wat niet weet, maar wel deert

onderzoek beveiliging van gevoelige informatie

Rekenkamer
Lansingerland

wat niet weet, maar wel deert

onderzoek beveiliging van gevoelige informatie

Rekenkamer
Lansingerland

Rekenkamer
LANSINGERLAND

voorwoord

Nadat de Rekenkamer Rotterdam eerder dit jaar in een ophefmakend rapport heeft moeten constateren dat de informatiebeveiliging van de Maasstad niet op orde was, zijn ook andere rekenkamers aan de slag gegaan met penetratie- en inlooptesten om een beeld te krijgen van de mate waarin bijzondere persoonsgegevens al dan niet adequaat zijn beschermd. Zo ook de Rekenkamer Lansingerland. Ook in dit geval blijkt dat de kwaliteit van de informatiebeveiliging te wensen overlaat.

Wat opvalt in de diverse bestuurlijke reacties op de conclusies van de rekenkamer is de neiging om de geconstateerde bevindingen enigszins te relativeren. Om vooral te benadrukken dat het een “zaak van lange adem is” en dat er “altijd sprake zal zijn van digitale en fysieke lekken”. Wat deze reacties in elk geval duidelijk maken, is het kennelijke gebrek aan urgentie en prioriteit met betrekking tot informatiebeveiliging. Zeker in situaties waarin (nog) geen sprake is van feitelijke incidenten. Te vaak wordt het ontbreken aan daadwerkelijke data-incidenten gezien als bewijs dat het wel goed zit met de informatiebeveiliging. Deze houding is – zoals blijkt uit vele onderzoeken – zeer risicovol.

Structurele awareness en feitelijke investeringen in digitale weerbaarheid zijn (helaas) noodzakelijk in een wereld waarin sprake is van een toenemende verschuiving van fysieke waarde naar digitale waarde.
De stappen die de gemeente Lansingerland zet zijn bemoedigend, maar moeten uiteindelijk ook op de langere termijn standhouden. Dat vereist een hoge mate van blijvende politiek-bestuurlijke awareness ook indien zich geen feitelijke datalekken voordoen.

Voor haar onderzoek heeft de rekenkamer veel informatie verzameld. De rekenkamer is de contactpersonen en geïnterviewden zeer erkentelijk voor hun medewerking. Het onderzoek werd verricht door Laurens Wijmenga (projectleider) en Yiman Fung (senioronderzoeker).

Paul Hofstra
Directeur Rekenkamer Lansingerland

Rekenkamer
LANSINGERLAND

bestuurlijke nota

Rekenkamer
LANSINGERLAND

1 inleiding

1-1 aanleiding

Gemeenten hebben als gevolg van de decentralisaties in het sociaal domein steeds meer (bijzondere) persoonsgegevens in beheer. Ook wordt steeds meer informatie digitaal opgeslagen en overgedragen en worden systemen en data steeds vaker aan elkaar gekoppeld. Het belang van gemeenten om de informatiebeveiliging op orde te hebben en weerbaar te zijn tegen dreigingen als cybercrime is als gevolg van deze ontwikkelingen aanzienlijk toegenomen. Het belang van dit onderwerp bleek ook uit de uitslag van de zogeheten stemkastsessie op 9 december 2015 met de gemeenteraad, waarbij het onderwerp informatiebeveiliging als zeer relevant werd benoemd.

De Rekenkamer Lansingerland heeft op 15 december 2015 aangegeven een onderzoek te willen starten naar de informatiebeveiliging in de gemeente Lansingerland. Naar later bleek was de timing van dit onderzoek naar informatiebeveiliging niet ideaal, zoals vervolgens is aangegeven in een brief van 25 mei 2016 aan de raad. Dit had er mee te maken dat binnen de gemeente Lansingerland veel ontwikkelingen gaande waren op het gebied van informatiebeveiliging.

