Rekenkamercommissie Meppel, Staphorst, Steenwijkerland en Westerveld

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

1. Inleiding

De gemeenteraad 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 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 Steenwijkerland 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 een kwetsbaarheidsscan in Steenwijkerland uitgevoerd.

2.2. Conclusies en aanbevelingen

De gemeente Steenwijkerland beschikt over een actueel informatie-beveiligingsbeleid. In de onderzoeksperiode is het beveiligingsbeleid niet voorafgegaan door een integrale risicoanalyse. Pas eind 2018 is voor het eerst zo’n risicoanalyse uitgevoerd. Het verdient aanbeveling dit periodiek te blijven doen. Bestuurlijk is er inmiddels meer aandacht gekomen voor het vraagstuk van informatiebeveiliging met het aanwijzen van één portefeuillehouder. Geadviseerd wordt de bestuurlijke aandacht te borgen om de organisatie scherp te houden op dit onderwerp. Merkbaar is dat de organisatie op dit punt in opbouw is omdat in de eerste jaren waarover dit onderzoek ook gaat, de organisatiegraad minder was. Hier worden nu stappen in gezet zoals het positioneren van de CISO op concernniveau, maar zijn er ook nog stappen te zetten door het management in de bewustwording. Temeer omdat er nog steeds kwetsbaarheden worden gezien (w.o. toegangsbeveiliging). Verder zijn, zoals verderop uit het rapport blijkt, nog een aantal concrete verbeteringen mogelijk door technische maatregelen te nemen.

Organisatie en beleid

Het informatiebeveiligingsbeleid van Steenwijkerland is het laatst in 2017 vastgesteld voor de periode 2017 tot 2020. Het vorige informatiebeveiligingsbeleid werd in 2015 vastgesteld voor de periode 2015 tot 2020. Er is bewust gekozen het beleid eerder te actualiseren vanwege de vele ontwikkelingen. Het huidige beleidsplan volgt de nieuwe richtlijnen zoals aangegeven in de handreiking voor gemeenten, de baseline informatiebeveiliging gemeenten (BIG). Deze richtlijnen gelden nu gemeentebreed als uitgangspunt voor alle processen, gegevensverzamelingen en systemen. In het nieuwe beleid is ook meer aandacht voor de bescherming van persoonsgegevens in het kader van de Algemene Verordening Gegevensbescherming (AVG). Het informatiebeveiligingsbeleid is uitgewerkt in diverse procedures, richtlijnen en handreikingen. In de afgelopen jaren is het algemene beleid niet vertaald naar een jaarplan of een plan van aanpak.

Er heeft voorafgaand aan het geactualiseerde beleid geen integrale risicoanalyse plaatsgevonden. Er is dus niet eerst een analyse uitgevoerd van bedreigingen en kwetsbaarheden op het gebied van informatiebeveiliging

voordat het beleidsplan is opgesteld. Wel is er een toets uitgevoerd op de eerder genoemde richtlijnen in de baseline informatiebeveiliging gemeenten (BIG). Inmiddels is in het najaar van 2018 een eerste integrale risicoanalyse uitgevoerd onder begeleiding van een extern bureau. Op basis daarvan kan de gemeente het jaarplan voor 2019 mede baseren op de gevonden risico's en daarbij prioriteiten kiezen.

Aanbeveling: Voer voorafgaand aan een volgende actualisatie van het informatiebeveiligingsbeleid een integrale risicoanalyse uit, zodat er een basis is om speerpunten en prioriteiten te kiezen.

In het informatiebeveiligingsbeleid wordt een jaarlijkse leercyclus beschreven die start met een jaarlijkse herijking van het beleid, het opstellen van een jaarplan, uitvoering van de geplande maatregelen en in de loop van de uitvoering verzamelen van interne en externe evaluaties om de effectiviteit van de maatregelen te bezien. In de praktijk is de gemeente medio 2018 gestart met het meer expliciet opbouwen van deze leercyclus door een risicoanalyse te starten mede op basis van de diverse zelfevaluaties en (vaak verplichte) vragenlijsten. Dit is het vertrekpunt voor het geplande eerste jaarplan voor 2019. De gemeente is medio 2018 ook gestart met kwartaalrapportages voor informatiebeveiliging, die belangrijke input kunnen vormen voor het jaarplan.

Aanbeveling: Continueer de jaarlijkse risicoanalyse en de opbouw van de beoogde jaarlijkse leercyclus door een jaarplan op te stellen en vervolgens daarvan, met de direct betrokkenen, te leren op basis van eigen en externe evaluaties/analyses.

In de gemeente functioneerde een stuurgroep informatiebeveiliging die één of enkele keren per jaar bijeenkwam en waaraan meerdere collegeleden, de gemeentesecretaris en enkele ambtenaren deelnamen. In het voorjaar van 2018 is dit gewijzigd en is er één portefeuillehouder voor informatiebeveiliging aangewezen. Deze portefeuillehouder overlegt iedere twee weken met de gemeentesecretaris, de CISO (Chief Information Officer) en eventueel andere betrokkenen zoals de FG (Functionaris Gegevensbescherming).

Vanaf 2017 is er een centrale functionaris die verantwoordelijk is voor informatiebeveiliging (de CISO). De CISO is in de zomer van 2018 niet meer in een lijnafdeling geplaatst maar, meer centraal in de organisatie, in de concernstaf. Daarnaast zijn er beveiligingsbeheerders die op hun vakgebied verantwoordelijk zijn voor het uitvoeren van maatregelen en het uitvoeren van (zelf)analyses en is er vanaf juli 2018 een verantwoordelijke voor het toezicht op de bescherming van persoonsgegevens (FG). Ook de FG is geplaatst in de concernstaf.

Sinds medio 2018 worden het college en de raad geïnformeerd over informatiebeveiliging in de reguliere PDCA-cyclus door middel van kwartaalrapportages. Bij de start is hier extra aandacht voor geweest in het college en tijdens een bredere informatieavond voor de raad in oktober 2018. In het laatst beschikbare jaarverslag, het jaarverslag van 2017, wordt gerapporteerd over informatiebeveiliging en wordt ingegaan op de bescherming van persoonsgegevens en de invoering van de éénduidige vragenlijst op het gebied van informatiebeveiliging (ENSIA). In de jaarverslagen van de jaren voor 2017 wordt niet specifiek ingegaan op informatiebeveiliging.

Aanbeveling: Relateer de verantwoording in het jaarverslag aan het geactualiseerde informatiebeveiligingsbeleid en het op te stellen jaarverslag en geef aan wat er geleerd en verbeterd is.

Mens en gedrag

Van de medewerkers weet 71% redelijk tot zeer goed wie de belangrijkste rollen vervullen op het gebied van informatiebeveiliging en 29% weet dit matig tot zeer beperkt. Verder weet 74% aan wie men vragen kan stellen op het gebied van informatiebeveiliging en 21% weet dat niet of onvoldoende. Daarmee scoort Steenwijkerland

dicht bij het gemiddelde van de vier onderzochte gemeenten. Uit het onderzoek blijkt dat het uitdragen van informatiebeveiliging door het management aandacht behoeft. Slechts 29% van de medewerkers vindt dat het management actief betrokken is bij het uitdragen van informatiebeveiliging, het gemiddelde in de vier onderzochte gemeenten is 38%. In het algemeen is ondersteuning door het management cruciaal voor het succes van informatiebeveiliging. Het "mystery guest" onderzoek uit 2017 heeft laten zien dat de fysieke toegangsbeveiliging kwetsbaar is op meerdere punten. Uit onze interviews blijkt dat dit nog steeds als een kwetsbaar punt wordt gezien. Steenwijkerland heeft in de afgelopen jaren regelmatig aandacht geschonken aan aspecten van informatiebeveiliging via activiteiten voor medewerkers. Medewerkers zijn meer dan gemiddeld in vergelijking met de andere drie onderzochte gemeenten bekend met het informatiebeveiligingsbeleid, de verwachtingen voor de medewerkers, bekendheid met datalekken en wat te doen als deze geconstateerd worden.

Aanbeveling: Schenk in de komende bewustwordingsactiviteiten extra aandacht aan een actieve rol van het management, zodat het management breder gezien wordt als voorbeeld en ambassadeur van informatiebeveiliging.

Techniek

In september 2016 typeerde een extern onderzoeksbureau na het uitvoeren van een penetratietest de gemeente als "zeer onveilig". De kwetsbaarheidsscan die tijdens dit onderzoek werd uitgevoerd laat verbetering op dit onderdeel zien. Er is wel aandacht nodig omdat (belangrijke) beveiligingsupdates werden gemist. Het periodiek en meer rigoureus toepassen van een updatecyclus (zogenaamd patch-management) kan deze kwetsbaarheden aanzienlijk terugdringen. Er zijn voortdurend nieuwe ontwikkelingen op het gebied van technische informatiebeveiliging. Periodieke penetratietesten geven inzicht in kwetsbaarheden en technische maatregelen om die kwetsbaarheden op te lossen.

Zoals eerder ook vermeld heeft de gemeente in 2018 voor het eerst een risicoanalyse uitgevoerd. Dit bevordert de samenhang tussen gekozen beveiligingsmaatregelen en de geïdentificeerde risico's voor informatiebeveiliging.

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

De fysieke toegangsbeveiliging kan waarschijnlijk verbeterd worden door een grotere bewustwording van medewerkers. Daarnaast werd er ook gewezen op mogelijke fysieke maatregelen om de toegangsbeveiliging te verbeteren.

Aanbeveling: Voer een nadere analyse uit om na te gaan hoe de fysieke toegangsbeveiliging is te versterken, denk daarbij aan een combinatie van de wijze waarop medewerkers hiermee omgaan als ook aan fysieke maatregelen.

De applicatieonderzoeken wijzen uit dat de gemeente een sterke focus heeft op het testen van nieuwe software en updates, vergeleken met de andere gemeenten. Wel bevatten drie van de vier onderzochte applicaties productiegegevens in de testomgeving, wat het risico op een datalek vergroot. Bij twee van de vier onderzochte applicaties zou de logging verbeterd kunnen worden, zodat inzichtelijk is welke acties zijn uitgevoerd op de informatie die de applicatie bevat.

