Meppel, Staphorst, Steenwijkerland en Westerveld:

‘Informatiebeveiliging redelijk tot goed op orde’

Rekenkameronderzoek naar informatiebeveiliging in de gemeenten Meppel, Staphorst, Steenwijkerland en Westerveld

De rekenkamercommissies (RKC) van de gemeenten Meppel, Staphorst, Steenwijkerland en Westerveld hebben, voor de eerste keer in hun bestaan, onderzoek gedaan naar een thema dat in alle vier gemeenten speelt. Informatiebeveiliging. Hiermee komt de rekenkamercommissie tegemoet aan de wens van de gemeenten om, wanneer dit kan, een synergie effect te realiseren. Met dit onderwerp heeft de RKC een actueel thema behandeld waar gemeenten volop mee bezig zijn en waarin ontwikkelingen zich snel opvolgen.
De RKC heeft geconstateerd dat het niveau van informatiebeveiliging in basis in de vier gemeenten redelijk tot goed op orde is. ‘Maar er is nog voldoende ruimte voor verbetering en mogelijkheden om van elkaar te leren’, zegt Arthur Rynja die vanuit de Rekenkamercommissies het onderzoek begeleidde.

De vier gemeenten zijn allen beoordeeld op de aspecten “Organisatie en beleid”, “Mens en gedrag” en “Techniek”. De gemeenten scoren alle vier verschillend en daarmee is het ook direct zichtbaar dat informatiebeveiliging mensenwerk is. Waar aansturing en aandacht vanuit het management cruciaal is voor het op orde krijgen en houden van informatiebeveiliging.

Per gemeente volgen hierna kort de belangrijkste aanbevelingen

Meppel.

1. Voer een integrale risicoanalyse uit als basis voor het informatiebeveiligingsbeleid en schenk hierin aandacht aan een continu proces van leren en verbeteren;
2. Gebruik de bestaande P&C-cyclus om ook te rapporteren over de voortgang van geplande maatregelen en ontwikkelingen;
3. Vergroot de bewustwording voor zowel management als medewerkers;

Staphorst.

1. Stel voldoende personeel beschikbaar voor maatregelen op het gebied van informatiebeveiliging en voor de rol van Chief Information Security Officer (CISO).
2. Investeer in de bestuurlijke informatievoorziening
3. Maak een bestuurder expliciet verantwoordelijk voor dit onderwerp
4. Vergroot de bewustwording voor zowel management als medewerkers
5. Voer regelmatig penetratietests uit en geef extra aandacht aan Patch management (nieuwe versies van/wijzigingen in software)

Steenwijkerland.

1. Het beleid op het gebied van informatiebeveiliging is actueel. Bij een volgende actualisatie zou er wel eerst een integrale risicoanalyse uitgevoerd moeten worden. Voer deze ook met enige regelmaat uit.
2. Er kan meer aandacht uitgaan vanuit het management voor bewustwordingsactiviteiten.

3. De fysieke toegangsbeveiliging wordt nog als kwetsbaar aangemerkt.
4. Patch management (nieuwe versies van/wijzigingen in software) behoeft aandacht.

Westerveld.

1. Voer regelmatig een integrale risicoanalyse uit op het gebied van informatiebeveiliging als basis voor het informatiebeveiligingsbeleid;
2. Doorloop een PDCA-cylcus om te leren van genomen maatregelen en doorloop deze als basis om het beleid eventueel bij te stellen;
3. Overweeg een bestuurder expliciet verantwoordelijk te maken voor dit onderwerp;
4. Betrek het management en medewerkers actief/periodiek bij bewustwordingsactiviteiten over informatieveiligheid;
5. Voer regelmatig penetratietests uit;
6. Patch management (nieuwe versies van/wijzigingen in software) behoeft aandacht.

De complete rapporten treft u in de bijlagen aan.

Toelichting: De gemeenten Meppel, Staphorst, Steenwijkerland en Westerveld hebben ieder een eigen zelfstandige rekenkamercommissie. Via een 'personele unie' worden deze commissies door vier (dezelfde) personen bemenst.

****

Noot voor de redactie (niet voor publicatie)

Meer info: Arthur Rynja, lid Rekenkamercommissie, 06 52502969

Rekenkamercommissie Meppel, Staphorst, Steenwijkerland en Westerveld

Onderzoek informatiebeveiliging gemeente Staphorst; 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 gaf 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 is het eerste onderzoek van deze rekenkamer 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 Staphorst 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 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 Staphorst ook een penetratietest (methode van hack-pogingen) uitgevoerd.

2.2. Conclusies en aanbevelingen

De gemeente beschikt over de gehele onderzoeksperiode over een goed informatiebeveiligingsbeleid. Tijdens dit onderzoek is echter wel vastgesteld dat implementatie en uitvoering onvoldoende van de grond komt door gebrek aan capaciteit om het beleid ook echt uit te voeren.

Door te investeren in bestuurlijke aandacht, ambtelijke sturing en met name in meer capaciteit moet de bewustwording bij de organisatie een impuls kunnen krijgen en kunnen de geconstateerde organisatorische en technische tekortkomingen snel het hoofd worden geboden. Denk daarbij aan het vergroten van de bewustwording in de organisatie, gebruik van de testomgeving, patchmanagement en het regelmatig uitvoeren van penetratietests.

Hieronder werken we dat verder uit voor de drie onderdelen van dit onderzoek: organisatie en beleid, mens en gedrag en techniek.

Organisatie en beleid

De gemeente Staphorst heeft als basis van het informatiebeveiligingsbeleid een Risico-inventarisatie en evaluatie (RI&E) uitgevoerd. Sinds 2015 heeft Staphorst een gemeentebreed informatiebeveiligingsbeleid. In de periode daarvoor was er sprake van beleid op specifieke vakgebieden. Kort na afronding van ons onderzoek, in december 2018, is een geactualiseerde versie van het informatiebeveiligingsbeleid beschikbaar gekomen. Het beleid is vertaald naar een jaarplan waarin specifieke maatregelen worden beschreven. In dit jaarplan, bij de beschrijving van maatregelen, wordt gebruik gemaakt van kennis en voorbeelden (good practices) van elders, zoals de Baseline Informatiebeveiliging Gemeenten (BIG). Het plan bevat ook enkele maatregelen die direct gerelateerd zijn aan het werken met (bijzondere) persoonsgegevens.
Veel verbetermaatregelen zijn in de afgelopen jaren echter niet uitgevoerd. In eigen informatiebeveiligingsanalyses constateert de gemeente dat ook zelf. De belangrijkste oorzaak hiervoor is het

ontbreken van tijd en capaciteit van de betrokken medewerkers. Daarnaast ontbreekt het aan sturing en regie op het gebied van informatiebeveiliging.

Doordat niet alle maatregelen worden uitgevoerd, kan ook de leercyclus met betrekking tot getroffen maatregelen niet worden doorlopen. De gemeente plant de maatregelen wel, voert slechts een deel uit en kan dus ook maar een deel evalueren en verbeteren.

Aanbeveling: Stel voldoende capaciteit beschikbaar voor het uitvoeren van de geplande maatregelen voor informatiebeveiliging.

De rollen en verantwoordelijkheden voor informatiebeveiliging zijn helder omschreven. Voor de rol van de Chief Information Security Officer (CISO) is echter in de praktijk beperkte capaciteit beschikbaar. De CISO heeft een cruciale rol in de overall coördinatie van informatiebeveiliging binnen de gemeente. De CISO is aanspreekpunt en stuurt medewerkers op diverse vakgebieden aan om maatregelen te nemen. Medewerkers in Staphorst weten in vergelijking met de andere drie onderzochte gemeenten minder goed wie welke taken vervullen op het gebied van informatiebeveiliging en aan wie men hierover vragen kan stellen.

Aanbeveling: Stel meer capaciteit beschikbaar voor het goed invullen van de rol van de Chief Information Security Officer, zodat de sturing en regie op informatiebeveiliging versterkt kan worden.

In de periode van 2013 tot heden wordt de raad geleidelijk uitvoeriger geïnformeerd over informatiebeveiliging en het belang en de voortgang daarvan. Gezien de achterstand in het uitvoeren van voorgenomen maatregelen is het belangrijk ook bestuurlijk inzicht te hebben in de mate waarin deze achterstanden worden ingelopen en in welke mate er vanwege nieuwe ontwikkelingen weer nieuwe maatregelen nodig zijn.