De Rekenkamer Lansingerland heeft daarom besloten om het onderzoek naar informatiebeveiliging op een later moment voort te zetten. Wel heeft de rekenkamer door middel van een tussentijdse rapportage de eerste bevindingen van haar onderzoek gedeeld met de raad.[1]

In de onderzoeksprogrammering voor 2017 heeft de rekenkamer aangegeven dit jaar het eerder geplande onderzoek uit te voeren. Het onderzoek richt zich op de bescherming van de (bijzondere) persoonsgegevens die de gemeente in beheer heeft.

1-2 doel- en vraagstelling

De rekenkamer beoogt met dit onderzoek na te gaan of (bijzondere) persoonsgegevens en andere gevoelige informatie bij de gemeente Lansingerland in veilige handen zijn.

De centrale vraag van het onderzoek luidt als volgt:
Zijn (bijzondere) persoonsgegevens en andere gevoelige informatie bij de gemeente Lansingerland in veilige handen?

1-3 leeswijzer

In de nota van bevindingen staan de resultaten van het onderzoek die als basis dienen voor de conclusies in de bestuurlijke nota. In de nota van bevindingen worden de

1 Rekenkamer Lansingerland, 'Notiebrief informatiebeveiliging', 3 oktober 2016.

onderzoeksvragen behandeld. De voorliggende bestuurlijke nota bevat de voornaamste conclusies en aanbevelingen.

Samen vormen de bestuurlijke nota en de nota van bevindingen het rekenkamerrapport.

2 conclusies en aanbevelingen

2-1 hoofdconclusies

1 Over het algemeen is gevoelige informatie, zoals (bijzondere) persoonsgegevens, bij de gemeente Lansingerland onvoldoende in veilige handen. Er is namelijk sprake van een combinatie van:
   a een tekortschietende beveiliging van digitale informatiesystemen voor aanvallen van binnenuit,
   b falende fysieke beveiliging van de kantoorlocatie en
   c een tekort aan benodigde 'social & security awareness' bij medewerkers.

2 De gemeentelijke informatiesystemen zijn in technische zin beter beveiligd tegen cyberaanvallen van buiten dan tegen aanvallen van binnenuit, onverlet kleinere kwetsbaarheden.

3 Door de tekortschietende informatiebeveiliging bestaan er reële risico's op identiteitsfraude, misbruik van publieke middelen en 'datalekken'.[2] Het optreden van deze risico's kan ten koste gaan van de effectiviteit van gemeentelijk beleid en het vertrouwen in de overheid.

4 Er zijn maatregelen genomen die kunnen bijdragen aan effectieve informatiebeveiliging, maar het ontbreekt aan passende maatregelen die volgen uit systematische en actuele risicoanalyses. Deze laatste worden namelijk niet integraal en volledig uitgevoerd, ondanks het juiste voornemen van het college om dit wel te doen.

5 De gemeente beschikt over een register van verwerkingen van persoonsgegevens, maar er ontbreken diepgaande risicoanalyses per verwerking van persoonsgegevens. Hierdoor kan de gemeente niet vaststellen of de beveiliging van persoonsgegevens toereikend is.

6 De kwaliteit van de beveiliging van drie specifieke applicaties, die veelvuldig worden gebruikt voor verwerkingen van (bijzondere) persoonsgegevens in het sociaal domein, schiet tekort.

2-2 toelichting hoofdconclusies

1 *Over het algemeen is gevoelige informatie, zoals (bijzondere) persoonsgegevens, bij de gemeente Lansingerland onvoldoende in veilige handen. Er is namelijk sprake van een combinatie van:*

2 Beveiligingsincidenten waarbij persoonsgegevens verloren zijn gegaan, of wanneer onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kan worden uitgesloten.

a een tekortschietende beveiliging van digitale informatiesystemen voor aanvallen van binnenuit,
b falende fysieke beveiliging van meerdere kantoorlocaties en
c een tekort aan benodigde 'social & security awareness' bij medewerkers.

