Rekenkamercommissie Meppel, Staphorst, Steenwijkerland en Westerveld

Onderzoek informatiebeveiliging gemeente Meppel; eindrapport

Eindrapport februari 2019

Inhoudsopgave

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 2019 komt er een BIO, 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, de functionaris die toezicht houdt op de toepassing en naleving van de Algemene verordening gegevensbescherming (AVG)
Patchmanagement	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 noemde in een inventariserende ronde van de rekenkamercommissie naar nieuwe mogelijke onderzoeksonderwerpen “informatiebeveiliging” als relevant onderwerp om te onderzoeken. 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 Meppel noemde tijdens een inventariserende ronde van de rekenkamercommissie het onderwerp “informatiebeveiliging” als relevant 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 Meppel ook een kwetsbaarheidsscan uitgevoerd.

2.2. Conclusies en aanbevelingen

De gemeente Meppel heeft in praktische zin een aantal zaken de afgelopen periode goed ‘op orde gebracht’. Bij de start van projecten, is er voldoende aandacht voor informatiebeveiliging. Er zijn minder (technische) kwetsbaarheden dan in vergelijkbare gemeenten. De medewerkers zijn goed op de hoogte van het beleid op het gebied van informatiebeveiliging en privacy en de rol die zij bij de uitvoering van dat beleid moeten vervullen.

De Rekenkamercommissie wijst erop dat dit geen aanleiding kan zijn om achterover te gaan leunen en af te wachten op nieuwe ontwikkelingen. De digitale wereld verandert razendsnel. Technieken veranderen, nieuwe risico’s kunnen ontstaan. De RKC adviseert daarom, de kwetsbaarheden aan de pakken en het informatiebeleid te versterken en actueel te houden door:
- het beleid jaarlijks te actualiseren
- het beleid te baseren op een integrale risicoanalyse
- jaarlijks een goed beschreven en op de materie gericht proces te doorlopen van ‘leren en verbeteren’.

Het verdient aanbeveling om daarbij de lessen en ervaringen uit andere gemeenten bij te betrekken.

Organisatie en beleid

De gemeente Meppel heeft een informatiebeveiligingsbeleid voor de periode 2014-2018. Er is een geactualiseerd informatiebeveiligingsbeleid gewenst. De gemeente geeft aan te wachten op de Baseline Informatiebeveiliging Overheid (BIO), om op basis daarvan het nieuwe beleid vorm te geven. De definitieve versie van de BIO wordt medio 2019, maar mogelijk ook later, verwacht.

Voor het huidige beleid is geen integrale risicoanalyse uitgevoerd als grondslag. Ook zijn er geen Data Protection Impact Assessments (DPIA’s) uitgevoerd. Daardoor ontbreekt een centraal overkoepelend inzicht in de risico’s voor informatiebeveiliging en voor privacy voor de gemeente Meppel.

Het beleid is uitgewerkt in diverse richtlijnen, procedures en handreikingen. Het beleid is niet uitgewerkt in een jaarlijks plan van aanpak. De gemeente hanteert een classificatie voor de bedrijfsmiddelen op basis van beschikbaarheid, integriteit en vertrouwelijkheid, maar past deze classificatie niet toe op (gevoelige) data.

In Meppel wordt sterk gestuurd op informatiebeveiliging per project, de gemeente maakt informatiebeveiliging een onderdeel van ieder project. Dat resulteert in maatregelen die per project, per informatiesysteem, specifiek en doeltreffend zijn. Leren op het gebied van informatiebeveiliging vindt daardoor vooral plaats in de projectencyclus en per project.

De CISO (Chief Information Security Officer) is bij de gemeente Meppel de centrale figuur als het om informatiebeveiliging gaat. Medewerkers weten de CISO te vinden en de CISO weet goed welke relevante ontwikkelingen er in de organisatie spelen. De door PwC gehouden enquête onder medewerkers van de gemeente Meppel onderstreept dat taken en verantwoordelijkheden helder zijn belegd binnen de organisatie.

De keuze van de gemeente Meppel om te wachten op de BIO, om daar het nieuwe beleid op aan te passen is begrijpelijk. Daarin schuilt niet direct een gevaar voor de huidige staat van informatiebeveiliging. Wel is het van belang om in het nieuwe beleid aandacht te geven aan de invoer van een leercyclus (Plan-Co-Check-Act-cyclus) inclusief een controle op de naleving en effectiviteit daarvan. In deze PDCA-cyclus is dan ook een integrale risicoanalyse opgenomen en een jaarplan voor informatiebeveiliging. Met deze risicoanalyse kan al op kortere termijn gestart worden. Dit is belangrijk, om zodoende een integraal, overkoepelend beeld te krijgen van de risico's en de risico mitigerende maatregelen. Dit integrale inzicht ontbreekt nu. Op basis daarvan zijn prioriteiten en speerpunten in het informatiebeveiligingsbeleid beter te bepalen.

Aanbeveling: Voer een integrale risicoanalyse uit als basis voor een op te stellen informatiebeveiligingsbeleid voor de gemeente, schenk in dat beleid ook aandacht aan een continu proces van leren en verbeteren en handhaaf de sterke rol die informatiebeveiliging speelt bij de uitvoering van projecten.

Rapportage over informatiebeveiliging vindt nu plaats in een apart jaarverslag dat vertrouwelijk aan de raad wordt aangeboden. In veel gemeenten maakt informatiebeveiliging onderdeel uit van de rapportage in de reguliere P&C-cyclus, waarbij geen technische details gedeeld hoeven te worden. Rapportage over het informatiebeveiligingsbeleid kan na vaststelling van het beleid onderdeel worden van rapportage aan de raad via de reguliere P&C-cyclus. Zo blijft de raad op de hoogte van belangrijke nieuwe ontwikkelingen, voortgang van maatregelen en het resultaat van het proces van leren en verbeteren.

Aanbeveling: Rapporteer in de reguliere P&C-cyclus over informatiebeveiliging op basis van het vastgestelde beleid, de algemene voortgang van geplande maatregelen, ontwikkelingen en het proces van leren en verbeteren.

Mens en gedrag

Geïnterviewde medewerkers en medewerkers die de enquête hebben ingevuld geven aan dat zij, met name het laatste jaar, een toenemende mate van betrokkenheid door het management zien. Medewerkers zien dat er concrete acties worden genomen, dat er trainingen rondom informatiebeveiliging worden aangeboden en dat er bewustwordingscampagnes zijn. Er werden enkele concrete punten genoemd die beter zouden kunnen, zoals (de nog ontbrekende) mogelijkheid om e-mail beveiligd te kunnen versturen.

De enquête laat zien dat medewerkers grotendeels bekend zijn met het informatiebeveiligingsbeleid, en een duidelijk beeld hebben van wat van hen verwacht wordt op dit gebied. De scores liggen dicht bij het gemiddelde van de vier onderzochte gemeenten. Iedere gemeente kiest daarbij voor andere methoden om informatiebeveiliging onder de aandacht te houden. De bewustwordingsactiviteiten kunnen uitgewisseld worden met de andere gemeenten om afwisseling te houden en medewerkers weer op andere manieren te bereiken.