Aanbeveling: Doe in de reguliere PDCA-cyclus meer expliciet verslag van de mate waarin geplande maatregelen zijn uitgevoerd in het kader van informatiebeveiliging.

De verantwoordelijkheid voor informatiebeveiliging is in Staphorst niet expliciet belegd bij een portefeuillehouder. Het college draagt daarmee deze verantwoordelijkheid gezamenlijk en mandateert deze aan de gemeentesecretaris (zie ook het gemeentebreed informatiebeveiligingsplan van december 2018). Andere gemeenten, zoals Steenwijkerland en Almere, hebben goede ervaring met een bestuurlijk aanspreekpunt voor informatiebeveiliging. Dit maakt zowel het bestuurlijk aanspreekpunt voor de raad als voor de ambtelijke organisatie duidelijk.

Aanbeveling: Overweeg een portefeuillehouder voor informatiebeveiliging aan te stellen.

Mens en gedrag

Bijna 40% van de medewerkers vindt het management actief betrokken bij informatiebeveiliging, de helft is neutraal en 13% vindt dit niet. Van de medewerkers is 43% matig op de hoogte van het informatiebeveiligingsbeleid en 14% beperkt of niet. Ook weet 25% matig wat van hen verwacht wordt en weet 13% dit niet. Deze scores geven veel ruimte voor verbetering aan, waarbij het management de voorbeeldrol krachtiger kan invullen. Hiervoor is meer inzet in de vorm van training en bewustwording nodig, zodat bijvoorbeeld datalekken beter worden herkend, men beter geïnformeerd is over het informatiebeveiligingsbeleid en men op de hoogte is van de wijze waarop met gevoelige gegevens moet worden

omgegaan. Het recent vastgestelde en geactualiseerde informatiebeveiligingsbeleid biedt hiervoor een goede aanleiding en een duidelijk vertrekpunt.

Aanbeveling: Intensiveer trainingen en bewustwordingsactiviteiten voor management en medewerkers op het gebied van informatiebeveiliging.

Techniek

Staphorst heeft strategisch een aantal goede en belangrijke technische maatregelen genomen ter beveiliging van de informatie. Toch leverde de penetratietest een aantal belangrijke kwetsbaarheden op. Gelet op de bevindingen was het volgens de onderzoekers te risicovol om te wachten deze te melden en is vooruitlopend op de oplevering van het onderzoeksrapport direct contact met de organisatie gezocht om hen in staat te stellen direct beheersmaatregelen te nemen op de geconstateerde kwetsbaarheden. Omdat de kwetsbaarheden steeds veranderen, omdat kwaadwillenden voortdurend nieuwe methoden en technieken ontwikkelen, wordt aangeraden regelmatig penetratietests uit te voeren.

Op basis van de penetratietest die PwC heeft uitgevoerd blijkt dat patch management de aandacht verdient, evenals beleid voor accounts hogere rechten (zogenaamde 'privileged accounts', waartoe beheeraccounts behoren). De applicatieonderzoeken laten zien dat de gemeente Staphorst minder tijd beschikbaar heeft om nieuwe software of nieuwe software updates te testen voor ingebruikname. Daarnaast was het mogelijk om vanuit de onderzochte applicaties gegevens te exporteren en los van de applicatie te gebruiken. De vraag is of dit noodzakelijk of wenselijk is.

Verbeterd patch management is de belangrijkste bevinding voor het onderdeel techniek. Het is van belang om zoveel mogelijk systemen regelmatig te voorzien van de nieuwste (veiligheids)updates. Voor systemen waar updates niet toegepast kunnen worden dienen andere beveiligingsmaatregelen getroffen te worden ter compensatie. Hierbij kan gedacht worden aan maatregelen als 'hardening' van systemen of netwerksegregatie. Voer vervolgens regelmatig (bijvoorbeeld jaarlijks) als onderdeel van het informatiebeveiligingsbeleid een penetratietest uit om het beveiligingsniveau te controleren en waar nodig bij te stellen.

Verder is het van belang om nieuwe software of updates te testen alvorens ze in gebruik te nemen.

Ten laatste is het belangrijk om te onderzoeken of gebruikers van de onderzochte applicaties in staat zouden moeten zijn om gegevens uit de applicaties de exporteren. Is dit noodzakelijk voor het werk dat zij verrichten? Gecombineerd met een risico-inschatting kan bepaald worden of aanvullende maatregelen nodig zijn en welke maatregelen dat zouden zijn.

Aanbeveling: Blijf regelmatig penetratietesten uitvoeren om alert te blijven op kwetsbaarheden en hiervoor de juiste maatregelen te kunnen treffen.

Aanbeveling: Herzie het beleid ten aanzien van patch management, zorg dat systemen systematisch en periodiek worden voorzien van (beveiligings)updates.

3. Onderzoeksvragen en aanpak

3.1. Onderzoeksvragen

We stellen in het onderzoek de volgende vraag centraal:

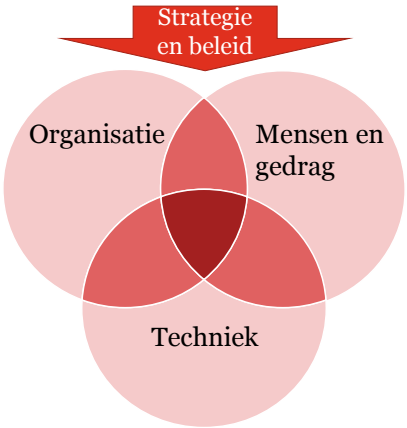
Is de informatiebeveiliging van de gemeenten Meppel, Staphorst, Steenwijkerland en Westerveld doeltreffend?

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 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.

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 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 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
Er zijn interviews gehouden met de direct betrokkenen bij informatiebeveiliging. Daarnaast is 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 Staphorst bleek een penetratietest al enige tijd niet uitgevoerd te zijn (dit is te zien als een meer uitvoerige kwetsbaarheidsscan die we in iedere gemeente gehouden hebben). Voor Staphorst is een interne en externe penetratietest uitgevoerd. Deze test beoogt kwetsbaarheden in het netwerk vast te stellen en te bezien of het

mogelijk is om ongeautoriseerde toegang te verkrijgen. De teskt levert ook op welke maatregelen kunnen helpen om de beveiliging waar mogelijk te verbeteren. De kwetsbaarheidsscans zijn beperkter van aard dan de penetratietest. 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 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 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 Staphorst heeft op 17 oktober 2017 een Risico-Inventarisatie en Evaluatie (RI&E) uitgevoerd. In het informatiebeveiligingsbeleid van de gemeente Staphorst staat dat het informatiebeveiligingsplan de risicoanalyse bevat. Het is de intentie om informatiebeveiligingsplan iedere 1 tot 2 jaar bij te stellen. Er wordt in het informatiebeveiligingsbeleid niet aangegeven met welke regelmaat de risicoanalyse (RI&E) wordt uitgevoerd.

De RI&E van 2017 laat zien dat bij een aantal risico's maatregelen worden getroffen die gericht zijn op het beheer van persoonsgegevens. Voorbeelden van dergelijke maatregelen zijn de bewustwordingssessies, een wachtwoordbeleid en het toepassen van functiescheiding en het 4-ogen principe.

Tijdens interviews is de werkwijze rond de uitvoer van de RI&E als volgt geschetst: In de RI&E worden bedreigingen geïdentificeerd. Het bijbehorende risico wordt vervolgens gekwantificeerd in termen van kans x impact. Voor het beheersen van geïdentificeerde risico's hanteert de gemeente Staphorst de BIG-standaard.

Eén van de uitkomsten van de afgelopen RI&E was dat er opnieuw gekeken moest worden naar het calamiteitenplan voor fysieke dossiers. Voor digitale dossiers moest er opnieuw gekeken worden naar de backups. De gemeente Staphorst heeft een zogenaamde 'On Premise' omgeving, met uitwijkmogelijkheden naar Zwartewaterland en Zoetermeer. Door de gemeente Staphorst is geconcludeerd dat die opzet voor dit moment voldoende is.

Norm: Relevante beheersmaatregelen worden vastgesteld op basis van good practices, zoals de BIG (Baseline Informatiebeveiliging Gemeenten).

De gemeente Staphorst heeft een plan van aanpak opgesteld voor informatiebeveiliging voor de jaarschijf 2018 – 2019. De criteria die worden gehanteerd bij de selectie van verbetermaatregelen verwijzen in vier van de zeven gevallen naar BIG-maatregelen. Daarnaast wordt gekeken naar de lokale situatie van de gemeente Staphorst alsook de resultaten van de risicoanalyse.