Bij één applicatie was het mogelijk om gegevens te exporteren. Het is de vraag of dit voor de werkzaamheden van de gebruikers noodzakelijk is en welke risico's eraan verbonden zijn. Dit zou onderzocht kunnen worden, waardoor duidelijk wordt of deze functionaliteit (het kunnen exporteren van gegevens) beschikbaar moet blijven, of er aanvullende maatregelen getroffen moeten worden, of dat de situatie zoals deze is acceptabel is.

Aanbeveling:
Voorkom het gebruik van productiegegevens in testomgevingen.

3. Onderzoeksvragen en aanpak

3.1. Onderzoeksvragen

We stellen in het onderzoek de volgende vraag centraal:

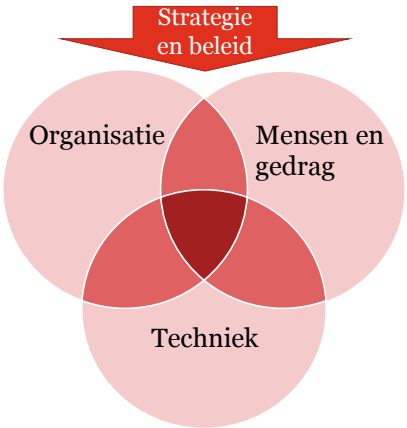
Is de informatiebeveiliging van de gemeenten Meppel, Staphorst, Steenwijkerland en Westerveld doeltreffend?

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 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 Steenwijkerland werden bij de inventarisatie expliciet enkele applicaties genoemd die aandacht behoeven. Voor Steenwijkerland 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

In dit onderzoek is ook een kwetsbaarheidsscan uitgevoerd. De kwetsbaarheidsscan beoogt kwetsbaarheden in het netwerk vast te stellen en te bezien of het mogelijk is om ongeautoriseerde toegang te verkrijgen tot één specifiek kritisch systeem. De scan levert ook op welke maatregelen kunnen helpen om de beveiliging waar mogelijk te verbeteren. De kwetsbaarheidsscans zijn beperkter van aard dan een penetratietest. 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, zijn direct op een veilige manier verstuurd aan de CISO van de 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 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 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.

Risico's op het gebied van informatiebeveiliging worden niet middels een periodieke integrale risicoanalyse geïdentificeerd en gekwantificeerd in termen van kans maal impact. Een initiële analyse van bedreigingen en kwetsbaarheden op het gebied van informatiebeveiliging als start van het informatiebeveiligingsbeleid ontbreekt. Het informatiebeveiligingsbeleid beschrijft dat beheersmaatregelen worden getroffen op basis van een toets aan de BIG (baseline gap-analyse). In deze baseline gap-analyse wordt niet beschreven welke risico's de geselecteerde beheersmaatregelen afdekken. Hierdoor is niet vast te stellen of de beheersmaatregelen effectief zijn in het mitigeren van alle voor de gemeente relevante informatiebeveiligingsrisico's.

Uit interviews blijkt dat de gemeente Steenwijkerland tot voor kort geen Risico-Inventarisatie en -Evaluatie (RI&E) aanpak hanteerde, waarbij risico's worden geïdentificeerd en geclassificeerd aan de hand van een initiële dreigingsanalyse. De gemeente Steenwijkerland hanteerde de BIG-baseline als uitgangspunt voor het identificeren van informatiebeveiligingsrisico's. Hierbij worden maatregelen vertaal naar risico's in plaats van andersom.

Eind oktober/ begin november is bij de gemeente Steenwijkerland voor het eerst een risicoanalyse uitgevoerd onder begeleiding van een externe partij (BMC). Het werd als voordeel gezien dat er nu prioriteiten kunnen worden gesteld. Wel werd de kanttekening gemaakt dat veel risico's als 'gemiddeld' werden beoordeeld en dus de vraag rijst of er voldoende onderscheid is gemaakt of kan worden gemaakt tussen de verschillende (mogelijke) dreigingen.

Verder is aangegeven dat de gemeente Steenwijkerland begin 2017 een plan van aanpak heeft gemaakt voor de invoering van de AVG. De verplichte zaken zijn nu opgezet, zoals een verwerkingsregister, de aanstelling van een Functionaris Gegevensbescherming (FG) en een Privacy Officer. Uit de interviews blijkt dat onder andere het gebruik en de inhoud van verwerkingsovereenkomsten nog verder valt te verbeteren. Grote leveranciers hebben daar al over nagedacht en komen met een eigen overeenkomst. Die overeenkomst is niet altijd in het belang van de gemeente.

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

Het informatiebeveiligingsbeleid beschrijft dat de BIG als baseline wordt gehanteerd voor het selecteren van beveiligingsmaatregelen. Hiervoor wordt een baseline gap-analyse uitgevoerd door de gemeente. In deze gap-analyse wordt niet beschreven welke risico's de geselecteerde beveiligingsmaatregelen afdekken.

In de interviews is het beeld bevestigd, dat op basis van de gap-analyse op de BIG de ontbrekende maatregelen worden geïmplementeerd door de beveiligingsbeheerders. Rapportage laat duidelijk zien dat hierin voortgang wordt geboekt.

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

Door de afwezigheid van een eerdere integrale risicoanalyse, ontbreekt de samenhang tussen informatiebeveiligingsrisico's en getroffen beveiligingsmaatregelen. In het informatiebeveiligingsbeleid van de gemeente worden kaders gesteld voor de implementatie van organisatorische en technische maatregelen. Het is niet vast te stellen of deze maatregelen volledig zijn om alle voor de gemeente relevante informatiebeveiligingsrisico's af te dekken. Daarnaast is niet te beoordelen hoe de kosten van beheersmaatregelen zich verhouden tot de risico's.

Uit interviews blijkt dat tot op heden is gewerkt met maatregelen die zijn voorgeschreven vanuit de BIG en de overige (verplichte) zelfanalyses. Zoals eerder ook aangegeven is er zeer recentelijk een eerste risicoanalyse uitgevoerd, waarvan de gemeente ten tijde van de interviews het rapport nog moest ontvangen. Op basis hiervan is de gemeente in staat om voor 2019 een jaarplan op te stellen voor informatiebeveiliging wat mede is gebaseerd op geïdentificeerde risico's.

In relatie tot dit onderwerp zijn in de enquête die gehouden is onder de medewerkers van de gemeente Steenwijkerland een aantal vragen gesteld. Steenwijkerland scoort op dit onderdeel in vergelijking met de andere drie onderzochte gemeenten gemiddeld. 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	3	4%	5%
Eens	31	45%	40%
Neutraal	29	42%	48%
Oneens	6	9%	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	4%	6%
Eens	27	39%	37%
Neutraal	36	52%	51%
Oneens	3	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	4	6%	7%
Eens	33	48%	46%
Neutraal	27	39%	42%
Oneens	4	6%	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 Steenwijkerland beschikt over een actueel informatiebeveiligingsbeleid. Het huidige informatiebeveiligingsbeleid van gemeente Steenwijkerland dient als beleidskader voor informatiebeveiliging voor de periode 2017-2020.

Hiervoor was er een informatiebeveiligingsbeleid voor de periode 2015-2020. Er is bewust gekozen voor een eerdere update, omdat er op het terrein voor ontwikkelingen zijn. Het huidige beleidsplan volgt de nieuwe richtlijnen (zoals in de BIG, baseline informatiebeveiliging voor gemeenten). Door de BIG als uitgangspunt te nemen zijn richtlijnen vastgesteld die nu voor alle processen, gegevensverzamelingen en systemen gelden. Dat betekent een belangrijk verschil met de vorige beleidsperiode.

Het beleidsdocument is in 2017 geactualiseerd door de gemeente. Een andere belangrijke herijking op het informatiebeveiligingsbeleid 2015-2020 is dat in het kader van de Algemene Verordening Gegevensbescherming (AVG) nu meer focus wordt gelegd op de bescherming van persoonsgegevens. Het informatiebeveiligingsbeleid 2017-2020 is op 1 november 2017 vastgesteld door de burgemeester en wethouders van de gemeente Steenwijkerland.

Uit interviews blijkt dat in de aanloop naar 25 mei 2018 sessies zijn georganiseerd over de AVG en ook over datalekken. De gemeente heeft op haar intranetpagina een formulier geplaatst om datalekken te melden. Ten tijde van de interviews waren er in 2018 in totaal 7 datalekken gemeld. De gemeente vindt het belangrijk om een veilige ‘meldcultuur’ te hebben, zodat medewerkers niet terughoudend zijn in het melden van een (mogelijk) datalek. Enkele van de intern gemelde datalakken zijn vervolgens ook gemeld bij de Autoriteit Persoonsgegevens (AP). De AP heeft geen verder onderzoek gedaan.

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

Het informatiebeveiligingsbeleid is gebaseerd op de Baseline Informatiebeveiliging voor Gemeenten (BIG). De structuur van dit beleidsdocument volgt de hoofdstukindeling van de BIG. De uitgangspunten voor informatiebeveiliging zijn ontleend aan de “Code voor informatiebeveiliging” ISO/IEC27002:2007 norm en BIG.

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

De opzet van de PDCA-cyclus rond informatiebeveiliging is beschreven in het informatiebeveiligingsbeleid 2017-2020. De cyclus begint met de jaarlijkse herijking van het informatiebeveiligingsbeleid en het opstellen van het informatiebeveiligingsjaarplan. Uitvoering van het beleid vindt op dagelijkse basis plaats. Externe audits vinden jaarlijks plaats om de effectiviteit van beheersmaatregelen te evalueren. De uitkomsten hiervan worden gerapporteerd aan de security-board, het concern management en het college van B&W. De cyclus wordt afgerond met de uitvoering van verbeteracties op basis van de uitgevoerde audits. Dit vormt de input voor de jaarplanning voor het komende jaar.

Een jaarplan is er echter nog niet geweest. Geïnterviewden geven aan een jaarplan wel nuttig te vinden, mogelijk wordt er volgend jaar mee gestart. De recent uitgevoerde risicoanalyse is daarbij belangrijke input.