- De rekenkamer heeft een gespecialiseerd bureau opdracht gegeven deze vormen van beveiliging te toetsen. De uitkomst is dat de informatieveiligheid binnen de gemeente Lansingerland tekortschiet.

a een tekortschietende beveiliging van binnenuit

- In een zogeheten interne penetratietest wordt geprobeerd vanaf gemeentelijke werkplekken en vanuit de gemeentelijke digitale omgeving oneigenlijke toegang tot kwetsbare informatiesystemen te verkrijgen.
- Uit de test kwamen drie kwetsbaarheden in de IT-infrastructuur met een hoog risico naar voren, die het mogelijk maken om oneigenlijke toegang tot het gemeentelijke netwerk te krijgen.
- Eenmaal in het gemeentelijke netwerk is veel informatie, waaronder persoonsgegevens, toegankelijk. Het bleek zelfs mogelijk beheerrechten te verkrijgen, waarmee nagenoeg alle systemen toegankelijk werden. Dit geldt ook voor ICT-applicaties met bijzondere persoonsgegevens in het sociaal domein.
- Verder bleek een aantal applicaties verouderd, waarbij de beschikbare beveiligingsupdates niet waren toegepast. Hierdoor kon toegang worden verkregen tot twee systemen. In verhouding tot gemeenten van vergelijkbare omvang is het aantal applicaties, waar geen beveiligingsupdates zijn toegepast, overigens beperkt.
- Een tekortkoming met een gemiddeld risico is het ontbreken van authenticatie van gebruikers bij toegang tot het bekabelde netwerk.
- Een andere tekortkoming met een gemiddeld risico is dat de systemen voor klimaatcontrole en noodstroomvoorzieningen onnodig toegankelijk zijn vanaf het netwerk.

b falende fysieke beveiliging

- Bij een toereikende fysieke beveiliging van kantoorlocaties, zouden de gemeentelijke informatiesystemen in principe alleen kwetsbaar zijn voor oneigenlijke toegang door kwaadwillende medewerkers.
- Het bleek bij de inlooptest echter eenvoudig om ongeautoriseerd toegang te krijgen tot het gemeentelijke kantoorpand. Eenmaal binnen was er vrije toegang tot diverse ruimtes en (vertrouwelijke) informatie.
- De onderzoeker die ongeautoriseerd binnen was gekomen, werd weliswaar éénmaal aangesproken, maar niet tegengehouden door medewerkers van de gemeente Lansingerland.
- Het is dus voor kwaadwillenden van buiten de gemeente mogelijk om van binnenuit oneigenlijke toegang tot de gemeentelijke informatiesystemen te krijgen.

c tekort aan 'social & security awareness'

- Zoals aangegeven werd tijdens de inlooptest de onrechtmatige bezoeker niet door medewerkers van de gemeente tegengehouden.
- Via een zogeheten spear phishing e-mail bleek het mogelijk drie medewerkers te verleiden een verdachte bijlage te openen, ondanks een beveiligingswaarschuwing.
- Bij telefonisch voice phishing was het mogelijk om geldige logincombinaties van vijf benaderde medewerkers te achterhalen waarmee toegang tot hun systeemaccounts kon worden verkregen. Hierdoor is het mogelijk om toegang te krijgen tot

(bijzondere) persoonsgegevens in applicaties waarvoor geen extra wachtwoord nodig is.