De RI&E is het middel dat de gemeente Staphorst gebruikt voor het identificeren van risico's. Voor het beheersen van geïdentificeerde risico's hanteert de gemeente Staphorst de BIG. De BIG vormt tevens de basis voor het door de gemeente vastgestelde informatiebeveiligingsbeleid. Dit beleid wordt om de 3 a 4 jaar vastgesteld. De gemeente heeft vergeleken welke maatregelen in de Baseline informatieveiligheid voor gemeenten (BIG) zijn opgenomen en welke daarvan nog door Staphorst uitgevoerd moeten worden.

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

In het plan van aanpak (PVA) voor informatiebeveiliging voor de jaarschijf 2018 – 2019 is beschreven dat het kader voor de prioritering van verbetermaatregelen gevormd wordt door de quick-wins van de IBD samen met de resultaten van de classificatie van informatiesystemen en van de RI&E en de lokale quick wins.

Het PVA bevat ook een aantal maatregelen (uit de BIG) die direct gerelateerd zijn aan het werken met (bijzondere) persoonsgegevens. In alle gevallen is in het PVA als actie “Direct implementeren” gekozen.

De gemeente Staphorst heeft op 29 december 2017 een informatiebeveiligingsanalyse uitgevoerd. Deze analyse geeft inzicht in wat de gemeente de afgelopen jaren heeft bereikt en wat de komende jaren nog aan beveiligingsmaatregelen uitgevoerd moet worden.

Het document stelt dat een belangrijk onderdeel van informatieveiligheid bestaat uit het uitvoeren van de verbetermaatregelen voortvloeiende uit de informatieveiligheidsanalyse. Enkele van de conclusies die zijn getrokken:

- Van het totaal van 303 maatregelen waren er bij aanvang van de gap-analyse in 2015 144 gerealiseerd;
- Per oktober 2017 zijn er in totaal 168 maatregelen daadwerkelijk gerealiseerd en 96 gedeeltelijk;
- Dat betekent dat in de periode 2015-2017 24 maatregelen gerealiseerd zijn;
- Het plan van aanpak van 2015 stelde dat 59 maatregelen gerealiseerd zouden worden tot aan 2017;
- Er moeten nog 135 maatregelen uitgevoerd worden (anno eind 2017).

Het document stelt dat de belangrijkste oorzaak voor het niet realiseren van verbetermaatregelen ligt bij het ontbreken van tijd voor de betrokken medewerkers. Men moet dit naast een bestaand takenpakket uitvoeren.

Tijdens de interviews met de medewerkers van de gemeente Staphorst is het proces besproken van het oppakken van de openstaande maatregelen. De openstaande punten van de gap-analyse worden in de gemeente Staphorst opgepakt in de werkgroep Informatiebeveiliging. De interne controle van de gemeente Staphorst wees als oorzaak voor het niet oppakken van het beoogde aantal verbeteracties het ontbreken van tijd bij de betrokken medewerkers. Tijdens interviews is dit door de medewerkers onderstreept.

Een andere oorzaak die tijdens de interviews werd genoemd is het gebrek aan sturing vanuit het management. Bij de gemeente Staphorst is met name sprake van een doe-mentaliteit. Geïnterviewden geven aan dat de gemeente Staphorst graag zelf problemen wil oplossen. Dat legt vaak een hoge druk op wat er op korte termijn moet gebeuren en geïnterviewden geven aan dat zij daarbij de regie en de strategie wel eens missen. Problemen die worden opgepakt worden kwalitatief goed opgepakt, maar daarbij wordt opgemerkt dat de centrale regie ontbreekt.

In relatie tot dit onderwerp zijn in de enquête die gehouden is onder de medewerkers van de gemeente Staphorst een aantal vragen gesteld. Staphorst scoort hier 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	4	6%	5%
Eens	32	44%	40%
Neutraal	35	49%	48%
Oneens	1	1%	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	4	6%	6%
Eens	29	40%	37%
Neutraal	35	49%	51%
Oneens	2	3%	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	5	4%	7%
Eens	35	49%	46%
Neutraal	29	40%	42%
Oneens	1	1%	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 Staphorst heeft sinds december 2015 een gemeentebreed informatiebeveiligingsbeleid, in de periode daarvoor was er nog geen gemeentebreed informatiebeveiligingsbeleid, maar was er wel beleid toegespitst op specifieke vakgebieden. Dit beleid is op een aantal onderdelen uitgewerkt in formeel opgestelde procedures en richtlijnen. Kort na afronding van dit onderzoek heeft de gemeente in december 2018 een nieuw beleid vastgesteld op het gebied van informatiebeveiliging (Gemeentebreed informatiebeveiligingsbeleid 2018, 18 december 2018).

Uit interviews blijkt dat er in de praktijk procedures worden gevolgd om continuïteit te borgen, zoals uitwijkmogelijkheden naar andere datacenters. Ook heeft de gemeente Staphorst ervoor gekozen om beveiligd e-mailen sinds de zomer van 2018 aan te bieden aan haar medewerkers. De richtlijn is dat vertrouwelijke documenten daarmee op een beveiligde manier kunnen worden verstuurd. Tevens is de website van de gemeente Staphorst in 2017 omgezet naar een beveiligde website, zodat de uitwisseling van gegevens tussen bezoekers en de website is beveiligd en niet kan worden “afgeluisterd”.

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

Hoofdstuk 1.3 van het informatiebeveiligingsbeleid van de gemeente Staphorst beschrijft dat het beleid volledig gebaseerd is op ISO 27001 en 27002. Verder toont documentatie dat de gemeente Staphorst een gap-analyse uitgevoerd op de BIG en in het plan van aanpak ‘gaps’ vertaald naar actiepunten.

Tijdens interviews is bevestigd dat de gemeente Staphorst (jaarlijks) gap-analyses uitvoert op de BIG en actiepunten baseert op de resultaten van die analyse.

Het privacybeleid van de gemeente Staphorst verwijst naar de BIG. Er wordt gesteld dat het privacybeleid met nadruk gekoppeld moet worden aan de BIG, omdat een groot aantal referentienummers van de BIG een directe werking hebben op de mate van privacybescherming. In het informatiebeveiligingsbeleid is een verwijzing naar

de Wet Bescherming Persoonsgegevens (WBP) opgenomen en nog niet naar de AVG die later in werking is getreden. In het in december 2018 vastgestelde informatiebeveiligingsbeleid is de verbinding met de AVG gelegd.

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

Het informatiebeveiligingsbeleid van de gemeente Staphorst beschrijft in hoofdstuk 2.5 de Plan-Do-Check-Act cyclus rondom informatiebeveiliging.

Uit de informatiebeveiligingsanalyse (uitgevoerd in 2017) blijkt dat de PDCA-cyclus voor 50% is geïmplementeerd. In de “plan” fase vinden de activiteiten op periodieke basis plaats, echter wordt als onderdeel van de “do” fase onvoldoende opvolging gegeven aan bijvoorbeeld de uitvoering van het plan van aanpak. Ook is aangegeven dat de “check” en “act” fase eigenlijk geheel achterwege blijven. Dit werd onderstreept tijdens de interviews.

Als oorzaak is (in de interviews) aangegeven dat er gebrek is aan tijd, maar ook gebrek aan regie. Gebrek aan regie werd ook genoemd als oorzaak voor het feit dat er minder actiepunten uit de gap-analyse op de BIG zijn opgepakt dan voorzien. Er is aangegeven dat de gemeente Staphorst een doe-mentaliteit heeft. Regie, sturing vanuit het management ontbreekt.

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 Staphorst beschrijft in hoofdstuk 2.5 dat het uitgangspunt is dat informatiebeveiligingsbeleid eenmaal per 3 tot 4 jaar wordt bijgesteld. Er is ruimte om tussentijds documenten bij te werken.

Uit interviews bleek dat het beleid rondom informatiebeveiliging in 2015 tot stand is gekomen onder begeleiding van het bedrijf BMC. Vanuit de gemeente Staphorst hebben de CISO en de Beveiligingsbeheerder de leiding gehad. Daarnaast zijn vanuit de gemeente een aantal andere mensen betrokken geweest bij de opzet van het beleid. Het beleid moet uiterlijk in 2019 opnieuw worden vastgesteld. Inmiddels is dit in december 2018 gebeurd.

