omgeving (Aeolus). Veilig Opgroeien en JVS hebben beide lijsten die uitgedraaid kunnen worden (met b.v. alle contactmomenten), dit is een Word bestand wat lokaal op de werkplekomgeving opgeslagen kan worden.

Voor Aeolus is er een anonimiseringsscript om de database in de Testomgeving te anonimiseren. Dit minimaliseert de kans op een datalek.

De Testomgeving van Veilig Opgroeien bevat per definitie geen productiedata. De Testomgeving van JVS bevat echter een oude versie van de productiedatabase.

AVG – Logging en monitoring
Elke activiteit die iemand doet bij Veilig Opgroeien wordt gelogd, zoals het aanmaken van een dossier. In Aeolus kan alles worden opgevraagd wat een gebruiker heeft gedaan. Ook activiteiten van beheerders worden vastgelegd. De techlogs (onder andere storingen in de applicatie) van Aeolus gaan tot 8 weken terug in het verleden, de gebeurtenissen logs tot 1 maand.

De logging is read-only voor Functioneel Beheer. De logging zou alleen aangepast kunnen worden door mensen met directe toegang tot de database. In de praktijk is dat alleen de Technisch Beheer, die toegang nodig heeft voor beheerdoeleinden. De logginginstellingen in de applicaties zijn alleen in te stellen door de beheerders, niet door gebruikers. Deze zaken zijn op deze manier goed ingesteld.

Er zijn geen standaard periodieke rapportages op de logging.

Leveranciersmanagement
Er zijn twee leveranciers betrokken bij de drie applicaties voor het sociale domein. Ieder jaar is er van beide leveranciers een klantendag. Daarnaast is de leverancier Horlings en Eerbeek (Aeolus) iedere 2 maanden bij de gemeente Westerveld aanwezig.

Er zijn wel afspraken vastgelegd met de leverancier over bijvoorbeeld de snelheid van het oppakken van support calls, maar de afspraken zijn nooit opgezocht, omdat de beheerder tevreden is over hoe de leveranciers de problemen oppakken.

Logische toegangsbeveiliging
Toegang tot Aeolus wordt verschaft via zogenaamde ‘Single Sign On’. Een gebruiker hoeft zich daardoor alleen aan te melden op zijn of haar werkplek en hoeft niet opnieuw in te loggen in de applicatie Aeolus. Bij het opvragen van de applicatie wordt toegang automatisch verschaft. Als ongeautoriseerde gebruiker kan de applicatie niet gestart worden.

Voor het inloggen op JVS en Veilig Opgroeien is wel een aanvullend gebruikersnaam en wachtwoord nodig. Iedere 9 weken verloopt het wachtwoord en dan moeten gebruikers een nieuwe bedenken.

Bij Aeolus blijft de sessie in theorie voor onbepaalde tijd actief. Bij VO en JVS moet opnieuw ingelogd worden na een periode van inactiviteit. Bij een langdurige periode van geen gebruik worden accounts niet vergrendeld, wel verloopt het wachtwoord. Bij het te vaak invoeren van een verkeerd wachtwoord wordt het account vergrendeld, alleen de functioneel beheerder kan het account dan weer vrijgeven.

De geldigheid van de wachtwoorden is in de applicaties in te stellen. Het wachtwoord moet elke 63 dagen gewijzigd worden. Als het wachtwoord gewijzigd moet worden, kan er nog 5 keer met het oude wachtwoord ingelogd worden. De gebruikers worden daarna meteen doorgestuurd naar de profielpagina om het wachtwoord te wijzigen. Als de gebruiker het wachtwoord niet wijzigt, kan hij/zij na 5 keer niet meer in JVS/VO. Alleen de applicatiebeheerder kan dan nog een nieuw, tijdelijk wachtwoord instellen. Na het wijzigen van het wachtwoord door de applicatiebeheerder krijgt de gebruiker wederom 5 kansen om met dit wachtwoord in te loggen en zelf een nieuw wachtwoord in te stellen.