2 *De gemeentelijke informatiesystemen zijn in technische zin beter beveiligd tegen cyberaanvallen van buiten dan tegen aanvallen van binnenuit, onverlet kleinere kwetsbaarheden.*

- Het is niet gelukt om binnen de beschikbare tijd van twee dagen via het internet binnen te dringen in systemen van de gemeente.
- Spear phishing mails met een kwaadaardige bijlage werden aanvankelijk tegengehouden door het spamfilter van de gemeente. Door een technische beveiligingsmaatregel konden medewerkers bovendien de bijlagen van de e-mails, die in het kader van de test werden doorgelaten, niet openen. Deze maatregelen compenseren gedeeltelijk het gebrek aan social & security awareness (zie hoofdconclusie 1c).
- Wel zijn er enkele kleinere kwetsbaarheden geconstateerd die aanvallers, die voldoende tijd tot hun beschikking hebben, in staat stellen om de informatiesystemen van de gemeente binnen te dringen:
  - De computer waarop de toegang tot het netwerk wordt geregeld is benaderbaar vanaf het internet. Als via spear-, voice- of e-mail-phishing een gebruikersnaam en wachtwoord is verkregen, wat in de test door het gespecialiseerde bureau ook daadwerkelijk is gelukt (zie de toelichting op hoofdconclusie 1c), kan via deze route toegang tot het netwerk verkregen worden.
  - Er zijn verouderde Javascript bibliotheken aangetroffen met kwetsbaarheden die mogelijk in de toekomst misbruikt kunnen worden.
  - Via valse links kan het uiterlijk van de gemeentelijke website worden veranderd, zodat bezoekers van de website verleid worden een valse link te bezoeken.

3 *Door de tekortschietende informatiebeveiliging bestaan er reële risico's op identiteitsfraude, misbruik van publieke middelen en 'datalekken'. Het optreden van deze risico's kan ten koste gaan van de effectiviteit van gemeentelijk beleid en het vertrouwen in de overheid.*

- Door toegang tot informatiesystemen met (bijzondere) persoonsgegevens kunnen kwaadwillenden zich NAW-gegevens en BSN-nummers toe-eigenen. Dit zijn noodzakelijke (hoewel nog niet voldoende) gegevens om identiteitsfraude te plegen.
- Ook is het mogelijk persoonsgegevens te wijzigen, zodat een kwaadwillende onrechtmatig uitkeringen kan doen of ontvangen.
- Er hebben zich sinds 1 januari 2016 reeds acht datalekken voorgedaan en 11 kleinere beveiligingsincidenten. Hierbij ging het vaak om menselijke fouten, waarbij persoonsgegevens per ongeluk zijn verspreid, en diefstal van laptops of tablets. De kans op een datalek met grote maatschappelijke gevolgen, zoals bijvoorbeeld in Amersfoort[3] en Rotterdam[4], is dan ook groot.
- De gevolgen van bovenstaande voorbeelden kunnen zijn dat burgers terughoudend worden met het vragen van hulp of het delen van informatie met de gemeente. Dit kan ten koste gaan van de effectiviteit van het gemeentelijke beleid en het vertrouwen in de overheid beschadigen.
- Ook kan een datalek, dat het gevolg is van onvoldoende beveiligingsmaatregelen, leiden tot een boete van de Autoriteit Persoonsgegevens. Vanaf 25 mei 2018 zijn de

3 In 2016 werd door een ambtenaar van de gemeente Amersfoort per ongeluk een e-mail met gegevens van 1.900 zorgcliënten verstuurd naar een externe relatie.

4 Door een fout van een Rotterdamse ambtenaar waren in februari 2016 persoonsgegevens van 32.000 personen tijdelijk via internet te bereiken.

potentiele boetes fors hoger door de inwerkingtreding van de Algemene verordening gegevensbescherming (AVG).

4 *Er zijn maatregelen genomen die kunnen bijdragen aan effectieve informatiebeveiliging, maar het ontbreekt aan passende maatregelen die volgen uit systematische en actuele risicoanalyses. Deze laatste worden namelijk niet integraal en volledig uitgevoerd, ondanks het juiste voornemen van het college om dit wel te doen.*