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

Het beleid wordt jaarlijks herijkt door het concernmanagement van de gemeente. Het informatiebeveiligingsbeleid 2017-2020 is in 2017 geactualiseerd en op d.d. 1 november 2017 vastgesteld door de burgemeester en wethouders van gemeente Steenwijkerland.

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

In het informatiebeveiligingsbeleid 2017-2020 wordt beschreven dat beveiligingsclassificaties worden gehanteerd voor het bepalen van beveiligingsmaatregelen. De beschermingseisen volgen uit het classificatieniveau (geen-laag-midden-hoog) dat op grond van de dataclassificatie moet worden toegekend. Er dient volgens het beleid te worden geclassificeerd op de drie kwaliteitsaspecten van informatiebeveiliging: beschikbaarheid, integriteit en vertrouwelijkheid. Het beleid geeft aan dat alle classificaties centraal worden vastgesteld door de CISO van de gemeente Steenwijkerland en jaarlijks gecontroleerd door de dataeigenaren.

Bij de bedrijfskritische applicaties is een dataclassificatiemodel van toepassing. Verder heeft de gemeente een overzicht van de gebruikte applicaties. Deze applicatielijst bevat een omschrijving, de afdeling waar de applicatie wordt gebruikt, de eigenaar van de applicatie, de functioneel beheerders en de hoofdgebruiker. Verder is aangegeven of de applicatie nuttig, handig, belangrijk of kritisch is (dit noemt men de criticaliteit). Dit is in het kader van classificatie van groot belang is. De criticaliteit van applicaties is echter niet direct herleidbaar naar formeel gedocumenteerde aanvullende maatregelen in het kader van informatiebeveiliging.

In de enquête die als onderdeel van het onderzoek is uitgezet onder de medewerkers van de gemeente Steenwijkerland, is ook een vraag gesteld over dataclassificatie. Steenwijkerland scoort hierop 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	28	41%	32%
Redelijk goed	31	45%	55%
Matig	7	10%	10%
Zeer beperkt	3	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.

De gemeente Steenwijkerland beschikt niet over een informatiebeveiligingsplan met activiteiten (inclusief urenraming en budget).

Zoals ook eerder als bevinding aangeduid heeft de gemeente Steenwijkerland eind oktober/ begin november voor de eerste maal een risicoanalyse uitgevoerd. Op basis daarvan kunnen risico's gekoppeld worden aan te nemen maatregelen. Dit wordt ten tijde van dit onderzoek in een jaarplan opgenomen. Er was in de jaren voor 2019 niet structureel geld beschikbaar voor activiteiten in het kader van informatiebeveiliging zoals bewustwording, hiervoor is vanaf 2019 wel structureel geld beschikbaar.

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

De gemeente Steenwijkerland 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:

- Procedure Autorisatie tot gemeentelijke voorziening (2015);
- Procedure Sleutel- en toegangsbeheer (2015);
- Procedure Toegangsbeleid gemeentelijke gebouwen en ruimten (2015);
- Wijzigingsbeheer (2018);
- Backup stwl (2017).

De inhoud van deze documenten wordt hierna toegelicht:

Procedure Autorisatie tot gemeentelijke voorziening 2015
In dit document wordt de procedure beschreven voor het toekennen, wijzigen en verwijderen van autorisaties in de gemeentelijke voorziening (BRP applicaties) en de GBA-V. Een belangrijke beheersmaatregel is dat autorisatieverzoeken schriftelijk ingediend worden door leidinggevenden. De verzoeken worden vervolgens beoordeeld en goedgekeurd door het afdelingshoofd OS. Hierdoor is sprake van functiescheiding. Het document beschrijft daarnaast dat toegekende autorisaties jaarlijks worden getoetst op juistheid. Ook zijn de minimale eisen voor het wachtwoordbeleid opgenomen in dit document. Deze eisen hebben betrekking op wachtwoordlengte, wachtwoordleeftijd, complexiteit, wachtwoordhistorie en lock-out.

Procedure Sleutel- en toegangsbeheer 2015
In dit document wordt de procedure beschreven voor het toekennen, wijzigen en verwijderen van toegang tot het gemeentehuis en bepaalde ruimtes in het gemeentehuis. Een belangrijke beheersmaatregel is dat autorisatieverzoeken voor toegang tot ruimtes schriftelijk ingediend worden door leidinggevenden. Toegang tot het RAAS en/of de rijbewijsmodule kan alleen aangevraagd worden door het afdelingshoofd I&O. Het document beschrijft daarnaast dat jaarlijks een controle plaatsvindt op het gebruik, uitgifte en inname van de toegangsmiddelen.

Procedure Toegangsbeleid gemeentelijke gebouwen en ruimten 2015
In dit document worden de beleidsuitgangspunten en huisregels beschreven voor de toegang tot gemeentelijke gebouwen en ruimten. Het toegangsbeleid heeft als scope de fysieke beveiliging van kantoren, ruimten en faciliteiten. De beleidsuitgangspunten zijn gebaseerd op de BIG en richten zich onder andere op het gebruik van beveiligingszones, alarmering, bewaking en periodieke controle op de autorisatie van fysieke toegang.

Wijzigingsbeheer 2018
In dit document wordt de procedure beschreven voor afhandelen van wijzigingsaanvragen. Een belangrijke beheersmaatregel is dat wijzigingsaanvragen geregistreerd worden. Vervolgens wordt de aanvraag beoordeeld op volledigheid en impact. Wijzigingen met een hoge impact worden beoordeeld en goedgekeurd door de Change Advisory Board (CAB). De resultaten van de uitgevoerde wijzigingsaanvragen worden getest en vervolgens goedgekeurd voor implementatie.

In de procedure worden beveiligingsmaatregelen niet expliciet genoemd, zoals het bepalen van de security impact van een wijzigingsaanvraag, het definiëren van security requirements, het testen van wijzigingen op security aspecten en het beveiligen van testdata. In het informatiebeveiligingsbeleid 2017-2020 worden de beleidsuitgangspunten hiervoor in grote lijnen beschreven.

Backup stwl 2015
In dit document wordt de procedure beschreven voor het maken en terugzetten (restoren) van back-ups. De gemeente Steenwijkerland maakt grotendeels gebruik van virtuele servers. Deze virtuele servers draaien op een

centrale storage met één systeem voor de gemeente Meppel en één systeem voor de gemeente Steenwijkerland. Hierdoor is sprake van realtime spiegeling, waardoor de data op beide locaties aanwezig zijn. Hierdoor is er dus een backup in de andere gemeente beschikbaar bij een calamiteit.

De procedure beschrijft dat het restoren van back-ups niet op regelmatige basis plaatsvindt. Tweemaal per jaar vindt er een uitwijktest plaats voor de Basisregistraties Adressen en Gebouwen (BAG), Basisregistratie Personen (BRP) en de volledige omgeving van gemeente Steenwijkerland. De laatste uitwijktest heeft op 12 oktober 2018 plaatsgevonden. De uitwijktest is succesvol uitgevoerd. De resultaten van de uitwijktest zijn vastgelegd in een uitwijkverslag.

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

Uit interviews blijkt dat de PDCA-cyclus in de praktijk nog niet volledig in uitvoering wordt gebracht. Zo is een jaarplan voor informatiebeveiliging niet aanwezig en zijn de interne controles op informatiebeveiliging niet uitgevoerd door de medewerkers IC.

In de gemeente functioneerde een stuurgroep informatiebeveiliging met onder andere de gemeentesecretaris en meerdere portefeuillehouders. Deze stuurgroep kwam echter niet vaak bijeen, in de praktijk één of enkele keren per jaar. Sinds het voorjaar van 2018 is er een overleg iedere twee weken als onderdeel van het portefeuillehoudersoverleg, waarbij naast de gemeentesecretaris (op een specifiek benoemd onderdeel van de agenda rond Informatiebeveiliging) ook de CISO aanwezig is. Afhankelijk van de onderwerpen die aan bod komen kunnen ook andere personen aanwezig zijn, zoals een FG of Privacy Officer.

De beveiligingsbeheerders zijn voor hun deel verantwoordelijk voor het invullen van de zelfanalyse(s) zoals Ensia, BRP, etc. Ook op individueel niveau wordt gekeken wat de verschillen waren ten opzichte van het vorige jaar. De acties die voortvloeien uit de evaluaties worden opgepakt door de beveiligingsbeheerders.

De raad wordt in de reguliere P&C-cyclus geïnformeerd door middel van kwartaalrapportages. Ieder kwartaal wordt gerapporteerd over incidenten en over de voortgang van informatiebeveiliging. Dit rapport gaat naar het CMT, naar de portefeuillehouder informatiebeveiliging (dat is de burgemeester) en naar het college. Er komt een jaarverslag als onderdeel van de reguliere planning en control cyclus, inclusief de jaarrekening, die ook naar de raad gaat.

In het jaarverslag van 2017 wordt verslag gedaan van het geactualiseerde informatiebeveiligingsbeleid, de ontwikkelingen op het gebied van privacy en bescherming van persoonsgegevens en de invoering van de eenduidige vragenlijst op dit gebied (ENSIA). In de jaarverslagen van de jaren daarvoor wordt niet specifiek ingegaan op informatiebeveiliging.

De FG's voor de vier onderzochte gemeenten bekijken nu hoe men zal omgaan met de rapportage over de uitvoering van de AVG. Dat is nu nog niet bekend. Het idee is om met jaarplannen te gaan werken voor de AVG.

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 de periode voor 2017 was er formeel geen centrale verantwoordelijke in de organisatie voor informatiebeveiliging (de CISO) en ook geen verantwoordelijke voor het toezicht op gegevensbescherming (de FG). In het informatiebeveiligingsbeleid 2017-2020 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 is integraal verantwoordelijk voor de informatiebeveiliging binnen de gemeente. Het college is verantwoordelijk voor het vaststellen van beleidskaders en normen voor informatiebeveiliging en legt verantwoording af aan de gemeenteraad;
- Het concernmanagement is verantwoordelijk voor verdere uitwerking en sturing op het vastgestelde informatiebeveiligingsbeleid;
- De Chief Information Security Officer (CISO) is verantwoordelijk voor het signaleren van informatiebeveiligingsrisico's, overall coördinatie van informatiebeveiliging, advisering, monitoring en rapportering;
- De Functionaris Gegevensbescherming (FG) is verantwoordelijk voor het toezien dat de AVG wordt nageleefd;
- De procesregisseurs zijn verantwoordelijk voor het uitvoeren, implementeren en uitdragen van het informatiebeveiligingsbeleid.