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

Hoofdstuk 4.4 van het informatiebeveiligingsbeleid beschrijft de classificatie van informatie en bedrijfsmiddelen. Op pagina 26 staat de classificatietabel:

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

In interviews is aangegeven dat op basis van een afhankelijkheids- en kwetsbaarheidsanalyse de informatiesystemen en processen van de gemeente zijn geclassificeerd naar beschikbaarheid, integriteit en vertrouwelijkheid. Systemen en processen waarbinnen (bijzondere) persoonsgegevens worden verwerkt zijn onderdeel van deze dataclassificatie.

In de enquête die als onderdeel van het onderzoek is uitgezet onder de medewerkers van de gemeente Staphorst is ook een vraag gesteld over dataclassificatie. De medewerkers van Staphorst zijn wat minder vaak zeer goed in staat de gevoeligheid van gegevens te beoordelen en wat vaker goed in staat. 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	14	19%	32%
Redelijk goed	47	65%	55%
Matig	8	11%	10%
Zeer beperkt	2	3%	4%
Helemaal niet	1	1%	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 Staphorst heeft een informatiebeveiligingsplan (Plan van Aanpak) opgesteld voor 2018 – 2019. Als we kijken naar het rapport informatiebeveiliging dan blijkt dat bij aanvang van de gap-analyse op de BIG in 2015 in totaal 144 van de 303 maatregelen had gerealiseerd. In het Plan van Aanpak van 2015 stond dat tot 2017 er 59 ontbrekende maatregelen gerealiseerd zouden worden. Uiteindelijk zijn in die periode niet alle maatregelen gerealiseerd.
In 2017 zijn alle maatregelen opnieuw kritisch bekeken, daaruit bleek dat een aantal maatregelen wel gedeeltelijk was gerealiseerd op een aantal afdelingen, maar nog niet in de gehele organisatie. Bij die analyse zijn er ook weer nieuwe noodzakelijke maatregelen geïdentificeerd. Daarmee is de achterstand in uit te voeren maatregelen niet ingelopen.
In interviews is als belangrijkste oorzaak genoemd dat de betrokken medewerkers beperkt beschikbaar zijn. Er zijn geen uren (FTE) beschikbaar gesteld voor het uitvoeren van de (benodigde) rollen, de medewerkers vervullen de rollen naast hun bestaande werkzaamheden. Per 1 december 2018 is er één privacy officer benoemd voor 0,5 fte.

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

De gemeente Staphorst heeft een aantal procedures en richtlijnen uitgeschreven.

Uit de interviews blijkt dat in de praktijk procedures worden gevolgd om continuïteit te borgen, zoals uitwijkmogelijkheden naar andere datacenters. Ook heeft de gemeente Staphorst ervoor gekozen om beveiligd e-mailen sinds de zomer van 2018 aan te bieden aan haar medewerkers. De richtlijn is dat vertrouwelijke documenten daarmee op een beveiligde manier kunnen worden verstuurd.

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

Hoofdstuk 2.5 van het informatiebeveiligingsbeleid beschrijft de volgende PDCA-cyclus:
- In het informatiebeveiligingsbeleid staat dat dit beleid eens per 3 tot 4 jaar wordt herzien. Het document stamt uit 2015 en zou dus in 2018 of 2019 opnieuw worden herzien.
- Het informatiebeveiligingsplan wordt iedere 1 tot 2 jaar bijgesteld.
- Het Plan van Aanpak met concrete acties uit de risicoanalyse wordt twee tot viermaal per jaar bijgesteld.
- De Risico-Inventarisatie en Evaluatie is van 17 oktober 2017. Het beleid stelt niet hoe vaak de RI&E wordt uitgevoerd.

Zie ook wat is beschreven bij onderzoeksvraag 1.3: Uit de informatiebeveiligingsanalyse (uitgevoerd in 2017) blijkt dat de PDCA-cyclus voor 50% is geïmplementeerd. In de “do” fase wordt onvoldoende opvolging gegeven aan bijvoorbeeld de uitvoering van het plan van aanpak. Ook is aangegeven dat de “check” en “act” fase eigenlijk geheel achterwege blijven. Dit werd onderstreept tijdens de interviews.

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 van de gemeente Staphorst in hoofdstuk 3 is de organisatie van informatiebeveiliging beschreven. In hoofdstuk 4 van het privacybeleid stelt de gemeente Staphorst dat de Functionaris Gegevensbescherming (FG) en de CISO intern toezicht houden, bijgestaan door interne auditors.

Uit interviews blijkt dat de definitie van de rollen van FG en CISO binnen de gemeente Staphorst duidelijk zijn, alsook voor de te starten Privacy Officer(s). De CISO-rol wordt momenteel echter al enige tijd waargenomen en voor de invulling daarvan is zeer beperkte capaciteit beschikbaar. De CISO heeft een cruciale rol in de overall coördinatie van informatiebeveiliging binnen de gemeente. De Privacy Officer heeft een cruciale rol ten aanzien van de implementatie van AVG-maatregelen binnen de gemeente.

In de enquête die PwC heeft uitgezet onder de medewerkers van Staphorst zijn twee vragen gesteld met betrekking tot dit onderwerp. Hieruit blijkt dat medewerkers in Staphorst in vergelijking met de andere drie onderzochte gemeenten minder goed weten wie welke taken vervuld op het gebied van informatiebeveiliging en aan wie men hierover vragen kan stellen. De resultaten zijn hieronder weergegeven.

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	15	21%	24%
Redelijk goed	24	33%	44%
Matig	23	32%	21%
Zeer beperkt	5	7%	7%
Helemaal niet	4	6%	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	17	24%	25%
Eens	30	42%	51%
Neutraal	15	21%	13%
Oneens	8	11%	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.

Hoofdstuk 1.5 van het informatiebeveiligingsbeleid beschrijft dat de verantwoordelijkheid voor informatiebeveiliging op bestuurlijk niveau bij het college van B&W ligt en op ambtelijk niveau bij de gemeentesecretaris/algemeen directeur.

Hoofdstuk 2.1 van het informatiebeveiligingsbeleid beschrijft dat het college van B&W een gemeentebreed beleidsdocument voor informatiebeveiliging behoort goed te keuren, uit te geven en kenbaar te maken aan alle medewerkers, alsmede hiernaar te handelen.

Uit interviews blijkt dat de CISO rapporteert aan het Hoofd Bestuur. Het Hoofd Bestuur rapporteert aan het college. De Controller rapporteert omtrent informatiebeveiliging in jaarlijkse P&C-rapportages, waarbij informatiebeveiliging een onderdeel is van de algehele rapportage. Doordat informatiebeveiliging (net als andere onderwerpen) beperkt wordt belicht in rapportages is de kans groot dat het onderwerp ondergesneeuwd raakt. Geïnterviewden geven aan dat er nu een grote kans is dat de raad het voor kennisgeving aanneemt en zich niet het belang ervan realiseert.

In het jaarverslag van 2013 wordt niet expliciet ingegaan op informatiebeveiliging. In 2014 wordt in het jaarverslag aangegeven dat de VNG heeft opgeroepen om meer aandacht te schenken aan dit thema. Concreet

gaat het om het benoemen van een collegelid als portefeuillehouder voor informatieveiligheid, vermelding in het collegeprogramma, uitwerking van beleid en rapportage aan de raad. Aangekondigd wordt dat er een risico-inventarisatie wordt gemaakt, dat de BIG hierbij als uitgangspunt zal dienen en dat er een beleidsplan zal worden opgesteld in samenwerking met de gemeenten Dalfsen en Zwartewaterland.

In 2015 wordt vermeld dat de risico-analyse is uitgevoerd en het beleidsplan is vastgesteld. Tevens wordt in het jaarverslag aangegeven dat een aantal technische en organisatorische maatregelen zijn genomen, die kort worden genoemd.

In 2016 wordt aangegeven dat op basis van het informatieveiligheidsbeleid acties zijn geformuleerd. Tevens wordt vermeld dat een beperkt aantal acties is uitgevoerd, dat er nog veel acties in behandeling zijn genomen en er ook nog acties moeten worden opgestart. De beschikbare capaciteit wordt als belangrijkste factor genoemd voor het niet kunnen uitvoeren van alle acties. In 2016 zijn er enkele beveiligingsincidenten onder andere op basis van een onderzoek van de IBD (Informatie Beveiligings Dienst) en van Binnenlands Bestuur die kwetsbaarheden aan het licht brengt.