- De gemeente heeft zowel technische als organisatorische beveiligingsmaatregelen getroffen die kunnen bijdragen aan effectieve informatiebeveiliging. Technische maatregelen zijn bijvoorbeeld het afdwingen van het gebruik van voldoende sterke wachtwoorden en een spamfilter. Organisatorische maatregelen zijn, naast de meer algemene beleidsdocumenten, de inrichting van een proces voor het rapporteren van beveiligingsincidenten en regels voor het gebruik van e-mail en internet door medewerkers.
- De maatregelen zijn onder meer in navolging van de Baseline Informatiebeveiliging Gemeenten (BIG)[5] getroffen. Genomen maatregelen vloeien niet direct voort uit een risicoanalyse.
- Het college heeft in het 'Gemeente breed informatiebeveiligingsbeleid' (mei 2015) vastgelegd dat de gemeente op basis van risicoanalyses tot passende beveiligingsmaatregelen wil komen. Voor een goede en doelmatige informatieveiligheid is dit een juiste beleidslijn.
- Onder risico's ten aanzien van informatieveiligheid wordt echter in het beleid verstaan: het niet voldoen aan de normen van de BIG. Dit is een onjuist uitgangspunt. Een risico is namelijk een potentiële gebeurtenis die het behalen van een bedrijfsdoelstelling negatief kan beïnvloeden. Door dit uitgangspunt kan het informatiebeveiligingsbeleid niet als 'risk-based', maar als 'compliance-based' worden omschreven.
- De capaciteit voor informatieveiligheid wordt, in navolging van het gemeentelijke beleid, ingezet voor de implementatie van maatregelen uit de BIG, waarbij de prioriteitsstelling is gebaseerd op niet nader uitgewerkte criteria, zoals 'bewustwording' of 'hacking'.
- Er zijn geen diepgaande risicoanalyses per applicatie of proces uitgevoerd, waarbij in kaart wordt gebracht welke dreigingen relevant zijn voor het informatiesysteem, met per dreiging het potentiële effect en de kans op optreden. Voorbeelden van risico's zijn defacement (vervanging door een eigen website) van de gemeentelijke website door hackers en infectie van gebruikers met malware door oneigenlijke installatie hiervan op de website. Door het optreden van deze risico's kan het vertrouwen van burgers in de digitale communicatie met de gemeente worden ondermijnd, waardoor de gemeentelijke doelstelling om de dienstverlening aan burgers te digitaliseren negatief wordt beïnvloedt.
- Wel is een risicoclassificatie van de data in informatiesystemen opgesteld, waarmee kan worden bepaald of het beveiligingsniveau van de BIG volstaat. Deze classificatie kan worden beschouwd als een vereenvoudigde risicoanalyse. Volgens de dataclassificatie is bij 75 applicaties het beveiligingsniveau van de BIG onvoldoende.

5 Een door de Vereniging Nederlandse Gemeenten (VNG) opgestelde beschrijving van de wijze waarop gemeenten de veiligheid van informatie conform internationale standaarden voor informatiebeveiliging kunnen borgen.

- De Informatiebeveiligingsdienst voor gemeenten[6] adviseert om voor applicaties, waarvoor het beveiligingsniveau van de BIG niet volstaat, diepgaande risicoanalyses uit te voeren en vervolgens, zo nodig, aanvullende beveiligingsmaatregelen te treffen. Dit is echter niet gebeurd.
- Omdat zowel gemeentebreed als op applicatieniveau geen adequate risicoanalyses worden uitgevoerd, ontbreekt de koppeling tussen risico's en de getroffen maatregelen. Hierdoor is niet goed te beoordelen of altijd de juiste maatregelen zijn genomen. Ook betekent het dat van de beveiligingsmaatregelen die wel zijn genomen, niet volledig is vast te stellen of deze gelet op de beveiligingsrisico's wel passend en (kosten)effectief zullen zijn.