In het Advies CMT (informatie)beveiligingsorganisatie is de verdere uitwerking van de beveiligingsorganisatie opgenomen.

Bij de gemeente Steenwijkerland is sinds deze zomer een wijziging doorgevoerd, waarbij de CISO hiërarchisch niet meer in een lijnafdeling is geplaatst, maar in de concernstaf. Dit moet helpen bij de brede bewustwording voor dit onderwerp.

Sinds 1 juli 2018 beschikt de gemeente Steenwijkerland over een FG, die verantwoordelijk is voor toezicht op naleving van de AVG. De FG heeft daarnaast een adviserende rol. De FG heeft wekelijks overleg met de CISO en Privacy Officer van de gemeente. Ook de FG is geplaatst in de concernstaf.

Vanaf 2017 werd er gewerkt met een stuurgroep informatiebeveiliging met daarin een vertegenwoordiging vanuit het college, de gemeentesecretaris, de CISO en de FG. Dit overleg kwam echter niet vaak en onregelmatig bijeen. Vanaf het voorjaar van 2018 is de burgemeester portefeuillehouder informatiebeveiliging en heeft hij dit onderwerp iedere twee weken geagendeerd in zijn stafoverleg met de gemeentesecretaris, de CISO en indien nodig andere betrokkenen.

De rollen zijn daarmee duidelijk belegd binnen de organisatie.

In de enquête die PwC heeft uitgezet onder de medewerkers van Steenwijkerland zijn twee vragen gesteld met betrekking tot dit onderwerp. De gemeente wijkt weinig af van de andere drie gemeenten in dit onderzoek.

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	13	19%	24%
Redelijk goed	36	52%	44%
Matig	14	20%	21%
Zeer beperkt	6	9%	7%
Helemaal niet	0	0%	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	13	19%	25%
Eens	38	55%	51%
Neutraal	7	10%	13%
Oneens	7	10%	8%
Helemaal oneens	1	1%	1%

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

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

In het informatiebeveiligingsbeleid 2017-2020 wordt beschreven dat het college van B&W-verantwoording aflegt over informatiebeveiliging aan de gemeenteraad middels een collegeverklaring in het jaarverslag.

Het college wordt ieder kwartaal geïnformeerd omtrent informatiebeveiliging door middel van een rapportage. Daar is de gemeente dit jaar mee gestart. Het eerste rapport is daadwerkelijk besproken in het college, zodat daar de bewustwording werd vergroot. Het rapport zal niet per definitie ieder kwartaal besproken worden in het college, maar het college zal wel ieder kwartaal, of bij incidenten, door de burgemeester schriftelijk geïnformeerd blijven.

Verder is op 2 oktober 2018 de kwartaalrapportage besproken met de raad tijdens een bredere avond over informatiebeveiliging, waarbij gelegenheid was voor discussie. Ook de AVG is daar aan bod gekomen.

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.

In het informatiebeveiligingsbeleid 2017-2020 wordt beschreven dat het concernmanagementteam duidelijk richting geeft aan informatiebeveiliging en in houding en gedrag betrokkenheid laat zien door het uitbrengen en handhaven van het beleid. Het informatiebeveiligingsbeleid is op d.d. 1 november 2017 vastgesteld door de burgemeester en wethouders van gemeente Steenwijkerland. In september en oktober 2017 hebben security awareness sessies plaatsgevonden bij de gemeente.

Meerdere geïnterviewden geven aan dat het gevoel is dat informatiebeveiliging door het management niet gezien wordt als een belangrijke pijler voor het functioneren van de gemeente. Geïnterviewden geven aan dat gerichte actie nodig zal zijn, bijvoorbeeld in de vorm van training en instructie van het management. Wel is aangegeven dat al langer een proces van organisatieontwikkeling gaande is, wat mogelijk bij medewerkers nog niet goed is gevallen.

De gemeente Steenwijkerland onderkent dat het uitdragen van informatiebeveiliging door het management een serieus aandachtspunt is. In het najaar van 2018 zal een crisissimulatie uitgevoerd worden, waarbij het bestuur in een rollenspel uitgedaagd wordt om effectief te handelen tijdens een cyberaanval. Dit moet bijdragen aan het verhogen van bewustwording rondom informatiebeveiliging bij het management.

In de enquête die is gehouden onder de medewerkers van de gemeente Steenwijkerland is een stelling opgenomen over de betrokkenheid van het management bij informatiebeveiliging. Daarop scoort Steenwijkerland minder goed dan 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	2	3%	6%
Eens	18	26%	32%
Neutraal	28	41%	46%
Oneens	17	25%	13%
Helemaal oneens	4	6%	3%

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

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

De gemeente Steenwijkerland heeft op 20 juni 2017 een mystery guest onderzoek in het gemeentehuis laten uitvoeren door een onafhankelijk onderzoeksbureau. Het doel van dit onderzoek was om kwetsbaarheden te identificeren in de fysieke toegangsbeveiliging. Tijdens het onderzoek zijn meerdere kwetsbaarheden geïdentificeerd. Uit het onderzoek blijkt onder meer dat:

- Onbevoegden zonder begeleiding en toezicht kunnen rondlopen in de beveiligde zone van het gemeentehuis;
- Tijdens het zoeken naar vertrouwelijke informatie op meerdere bureaus veelvuldig dossiers zijn gevonden;
- Speciale bedrijfskleding toegankelijk is;
- ICT-hulpmiddelen onbeheerd worden achtergelaten.

Door meerdere geïnterviewden is aangegeven dat er twijfels zijn of medewerkers van de gemeente zich voldoende bewust zijn van informatiebeveiligingsrisico's. Als oorzaak voor de kwetsbaarheid van fysieke toegang wordt er met name op gewezen dat medewerkers onbekenden toelaten en niet voorzichtig met (gevoelige) informatie omgaan. Medewerkers vinden het mogelijk lastig om anderen aan te spreken. Ook wordt de bezoekerspas vaak niet uitgegeven. Deels moet men zich bewust worden, maar de andere kant is dat bezoekerspassen uitgedeeld moeten worden, zichtbaar moeten worden gedragen en voor de toekomst dat er herkenbare medewerkerspassen komen.

In het najaar van 2017 hebben security awareness sessies plaatsgevonden bij de gemeente. In de evaluatierapportage van deze sessies wordt benoemd dat medewerkers vaak aangeven niet te weten bij wie ze een beveiligingsincident moeten melden. De CISO is niet bekend bij iedereen. Daarnaast wordt benoemd dat er behoefte is om gebruikers vaker te informeren over informatiebeveiliging middels periodieke teammeetings, intranet, posters en mailings. Opgemerkt dient te worden dat kort na deze sessies het informatiebeveiligingsbeleid is vastgesteld, waarin deze vragen worden beantwoord. Uit onze vragenlijst die we tijdens dit onderzoek hebben gehouden (zie hieronder) komt een positiever beeld naar voren.

In de laatste weken van 2017 en de eerste weken van 2018 heeft de gemeente Steenwijkerland een social engineering onderzoek laten uitvoeren door een onafhankelijk onderzoeksbureau. Het doel van dit onderzoek was het vaststellen in hoeverre medewerkers hun medewerking verlenen in het overhandigen van (privacy-) gevoelige informatie. De scope van dit onderzoek was beperkt tot het Bestuurssecretariaat en het Klant Contact

Center. De belangrijkste conclusie van het onderzoek is dat tijdens de uitgevoerde social engineering activiteiten geen gevoelige (persoons-) gegevens zijn verkregen.

Op de dag voor de interviews is een clean-desk actie gehouden, waarbij 's avonds is gecontroleerd of medewerkers hun bureau opgeruimd hebben achtergelaten. Bij de eerste actie in juni waren ongeveer 50 bureaus in orde, bij deze tweede actie waren 150 bureaus in orde. De mensen van wie het bureau 'clean' was ontvingen daarbij een chocoladeletter.

In de enquête die als onderdeel van dit onderzoek is uitgezet onder de medewerkers van de gemeente Steenwijkerland zijn een aantal vragen gesteld met betrekking tot dit onderwerp. 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 67 cijfers): **6,8**

In vergelijking met de andere gemeenten vinden medewerkers van Steenwijkerland dat ze beter op de hoogte zijn van het informatiebeveiligingsbeleid en weten ze ook vaker wat er van hen verwacht wordt op dit gebied. Men weet meer dan gemiddeld in de vier onderzochte gemeenten wat een datalek is en wat er gedaan moet worden als er een datalek geconstateerd wordt. Onderstaand zijn de resultaten weergegeven.

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	4	6%	8%
Redelijk goed	42	61%	47%
Matig	14	20%	31%
Zeer beperkt	9	13%	10%
Helemaal niet	0	0%	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	9	13%	13%
Redelijk goed	46	67%	58%
Matig	9	13%	20%
Zeer beperkt	2	3%	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	47	68%	50%
Matig	11	16%	24%
Zeer beperkt	1	1%	6%
Helemaal niet	1	1%	7%

U wordt regelmatig en goed geïnformeerd over informatiebeveiliging:

Keuze:	Aantal antwoorden:	Percentage:	Percentage gemiddelde van de vier onderzochte gemeenten:
Helemaal eens	6	9%	8%
Eens	27	39%	38%

Neutraal	23	33%	36%
Oneens	10	14%	17%
Helemaal oneens	2	3%	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	9	13%	17%
Eens	41	59%	51%
Neutraal	10	14%	18%
Oneens	8	12%	12%
Helemaal oneens	0	0%	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	12%	17%
Eens	40	58%	51%
Neutraal	14	20%	23%
Oneens	4	6%	6%
Helemaal oneens	1	1%	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 heeft een overzicht van applicaties en het doel ervan, gekoppeld aan onder meer de eigenaar en de beheerders van de applicatie. Ook is de criticaliteit van de applicaties bepaald op basis van Beschikbaarheid, Integriteit en Vertrouwelijkheid.