In het jaarverslag van 2017 wordt vrij uitvoerig ingegaan op informatiebeveiliging. Het informatiebeveiligingsbeleid wordt toegelicht, evenals de ENSIA (Eénduidige Normatiek Single Information Audit); de vragenlijst die diverse vragenlijsten voor die diverse werkvelden samenvoegt. Daarnaast wordt aangegeven dat een aantal acties zijn uitgevoerd, maar een groter aantal nog niet en dat voldoende capaciteit hiervoor belangrijk is. Concrete aantallen van de acties worden niet genoemd.

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.

Hoofdstuk 1.5 van het informatiebeveiligingsbeleid beschrijft dat de verantwoordelijkheid voor informatiebeveiliging op bestuurlijk niveau bij het college van B&W ligt en op ambtelijk niveau bij de gemeentesecretaris/algemeen directeur.

Hoofdstuk 2.1 van het informatiebeveiligingsbeleid beschrijft dat het college van B&W een gemeentebreed beleidsdocument voor informatiebeveiliging behoort goed te keuren, uit te geven en kenbaar te maken aan alle medewerkers, alsmede hiernaar te handelen. Het informatiebeveiligingsbeleid is echter niet ondertekend (door de verantwoordelijken).

Met betrekking tot het management werd in de interviews aangegeven dat het management betrokken is, maar of het management zich actief bezighoudt met informatiebeveiliging en het uitdragen daarvan werd niet herkend. Het management werd als 'volgend' ervaren, niet leidend.

In de enquête die is gehouden onder de medewerkers van de gemeente Staphorst is een stelling opgenomen over de actieve betrokkenheid van het management bij informatiebeveiliging. Uit de resultaten blijkt dat de gemeente Staphorst ongeveer op het gemiddelde scoort 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	3%	6%
Eens	25	35%	32%
Neutraal	36	50%	46%
Oneens	7	10%	13%
Helemaal oneens	2	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.

In het Risico-Inventarisatie en Evaluatiedocument wordt bij risico 13 t/m 16 gesproken over een Bewustwordingskalender als getroffen maatregel. Bij 'Nog te nemen maatregelen' staat dat de risico's onder de aandacht zijn gebracht bij bewustwordingssessies, maar dat deze maatregel continue aandacht behoeft.

Uit de interviews blijkt dat er vanaf 2017 jaarlijks meerdere bewustwordingsacties worden uitgevoerd. Voor die tijd gebeurde dit nog niet. In 2017 werd gestart met bewustwordingsbijeenkomsten voor medewerkers. In 2018 is een eLearning uitgerold, voorafgegaan door een phishingmail test. Ook wordt eens per kwartaal een poster gewisseld bij de koffieautomaat. Iedere maand staat er een ander onderwerp met betrekking tot

informatiebeveiliging op het intranet. Het was ook de bedoeling om bij het werkoverleg de coördinatoren een onderwerp rondom informatiebeveiliging in te laten brengen. Daarover zou dan gediscussieerd zou kunnen worden. Dit is nog niet gelukt. De discussieonderwerpen zijn benoemd in de bewustwordingskalender 2018, maar door prioritering van werkzaamheden is dit nog niet verder opgepakt.

De algemene ervaring bij de geïnterviewden is dat mensen zich sinds de komst van de AVG veel bewuster zijn geworden. Toch is de gedachte dat bewustwording sterk kan variëren per afdeling en medewerkers mogelijk niet weten waar zij een datalek kunnen of moeten melden. Ook werd er een ander effect van de AVG benoemd: een medewerker die betrokken was bij een (relatief onschuldig) datalek had zich daar zonder reden erg veel zorgen om gemaakt. Dit is een indicatie dat mensen ook bang kunnen zijn om iets fout te doen.

In de enquête die als onderdeel van dit onderzoek is uitgezet onder de medewerkers van de gemeente Staphorst zijn een aantal vragen gesteld met betrekking tot dit onderwerp. In het algemeen vinden medewerkers van de gemeente Staphorst in vergelijking met de medewerkers in de andere drie gemeenten dat zij minder goed op de hoogte zijn van het informatiebeveiligingsbeleid en ook wat minder goed geïnformeerd worden. De resultaten zijn hieronder vermeld:

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 cijfer van 72 respondenten): **6,7**

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	2	3%	8%
Redelijk goed	29	40%	47%
Matig	31	43%	31%
Zeer beperkt	8	11%	10%
Helemaal niet	2	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	3	4%	13%
Redelijk goed	42	58%	58%
Matig	18	25%	20%
Zeer beperkt	7	10%	5%
Helemaal niet	2	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	9	13%	14%
Redelijk goed	35	49%	50%
Matig	15	21%	24%
Zeer beperkt	5	7%	6%
Helemaal niet	8	11%	7%

U wordt regelmatig en goed geïnformeerd over informatiebeveiliging:

Keuze:	Aantal antwoorden:	Percentage:	Percentage gemiddelde van de vier onderzochte gemeenten:
Helemaal eens	5	7%	8%
Eens	21	29%	38%
Neutraal	30	42%	36%
Oneens	14	19%	17%
Helemaal oneens	1	1%	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	13	18%	17%
Eens	31	43%	51%
Neutraal	20	28%	18%
Oneens	7	10%	12%
Helemaal oneens	1	1%	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	7	10%	17%
Eens	36	50%	51%
Neutraal	21	29%	23%
Oneens	6	8%	6%
Helemaal oneens	2	3%	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 Staphorst heeft een document met het applicatielandschap (per maart 2017). Het document geeft een overzicht van de applicaties. Bijlage 2 in het document 'Informatiebeveiligingsanalyse Staphorst 2017' geeft een overzicht van applicaties, met een bepaling van de Beschikbaarheid, Integriteit en Vertrouwelijkheid. Tevens blijkt uit dat laatste document dat nog niet alle voorgenomen technische maatregelen zijn geïmplementeerd.

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

In het RI&E-document van de gemeente Staphorst worden bij verscheidene risico's technische maatregelen genoemd om de risico's tegen te gaan. In het RI&E-document worden de volgende maatregelen benoemd:

- UPS/generator/noodstroom voorziening;
- Antivirus;

- Virtual patching;
- Gereguleerd internet;
- 2-factor authenticatie;
- Application whitelisting;
- Firewall.

Bovenstaande lijst is geen uitputtende beschrijving van de technische maatregelen die de gemeente Staphorst heeft getroffen; zo heeft de gemeente bijvoorbeeld ook een applicatie in gebruik genomen om beveiligd te kunnen e-mailen.

De gemeente Staphorst heeft in 2018 een externe penetratietest laten uitvoeren door een extern onderzoeksbureau. Verder heeft de gemeente Staphorst zich verzekerd tegen cybercrime en datalekrisico's. Bij dergelijke calamiteiten/incidenten krijgt de gemeente ondersteuning van externe specialisten in het kader van forensisch onderzoek en communicatie.

Tijdens interviews werd aangegeven dat de verwachting is dat de gemeente op technisch vlak een '9' scoort. Beveiliging is in technisch opzicht goed georganiseerd. Bij de implementatie van nieuwe producten of diensten wordt goed nagedacht over de beveiliging ervan.

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

Het belangrijkste resultaat van ons onderzoek is dat missende beveiligingsupdates, onveilige configuratie en het wijdverspreid gebruik van lokale administratieve accounts met eenzelfde wachtwoord ongeautoriseerde toegang mogelijk maken tot het interne netwerk van de gemeente Staphorst. Zonder enige vorm van rechten op de infrastructuur van gemeente Staphorst 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 Staphorst. In een reactie geeft de ambtelijke organisatie aan dat tijdens onze penetratietest de aanvallers gelokaliseerd werden en geblokkeerd hadden kunnen worden. We merken daarbij op dat deze detectie en de te nemen tegenmaatregelen niet de gehele dag en 7 dagen per week direct mogelijk zijn en ook niet zeker is dat de blokkades tijdig en afdoende zullen zijn.

Missende kritieke updates maken gemeente Staphorst kwetsbaar voor ransomware aanvallen
Uit onze werkzaamheden bleek dat 16 systemen op het netwerk van gemeente Staphorst specifieke beveiligingsupdates missen, die nodig zijn om een ransomware aanval te stoppen. De kwetsbaarheid die het hier betreft, heeft destijds 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.

Wijdverspreid gebruik van 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.