5 *De gemeente beschikt over een register van verwerkingen van persoonsgegevens, maar er ontbreken diepgaande risicoanalyses per verwerking van persoonsgegevens. Hierdoor kan de gemeente niet vaststellen of de beveiliging van persoonsgegevens toereikend is.*

- Organisaties die persoonsgegevens verwerken met een hoog risico[7], moeten deze verwerkingen melden bij de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens doet daarom de aanbeveling om een inventarisatie te maken van de verwerkingen van persoonsgegevens.[8] Wanneer de Algemene verordening gegevensbescherming (AVG) op 25 mei 2018 van kracht wordt, is het verplicht om een verwerkingsregister van persoonsgegevens aan te leggen. De gemeente beschikt inderdaad over een dergelijk register.
- Voor verwerkingen van persoonsgegevens met een hoog risico zijn geen diepgaande risicoanalyses opgesteld, inclusief een inschatting van de kans op het optreden van risico's en de impact daarvan. Ook zijn geen privacy impact assessments opgesteld.
- Door het ontbreken hiervan is de gemeente niet in staat vast te stellen welke gegevens kwetsbaar zijn en welke passende beveiligingsmaatregelen getroffen moeten worden.

6 *De kwaliteit van de beveiliging van drie specifieke applicaties, die veelvuldig worden gebruikt voor verwerkingen van (bijzondere) persoonsgegevens in het sociaal domein, schiet tekort.*

- De rekenkamer heeft de beveiliging van drie applicaties op acht aspecten beoordeeld. Het betreffen applicaties die worden gebruikt voor verwerkingen van (bijzondere) persoonsgegevens in het sociaal domein. Deze drie applicaties vereisen volgens de dataclassificatie een hoger beveiligingsniveau dan de maatregelen uit de BIG. Aangezien in deze applicaties veel (privacy)gevoelige informatie wordt opgeslagen en verwerkt, dient de beveiliging van deze systemen zonder meer op orde te zijn.
- Ten aanzien van alle acht aspecten zijn tekortkomingen gesignaleerd bij een of meerdere applicaties:
  - Bij alle applicaties ontbreekt een ondertekende service level agreement (SLA) met de leverancier. Er vindt geen periodieke monitoring op SLA-afspraken plaats. De consequentie is dat de verantwoordelijke afdeling geen inzicht krijgt in de staat van de informatieveiligheid.

6 De Informatiebeveiligingsdienst voor gemeenten (IBD) is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING). De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging.

7 In artikel 31 van de Wbp is bepaald om welke verwerkingen het gaat.

8 https://autoriteitpersoonsgegevens.nl/nl/melden/melden-verwerking-persoonsgegevens#hoe-meld-ik-mijn-verwerking-bij-de-ap-6206, geraadpleegd op 13 november 2017.

- Er is geen formeel vastgestelde procedure voor het maken van back-ups. Back-ups worden wel periodiek uitgevoerd. Ook is voorzien in een uitwijkmogelijkheid bij calamiteiten. Deze is echter niet getest voor één van de twee onderzochte applicaties die de gemeente beheert. De toegang tot de back-ups is wel beveiligd. Ten aanzien van één applicatie heeft de gemeente geen zicht op de beveiliging van de back-ups.
- Er wordt geen toezicht gehouden op het gebruik van autorisaties. De gebruikte wachtwoorden zijn wel voldoende sterk en worden periodiek gewijzigd.
- Het eigenaarschap van de applicaties en de data wordt onvoldoende betekenisvol ingevuld door het management (de systeemeigenaren): er ontbreekt actief toezicht op de beveiliging en het beheer van gegevens. De systeemeigenaren steunen op gemeentebrede maatregelen op het gebied van informatiebeveiliging, interne werkafspraken en afspraken met derden (bijvoorbeeld zorgaanbieders) over het niveau van informatiebeveiliging. De werking van deze maatregelen en de naleving van de gemaakte afspraken worden echter niet getoetst.
- Bij geen van de applicaties is een recente risicoanalyse aangetroffen. Wel is, zoals eerder opgemerkt, een risicoclassificatie gemaakt van de data in de drie applicaties.
- Onafhankelijke assurance over de kwaliteit van de dienstverlening rond het technisch beheer van de applicaties ontbreekt bij de drie applicaties.
- Bij één applicatie heeft de gemeente geen zicht op de beveiliging van persoonsgegevens bij testwerkzaamheden. Bij de andere twee applicaties is er weliswaar een aparte testomgeving, maar worden niet-geanonimiseerde gegevens gebruikt om te testen. Dit betekent dat privacygevoelige informatie mogelijk wordt blootgesteld aan onbevoegden (systeemontwikkelaars en testers).