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

De gemeente Steenwijkerland heeft in de periode van 12 september 2016 tot en met 14 september 2016 een penetratietest op het interne en externe netwerk laten uitvoeren door een onafhankelijk onderzoeksbureau. Het doel van deze scan was het identificeren van kwetsbaarheden in de beveiliging van het interne en externe netwerk van de gemeente.

Op basis van de uitkomsten van de kwetsbaarheidsscan wordt het beveiligingsniveau van de gemeente Steenwijkerland door het externe onderzoeksbureau geclassificeerd als ‘zeer onveilig’. Tijdens het onderzoek zijn meerdere kwetsbaarheden geïdentificeerd met een “midden”, “hoog” en “kritisch” beveiligingsrisico. De belangrijkste kwetsbaarheden hebben onder andere betrekking op het ontbreken van up-to-date patches,

het gebruik van verouderde software, het gebruik van zwakke wachtwoorden en zwakke systeemconfiguratie. Naar aanleiding van deze test zijn maatregelen getroffen om deze beveiligingsrisico's te mitigeren.

De gemeente Steenwijkerland beschikt over een Collegeverklaring ENSIA 2017 inzake Informatiebeveiliging van DigiD en Suwinet. In deze Collegeverklaring wordt beschreven dat op 31 december 2017 is vastgesteld dat beveiligingsmaatregelen in opzet en bestaan voldoen aan de geselecteerde normen inzake DigiD en Suwinet. Er zijn tijdens de audit wel enkele uitzonderingen aangetroffen. De opvolging hiervan zijn volgens de collegeverklaring opgenomen in verbeterplannen.

Als onderdeel van het Rekenkameronderzoek Informatiebeveiliging heeft PwC bij Steenwijkerland een kwetsbaarheidsscan uitgevoerd. Het doel van dit onderzoek is om inzicht te verschaffen in de veiligheid van het interne netwerk van de gemeente en mogelijke verbeterpunten te identificeren. Hieronder volgen de resultaten van dat onderzoek:

Ongeautoriseerde toegang mogelijk tot persoonsgegevens van inwoners
De systemen waarop wij hebben gescand missen (belangrijke) beveiligingsupdates. Dit is een veel voorkomend soort kwetsbaarheid bij veel organisaties, veroorzaakt doordat systemen niet voldoende of niet regelmatig worden bijgewerkt. Het niet voldoende bijwerken/updaten van systemen brengt als risico met zich mee dat een aanvaller zich ongeautoriseerd toegang kan verschaffen tot de systemen, door gebruik te maken van een kwetsbaarheid waarvoor nog geen update is geïnstalleerd.

Missende kritieke updates maken gemeente Steenwijkerland kwetsbaar voor ransomware aanvallen
Uit onze werkzaamheden bleek dat zeven systemen op het netwerk van gemeente Steenwijkerland 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.

Naast de missende kritieke beveiligingsupdates hebben wij vastgesteld dat er diverse minder kritieke, maar desalniettemin belangrijke updates niet zijn toegepast op de systemen van gemeente Steenwijkerland. Dit leidt tot een lager risico als eerder geschetst in deze paragraaf. Deze missende updates zouden namelijk alleen een zeer bekwame aanvaller, onder bepaalde omstandigheden, in staat kunnen stellen volledige administratieve controle te verkrijgen op het interne netwerk.

Het periodiek en meer rigoureus toepassen van een updatecyclus (het zogenaamde patch management) zou deze kwetsbaarheden aanzienlijk terugdringen. Aan de hand van de bevindingen van de kwetsbaarheidsscan heeft de ambtelijke organisatie aangegeven dat de noodzakelijke maatregelen zijn getroffen.

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 een nog niet volledige dataclassificatie (nu alleen voor de bedrijfskritische applicaties), 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.

Applicatieonderzoeken

In het kader van deze norm zijn bij de gemeente Steenwijkerland vier applicaties onderzocht, te weten Green Valley, Key2Belastingen, Wmo-Ned en Key2Burgerzaken. 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.

Green Valley: Er is een vastomlijnd proces voor het aanvragen, wijzigen en verwijderen van autorisaties. Accounts worden niet verwijderd als autorisaties worden ingetrokken. Dit zorgt dat de audittrail (wie heeft wat gedaan) bewaard blijft.

Key2Belastingen: Er is een vastomlijnd proces voor het aanvragen, wijzigen en verwijderen van autorisaties. Accounts worden niet verwijderd als een medewerker uit dienst gaat. De accounts worden uitgeschakeld/op inactief gezet maar niet verwijderd, zodat de audit-trail beschikbaar blijft.

Wmo-Ned: Er is een vastomlijnd proces voor het aanvragen, wijzigen en verwijderen van autorisaties. Een standaard periodieke controle op autorisaties wordt niet uitgevoerd. De beheerders hebben de fysieke werkplek midden tussen de medewerkers die gebruik maken van de applicatie. Op die manier is er zicht op de medewerkers die toegang nodig hebben of niet (als iemand uitdienst treedt).

Key2Burgerzaken: Ook hier is een vastomlijnd proces voor het aanvragen, wijzigen en verwijderen van autorisaties. Voor Key2Burgerzaken wordt één of tweemaal per jaar gecontroleerd op de autorisaties.

- *Beschikbaarheid*

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

Green Valley is een SaaS oplossing, het draait 'in de cloud'. De leverancier belooft een uptime van 99,5%. In het verleden waren er problemen met de capaciteit van de applicatie, maar dit is tegenwoordig verholpen.

Key2Belastingen, Wmo-Ned en Key2Burgerzaken: de data die in Steenwijk staat, is ook altijd aanwezig in Meppel. Van de virtuele servers wordt elke nacht een back-up gemaakt naar disk op de locatie Meppel. Het is mogelijk om individuele bestanden, mailboxen en databases te restoren. De back-ups zijn 14 dagen direct beschikbaar. Een keer per week worden de back-ups naar tape, deze worden 6 weken bewaard.

- *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.

Green Valley: wijzigingen en versiebeheer worden bijgehouden in TOPdesk (een helpdesk applicatie). Nieuwe versies van de applicatie worden eerst klaargezet in een Testomgeving. Pas na akkoord van de gemeente worden wijzigingen doorgezet naar Productie.

Key2Belastingen: Wijzigingen in de applicatie worden eerst getest in een testomgeving. Wanneer de wijzigingen succesvol worden getest in de testomgeving worden ze doorgezet naar de productieomgeving. Een historie van configuraties en geïnstalleerde versies wordt bijgehouden in de applicatie zelf.

Wmo-Ned: Naast de Productieomgeving is er voor Wmo-Ned ook een Testomgeving. Nieuwe updates worden door de leverancier geïmplementeerd in de testomgeving. Enkele gebruikers testen vervolgens eerst de update.

Key2Burgerzaken: De leverancier test nieuwe versies en wijzigingen allereerst in de testomgeving van de gemeente Steenwijkerland. De gemeente volgt vervolgens het testprotocol om de nieuwe versie op een aantal punten te controleren.

- *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.

Green Valley: De testomgeving staat op zichzelf en bevat geen data vanuit Productie. Verder kunnen alleen bepaalde gebruikers rapportages draaien. De rapportages kunnen als Excel sheet worden geëxporteerd uit de applicatie en bevatten dan eventueel zaaknummers en persoonsgegevens.

Key2Belastingen: De testomgeving bevat een kopie van de database van Productie.

Wmo-Ned: Periodiek wordt de database van de productiekant van de omgeving gekopieerd naar de testomgeving. De testomgeving wordt op dezelfde server uitgevoerd als de productieomgeving.
Er zijn twee gebruikersaccounts met toegang tot de testomgeving. Medewerkers met toegang tot de productieomgeving kunnen hebben dus in principe geen toegang tot de testomgeving.

Key2Burgerzaken: De productiedatabase wordt gekopieerd naar de testomgeving en wordt dus gebruikt in de testomgeving. Tests worden uitgevoerd door medewerkers burgerzaken en de functioneel beheerder.

- *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.

Green Valley: Vanaf het moment dat een 'Zaak' geopend wordt, wordt daar logging van bijgehouden. De logging is minstens net zo lang beschikbaar als dat de zaak openblijft. Als een zaak wordt vernietigd dan is hoogstwaarschijnlijk de logging ook weg. Het raadplegen van een zaak wordt niet gelogd, het wijzigen van gegevens in een zaak wel. De gemeente Steenwijkerland voert geen standaard periodieke checks of rapportages uit op de logging.

Key2Belastingen: De applicatie Key2Belastingen logt wel een aantal zaken, maar dat is zeer beperkt in inhoud. Wat in te stellen is aan logging is onduidelijk. De logging die beschikbaar is gaat wel terug tot aan de ingebruikname van de applicatie.

Wmo-Ned: De applicatie logt logins van gebruikers, zowel succesvolle als foutieve logins. Ook wordt gelogd wanneer een medewerker informatie probeert te raadplegen waartoe hij/zij geen toegang heeft. Ook activiteiten van beheerders en beheerstaken worden gelogd. Tenslotte logt de applicatie ook foutmeldingen, indien die zich voordoen. Er kan tot 9 maanden terug in de tijd in de logging gekeken worden.

Key2Burgerzaken: Iedere wijziging en raadpleging op de BRP wordt bijgehouden door de applicatie. Het inloggen en uitloggen van accounts wordt door de applicatie niet gelogd, wel is voor beheerders te zien op welk moment een gebruiker voor het laatst ingelogd is geweest.

- *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.

Green Valley: In het contract tussen de gemeente en de leverancier is afgesproken welke procedures er zijn voor toegang van de leverancier tot de omgeving van de gemeente. Ook in de verwerkersovereenkomst zijn afspraken vastgelegd. Bij een eventuele opvolger van deze applicatie neemt de gemeente de GIBIT-voorwaarden over.

Key2Belastingen: De leverancier krijgt enkel toegang tot het systeem wanneer nodig. Er is geen standaard toegang tot de applicatie voor de leverancier. Door tussenkomst van een beheerder van de gemeente krijgt de leverancier toegang tot de omgeving, waarbij door de beheerder wordt meegekeken in de sessie.