Inferieure configuratie maakt het mogelijk om toegang te verkrijgen tot het draadloze *govroam* netwerk
Bij gemeente Staphorst wordt het draadloze *govroam* netwerk aangeboden, welke gebruik maakt van een onveilig authenticatiemechanisme. Een kwaadwillende is in staat een vijandig draadloos netwerk aan te bieden met dezelfde naam. Systemen van gebruikers zullen vervolgens automatisch connectie proberen te maken met dit vijandige netwerk, waarbij de aanvaller in bezit komt van gebruikersnamen en wachtwoorden die de verbonden systemen aanbieden. Met deze gegevens kan vervolgens ongeautoriseerde toegang verkregen worden tot het originele draadloze *govroam* netwerk.

Om deze aanval te kunnen uitvoeren moet de aanvaller een gevorderde zijn voor wat betreft kennis van aanvallen en bijvoorbeeld bekend zijn met de techniek achter wifiverbindingen. Iemand met de vaardigheden van een systeembeheerder zou dit kunnen uitvoeren.

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

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

De RI&E bevat maatregelen op risico's betreffende persoonsgegevens, zoals bewustwordingssessies, clean desk, clear screen en bezoekers begeleiden.

In interviews werd aangegeven dat de gemeente veel aandacht besteed aan de beveiliging wanneer nieuwe producten of diensten worden geïntroduceerd.

Applicatieonderzoeken
In het kader van deze norm zijn bij de gemeente Staphorst twee applicaties onderzocht, te weten Topicus Overheid Platform (TOP) en Participatie en Wmo. 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.

Toegangsbeleid voor de applicaties is verwerkt in rechten en rollen. Bij indiensttreding van een medewerker wordt bepaald welke rechten hij/zij dient te krijgen in de applicaties. Functioneel Beheerders maken de nieuwe accounts aan voor de gebruikers. De applicaties zijn alleen ontsloten voor medewerkers van de gemeente waarvoor een account is aangemaakt.

Als een medewerker voor korte tijd toegang nodig heeft tot Participatie en Wmo dan wordt bij het aanmaken van het account ook direct een einddatum ingesteld.

Voor TOP geldt dat een nieuwe gebruiker geen standaard wachtwoord krijgt ingesteld. De gebruiker dient zelf een nieuw wachtwoord in te stellen via het "Wachtwoord vergeten" proces. Dit is een veilig proces. Bij Participatie en Wmo krijgt een gebruiker wel direct een gebruikersnaam en wachtwoord, maar moet het wachtwoord direct de eerste keer worden gewijzigd.

De leverancier Topicus heeft niet standaard toegang tot de applicatie TOP. In geval van support calls krijgt de leverancier tijdelijk toegang tot de applicatie onder een eigen account, wat tijdelijk wordt opengesteld.

- *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.

TOP is een SaaS oplossing, het draait 'in de cloud'. Daardoor is de leverancier verantwoordelijk voor de beschikbaarheid van de omgeving. Voor zover bekend bij de gemeente Staphorst is de applicatie nooit offline (en dus nooit onbeschikbaar) geweest.

Het Technisch Beheer van Participatie en Wmo ligt bij de gemeente Dalfsen. Die gemeente is verantwoordelijk voor de beschikbaarheid van de applicatie en het maken van backups. De beschikbaarheid van de applicatie is nooit in het geding geweest. De gemeente Dalfsen maakt dagelijkse backups van de applicatie.

- *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.

Topicus voorziet de gemeente Staphorst voor TOP van een Acceptatie- en een Productieomgeving. Nieuwe updates en wijzigingen worden eerst in de Acceptatieomgeving klaargezet. Gemeenten (in heel Nederland) kunnen de update/wijzigingen testen en ze vervolgens accorderen of blokkeren. Wegens tijdgebrek test de gemeente Staphorst de nieuwe updates van TOP niet actief.

Voor Participatie en Wmo is er een Testomgeving, Opleidingsomgeving en Productieomgeving. Ook hier worden updates eerst getest in de Testomgeving. Er wordt grotendeels eerst in Dalfsen getest, al mag vanuit Staphorst ook getest worden. Het kan voorkomen dat een regeling alleen door Staphorst wordt gebruikt, dan moet deze specifiek door Staphorst worden getest.

- *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.

Beveiligingsincidenten bij de gemeente Staphorst kunnen worden gemeld bij de CISO van de gemeente Staphorst of zijn plaatsvervanger.

Het is mogelijk voor gebruikers om gegevens uit TOP te exporteren en op te slaan als pdf-document op het lokale systeem van waaraf gewerkt wordt. Ook is het mogelijk om documenten van het lokale systeem te uploaden in de applicatie.

De Testomgeving van Participatie en Wmo bevat dezelfde gegevens als de Productieomgeving. Eenmaal in de zoveel tijd worden de gegevens uit productie gekopieerd naar Test waardoor de gegevens in Test in principe wel verouderd zijn.

- *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.

Activiteiten van medewerkers en van (systeem)beheerders van beide applicaties worden vastgelegd in de logging. Hierbij kan gedacht worden aan het aanmaken van een medewerker, het inloggen, raadplegen van dossiers, het downloaden van managementexports, alsook configuratiewijzigingen binnen de applicatie. De logging is alleen in te zien door medewerkers met de beheerdersrol. De logging bevat zelf geen gevoelige informatie, zoals wachtwoorden of inhoudelijke informatie over dossiers.

Waarschijnlijk kan er in de logging van TOP worden teruggekeken vanaf het eerste moment dat de applicatie in gebruik werd genomen. Voor Participatie en Wmo geldt dat de logging ten minste drie maanden terug in de tijd gaat.

- *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.

Welke afspraken er zijn gemaakt met de leverancier (Topicus), is onbekend. Wel is er jaarlijks contact met de leverancier, waarbij gesproken wordt over tevredenheid.

Participatie en Wmo is van de leverancier Centric. Het contact vindt tenminste jaarlijks plaats en draait dan om de jaarafwikkeling.

- *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.

De applicatie TOP is ontsloten voor bekende IP-adressen. De beheerder beheert de IP-adressen van waaraf direct ingelogd mag worden op de applicatie. In dat geval kan worden ingelogd met een gebruikersnaam en wachtwoord. Vanaf onbekende IP-adressen kan ook worden ingelogd, maar in dat geval door middel van twee-factor authenticatie. Een gebruiker moet dan een gebruikersnaam, wachtwoord en een sms-code invullen.

Wachtwoorden dienen iedere 90 dagen te worden gewijzigd in TOP.

Ongeveer 20 medewerkers hebben toegang tot TOP. De accounts worden periodiek gecontroleerd, op ieder moment dat er wijzigingen zijn van een account. Meestal is dat op het moment dat gecommuniceerd wordt dat een gebruiker verwijderd kan worden uit het systeem.

Toegang tot Participatie en Wmo is alleen mogelijk vanuit het netwerk van de gemeente Staphorst (en Dalfsen, waar de applicatie mee gedeeld wordt). Wanneer een gebruiker inlogt, wordt de datum en tijd van de vorige succesvolle inlog in het scherm getoond. Zodoende kunnen gebruikers valideren dat zij daadwerkelijk degene waren die de vorige keer ingelogd zijn geweest.

Die kans dat vanuit de gemeente Dalfsen ingebroken kan worden bij de gemeente Staphorst via de applicatie Participatie en Wmo is zeer klein, omdat de applicatie web-based is. Dat betekent dat de gemeente Dalfsen als het ware alleen een website beschikbaar dient te stellen aan de gemeente Staphorst. Op netwerk niveau is dan geen toegang vereist, die het mogelijk zou maken om in te breken op de systemen van de andere gemeente.

A. Applicatieonderzoeken

A.1. Topicus Overheid Platform (TOP)

Autorisatiebeheer
Toegangsbeleid voor de applicatie is verwerkt in rechten en rollen. Bij indiensttreding van een medewerker wordt bepaald welke rol hij of zij vervult en welke rechten derhalve worden toegekend binnen TOP.

Voor een nieuwe gebruiker wordt geen (standaard) wachtwoord ingesteld. De nieuwe gebruiker kan zelf een wachtwoord instellen via het “Wachtwoord vergeten” proces.

Verantwoordelijkheden voor beheer, wijziging van gegevens en bijbehorende informatiesysteemfuncties zijn toegewezen aan specifieke rollen. Wel heeft het administratieteam de rechten op alle handelingen/dossiers in de cyclus. Andere rollen hebben geen rechten die de gehele cyclus beslaan.