Aanbeveling:
Continueer de inzet op bewustwording bij management en medewerkers en ga na of er waardevolle ervaringen zijn uit te wisselen met andere gemeenten op dit terrein.

Techniek

De gemeente Meppel heeft goed inzicht in het applicatielandschap. En omdat informatiebeveiliging onderdeel is van ieder (implementatie)project, is de technische beveiliging sterk in vergelijking met andere gemeenten. Daarnaast voert de gemeente regelmatig een penetratietest uit en neemt op basis daarvan aanvullende maatregelen. Dat de technische beveiliging relatief sterk is bleek uit de door PwC uitgevoerde kwetsbaarheidsscan. Ook de applicatieonderzoeken lieten zien dat er is nagedacht over zaken als autorisatiebeheer, het testen van nieuwe software en software-updates en toegangsbeveiliging.

Aanbeveling:
Continueer de sterke focus op beveiligingsmaatregelen per project, per informatiesysteem, de regelmatige penetratietesten en de beveiligingsmaatregelen per applicatie.

3. Onderzoeksvragen en aanpak

3.1. Onderzoeksvragen

We stellen in het onderzoek de volgende vraag centraal:

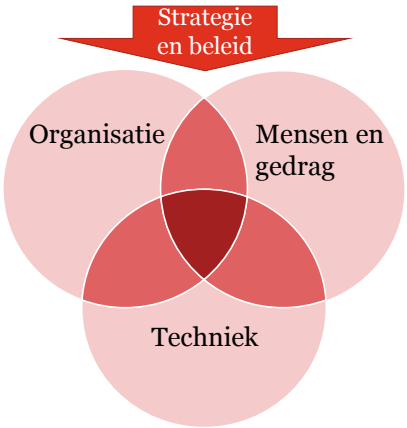
Is de informatiebeveiliging van de gemeenten Meppel, Staphorst, Steenwijkerland en Westerveld doeltreffend?

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 zoals de Baseline Informatiebeveiliging Gemeenten (BIG) en ISO27001:2013 en wetgeving zoals de Algemene verordening gegevensbescherming (AVG). 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.

3.2. 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.

3.3. 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. In Meppel werden bij de inventarisatie expliciet enkele applicaties genoemd die aandacht behoeven. Voor Meppel zijn daarom extra applicaties in het onderzoek opgenomen. 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.

Bij het evalueren van het bestaan en de werking van een applicatie die werkt met (gevoelige) persoonsgegevens richten we ons op het autorisatiebeheer, de logische toegangsbeveiliging, back-up & recovery, het beheer van databeveiligingsincidenten en het leveranciersmanagement.

Kwetsbaarheidsscan of penetratietest

In Meppel is een kwetsbaarheidsscan gehouden en geen penetratietest. Een penetratietest had de gemeente zelf al gepland voor eind 2018. 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 kwetsbaarheidsscans zijn beperkter van aard dan de penetratietests. Bij de interne scan wordt er gewerkt vanuit het perspectief van een interne aanvaller, bij een externe scan 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 op dit vlak zijn daarom niet goed onderling te vergelijken.

De (technische) kwetsbaarheden die we gevonden hebben bij de kwetsbaarheidsscans hebben we direct op een veilige manier verstuurd aan de CISO. 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 een kort verslag op hoofdlijnen op dit punt.

Stap 5: Rapportage

Tenslotte is na ambtelijke en bestuurlijke hoor- en wederhoor deze rapportage opgesteld.

4. 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.

4.1. 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.

De gemeente Meppel beschrijft in het informatiebeveiligingsbeleid dat de gemeente beveiligingsmaatregelen implementeert op basis van een risicoanalyse. Voor kwetsbare en vitale componenten van de informatievoorziening, zoals de Basisregistratie Personen (BRP) en voor gegevens op het gebied van bijvoorbeeld Werk en Inkomen kan op basis van deze risicoanalyse een hoger beveiligingsniveau noodzakelijk zijn.

Bij het opstellen van het informatiebeveiligingsbeleid is er geen integrale risicoanalyse uitgevoerd om risico's op het gebied van informatiebeveiliging te identificeren en te kwantificeren in termen van kans en impact. Een basis op grond van een analyse van bedreigingen en kwetsbaarheden op het gebied van informatiebeveiliging ontbreekt dus. Daarnaast worden geen beveiligingsclassificaties gehanteerd voor het bepalen van beveiligingsmaatregelen. (Gevoelige) data wordt niet geclassificeerd op basis van de kwaliteitsaspecten zoals: beschikbaarheid, integriteit en vertrouwelijkheid.

Uit de interviews en ondersteunende documenten blijkt dat de gemeente wel jaarlijks een aantal analyses uitvoert om op belangrijke onderdelen risico's te identificeren. Zo wordt er jaarlijks een zelfanalyse in het kader van de BRP (Basisregistratie Persoonsgegevens) uitgevoerd, die ook verplicht is. De maatregelen die daaruit voortvloeien worden gerapporteerd aan het MT en opgepakt op de betreffende afdeling. Jaarlijks wordt de ENSIA-vragenlijst (Eénduidige Normatiek Single Information Audit) ingevuld door de diverse betrokkenen voor hun onderdeel. Deze vragenlijst betreft naast de BRP ook de andere basisregistraties. Een ander belangrijk onderdeel is de PUN (Paspoort Uitvoeringsregeling Nederland). De resultaten worden toegestuurd en besproken met de CISO. Verder wordt er jaarlijks een penetratietest uitgevoerd en worden er naar aanleiding van de uitkomsten maatregelen vastgesteld en genomen. Verder voert de gemeente audits uit die de informatiebeveiliging raken. Zo werden audits uitgevoerd in het kader van de wet Suwi (Wet Structuur Uitvoeringsorganisatie Werk en Inkomen) en de aansluiting op DigiD. Er worden (nog) geen DPIA's uitgevoerd.

PIA staat voor Privacy Impact Assessment en DPIA staat voor Data Protection Impact Assessment. De DPIA is de opvolger van de PIA. De PIA gold vanuit de Wbp en DPIA geldt vanuit de AVG. Een DPIA wordt uitgevoerd voor verwerkingen van persoonsgegevens met een (mogelijk) hoog risico en kan in sommige situaties verplicht zijn.

Om te bepalen of een DPIA verplicht is kan er een zogenaamde Pre-DPIA worden uitgevoerd. Dit is een korte vragenlijst om te bepalen of de verwerking (mogelijk) een verhoogd risico heeft (voor de rechten en vrijheden van de betrokkenen) en of er al dan niet een volledige DPIA uitgevoerd moet worden.