De contracten met de leverancier waren recentelijk inmiddels 18 jaar oud. Daarom is het voornemen ze in 2019/2020 nogmaals onder de loep te nemen.

Wmo-Ned: Binnen de overeenkomst met de leverancier is geregeld hoe met escalaties en aansprakelijkheid wordt omgegaan. Jaarlijkse standaard rapportages over het naleven van afspraken zijn er niet. Indien gewenst verstrekt de leverancier op aanvraag de uitkomsten van audits.

Key2Burgerzaken: In contractuele afspraken is vastgelegd hoe de leverancier moet reageren op incidenten en problemen. De gemeente Steenwijkerland heeft nooit de behoefte gehad om de contractuele afspraken na te kijken en af te dwingen, omdat de leverancier altijd tijdig heeft gereageerd.

- *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.

Green Valley: Toegang tot de applicatie wordt alleen ontsloten vanuit het netwerk van de gemeente. Wanneer te vaak een verkeerd wachtwoord wordt ingegeven wordt het account geblokkeerd. Het account moet vervolgens handmatig worden vrijgegeven. Een gebruiker moet periodiek het wachtwoord wijzigen.

Key2Belastingen: Gebruikers hebben een wachtwoord nodig om in te loggen op de applicatie. Dit wachtwoord staat los van het wachtwoord dat een gebruiker nodig heeft om in te loggen op zijn werkplek / de netwerkomgeving. Complexiteitseisen voor het wachtwoord zijn tijdens het onderzoek (eind november 2018) geïmplementeerd.

Wmo-Ned: Authenticatie voor deze applicatie geschiedt op basis van zogenaamde Single-Sign-On (SSO). Dat betekent dat een gebruiker automatisch wordt ingelogd (er wordt niet om een gebruikersnaam en wachtwoord gevraagd). Dit geldt overigens alleen voor gebruikers die door Functioneel Beheer zijn toegevoegd aan de applicatie. Een medewerker van de gemeente kan dus niet zomaar inloggen.

Key2Burgerzaken: Toegang tot de applicatie wordt verschaft door middel van gebruikersnaam en wachtwoord. Er is geen sprake van Single-Sign-On (SSO).

Voor alle applicaties geldt: Vanaf een externe (thuis)werkplek dient een gebruiker eerst via 2-factor authenticatie in te loggen op de virtuele werkplekomgeving. Data die eventueel geëxporteerd kan worden uit de omgeving kan niet op de thuis-pc opgeslagen worden, maar kan enkel in de werkplekomgeving van de gemeente worden opgeslagen.

A. Applicatieonderzoeken

A.1. Green Valley Zaaksysteem

Autorisatiebeheer
De aanvraag voor een nieuw account begint bij de teamleider, die via de servicedesk een aanvraag indient tot toegang. Via het ticketing systeem TOPdesk komt dat terecht bij Technisch Beheer.
De uitdienstprocedure verloopt via hetzelfde mechanisme. Via P&O en TOPdesk komt de uitdienstmelding bij Technisch Beheer terecht. Het account wordt in dit geval niet verwijderd, maar de rechten worden verwijderd en het account wordt uitgeschakeld.
Ook bij het wijzigen van functie komt de melding bij Technisch Beheer via TOPdesk, waarop de rechten van het betreffende account worden aangepast.

Accounts die worden aangemaakt in de applicatie zelf hebben geen standaard einddatum. P&O is hierin leidend. Wanneer een medewerker een contract heeft voor bepaalde tijd, dan loopt het account af in PIMS. Op dat moment heeft het netwerkaccount van de medewerker een einddatum. Bij het verstrijken van de einddatum wordt het netwerkaccount van de medewerker uitgeschakeld en parallel wordt via TOPdesk een melding verstuurd richting Technisch Beheer.

In iManager worden de accounts die kunnen inloggen in Green Valley eenmaal per kwartaal vergeleken met de netwerkaccounts.

Er is een scheiding aangebracht in een aantal rollen binnen de applicatie. In de basis is er een Behandelaarsrol en een Gebruikersrol. Daarnaast zijn nog een aantal rollen gedefinieerd, specifiek voor bepaalde functies. Beheerdersaccounts zijn hierbij gescheiden van gebruikersaccounts.

Beschikbaarheid
De Green Valley applicatie is een cloud applicatie. De leverancier is verantwoordelijk voor beschikbaarheid en belooft een uptime van 99,5%.

In het verleden waren er problemen met de capaciteit van de applicatie, omdat de omgeving werd gedeeld met andere gemeenten. De leverancier heeft dit opgelost, waarschijnlijk door de capaciteit te verhogen.

Change Management
Changes worden bijgehouden in de applicatie TOPdesk, net als het versiebeheer.

De leverancier zet nieuwe updates en nieuwe wijzigingen allereerst klaar in een Testomgeving. Pas na akkoord van de gemeente worden een nieuwe update of wijzigingen doorgezet naar de Productieomgeving. Dit was een eis van de gemeente.

Wanneer een nieuwe of gewijzigde versie problemen geeft is er niet de mogelijkheid om terug te rollen. Als de leverancier na de test de nieuwe versie eenmaal heeft doorgezet, dan is er een commitment om door te gaan met die nieuwe versie. Eventuele problemen moeten dan zo spoedig mogelijk door de leverancier worden opgelost.

Databeveiligingsincidenten
De testomgeving is een op zichzelf staande omgeving. De data in de testomgeving is geen kopie van de data in de productieomgeving.

Een gebruiker is in staat op een rapport te draaien. Overigens kunnen niet alle gebruikers dit, alleen de gebruikers met de benodigde rechten. De rapportages kunnen als een Excel sheet wordt geëxporteerd uit de applicatie. Een rapport bevat onder andere zaaknummers en persoonsgegevens.

AVG – Logging en monitoring

Vanaf het moment dat een 'Zaak' geopend wordt, wordt daar logging van bijgehouden. De logging is minstens net zo lang beschikbaar als dat de zaak openblijft. Als een zaak wordt vernietigd dan is hoogstwaarschijnlijk de logging ook weg.

De functioneel beheerder kan in iManager zien wanneer een gebruiker voor het laatst heeft ingelogd. Het raadplegen van een zaak wordt niet gelogd, het wijzigen van gegevens in een zaak wel. Handelingen die een beheerder uitvoert in iManager, zoals het aanmaken van een nieuw account, wordt waarschijnlijk niet gelogd.

De gemeente Steenwijkerland heeft geen periodieke checks of rapportages rondom de logging.

Leveranciersmanagement
In het contract tussen de gemeente en de leverancier is afgesproken welke procedures er zijn voor toegang van de leverancier tot de omgeving van de gemeente. Ook in de verwerkersovereenkomst zijn afspraken vastgelegd. Bij een eventuele opvolger van deze applicatie neemt de gemeente de GIBIT-voorwaarden over.

Logische toegangsbeveiliging
Toegang tot de applicatie wordt ontsloten vanuit het netwerk van de gemeente. Een medewerker die vanuit huis werkt moet eerst een Citrix sessie opzetten bij de gemeente, om bij de applicatie te kunnen. Toegang tot de applicatie is normaliter door middel van gebruikersnaam en wachtwoord. Voor de citrix sessie is er 2 factor authenticatie. Overigens heeft niet iedere medewerker de mogelijkheid om vanuit huis te werken.

Wanneer te vaak een verkeerd wachtwoord wordt ingegeven wordt het account geblokkeerd. Het account moet vervolgens handmatig worden vrijgegeven. Een gebruiker moet periodiek het wachtwoord wijzigen.

De applicatie is alleen toegankelijk vanuit de gemeente over het gemnet netwerk en de gegevens worden versleuteld uitgewisseld.

A.2. Key2Belastingen

Autorisatiebeheer
De applicatie Key2Belastingen heeft een eigen authenticatiesysteem, los van het netwerk. Account die door de beheerder worden aangemaakt hebben een geldigheid voor onbepaalde tijd. Wanneer een medewerker uit dienst gaat wordt het account uitgeschakeld/op inactief gezet, zodat de audit-trail beschikbaar blijft.

Wanneer er een nieuw account aangemaakt moet worden, geeft de teamleider belastingen aan dat er een nieuwe medewerker is, met een indicatie van de rol die de persoon gaat vervullen. De beheerder maakt het account aan en geeft het de rechten die passen bij de functie.

Ten behoeve van het vervullen van verschillende functies zijn er verschillende rollen aangemaakt, waaronder belastingen heffen, belastingen innen en een rol voor de WOZ. Enkele selecte medewerkers hebben de beheerdersrol.

Beschikbaarheid
Om beschikbaarheid te kunnen garanderen kan er een uitwijk naar de gemeente Meppel plaatsvinden, als het datacenter van de gemeente Steenwijkerland onbeschikbaar zou zijn geworden. Jaarlijks wordt er een in- en uitwijktest uitgevoerd om te controleren of de uitwijkmogelijkheid werkt. De backupvoorzieningen worden geregeld door de afdeling Technisch Beheer.

Change management
Wijzigingen in de applicatie worden eerst getest in een testomgeving. Wanneer de wijzigingen succesvol worden getest in de testomgeving worden ze doorgezet naar de productieomgeving.

Een historie van configuraties en geïnstalleerde versies wordt bijgehouden in de applicatie zelf.

Databeveiligingsincidenten
Ten behoeve van de testomgeving wordt gebruik gemaakt van een kopie van de database van de productieomgeving.

Een gebruiker die vanuit huis werkt dient eerst in te loggen op de Citrix omgeving van de gemeente Steenwijkerland. Wanneer deze sessie is opgezet is het niet mogelijk om lokale bronnen te gebruiken, zoals een harde schijf of een verwisselbaar medium (usb stick).

AVG – Logging en Monitoring
De applicatie Key2Belastingen logt wel een aantal zaken, maar dat is zeer beperkt in inhoud. Wat in te stellen is aan logging is onduidelijk. De logging die beschikbaar is gaat wel terug tot aan de ingebruikname van de applicatie.