Er is een gebruikersaccount voor de helpdesk van Topicus, de leverancier van de applicatie. De leverancier heeft niet standaard toegang tot het systeem. Enkel in het geval van support calls bij de leverancier en wanneer de leverancier zelf een probleem niet kan reproduceren, wordt het leveranciersaccount geactiveerd. Daarna heeft de leverancier (tijdelijk) toegang tot de omgeving.

Beschikbaarheid
TOP is een cloud-based SaaS oplossing. Daardoor is de leverancier verantwoordelijk voor de beschikbaarheid van de omgeving. Voor zover bekend is de oplossing nooit offline (en dus nooit onbeschikbaar) geweest.

Change management
De leverancier voorziet de gemeente Staphorst in een Acceptatie- en een Productie-omgeving. Nieuwe updates en wijzigingen worden eerst in de Acceptatie-omgeving klaargezet. Gemeenten (in heel Nederland) kunnen de update/wijziging testen en accorderen of blokkeren. Wegens tijdgebrek test de gemeente Staphorst nieuwe updates en wijzigingen niet actief.

Databeveiligingsincidenten
Beveiligingsincidenten kunnen worden gemeld bij de CISO van de gemeente Staphorst of zijn plaatsvervanger.

Het is mogelijk voor gebruikers om gegevens uit de applicatie te exporteren en op te slaan als pdf-document op het lokale systeem van waaraf gewerkt wordt. Ook is het mogelijk om documenten van het lokale systeem te uploaden in de applicatie.

AVG
De bewaartermijn van de dossiers in TOP is gesteld op 15 jaar (dat gaat in vanaf de leeftijd van 18 jaar van de betreffende persoon). Binnen de gemeente Staphorst is er één persoon met de rechten om dossiers te verwijderen.

Activiteiten van medewerkers en van (systeem)beheerders worden vastgelegd in logging. Hierbij kan gedacht worden aan het aanmaken van een medewerker, het inloggen, raadplegen van dossiers, het downloaden van managementexports, alsook configuratiewijzigingen binnen de applicatie. De logging is alleen in te zien door medewerkers met de beheerdersrol. De logging bevat zelf geen gevoelige informatie, zoals wachtwoorden of inhoudelijke informatie over dossiers. Waarschijnlijk kan er in de logging worden teruggekeken vanaf het eerste moment dat de applicatie in gebruik werd genomen (1-1-2015).

Leveranciersmanagement
Er is jaarlijks contact met de leverancier Topicus waarbij wordt gesproken over de tevredenheid. De afspraken met Topicus zijn vastgelegd in een SLA (service level agreement) en verwerkersovereenkomst.

Logische toegangsbeveiliging

De applicatie TOP is ontsloten voor bekende IP-adressen. De beheerder beheert de IP-adressen van waaraf direct ingelogd mag worden op de applicatie. In dat geval kan worden ingelogd met een gebruikersnaam en wachtwoord. Vanaf onbekende IP-adressen kan ook worden ingelogd, maar in dat geval door middel van twee-factor authenticatie. Een gebruiker moet dan een gebruikersnaam, wachtwoord en een sms-code invullen.

Wachtwoorden dienen iedere 90 dagen te worden gewijzigd.

Ongeveer 20 medewerkers hebben toegang tot de applicatie. De accounts worden periodiek gecontroleerd, op ieder moment dat er wijzigingen zijn van een account. Meestal is dat op het moment dat gecommuniceerd wordt dat een gebruiker verwijderd kan worden uit het systeem.

De meeste medewerkers hebben de 'Medewerkersrol'. Daarmee kan alleen een dossier geopend worden wanneer de medewerker daarbij betrokken is.

A.2. Participatie en Wmo

Autorisatiebeheer
Automatisering maakt een melding in TOPdesk dat er een gebruiker aangemaakt moet worden in de applicatie. Daarbij wordt aangegeven welke rol de gebruiker moet hebben, zoals bijvoorbeeld Wmo-Consulent. De gebruiker wordt dan met die rol aangemaakt in de applicatie. Nieuwe gebruikers moeten door Functioneel Beheer worden aangemaakt. Alleen aangemaakte gebruikers kunnen inloggen in de applicatie, dus niet alle medewerkers van de gemeente. Inloggen kan met een gebruikersnaam en wachtwoord. Dit wachtwoord staat los van het netwerk/Windows wachtwoord. Het wachtwoord heeft bepaalde complexiteitseisen en verloopt om de drie maanden.

Als een medewerker voor korte tijd in dienst komt en toegang tot de applicatie nodig heeft, dan wordt bij het aanmaken van het account deze ook direct voorzien van een geldigheids-einddatum.

Applicatiebeheer wordt gedeeld met de gemeente Dalfsen. Medewerkers van de ene gemeente kunnen niet de gegevens inzien van een andere gemeente, ook beheerders niet. Zelfs als een inwoner verhuist van de ene gemeente naar de andere, dan is de historie niet te zien voor de nieuwe gemeente. De gegevens zijn strikt gescheiden, ook al wordt de applicatie gedeeld.

Binnen de applicatie is verschil aangebracht tussen de rollen van onder meer administratie en consultenten. Consulenten kunnen rapporten en beschikkingen aanmaken, administratie vult het werkproces en het indicatiebesluit en uitkeringsdossier in. Een beheerder is niet in staat om bijvoorbeeld frauduleuze zaken te regelen, zoals het regelen van uitkeringen. Daar vindt altijd een extra autorisatieslag plaats.

Beschikbaarheid
Het Technisch Beheer van de applicatie ligt bij de gemeente Dalfsen. Zij zijn verantwoordelijk voor de beschikbaarheid van de applicatie en het maken van backups. De beschikbaarheid van de applicatie is nooit in het geding geweest. De gemeente Dalfsen maakt dagelijkse backups van de applicatie.

Change management
Er is een Testomgeving, Opleidingsomgeving en een Productieomgeving. Nieuwe updates worden eerst altijd getest in de Testomgeving. Er wordt grotendeels eerst in Dalfsen getest, al mag vanuit Staphorst ook getest worden. Het kan voorkomen dat een regeling alleen door Staphorst wordt gebruikt, dan moet deze specifiek door Staphorst worden getest.

Een historie van configuraties en updates wordt niet bijgehouden. Wel kunnen beheerders in logging terugzien welke gebruikers wijzigingen hebben aangebracht.

Risico op Databeveiligingsincidenten
Beveiligingsincidenten kunnen worden gemeld bij de CISO van de gemeente Staphorst of zijn plaatsvervanger.

Indien een medewerker van Staphorst vanuit huis kan werken, is ook toegang tot deze applicatie mogelijk. De applicatie is niet direct vanaf een systeem met internetverbinding te benaderen, er dient eerst een verbinding

met de gemeente opgezet te worden. Het opzetten van deze verbinding verloopt via 2-factor authenticatie (gebruikersnaam, wachtwoord en aanvullende code).

De testomgeving bevat dezelfde gegevens als de productieomgeving. Eenmaal in de zoveel tijd worden de gegevens uit productie gekopieerd naar Test waardoor de gegevens in Test in principe altijd verouderd zijn. Ook in de testomgeving geldt dat gegevens van de andere gemeente niet geraadpleegd kunnen worden.

AVG – Logging en monitoring
Activiteiten van medewerkers en systeembeheerders wordt vastgelegd in logging, zoals bijvoorbeeld het aanmaken van een gebruiker of het veranderen van een instelling in de configuratie. Ook storingen zijn terug te vinden in de logging. De logging bevat geen gevoelige informatie, zoals wachtwoorden.

Een beheerder kan meer dan drie maanden terug in de logging om te kijken wat er gebeurd is. Standaard rapportages op of periodieke controles van logging zijn er niet.

De applicatie heeft een bescherming tegen het verwijderen van gegevens. Sommige data kan verwijderd worden, maar niet alles. Een uitkeringsdossier is bijvoorbeeld niet te verwijderen, een klant ook niet. Deze gegevens zouden überhaupt ook niet verwijderd mogen worden.

Leveranciersmanagement
Er is jaarlijks contact met de leverancier Centric, waarbij het contact draait om de jaarafwikkeling.

Logische toegangsbeveiliging
Wanneer een medewerker vertrekt/uitdienst gaat, wordt het account afgesloten. Eenmaal per jaar wordt geïnventariseerd welke accounts actief zijn en of dit strookt met de praktijk. Overbodige accounts worden afgesloten.