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

Als normenkader en uitgangspunt hanteert de gemeente Meppel de Baseline voor Informatiebeveiliging (BIG). Uit de interviews blijkt dat deze onder andere in de praktijk wordt gebruikt bij het invullen van de ENSIA-vragenlijst, dit is de jaarlijkse verplichte vragenlijst die op veel onderdelen van informatiebeveiliging ingaat. Verder wordt BIG als referentiekader gebruikt bij projecten op het gebied van informatisering.

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

In het jaarverslag IB 2017 wordt benoemd dat de zelfevaluaties BRP (Basisregistratie Personen, voorheen GBA) en Paspoorten en Nederlandse identiteitskaarten in hun geheel met voldoende resultaat zijn afgerond. Bij de inhoudelijke controle op de BRP is er onvoldoende gescoord. Het verbeterplan dat naar aanleiding van de zelfevaluaties is opgesteld is in uitvoering. Alle resultaten zijn gerapporteerd aan het MT.

Uit de interviews blijkt dat uit de diverse analyses en vragenlijsten maatregelen en acties voortvloeien. Bij geen enkel interview werd melding gemaakt van een achterstand of van capaciteitsproblemen om de aangegeven maatregelen uit te voeren.

Door de afwezigheid van een dataclassificatieschema en integrale risicoanalyse is niet vast te stellen of op alle onderdelen voldoende maatregelen worden genomen. Het totaaloverzicht ontbreekt daarvoor. Daarnaast is niet te beoordelen hoe de kosten van beheersmaatregelen zich verhouden tot de risico's.

In relatie tot dit onderwerp zijn in de enquête die gehouden is onder de medewerkers van de gemeente Meppel een aantal vragen gesteld. Uit de resultaten komt het beeld naar voren dat er een groep zeer goed op de hoogte is. Deze groep is groter dan in de andere drie gemeenten. Vervolgens scoort de gemeente wat minder goed bij de groep medewerkers die redelijk goed op de hoogte is, in vergelijking met de andere drie 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 gemeenten:
Helemaal eens	3	12%	5%
Eens	7	28%	40%
Neutraal	13	52%	48%
Oneens	2	8%	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	3	12%	6%
Eens	6	24%	37%
Neutraal	15	60%	51%
Oneens	1	4%	4%
Helemaal oneens	0	0%	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	3	12%	7%
Eens	9	36%	46%
Neutraal	11	44%	42%

Oneens	1	4%	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 Meppel beschikt over een informatiebeveiligingsbeleid voor de periode 2014-2018. Dit beleid is daarom per eind 2018 verouderd en dient conform het jaarverslag informatiebeveiliging 2017 geëvalueerd en bijgesteld te worden voor een nieuw tijdsbestek van 4 jaar.

Uit de interviews blijkt dat de informatiebeveiliging sterk wordt gefocust op projecten en daar een integraal onderdeel van is. De gemeente werkt in de praktijk niet op basis van de genoemde cyclus van 4 jaar en ook niet op basis van een jaarlijkse cyclus in bijvoorbeeld de vorm van een jaarplan en een jaarverslag. Uit de gesprekken kwam naar voren dat een evaluatie van het beleid nog niet is opgestart en ook een nieuw informatiebeveiligingsbeleid nog niet in voorbereiding is.

Bij de gesprekken is aangegeven dat de gemeente werkt aan een privacyprotocol. Op de website is een privacy statement geplaatst, waarin per afdeling is aangegeven met welke informatie er wordt gewerkt.

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

Het informatiebeveiligingsbeleid schetst in een introducerend hoofdstuk de context van nationale wet- en regelgeving. Vervolgens gaat het document in op de verdeling van bevoegdheden en verantwoordelijkheden en een aantal belangrijke aspecten zoals applicatiebeheer, interne controle, classificatie van informatie en de basisregistraties. De gemeente Meppel beschrijft in het informatiebeveiligingsbeleid dat dit beleid is gebaseerd op de BIG. De richtlijnen en normen in deze baseline zijn afgeleid van de ISO 27001 en specifiek toegespitst op gemeenten. In het informatiebeveiligingsbeleid ontbreken echter belangrijke beleidsuitgangspunten ten aanzien van:

- Het beheer van bedrijfsmiddelen;
- De beveiliging van personeel;
- Het managen van leveranciers;
- Bedrijfscontinuïteit;
- Naleving.

Daarnaast wordt in het informatiebeveiligingsbeleid geen Plan-Do-Check-Act (PDCA) cyclus beschreven.

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

In het informatiebeveiligingsbeleid van de gemeente Meppel wordt niet beschreven op welke wijze naleving en effectiviteit van het beleid wordt geborgd, bijvoorbeeld middels een PDCA-cyclus.

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

Het informatiebeveiligingsbeleid 2014-2018 beschrijft dat de gemeente Meppel het beleidsplan eens in de 4 jaar herziet of tussentijds wanneer hiertoe aanleiding is. In het jaarverslag informatiebeveiliging 2017 wordt benoemd dat het huidige beleid in 2018 wordt geëvalueerd en bijgesteld. Deze actie heeft echter niet plaatsgevonden, waardoor het beleid niet is herzien, daarnaast ontbreekt een jaarplanning voor informatiebeveiliging.

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

In het informatiebeveiligingsbeleid 2014-2018 wordt beschreven dat beveiligingsclassificaties worden gehanteerd voor het bepalen van beveiligingsmaatregelen. De beschermingseisen volgen uit het classificatieniveau (normaal-hoog-zeer hoog) dat op grond van de dataclassificatie moet worden toegekend. Er wordt geclassificeerd op de drie kwaliteitsaspecten van informatiebeveiliging: beschikbaarheid, integriteit en vertrouwelijkheid. Een nadere uitwerking van het dataclassificatieschema is niet aanwezig voor de gemeente Meppel.

In de enquête die als onderdeel van het onderzoek is uitgezet onder de medewerkers van de gemeente Meppel, is ook een vraag gesteld over dataclassificatie. Meppel scoort hierbij dicht bij het gemiddelde van de vier onderzochte gemeenten. 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	10	40%	32%
Redelijk goed	12	48%	55%
Matig	2	8%	10%
Zeer beperkt	1	4%	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.

Het jaarverslag 2017 biedt een korte vooruitblik op de activiteiten van het komende jaar.

Uit de interviews blijkt dat informatiebeveiliging een sterke rol speelt bij het ontwerp en de uitvoering van projecten. De activiteiten worden dus niet gestuurd vanuit een jaarlijkse planning, maar vormen onderdeel van de projecten die de gemeente start en tot uitvoering brengt. Daarnaast blijkt uit de gesprekken dat de CISO een centrale rol speelt en goed bekend is in de organisatie. Bij vragen of issues op het gebied van informatiebeveiliging wordt de CISO geïnformeerd en onderneemt hij actie. In de derde plaats worden acties en maatregelen gestuurd door het werkoverleg van het ICT-team van de gemeente. Daar staat informatiebeveiliging regulier op de agenda. Doordat de applicatiebeheerders bij dit overleg aanwezig zijn, kan volgens de geïnterviewden vanuit alle werkvelden en applicaties worden meegedacht en kunnen aandachtspunten worden aangegeven.