Leveranciersmanagement
De leverancier krijgt geen toegang zonder tussenkomst van de gemeente. Er is geen standaard toegang tot de applicatie voor de leverancier. Door tussenkomst van een beheerder van de gemeente krijgt de leverancier toegang tot de omgeving, waarbij door de beheerder wordt meegekeken in de sessie.

De contracten met de leverancier waren recentelijk inmiddels 18 jaar oud. Daarom worden ze in 2019/2020 nogmaals onder de loep genomen.

Welke specifieke afspraken er zijn gemaakt met de leverancier is niet bekend bij de geïnterviewde persoon.

Logische toegangsbeveiliging
Gebruikers hebben een wachtwoord nodig om in te loggen op de applicatie. Dit wachtwoord staat los van het wachtwoord dat een gebruiker nodig heeft om in te loggen op zijn werkplek / de netwerkomgeving. Complexiteitseisen voor het wachtwoord worden op korte termijn geïmplementeerd.

Wanneer een gebruiker te vaak een verkeerd wachtwoord opgeeft wordt het account vergrendeld. Deze moet dan weer door een beheerder worden vrijgegeven.

Als een nieuw account wordt verstrekt aan een medewerker dan heeft dit account een door beheer ingesteld wachtwoord. Aan de medewerker wordt verzocht om het wachtwoord direct aan te passen.

Actieve gebruikerssessies kunnen niet afgesloten worden door functioneel beheer, maar wel door technisch beheer.

De sessie van een gebruiker in de applicatie verloopt via een versleutelde verbinding, waardoor het uitlezen van het netwerkverkeer niet mogelijk is.

A.3. Wmo-Ned

Autorisatiebeheer
Medewerkers die in dienst komen moeten expliciet door de beheerder toegang worden gegeven in Wmo-Ned. De beheerder maakt een account aan in de applicatie. Authenticatie is verder Single-Sign-On (SSO), wat betekent dat een gebruiker niet nog eens expliciet hoeft in te loggen op de applicatie. Als de rechten zijn toegekend, dan kan de gebruiker er automatisch in. Een gebruiker die geen rechten heeft kan uiteraard niet in de applicatie komen.

Bij indiensttreding van een nieuwe medewerker doet de betreffende teamleider een aanvraag bij ICT voor toegang tot bepaalde applicaties. Per e-mail wordt dit verzoek doorgezet naar de beheerders van Wmo-Ned. Bij uitdiensttreding wordt een gebruikersaccount geblokkeerd. Het is niet mogelijk om bij het aanmaken van een account (alvast) een einddatum op te geven waarop het account verloopt.

Een aantal rollen zijn gedefinieerd binnen de applicatie, waaronder (maar niet beperkt tot) Consulenten, Systeembeheer, Functioneel Beheer, Interne Controle en Backoffice medewerkers. Een gebruikersaccount wat wordt aangemaakt krijgt een van deze rollen toebedeeld. Hieruit blijkt dat er onderscheid is gemaakt tussen rollen met beheertaken en gebruikstaken.

Een standaard periodieke controle op autorisaties wordt niet uitgevoerd. De beheerders hebben de fysieke werkplek midden tussen de medewerkers die gebruik maken van de applicatie. Op die manier is er zicht op de medewerkers die toegang nodig hebben of niet (als iemand uitdienst treedt).

Beschikbaarheid
Vanuit ICT zijn er in- en uitwijkplannen en dit wordt jaarlijks getest.

Bijna alle servers, inclusief de file servers, zijn virtuele servers die gebruik maken van centrale storage. Deze storage bestaat uit 2 systemen, 1 in Steenwijk en 1 in Meppel die realtime worden gespiegeld, dus de data die in Steenwijk staat, is ook altijd aanwezig in Meppel. Van de virtuele servers wordt elke nacht een (incremental) back-up gemaakt naar disk op de locatie Meppel indien er een full back-up aanwezig is. Het mogelijk om individuele bestanden, mailboxen en databases te restoren. De back-ups zijn 14 dagen beschikbaar op disk en daarna samengevoegd met de full back-up. Een keer per week worden de back-ups naar tape geschreven via data-protector, deze worden 6 weken bewaard.

Change management
Naast de Productieomgeving is er voor Wmo-Ned ook een Testomgeving. Nieuwe updates worden door de leverancier geïmplementeerd in de testomgeving. Enkele gebruikers testen vervolgens eerst de update. Wanneer er geen problemen worden geconstateerd wordt de update geïnstalleerd in de Productieomgeving.

Een historie van releases wordt bijgehouden, inclusief wijzigingsdocumenten. Een historie van configuraties van de applicatie wordt niet bijgehouden.

Risico op databeveiligingsincidenten
De informatie die in de applicatie beschikbaar is kan niet door gebruikers worden geëxporteerd. Daarnaast is het nog zo dat wanneer een medewerker vanuit huis inlogt, lokale bronnen van de thuis-pc niet beschikbaar zijn en daar geen informatie mee kan worden uitgewisseld vanuit de werkomgeving van de gemeente.

Er zijn twee gebruikersaccounts met toegang tot de testomgeving. Medewerkers met toegang tot de productieomgeving kunnen hebben dus in principe geen toegang tot de testomgeving.

Periodiek wordt de database van de productiekant van de omgeving gekopieerd naar de testomgeving. De testomgeving wordt op dezelfde server uitgevoerd als de productieomgeving.

AVG – Logging en monitoring
De applicatie logt logins van gebruikers, zowel succesvolle als foutieve logins. Ook wordt gelogd wanneer een medewerker informatie probeert te raadplegen waartoe hij/zij geen toegang heeft. Ook activiteiten van beheerders en beheerstaken worden gelogd. Tenslotte logt de applicatie ook foutmeldingen, indien die zich voordoen.

De applicatie logt in bestanden van vaste grootte en houdt daarbij 1 actueel bestand aan en vier archiefbestanden. Wanneer het actuele bestand vol is, wordt het principe van roteren toegepast. Dat betekent dat het oudste bestand wordt verwijderd, het actuele bestand wordt het nieuwste archiefbestand en de applicatie logt door in een nieuw actueel bestand. Op deze manier kan tot 9 maanden terug in de logging worden gekeken.

De logginginstellingen liggen vast in de applicatie en zijn niet door functioneel beheerders aan te passen.

De gemeente voert geen standaard periodieke controles uit op de logging van Wmo-Ned.

Leveranciersmanagement
Binnen de overeenkomst met de leverancier is geregeld hoe met escalaties en aansprakelijkheid wordt omgegaan.

Jaarlijkse standaard rapportages over het naleven van afspraken zijn er niet. Indien gewenst verstrekt de leverancier op aanvraag de uitkomsten van audits.

De leverancier heeft geen standaard toegang tot de applicatie. Als de leverancier toegang tot de applicatie nodig heeft dan gebeurt dat altijd door tussenkomst van een medewerker van de gemeente.

Logische toegangsbeveiliging
Toegang tot de applicatie verloopt via SSO, maar de gebruiker moet zich op zijn werkplek aanmelden met een gebruikersnaam en wachtwoord en van buitenaf via 2-factor authenticatie. Alle gebruikers in de gemeente Steenwijkerland moet hun netwerkwachtwoord periodiek wijzigen.

Op het moment dat een gebruiker inlogt in de applicatie dan ziet hij/zij in beeld staan wat het vorige moment van inloggen was.

De leverancier heeft geen account met een standaard wachtwoord en kan niet zonder tussenkomst van de gemeente op afstand bij de applicatie. Dat verloopt door tussenkomst van een medewerker van de gemeente.

De applicatie wordt benaderd via een browser en de verbinding is versleuteld (https).

A.4. Key2Burgerzaken

Autorisatiebeheer
Wanneer een medewerker in dienst komt, dan vindt er eerst een technische handeling plaats. Er wordt een Windows account gemaakt en de teamleider doet een verzoek tot toegang tot (oa) Burgerzaken. Vanuit TOPdesk komt dan een verzoek om toegang tot Burgerzaken voor een account.

Vanuit Umra wordt ook aangegeven dat een autorisatieformulier moet worden getekend (handtekening van medewerker, teamleider, privacybeheerder, en nog een vierder persoon). Zonder getekend document wordt het account niet aangemaakt.

Als onderdeel van het overdragen van een account aan de gebruiker moeten ze bij de beheerder komen en in de applicatie ter plekke zelf een nieuw wachtwoord instellen. Een account blijft gedisabled totdat de persoon een afspraak heeft met de functioneel beheerder van de applicatie, pas dan wordt het account enabled. Het komt ook voor dat de functioneel beheerder naar de gebruiker gaat. Het account blijft uitgeschakeld en dus onbruikbaar tot het moment van de afspraak.

Het uitdienstproces verloopt min of meer net zoals indienst. Vanuit salarisadministratie komt automatisch een signaal door dat iemand weggaat. Een account wordt niet verwijderd, maar op inactief gezet, zodat de audit trail bewaard blijft. Als een medewerker vertrokken is en het account nog is blijven openstaan wordt het account inactief gezet, niet opgeschoond.

Er vinden periodieke controles plaats op de autorisaties in de applicatie. Dat gebeurt 1 of 2 maal per jaar. De controle werd niet gedocumenteerd, vanaf juli 2018 is dat wel het geval.

Wachtwoorden op de accounts verlopen iedere 60 dagen, waarna een gebruiker een nieuw wachtwoord moet ingeven.

Rollen tussen gebruikers en beheerders zijn gescheiden. Medewerkers van Burgerzaken kunnen alleen inloggen vanaf een werkplek van de gemeente, niet vanuit huis.

Beschikbaarheid
De gemeente beschikt voor deze applicatie ook over een testomgeving, naast de productieomgeving. Een upgrade van de omgeving heeft er nog nooit toe geleid dat er een ‘rollback’ uitgevoerd moest worden.

Het systeem moet vanwege overheidsverplichting binnen 48 uur weer online zijn na een verstorende gebeurtenis. Eventuele berichten die verloren zijn gegaan kunnen opnieuw verstuurd worden.

Vanuit ICT zijn er in- en uitwijkplannen en dit wordt jaarlijks getest.