Toegang tot de applicatie is alleen mogelijk vanuit het netwerk van de gemeente Staphorst (en Dalfsen) en de verbinding tussen de gebruiker en de applicatie is versleuteld (https). Wanneer een gebruiker inlogt, wordt de datum en tijd van de vorige succesvolle inlog in het scherm getoond. Zodoende kunnen gebruikers valideren dat zij daadwerkelijk degene waren die de vorige keer ingelogd zijn geweest. De gebruiker hoeft op de melding geen actieve handeling uit te voeren, de vermelding wordt enkel ter kennisgeving geplaatst.

Wanneer een gebruiker inactief is voor 10 tot 15 minuten gaat het scherm op zwart. Geeft een gebruiker te vaak een verkeerd wachtwoord in, dan wordt het account vergrendeld. Dit gebeurt ook als een gebruiker zich meer dan 30 dagen niet heeft aangemeld bij de applicatie. Functioneel Beheer moet het account dan weer handmatig vrijgeven.

Een nieuwe gebruiker krijgt een gebruikersnaam en wachtwoord om in te loggen op de applicatie. Bij de eerste keer dat de gebruiker zich aanmeldt, moet direct een nieuw, eigen, wachtwoord gekozen worden. Gebruikers zijn daarna te allen tijde in staat om een nieuw wachtwoord in te stellen.

De leverancier heeft geen eigen standaardaccount en verkrijgt alleen toegang tot de applicatie door tussenkomst van een medewerker van de gemeente.

B. Bijlage: gebruikte documenten en interviews

B.1. Documenten

Gemeentebreed Informatiebeveiligingsbeleid Staphorst 2015

Gap-analyse Staphorst 2017

Informatiebeveiligingsanalyse Staphorst 2017

Risico inventarisatie en Evaluatie (RIE) 2017

Jaarplanner informatiebeveiliging 2018

Plan van Aanpak Informatiebeveiliging Staphorst 2018 – 2019

Patchbeleid gemeente Stphorst 2017 V1.2

Procedure wijzigingen in applicaties

Protocol backup en restore (2.0, jan '17)

Gedragscode e-mail en internetgebruik Staphorst 2015

Privacyreglement e-mail- en internetgebruik Staphorst 2015

Richtlijnen gebruik sociale media

Privacybeleid gemeente Staphorst

Applicatielandschap gemeente Staphorst – maart 2017

Communicatiekalender informatiebeveiliging

Protocol Incidentmanagement gemeente Staphorst

Protocol Melden Datalekken

Verslag overleg informatieveiligheid 20180423

Assurance-rapportage gemeente Staphorst SH

Collegeverklaring ENSIA – bijlage 2 Rapportage Suwinet 2017

Collegeverklaring ENSIA 2017 Staphorst

Collegeverklaring ENSIA Staphorst – bijlage 1 Rapportage DigiD Assessment 2017SH

IC rapport informatiebeveiliging 2017

Doorrekening AVG –advies BVNG

PEN-test Eset 2017

B&W-advies verzekering datarisico en cybercrime

Polisblad verzekering datarisico en cybercrime

Huidige situatie Informatiebeveiliging Staphorst 2015 (bijlage 5 IB-beleid)

Procedure autoriseren van gebruikers voor toegang tot applicaties

Procedure toegang tot en gebruik van systemen (incl RAAS)

Procedure beheer van certificaten en encryptiesleutels

MT-advies uitwijktest 2017

Protocol uitwijk

Rapportage uitwijktest 2017

Uitwijkcertificaat 2017

Uitwijktestverslag 2017

Aanpassen integriteit- en geheimhoudingsverklaring en VOG personeel en externen

Integriteits- en geheimhoudingsverklaring Externe Medewerkers

Integriteits- en geheimhoudingsverklaring personeel

Geteken rapport informatiebeveiliging

B.2. Interviews

Ter bescherming van persoonsgegevens zijn hier alleen de functiebenamingen opgenomen.

Functionaris Gegevensbescherming

Systeembeheerder / Beveiligingsbeheerder

Beveiligingsbeheerder

Privacybeheerder

Project Manager / Zaakgericht werken

Hoofd Bestuur & Management ondersteuning

Beveiligingsbeheerder

Controller Informatiebeveiliging

Bestuurlijke reactie ontvangen van het college van burgemeester en wethouders

gemeente Staphorst

Uw brief van	19 februari 2019
Uw kenmerk	
Ons kenmerk	UIT/19-080600
Zaaknummer	Z29620
Afdeling	Bestuur- & Managementondersteuning
Informant	dhr. G. Kappert
Doorkiesnummer	(0522) 46 74 32
Bijlagen	geen

Rekenkamercommissie
bram.de.groot@steenwijkerland.nl

Staphorst, 19 maart 2019
Verzonden 22 MAART 2019

Onderwerp Bestuurlijke reactie onderzoek informatiebeveiliging

Beste meneer/mevrouw,

Op 19 februari ontvingen wij uw concept-eindrapport over het onderzoek naar informatiebeveiliging bij de gemeente Staphorst. Via deze brief maken wij graag gebruik van uw aanbod om een reactie te geven.

Wij hebben het rapport met interesse gelezen en herkennen ons grotendeels in uw bevindingen en aanbevelingen. Wij vinden het positief dat diverse betrokkenen zijn gevraagd naar hun mening waardoor er een goed beeld is gevormd over informatieveiligheid bij de gemeente Staphorst.

Het rapport hebben wij behandeld in onze vergadering van dinsdag 19 maart. Hieruit is naar voren gekomen dat wij de conclusies en aanbevelingen uit de rapportage delen. Wel willen we de volgende opmerkingen plaatsen.

Capaciteit
Eind 2015 is voor het eerst het informatiebeveiligingsbeleid op basis van de BIG vastgesteld. De afgelopen jaren hebben we het beleid geïmplementeerd op basis van een plan van aanpak. Destijds was onvoldoende inzichtelijk welke capaciteit daarvoor nodig was. Inmiddels is het duidelijk dat er niet genoeg capaciteit is ingezet om de ambitie uit het plan van aanpak waar te kunnen maken. Er zijn minder maatregelen geïmplementeerd dan voorzien. In 2019 stellen we de raad voor de formatie voor informatiebeveiliging op orde te brengen zodat er meer sturing en regie komt en er voldoende capaciteit is om de noodzakelijke maatregelen op het gebied van informatiebeveiliging te implementeren.

Techniek
We delen uw mening dat er strategisch een aantal goede en belangrijke technische maatregelen zijn genomen ter beveiliging van de informatie. Desondanks is het onmogelijk een garantie af te geven dat er geen kwetsbaarheden in de technische infrastructuur overblijven.

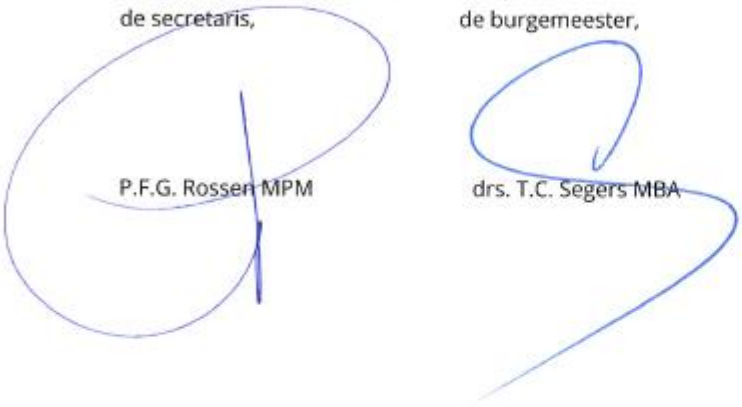
Postadres Postbus 2 - 7950 AA Staphorst **Bezoekadres** Binnenweg 26 - 7951 DE Staphorst
Tel. 0522 46 74 00 **E-mail** gemeente@staphorst.nl **Informatie** www.staphorst.nl

Nieuwe kwetsbaarheden worden ontdekt en kwaadwillenden ontwikkelen voortdurend nieuwe methoden en technieken om daarvan gebruik te maken. Om die reden houden wij vanaf 2017 jaarlijks een penetratietest. De uitkomsten uit de penetratietesten gebruiken we om de beveiliging verder aan te scherpen.

Wij wensen u succes toe met de afronden van de eindrapportage en zien uit naar de behandeling van het rapport in de raad.

Met vriendelijke groet,
Burgemeester en wethouders van Staphorst,

de secretaris, de burgemeester,



P.F.G. Rossen MPM drs. T.C. Segers MBA