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

De gemeente Meppel beschikt naast het informatiebeveiligingsbeleid over diverse procedures, richtlijnen en handreikingen, waarin aan informatiebeveiliging gerelateerde onderwerpen (nader) zijn uitgewerkt. De rekenkamer heeft de volgende documenten aangetroffen:

- Afspraken bij procedures Werving & Selectie versie 2 (2017);
- Autorisatiebeleid gemeente Meppel (2017);
- Backupprocedure – Miki (2018);
- Cyptografische beveiliging – Miki (2018);
- Procedure uitwijk BRP (2018);
- Regeling gebruik internet en e-mail op de werkplek- Intranet (2018);
- Wijzigingbeleid – Miki (2018).

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

De opzet van de PDCA-cyclus is niet beschreven in het informatiebeveiligingsbeleid. In de praktijk krijgt deze cyclus niet vorm door een vaste jaarlijkse cyclus, maar wordt er vooral geleerd aan de hand van de projectencyclus. Uit de gevoerde gesprekken blijkt dat aan het begin van een project wordt stil gestaan bij de risico's op het gebied van informatiebeveiliging, dat daarvoor vervolgens maatregelen in het project worden opgenomen. Deze maatregelen worden tijdens het project uitgevoerd en vervolgens wordt aan het einde van het project geëvalueerd of deze maatregelen effectief zijn gebleken voor de beveiliging van informatie.

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 2014-2018 zijn de verantwoordelijkheden ten aanzien van informatiebeveiliging duidelijk beschreven. Het informatiebeveiligingsbeleid van de gemeente gaat uit van de volgende verantwoordelijkheidsverdeling:

- Het college van B&W van de gemeente Meppel is verantwoordelijk voor het vaststellen van het informatiebeveiligingsbeleid en delegeert de uitvoering hiervan aan het management;
- Het management van de gemeente is verantwoordelijk voor het dragen van de gedelegeerde verantwoordelijkheden en rapporteert hierover aan het college van B&W;
- Het management belegt de uitvoering van haar taken bij een Security Officer (SO), die een adviserende en coördinerende taak heeft. We merken hierbij op dat deze SO de functie vervult die voor de VNG wordt omschreven als de CISO (Chief Information Security Officer). De SO is onder andere verantwoordelijk voor het opstellen en uitvoeren van het informatiebeveiligingsplan en rapporteert aan het management en bestuur;
- De medewerker Interne Controle (IC) is verantwoordelijk voor het monitoren dat het informatiebeveiligingsbeleid actueel gehouden wordt en dat het informatiebeveiligingsplan wordt uitgevoerd. Ook monitort de medewerker IC de naleving, effectieve werking en kwaliteit van aanwezige beveiligingsmaatregelen.
- De teamleiders zijn verantwoordelijk voor het uitdragen van het informatiebeveiligingsbeleid en het (laten) uitvoeren van maatregelen uit het informatiebeveiligingsplan op de afdelingen.

De CISO heeft in 2017 inderdaad op de beschreven wijze gerapporteerd, dit blijkt uit het daartoe opgestelde jaarverslag. Uit onze gesprekken blijkt daarnaast dat de meest betrokken medewerkers van deze verdeling van verantwoordelijkheden op de hoogte zijn. De CISO heeft in de uitvoering van zijn taak ondersteuning van de systeembeheerder die verantwoordelijk is voor een technisch goed werkend systeem. Daarnaast zijn er de applicatiebeheerders die voor goed werkende applicaties zorgen met de daarbij horende juiste autorisaties. De CISO heeft nu zelf de taak van het verder versterken van de bewustwording van medewerkers op zich genomen, door diverse acties te initiëren en is tevens het aanspreekpunt voor vragen en problemen op het gebied van informatiebeveiliging.

Op het gebied van persoonsgegevens is in het voorjaar van 2018 een functionaris gegevensbescherming (FG) aangesteld voor 1 dag per week. Daarnaast is er sinds juni 2018 een privacy officer voor 20 uur per week.

In de enquête die PwC heeft uitgezet onder de medewerkers van Meppel zijn twee vragen gesteld met betrekking tot dit onderwerp, waarbij Meppel dicht bij het gemiddelde van de andere onderzochte gemeenten scoort.

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	8	32%	24%
Redelijk goed	9	36%	44%
Matig	5	20%	21%
Zeer beperkt	2	8%	7%
Helemaal niet	1	4%	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	6	24%	25%
Eens	13	52%	51%
Neutraal	4	16%	13%
Oneens	2	8%	8%
Helemaal oneens	0	0%	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.

Het jaarverslag 2017 is in eerste instantie ter bespreking aangeboden aan het managementteam. Vervolgens is het vastgesteld door het college en is het vertrouwelijk ter inzage aangeboden aan de raad.

4.2. 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.

Uit gesprekken met medewerkers blijkt dat zij grotendeels vinden dat het management het laatste jaar meer betrokkenheid toont voor het thema van informatiebeveiligingsbeleid en hier ook concrete acties aan verbindt. In dat kader wordt de aanstelling van de FG genoemd en de aanstelling van de privacy officer. De aanstelling van een FG is bij de invoering van de AVG verplicht geworden. Verder zijn er door goedkeuring van het managementtrainingen gestart om de bewustwording te vergroten, is er tevens een aparte training over informatiebeveiliging gestart voor de teamleiders en wordt er door het management regelmatig aandacht gevraagd voor dit thema bij het teamleidersoverleg.

Aan de andere kant noemen medewerkers ook concrete zaken die het management nog verder zou kunnen versterken op dit terrein. Daarbij gaat het om zaken als de beschikbaarheid van afsluitbare werkkasten om documenten in op te bergen of een betere facilitering om e-mail op een veilige manier te versturen als dat nodig is.

In de enquête die is gehouden onder de medewerkers van de gemeente Meppel is een stelling opgenomen over de actieve betrokkenheid van het management op het gebied van informatiebeveiliging. De medewerkers beoordelen ongeveer hetzelfde als de medewerkers in de andere drie 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	3	12%	6%
Eens	7	28%	32%
Neutraal	13	52%	46%
Oneens	2	8%	13%
Helemaal oneens	0	0%	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.