Bijna alle servers, inclusief de file servers, zijn virtuele servers die gebruik maken van centrale storage. Deze storage bestaat uit 2 systemen, 1 in Steenwijk en 1 in Meppel die realtime worden gespiegeld, dus de data die in Steenwijk staat, is ook altijd aanwezig in Meppel. Van de virtuele servers wordt elke nacht een (incremental) back-up gemaakt naar disk op de locatie Meppel indien er een full back-up aanwezig is. Het mogelijk om individuele bestanden, mailboxen en databases te restoren. De back-ups zijn 14 dagen beschikbaar op disk en

daarna samengevoegd met de full back-up. Een keer per week worden de back-ups naar tape geschreven via data-protector, deze worden 6 weken bewaard.

Change management
De leverancier test nieuwe versies en wijzigingen allereerst in de testomgeving van de gemeente Steenwijkerland. De gemeente volgt vervolgens het testprotocol om de nieuwe versie op een aantal punten te controleren. De nieuwe versie wordt na verloop van tijd overgezet naar de productieomgeving.

De applicatie laat geen historie zien van versies die in het verleden hebben gedraaid. De beheerder houdt dit wel bij en ook in TOPdesk is de historie te vinden en er is een updatelog.

Over het algemeen werkt de gemeente de applicatie binnen 2 maanden na het uitkomen van een nieuwe versie bij. Kritische updates doorlopen een verkort programma en worden geïmplementeerd binnen 2 weken.

Risico op databeveiligingsincidenten
Alle gebruikers die een actief account hebben kunnen niet alleen inloggen op de productieomgeving maar ook op de testomgeving.

Wanneer een medewerker vanuit huis werkt is het onmogelijk om op de lokale thuis-pc bestanden vanuit de werkomgeving van de gemeente Steenwijkerland te benaderen, maar niet buiten de werkomgeving op te slaan. Dit betekent dat malware zich ook niet kan verspreiden naar het netwerk van de gemeente vanaf een thuis-pc.

De productiedatabase wordt gekopieerd naar de testomgeving en wordt dus gebruikt in de testomgeving.
In de operationele omgeving wordt niet getest. Om te kunnen testen met consistente gegevens wordt een kopie gemaakt naar de testomgeving om te testen. Tests worden alleen uitgevoerd door medewerkers burgerzaken en functioneel beheerder.

AVG – Logging en monitoring
Iedere wijziging en raadpleging op de BRP wordt bijgehouden door de applicatie. Voor beheerders is te zien op welk moment een gebruiker voor het laatst ingelogd is geweest. Voor gebruikers is niet te zien op welk moment zij voor het laatst hebben ingelogd. Verder worden beheerfuncties, zoals het aanmaken of uitschakelen van een account, ook niet gelogd.

De logging wordt opgeslagen in de database van de applicatie en de logging gaat terug tot het moment van ingebruikname van de applicatie, meer dan 8 jaar geleden.

Er zijn geen standaard periodieke rapportages op basis van de logging. Alleen op verzoek wordt logging bekeken en rapportage opgesteld.

De applicatie logt storingen en foutmeldingen niet, voor zover bekend. Een foutmelding die een gebruiker in beeld ziet is niet direct door beheerders terug te zien in logging.

Leveranciersmanagement
De applicatieleverancier (Centric) neemt het systeem alleen over in overleg, met behulp van een medewerker van de gemeente Steenwijkerland. Het is onder geen beding mogelijk dat de leverancier zelfstandig toegang verkrijgt tot de applicatie.

In contractuele afspraken is vastgelegd hoe de leverancier moet reageren op incidenten en problemen. De gemeente Steenwijkerland heeft nooit de behoefte gehad om de contractuele afspraken na te kijken en af te dwingen, omdat de leverancier altijd tijdig heeft gereageerd.

Logische toegangsbeveiliging
Toegang tot de applicatie wordt verschaft door middel van gebruikersnaam en wachtwoord. Er is geen sprake van Single-Sign-On (SSO). Vanaf een externe (thuis)werkplek dient een gebruiker eerst via 2-factor authenticatie in te loggen op de virtuele werkplekomgeving.

Wanneer een gebruiker te vaak een verkeerde combinatie van gebruikersnaam en wachtwoord opgeeft sluit de applicatie af en mogelijk wordt het account geblokkeerd. Wachtwoorden verlopen na 60 dagen, zowel van die van gebruikers als beheerders.

De applicatie is een webapplicatie. De verbinding tussen gebruiker en applicatie is versleuteld (een equivalent van https).

Het standaard admin account van de applicatie wordt gebruikt, het wachtwoord wordt periodiek gewijzigd.

B. Bijlage: gebruikte documenten en interviews

B.1. Documenten

2016.287 CR Security scan interne en externe systemen Gemeente Steenwijkerland

20180702 - Steenwijkerland - BPA - versie 1_0

20180702 - Steenwijkerland - SLR - versie 1_0

Advies CMT (informatie)beveiligingsorganisatie

Assurance-rapportage gemeente Steenwijkerland

Backup stwl v1.7

Basic_Network_Scan_New__2ey1t7

BIG STWL - Gemeente Steenwijkerland SA-Evaluatie

BIG STWL - P501504 Rapport - Bevindingen Mystery Guest Gemeente Steenwijkerland

BIG STWL - Rapportage Vhishing Gemeente Steenwijkerland

Bijlage 1 Aansluiting 1 SH

Bijlage 2 SH

Collegeverklaring SH

GAP analyse 2017

Informatiebeveiligingsbeleid 2017-2020

privacybeleid en reglement Steenwijkerland getekend exemplaar

Procedure Autorisatie tot gemeentelijke voorziening definitief

Procedure Sleutel- en toegangsbeheer v2 2 definitief

Procedure Toegangsbeleid gemeentelijke gebouwen en ruimten v1.1 definitief

Technische rapportage extern

Technische rapportage Intern

Verklaring omtrent geheimhouding en integriteit. DEFINITIEF.docx

Verslag uitwijktest 10-11-2017

Verslag uitwijktest 10-11-2017_1

Wijzigingsbeheer - mei 2015

Verslag uitwijktest

Applicatielijst 2018

Besluitenlijst_Concern_Managementteam_16_augustus_2018

Draaiboek maatregelen realiseren uit- en inwijk - versie 1.0 (B 0450)

IPMT Bewustwording informatiebeveiliging (9-3-2017)

Kwartaalrapportage Informatiebeveiliging 1e en 2de kwartaal 2018

Uiit en inwijk test - versie 1.0 (B 0450)

uitgevoerde acties nav pentest 27 september 2016

Uitvoeren maatregelen realiseren uit- en inwijk - versie 1.0 (B 0450)

Vastgestelde besluitenlijst 9 maart 2017

Wijzigingsverzoeken systemen en applicaties (B1370 en B1377) - versie 2.00

Procedure meldplicht datalekken gemeente Steenwijkerland.

Risico-tabel privacy

BIG STWL - P501504 Rapport - Bevindingen Mystery Guest Gemeente Steenwijkerland

GAP analyse 2017 - voortgang Q1+Q2 2018

Gemeente Steenwijkerland SA – Marcel

Gemeente Steenwijkerland SA-handout gouden regels

Interne rapportage ENSIA 2017 Gemeente Steenwijkerland

P501466 Phishing Steenwijkerland v1.0

Rapportage PHISHdag Steenwijkerland 2015

B.2. Interviews

Ter bescherming van persoonsgegevens zijn hier alleen de functies genoemd.

Functionaris Gegevensbescherming (FG)

Chief Information Security Officer (CISO)

Adviseur informatiemanagement

Burgemeester en portefeuillehouder Informatiebeveiliging

Concern controller

Privacy Officer

Beveiligingsbeheerder

Beveiligingsbeheerder

Beveiligingsbeheerder

Beveiligingsbeheerder

Beveiligingsbeheerder

Beveiligingsbeheerder

Beveiligingsbeheerder

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

Rekenkamercommissie Steenwijkerland
De heer J. Mastwijk
Postbus 162
8330 AD STEENWIJK

Steenwijkerland

Steenwijk, 12 maart 2019

Onderwerp Bestuurlijke reactie rapport 'Onderzoek informatiebeveiliging gemeente Steenwijkerland'

Geachte heer Mastwijk,

Met grote interesse hebben wij uw concept-rapport " Onderzoek informatiebeveiliging gemeente Steenwijkerland" gelezen. Wij danken u voor het uitgevoerde onderzoek en de onderhavige rapportage.

In de ambtelijke reactie van 3 januari j.l. is aandacht besteed aan enkele tekstuele aanpassingen die in het huidige concept zijn verwerkt. Ook hiervoor dank.

Onze bestuurlijke reactie is met name gericht op de conclusies en aanbevelingen.
Het verheugt ons te kunnen constateren dat de rekenkamercommissie de ingezette verbeteringen om daarmee de digitale weerbaarheid van de gemeente te verhogen, herkent en onderschrijft.

Wij herkennen en erkennen de aanbevelingen en conclusies zoals deze zijn opgenomen in deze concept-rapportage met uitzondering van de aanbeveling over het gebruik van productiegegevens in testomgevingen.
Bij het implementeren van nieuwe software hechten wij grote waarde aan het vooraf zorgvuldig testen van de software binnen een testomgeving. Om het volledig doortesten zorgvuldig te kunnen uitvoeren wordt binnen de testomgeving gebruik gemaakt van productiegegevens. Binnen het applicatielandschap heeft zowel de productie- als de testomgeving eenzelfde beveiligingsniveau. Hierdoor wordt het gebruik van productiegegevens onder deze omstandigheden als geaccepteerd risico beoordeeld. Wel zal ten alle tijde de noodzakelijk zorgvuldigheid worden betracht bij het gebruik van (productie) gegevens bij het testen van nieuwe software.

De overige aanbevelingen uit uw onderzoek waarvoor u aandacht vraagt zijn inmiddels opgenomen in het op 13 februari 2019 vastgestelde 'Informatiebeveiligingsplan 2019'.

Met vriendelijke groet,

Burgemeester en wethouders van Steenwijkerland
De secretaris, de burgemeester,

Judith de Groot Rob Bats