B. Bijlage: gebruikte documenten en interviews

B.1. Documenten

2014.informatiebeveiligingsbeleid.plan

2014 jaarplan informatiebeveiliging

2018.23jul.overzicht applicaties

2018.beleidsplan westerveld.def

20180605 GAP analyse Westerveld

Gemeentebreed informatiebeveiligingsbeleid Westerveld concept 050312018docx

Procedure Afvoeren van computers v2.1

Procedure Autorisatie RAAS Aanvraagstations en Rijbewijsmodule v2.1doc

Procedure Autorisatie tot gemeentelijke voorziening v1.1

Procedure Autorisatie tot het lokale netwerk v1.1

Procedure Back-up en restore RAAS v2.0

Procedure Continuiteitsbeheer v1.1

Procedure Goedkeuren updates applicatie v2.1

Procedure Rapportage van incidenten v2.0

Procedure Sleutel- en toegangsbeheer v2.1

Procedure Toegangsbeleid gemeentelijke gebouwen en ruimten v1.0

Procedure Vernietiging van verwijderbare media v2.1

Uitwijkdraaiboek versie augustus 2018

B.2. Interviews

Ter bescherming van persoonsgegevens zijn hier alleen de functiebenamingen opgenomen.

(oud) CISO

CISO

Informatiemanager

Gegevensbeheer

Technisch Beheer ICT

Beveiligingsfunctionaris

Beveiligingsfunctionaris

HR Manager

Fysieke beveiliging

B.3. Bestuurlijke reactie ontvangen van het college van burgemeester en wethouders

Rekenkamercommissie
t.a.v.

Datum	Ons kenmerk	Uw brief	Uw kenmerk
18 maart 2019		19 februari 2019	

Onderwerp
Rapport onderzoek informatiebeveiliging

Geachte

U hebt ons op 19 februari jl. per mail het rapport van uw Rekenkamercommissie over het onderzoek naar de informatiebeveiliging in de gemeente Westerveld gestuurd. Bij deze ontvangt u onze bestuurlijke reactie.

Onze reactie spitst zich in hoofzaak toe op de samenvatting, conclusies en aanbevelingen. Wij hebben met instemming kennis genomen van uw ter zake kundige rapportage. Wij onderschrijven uw aanbevelingen, en zullen deze deel laten uitmaken van het jaarplan informatiebeveiliging c.q. het jaarplan van ons informatiebeveiligingsteam (bestaande uit de CISO, privacy-officer en de functionaris gegevensbescherming). Rest ons nog een tweetal opmerkingen te maken.

Algemeen
Tijdens de startbijeenkomst is door ons al aandacht gevraagd voor de verslaglegging in de openbare rapportage. Op blz. 13 van de rapportage gaat u hier terecht op in. In de ambtelijke reactie hebben we al aangegeven dat…"de eerste bevindingen die aan de hand van de penetratietest op die dag zijn gedaan en die direct op te lossen waren inderdaad ook meteen verholpen zijn. Voor het verhelpen van de overige bevindingen wordt door de CISO een plan van aanpak voorbereid…".

CISO (hoofdstuk 2.2)
Ten overvloede willen we er nogmaals op wijzen dat de rol van de CISO-functionaris vanaf 2014 wel degelijk ingevuld is. Daar waar deze functie vanaf 2014 echter in combinatie met andere functies werd ingevuld wordt deze vanaf september 2018 fulltime ingevuld.

Als u nog vragen heeft kunt u contact opnemen met de gemeente via telefoonnummer 14 0521 en via info@gemeentewesterveld.nl .

Met vriendelijke groet,
burgemeester en wethouders

N.L.J.J. Dusink	H. Jager
secretaris	burgemeester

Bezoekadres: Raadhuislaan 1, 7981 EL Diever Postadres: Postbus 50, 7970 AB Havelte
T 14 0521| E info@gemeentewesterveld.nl | I www.gemeentewesterveld.nl
BTW-identificatie: NL 8062.98.844.B.01 | KvK: 01172480 | Bankrekening: NL27BNGH0285079085