In het jaarverslag informatiebeveiliging 2017 wordt beschreven dat ten aanzien van informatiebeveiliging regelmatig bewustwordingssessies worden georganiseerd voor nieuwe medewerkers. Daarnaast worden gebruikers geïnformeerd over belangrijke informatiebeveiligingsonderwerpen via het Intranet en screensavers. Ook bezoekt de CISO regelmatig werkoverleggen om knelpunten te bespreken. Uit de interviews blijkt dat dit in het afgelopen jaar inderdaad is gedaan. Medewerkers hebben gemerkt dat er meer aandacht aan het thema wordt gegeven, onder andere doordat men verplicht moest deelnemen aan een training. Daarnaast is er een mail verstuurd waarvan men had moeten onderkennen dat hierop niet gereageerd zou moeten worden. Er hebben toch zo'n 15-20 medewerkers wel op gereageerd. Deze medewerkers zijn daar vervolgens op gewezen.

In de enquête die als onderdeel van dit onderzoek is uitgezet onder de medewerkers van de gemeente Meppel zijn een aantal vragen gesteld met betrekking tot dit onderwerp. In vergelijking met de andere drie gemeenten komt naar voren dat er een wat grotere groep medewerkers zeer goed op de hoogte is en een wat kleinere groep redelijk op de hoogte. 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 25 cijfers): **6,8**

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	12%	8%
Redelijk goed	10	40%	47%
Matig	8	32%	31%
Zeer beperkt	1	4%	10%
Helemaal niet	3	12%	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	5	20%	13%
Redelijk goed	12	48%	58%
Matig	5	20%	20%
Zeer beperkt	2	8%	5%
Helemaal niet	1	4%	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	5	20%	14%
Redelijk goed	10	40%	50%
Matig	6	24%	24%
Zeer beperkt	2	8%	6%
Helemaal niet	2	8%	7%

U wordt regelmatig en goed geïnformeerd over informatiebeveiliging:

Keuze:	**Aantal antwoorden:**	**Percentage:**	**Percentage gemiddelde van de vier onderzochte gemeenten:**
Helemaal eens	3	12%	8%
Eens	10	40%	38%
Neutraal	8	32%	36%
Oneens	4	16%	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	6	24%	17%
Eens	10	40%	51%
Neutraal	4	16%	18%
Oneens	4	16%	12%
Helemaal oneens	1	4%	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	8	32%	17%
Eens	9	36%	51%
Neutraal	6	24%	23%
Oneens	2	8%	6%
Helemaal oneens	0	0%	1%

4.3. 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 Meppel heeft een overzicht van alle applicaties in een Excel sheet. Hierbij wordt vermeld wat de leverancier is, de naam van het pakket, de versie, referentiecomponenten van de gemeente, de status (in productie, gepland), datum ingang status, gebruikte technologie, en nog enkele zaken.

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

De gemeente Meppel werkt aan de vernieuwing van de netwerkinfrastructuur. Daardoor is het treffen van technische beveiligingsmaatregelen relevant.

Om vast te stellen of op technisch vlak afdoende maatregelen zijn getroffen, is bij de gemeente Meppel een kwetsbaarheidsscan uitgevoerd door PwC.

Hieronder staan de belangrijkste bevindingen van de kwetsbaarheidsscan die PwC heeft uitgevoerd bij de gemeente Meppel:

Beveiligingsupdates worden adequaat toegepast, maar verbeteringen zijn mogelijk
Het belangrijkste resultaat van ons onderzoek is dat gemeente Meppel adequaat aandacht besteedt aan het toepassen van beveiligingsupdates op het Windows besturingssysteem. Het kans op misbruik door het ontbreken van updates is daardoor zo gering mogelijk.

Missende applicatie updates stellen een aanvaller in staat om toegang tot gegevens te krijgen

We hebben daarnaast vastgesteld dat diverse beveiligingsupdates met een minder kritiek karakter echter niet toegepast zijn. Hoewel dit niet eenvoudig te misbruiken is, zou dit onder bepaalde omstandigheden wel degelijk kunnen leiden tot ongeautoriseerde toegang tot systemen en gegevens. De aanvaller dient in deze gevallen zeer kundig te zijn en in staat moeten zijn om zelf een zeer geavanceerde aanval op te zetten. We achten de kans op het verkrijgen van ongeautoriseerde toegang met behulp van kant en klaar verkrijgbare (illegale) tooling als zeer klein tot nihil.

Dit betekent dat de gemeente Meppel verminderd kwetsbaar is voor aanvallers die zich ongeautoriseerd toegang willen verschaffen.

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.

Door de afwezigheid van een integrale risicoanalyse en dataclassificatie, ontbreekt de samenhang tussen informatiebeveiligingsrisico's en getroffen beveiligingsmaatregelen. In het informatiebeveiligingsbeleid van de gemeente worden technische maatregelen beschreven. Het is niet vast te stellen of deze maatregelen volledig zijn om alle voor de gemeente relevante informatiebeveiligingsrisico's voor gevoelige informatie af te dekken.

De gemeente heeft verbeterplannen opgesteld voor ENSIA, BRP en PNIK, naar aanleiding van een audit die is uitgevoerd. De verbeterplannen zijn gericht op enkele specifieke zaken, zoals het opnemen van risicoklassen van gegevens ten aanzien van Suwinet, in het Suwinet aansluitbeleid.

Applicatieonderzoeken
In het kader van deze norm zijn bij de gemeente Meppel twee applicaties onderzocht, te weten Key2Burgerzaken (van Centric) en Suite4Sociaal Domein (ook van Centric). 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.

Bij de gemeente Meppel geldt dat autorisatiebeheer bij beide applicaties strikt wordt gehandhaafd en dat er een rigoureuze aanpak is voor de bepaling van rechten en rollen. Tweemaal per jaar worden autorisaties gecontroleerd, waarbij leidinggevenden expliciet moeten tekenen voor de accounts van hun afdeling. Afwijkingen worden direct opgevolgd.

- *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.

De gemeente Meppel maakt van beide applicaties dagelijkse en maandelijkse backups. Daarnaast vinden uitwijktests plaats om te valideren dat tijdens een calamiteit de service geborgd blijft.

Als de upgrade van een applicatie niet goed zou zijn gegaan, dan is de mogelijkheid om terug te rollen (lees: beschikbaarheid herstellen door de upgrade ongedaan te maken) eigenlijk niet aanwezig. Bij iedere upgrade is commitment om met de nieuwe versie verder te gaan. Mocht er iets mis blijken te zijn, dan is de leverancier

direct aan zet om (onder begeleiding van een medewerker) in te loggen op het systeem en te werken aan een oplossing. In de praktijk blijkt de leverancier dan (zeer) snel te zijn met opvolging.

- *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.

Voor beide applicaties geldt dat er naast de Productieomgeving ook een Testomgeving is. Nieuwe updates worden eerst getest in de testomgeving voordat zij worden doorgezet naar productie. De gemeente Meppel constateert regelmatig bij nieuwe updates dat er fouten in zitten. Dat betekent dat de leverancier aan zet is om verbeteringen aan te brengen, zodat de update goed is. Pas na succesvolle tests worden updates doorgezet naar productie.

- *Risico op databeveiligingsincidenten*

Het risico op databeveiligingsincidenten 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.

De testomgeving van Key2Burgerzaken bevat dezelfde database als de productieomgeving. De gemeente is niet in staat om de gegevens te anonimiseren, dit is functionaliteit die door de leverancier geboden zou moeten worden. De gegevens in Key2Burgerzaken kunnen echter niet door gebruikers geëxporteerd worden om ze lokaal op te slaan op bijvoorbeeld USB-stick of om ze te verzenden per e-mail.

- *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 ondersteund dit bij enkele rechten van betrokkenen, zoals het recht om te weten wat er met persoonsgegevens gebeurd is. Audit logging biedt inzicht in wat er met gegevens is gebeurd (zoals raadplegen, kopiëren, wijzigen, verwijderen). Dit is bijvoorbeeld cruciaal wanneer een betrokkene vraagt om aan te geven wie zijn/haar gegevens heeft geraadpleegd.

De applicaties loggen een aantal zaken, zoals het inloggen van gebruikers, het raadplegen van informatie door een gebruiker, activiteiten van beheerders en ook foutmeldingen. Ook wijzigingen door middel van updates van de software worden gelogd. Deze logs gaan qua tijdslijnen helemaal terug tot aan de ingebruikname van de applicatie.

- *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.

De leverancier heeft geen standaard toegang tot de applicatie. Wanneer toegang door de leverancier benodigd is, dan wordt door middel van tussenkomst van een medewerker van de gemeente toegang verstrekt. Op tijdelijke basis heeft de leverancier toegang, waarin kan worden meegekeken door de medewerker van de gemeente.

De leverancier pakt problemen met Key2Burgerzaken relatief snel op in vergelijking met andere applicaties van dezelfde leverancier.

- *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.

Om in te loggen op de applicatie wordt het netwerkaccount (c.q. Windows-account) gebruikt. Voordat een gebruiker echter kan inloggen op een werkplek moet de persoonlijke pas gebruikt worden. Om in te loggen vanaf een externe locatie (bijv. thuis werken) moet ingelogd worden door middel van 2-factor authenticatie.

Inloggen geschiedt dus in principe altijd (indirect) via 2-factor authenticatie, wat erg sterk is.

A. Applicatieonderzoeken

A.1. Key2Burgerzaken

Autorisatiebeheer
Bij indiensttreding, uitdiensttreding of bij functiewijziging dient de (betreffende) manager daarvan melding te maken. Via de applicatie TOPdesk worden wijziging en nieuwe autorisatieverzoeken doorgegeven. In geval van het verkrijgen van autorisatie is een handtekening nodig van verschillende personen. Wanneer een tijdelijk dienstverband wordt verlengd, dient de teamleider het account opnieuw te valideren.

De vereiste rechten en rollen binnen applicaties worden centraal bepaald door de Beheerder BRP. Er is een strikte bepaling van rollen en autorisaties. Zo zijn bijvoorbeeld ook de verantwoordelijkheden voor beheer en wijziging van gegevens toegewezen aan een specifieke beheerdersrol.

Tweemaal per jaar worden de autorisaties gecontroleerd. De CISO maakt een hoofdmelding aan (in TOPdesk) en door de verschillende functioneel beheerders wordt er informatie aangeleverd vanuit de applicatie. Een overzicht van autorisaties wordt dan aangeleverd aan de lijnmanager en de lijnmanager tekent voor akkoord. Wanneer alles akkoord is kan de melding weer gesloten worden. Zo niet, dan worden de nodige aanpassingen aan autorisaties gemaakt.

Beschikbaarheid
Dagelijks en maandelijks worden back-ups gemaakt van het systeem. De afdeling Systeembeheer is de enige afdeling met toegang tot de back-ups.

Er vinden uitwijktests plaats om te valideren dat tijdens een calamiteit de applicatie door kan draaien (in een andere omgeving).

Als een upgrade van de applicatie niet goed blijkt te gaan dan wordt in principe niet teruggerold naar de vorige versie. Dat zou in theorie wel kunnen, maar dan gaat er ook data verloren. Er is bij een upgrade dus direct commitment om met de nieuwe versie verder te gaan. In geval van kritieke disrupties (mogelijk dus naar aanleiding van een upgrade) van de applicatie wordt de leverancier direct ingeschakeld. Er wordt ingebeld om het probleem op te lossen.

De afdeling ICT beschikt over een monitoringsysteem waarmee de beschikbare bronnen worden gemonitord. Als een server zwaar belast wordt dan is dat direct inzichtelijk. Daarbij wordt gemonitord op beschikbaarheid, ook voor Key2Burgerzaken.

Change Management
Naast de productieomgeving heeft de gemeente Meppel een testomgeving voor Key2Burgerzaken. In de testomgeving worden nieuwe updates getest en de gemeente Meppel vindt daarin regelmatig fouten. Als een update eenmaal succesvol is getest wordt de organisatie op de hoogte gesteld van de update. Daarna wordt hij op een bepaald moment doorgevoerd in productie.

Risico op databeveiligingsincidenten
De testomgeving is een kopie van de productie omgeving en bevat daardoor echte informatie die niet is geanonimiseerd. De gemeente is afhankelijk van de leverancier om de gegevens eventueel geanonimiseerd over te kunnen zetten naar de testomgeving. Die optie is er nu niet.

Vanuit de applicatie is een link gelegd met een andere applicatie, Cognos. Vanuit die applicatie kunnen beheerders rapportages maken, zoals exports uit de database. Gewone gebruikers kunnen vooraf bepaalde rapportages draaien, zoals een huwelijksagenda. Gewone gebruikers kunnen de data vervolgens niet exporteren uit de applicatie. Beheerders, teamleiders of seniors kunnen de rapportages bevragen.

De logging die de applicatie genereert bevat geen gevoelige informatie en wordt opgeslagen in de database van de applicatie zelf.

AVG – Logging en monitoring
De applicatie logt een aantal zaken, zoals het inloggen van gebruikers, het raadplegen van informatie door een gebruiker, activiteiten van beheerders en storingen (foutmeldingen). Bij het updaten van het systeem worden de wijzigingen ook gelogd, zoals het wijzigen van tabellen.

De logging van de applicatie gaat terug tot aan de implementatie van de applicatie. Vanaf de de ingebruikname is dus terug te zien wie en wanneer is ingelogd en welke informatie is geraadpleegd.

Een aantal van de logginginstellingen zijn door de functioneel beheerder in te stellen. ICT is in staat om nog meer detailinstellingen te beheren.

De gemeente Meppel controleert niet periodiek en systematisch op de logging van de applicatie. Dit gebeurt specifiek op aanvraag en soms steekproefsgewijs.

Leveranciersmanagement
De leverancier heeft geen standaard toegang tot de applicatie. Wanneer toegang door de leverancier benodigd is, dan wordt door middel van tussenkomst van een medewerker van de gemeente toegang verstrekt. Op tijdelijke basis heeft de leverancier toegang, waarin kan worden meegekeken door de medewerker van de gemeente.

De leverancier pakt problemen met deze applicatie relatief snel op in vergelijking met andere applicaties (van dezelfde leverancier).

Logische toegangsbeveiliging
Om in te loggen op de applicatie wordt het netwerkaccount (c.q. Windows-account) gebruikt. Voordat een gebruiker echter kan inloggen op een werkplek moet de persoonlijke pas gebruikt worden. Om in te loggen vanaf een externe locatie (bijv. thuis werken) moet ingelogd worden door middel van 2-factor authenticatie.

Dat gebruik gemaakt wordt van het netwerkaccount om ook in te loggen in de applicatie, betekent dat het wachtwoordbeleid van het netwerk ook van toepassing is voor toegang tot de applicatie. Dit heeft dus betrekking op de complexiteitseisen van het wachtwoord en de geldigheidsduur.

Wanneer een gebruiker is ingelogd dan ziet hij/zij het tijdstip van de vorige login.

Als te vaak een verkeerd wachtwoord wordt ingegeven dan wordt het account vergrendeld. Het account moet dan weer handmatig worden vrijgegeven door een beheerder.

Vanuit de managementsoftware van de applicatie zijn beheerders niet in staat om actieve gebruikerssessies af te sluiten. Dat zou ICT wel kunnen vanuit de database.

De gebruikersinterface vereist een (java) applicatie en verloopt dus niet via de browser. Alleen medewerkers van de gemeente Meppel die geautoriseerd zijn om de applicatie te gebruiken hebben deze beschikbaar in hun werkomgeving.

A.2. Suite4Sociaal Domein

Autorisatiebeheer
Ieder half jaar worden de autorisaties op de applicatie gecontroleerd. Controle op autorisaties verloopt op dezelfde manier als bij Key2Burgerzaken, zie hoofdstuk 5.1

De leverancier heeft geen standaard toegang tot de applicatie, kan er niet op afstand bij en heeft geen eigen account om in te loggen. Toegang wordt altijd verschaft door tussenkomst van een medewerker van de gemeente Meppel.

Er zijn een aantal rollen gedefinieerd binnen de applicatie, die variëren van het kunnen raadplegen tot aan de beheerdersrol. Beheerstaken zijn daarmee duidelijk gescheiden van gebruikerstaken.

Tweewekelijks wordt een rapport gedraaid waarin wordt weergegeven welke accounts op korte termijn verlopen, zodat daar tijdig op kan worden geacteerd.

Bij Suite4Sociaal Domein zijn de accounts van de gebruikers niet gekoppeld aan het domein. Dit betekent dat een gebruiker voor deze applicatie een andere gebruikersnaam en wachtwoord heeft dan het gebruikersnaam en wachtwoord waarmee hij/zij inlogt op de werkplek.

Beschikbaarheid
Iedere nacht wordt een back-up gemaakt van Suite4Sociaal Domein.

Wanneer een nieuwe update ondanks testen toch een probleem blijkt te geven, dan is terugrollen geen mogelijkheid. Op dat moment wordt er melding met 'kritieke ernst' gemaakt bij de leverancier, die de melding direct moet oplossen.

De afdeling ICT beschikt over een monitoringsysteem waarmee de beschikbare bronnen worden gemonitord. Als een server zwaar belast wordt dan is dat direct inzichtelijk. Daarbij wordt gemonitord op beschikbaarheid, ook voor Suite4Sociaal Domein.

Iedere nacht worden incremental backups gemaakt. De backup staat op een andere locatie, bij de brandweer van Meppel. Dat is ook de primaire bron voor herstelacties. Elk weekend wordt er een full backup naar tape gemaakt die naar BCM (KPN Business Continuity Management) in Almere vervoerd wordt. Daarnaast wordt nog een maandbackup gemaakt voor herstelacties die verder terug gaan (in de tijd).

De nachtelijke incremental backup wordt off-site (bij de brandweer) bewaard. Daarnaast wordt de wekelijkse tape in Almere bewaard. Maandtapes worden op het Stadhuis bewaard in een afgesloten brandveilige kast.

Alleen systeembeheerders hebben toegang tot de backups. De koffer met tapes bestemd voor Almere wordt bewaard in de kluis van Burgerzaken. De koffer is verzegeld. Deze verzegeling kan alleen na toestemming verbroken worden door medewerkers van BCM in geval van een uitwijk.

Change Management
Naast de productieomgeving heeft de gemeente Meppel een testomgeving voor Suite4Sociaal Domein. In de testomgeving worden nieuwe updates getest. Als een update eenmaal succesvol is getest wordt de organisatie op de hoogte gesteld van de update. Daarna wordt hij op een bepaald moment doorgevoerd in productie.

Een proces rondom wijzigingsbeheer is niet formeel vastgesteld op papier, maar in de praktijk wordt wel degelijk een wijzigingsproces gevolgd.

Updates en de historie daarvan worden bijgehouden in TOPdesk. Configuratiewijzigingen worden niet gedocumenteerd.

Risico op databeveiligingsincidenten
Vanuit de gebruikersinterface van de applicatie is het niet mogelijk om gegevens te exporteren.

De leverancier heeft scripts aangeleverd waarmee gegevens uit de productie-omgeving geanonimiseerd worden gekopieerd naar de testomgeving

AVG – Logging en monitoring
De applicatie logt de logins van gebruikers. Het raadplegen van dossiers wordt niet gelogd, mutaties weer wel. Het loggen van raadplegingen is een aanvullende optie waarvoor moet worden betaald. Voorheen logde de applicatie raadplegingen wel, nu is het een betaalde optie geworden. Verder wordt bijvoorbeeld het aanmaken van een gebruiker gelogd alsook foutmeldingen en het uitvoeren van een update.

In theorie wordt de logging voor onbepaalde tijd bewaard.

De gemeente voert geen standaard periodieke controles uit op de logging van de applicatie.

Leveranciersmanagement
Applicatiebeheerders communiceren met leveranciers van software. Zij hebben de taak de applicaties zo goed mogelijk in te richten, gebruikers te instrueren en verbeteringen aan te brengen. Ze overleggen met de leveranciers en gebruikers over updates en gewijzigde functionaliteit. Ze organiseren werkzaamheden of voeren updates zelf uit. Zij zijn verantwoordelijk voor het actueel houden van de applicatie.

De budgethouder ziet toe op de kosten voor een pakket. In overleg met proceseigenaren (teamleiders) wordt overwogen of nieuwe functionaliteit aangeschaft moet worden en hoe dit gefinancierd wordt. De budgethouder loopt met applicatiebeheerders regelmatig contracten na op actualiteit van modules en functionaliteiten. Onderhoud van modules en applicaties die niet meer gebruikt worden, wordt beëindigd.

In het geval van Centric zijn er regelmatig gesprekken account- en productmanagers. Juist dit jaar zijn er gesprekken gestart over onderhoudscontracten met Centric om tot een voordeliger overeenkomst te komen.

Logische toegangsbeveiliging
Voor toegang is (indirect) altijd 2-factor authenticatie nodig: als een gebruiker zich in het gemeentehuis bevindt dan moet ingelogd worden met behulp van gebruikersnaam, wachtwoord en toegangspas. Van buitenaf wordt gebruik gemaakt van 2-factor authenticatie (gegenereerde code). Daarna logt de gebruiker in, in de applicatie door middel van een gebruikersnaam en wachtwoord. Echter, alle gebruikers hebben hetzelfde wachtwoord. Dit wachtwoord is bij geen van de gebruikers bekend, maar wordt (versleuteld) in een script gebruikt om ervoor te zorgen dat ze automatisch inloggen. Het standaard leveranciersaccount is uitgeschakeld en wordt niet gebruikt.

Gebruikers die geen toegang hebben tot de applicatie zien in hun werkomgeving ook geen link naar de applicatie staan. Iemand zou in zo'n geval de link van de website uit het hoofd moeten weten om verbinding te maken met de applicatie.

Wanneer een wachtwoord te vaak verkeer wordt ingegeven dan wordt het account vergrendeld. Daarna moet het handmatig worden vrijgegeven. Na 100 dagen inactiviteit wordt het account automatisch ook vergrendeld.

Een beheerder heeft niet de mogelijkheid om een actieve gebruikerssessie af te sluiten.

B. Bijlage: gebruikte documenten en interviews

B.1. Documenten

Autorisatiebeleid gemeente Meppel, geen datum

Backup and restore procedure

Cyptografische beveiliging

Gemeentelijke inkoopvoorwaarden bij IT (GIBIT), versie 2016

Informatiebeveiligingsbeleid 2014-2018 gemeente Meppel

Informatiebeveiligingsplan BRP en waardedocumenten, versie 25 september 2017 (7.0)

Inkoophandleiding, Inkoop en aanbesteding

Jaarverslag informatiebeveiliging 2017

Overzicht applicaties gemeente Meppel

Penetratietest 2016

Procedure werving en selectie

Procedure uitwijk BRP

Procedure restore

Wijzigingsbeleid gemeente Meppel

Regeling gebruik e-mail en intranet op de werkplek

Tips & gedragsregels e-mail, gemeente Meppel

B.2. Interviews

Ter bescherming van persoonsgegevens zijn alleen de functie-omschrijvingen in deze lijst opgenomen.

controller AO/IC

Functionaris Gegevensbescherming

kwaliteitsadviseur BRP

installatieverantwoordelijke

Chief Information Security Officer

Privacy Officer

teamleider Beheer

Burgemeester

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

meppel.nl

Rekenkamercommissie Meppel
T.a.v. de heer J.J. Mastwijk, voorzitter
via: rekenkamer@meppel.nl

Uw brief van
Uw kenmerk
Ons kenmerk 1313709

Behandeld door A. Uiterwijk
Telefoon 14 0522 Bijlage(n) Datum 11 MAART 2019
Onderwerp onderzoek informatiebeveiliging gemeente Meppel

Geachte heer Mastwijk

Met plezier hebben wij kennis genomen van het eindrapport Onderzoek Informatiebeveiliging gemeente Meppel. Wij zijn blij met uw oordeel dat het ingezette beleid het beoogde effect heeft en dat uw overall conclusie is dat de gemeente haar informatiebeveiliging goed op orde heeft gebracht.

In uw rapport doet u een viertal aanbevelingen, hieronder willen wij hier graag op reageren.

Er zijn twee aanbevelingen gedaan in de categorie Organisatie en Beleid:

- Voer een integrale risicoanalyse uit als basis voor een op te stellen informatiebeveiligingsbeleid voor de gemeente, schenk in dat beleid ook aandacht aan een continu proces van leren en verbeteren en handhaaf de sterke rol die informatiebeveiliging speelt bij de uitvoering van projecten.

Deze aanbeveling nemen wij over, in 2019 wordt het informatiebeveiligings-beleid aangepast conform de BIO (baseline informatiebeveiliging overheden). De BIO vraagt om een integrale risicoanalyse.

- Rapporteer in de reguliere P&C-cyclus over informatiebeveiliging op basis van het vastgestelde beleid, de algemene voortgang van geplande maatregelen, ontwikkelingen en het proces van leren en verbeteren.

Wij zijn van mening dat we regelmatig rapporteren, ook in de P&C-cyclus. In het kader van het voortdurend verbeteren van onze bedrijfsvoering en communicatie nemen we kennis van deze aanbeveling.

Er is een aanbeveling gedaan in de categorie Mens en Gedrag

- Continueer de inzet op bewustwording bij management en medewerkers en ga na of er waardevolle ervaringen zijn uit te wisselen met andere gemeenten op dit terrein.

Stadhuis Grote Oever 26 ▮ Postbus 501 ▮ 7940 AM Meppel ▮ postbus@meppel.nl ▮ www.meppel.nl ▮ tel. 14 0522 ▮ fax (0522) 850 580

meppel.nl

Hiervoor werkt de gemeente Meppel iBewust! Voortdurend wordt er op verschillende momenten en op verschillende manieren (opnieuw) aandacht gevraagd van management en medewerkers. Als er aanleiding voor is wordt dit ook graag gedeeld met anderen

Tot slot is er een aanbeveling gedaan in de categorie Techniek.

- Continueer de sterke focus op beveiligingsmaatregelen per project, per informatiesysteem, de regelmatige penetratietesten en de beveiligingsmaatregelen per applicatie.

Deze aanbeveling nemen we graag over

Verder willen wij nog graag een enkele opmerking aan u meegeven. Op pagina 20 van het rapport staat onderstaande (cursief genoteerde) tekst. Er kunnen vraagtekens worden geplaatst bij de verwoording hierover in het rapport en anders vraagt het op zijn minst een nadere duiding.
'Aan de andere kant noemen medewerkers ook concrete zaken die het management nog verder zou kunnen versterken op dit terrein. Daarbij gaat het om zaken als de beschikbaarheid van afsluitbare werkkasten om documenten in op te bergen of een betere facilitering om e-mail op een veilige manier te versturen als dat nodig is.'
Er zijn veel voorzieningen gecreëerd om medewerkers veilig te laten communiceren via e-mail. De voorzieningen zijn zo laagdrempelig mogelijk gemaakt, maar vereisen wel extra gebruikershandelingen. De opmerking zal dus eerder te maken hebben met de gebruikerservaring/het gebruikersgemak, dan met de beschikbare faciliteiten.

Hoogachtend,
Burgemeester en wethouders,
de secretaris, de burgemeester,

1.0.

Stadhuis Grote Oever 26 ▮ Postbus 501 ▮ 7940 AM Meppel ▮ postbus@meppel.nl ▮ www.meppel.nl ▮ tel. 14 0522 ▮ fax (0522) 850 580