- Door de systeemeigenaren worden twee oorzaken genoemd van de tekortschietende informatiebeveiliging: te beperkte personele capaciteit en het ontbreken van landelijke (dwingende) eisen en ondersteuning. Die eisen en ondersteuning zijn er wel voor landelijke koppelingen die gebruikt worden voor de uitwisseling van persoonsgegevens, zoals bijvoorbeeld SUWI-net en DigiD. Wanneer niet voldaan wordt aan de eisen worden deze landelijke koppelingen afgesloten.
- De rekenkamer acht deze oorzaken plausibel: klaarblijkelijk heeft informatiebeveiliging niet vanzelfsprekend prioriteit bij het management.

2-3 aanbevelingen aan B en W

Gezien de conclusies uit het onderzoek doet de rekenkamer de volgende aanbevelingen aan het college van B en W.

1 Stel veiligheidsrisico's, in plaats van beveiligingsnormen, centraal bij de inrichting van de informatiebeveiliging:
   a Voer voor de informatiesystemen, die volgens de risicoclassificatie een hoog risico kennen, een diepgaande risicoanalyse uit, waarbij een inschatting wordt gemaakt van de kans dat een risico zich voordoet en de impact als een risico zich voordoet; hierbij gaat het niet alleen om gevolgen voor de gemeentelijke organisatie, maar met name ook voor de burgers.
   b Neem passende maatregelen om de specifieke risico's die uit deze analyses naar voren komen te mitigeren (of accepteer de risico's).
   c Maak een planning voor de implementatie van de maatregelen.
2 Stel voor de uit te voeren beveiligingsmaatregelen de benodigde middelen ter beschikking, voer de maatregelen daadwerkelijk onverkort uit en laat per kwartaal

door de Chief Information Security Officer (CISO) rapporteren over de voortgang en de resultaten daarvan. Grijp in als de resultaten afwijken van de verwachting.

Met de opvolging van de bovenstaande organisatorische aanbevelingen wordt uitvoering gegeven aan een op termijn adequate en duurzame informatiebeveiliging. Het rekenkameronderzoek heeft daarnaast diverse meer concrete kwetsbaarheden aangetroffen die op korte termijn verholpen dienen te worden. De volgende aanbevelingen aan het college vloeien hieruit voort.

3 Pak systematisch en gericht de diverse kwetsbaarheden aan die uit de interne penetratietest naar voren zijn gekomen en monitor dit door middel van een kwartaalrapportage. Beoordeel uiterlijk na een jaar aan de hand van een nieuwe interne penetratietest of de kwetsbaarheden naar behoren zijn aangepakt.
4 Verbeter de toegangsbeveiliging op kantoorlocaties, daarbij gebruikmakend van de uitkomsten van de inlooptest van de rekenkamer. Beoordeel uiterlijk na een jaar met nieuwe inlooptesten of de zwakke plekken zijn verholpen.

5 Versterk het bewustzijn van medewerkers ten aanzien van informatiebeveiliging door een awareness programma. Beoordeel met testen in welke mate dit awareness programma effectief is geweest.
6 Neem alle mogelijke organisatorische en technische maatregelen om (onbewust) slordig omgaan met vertrouwelijke informatie door medewerkers te voorkomen.

7 Neem maatregelen tegen de kwetsbaarheden die uit de externe penetratietest van de rekenkamer naar voren zijn gekomen.
8 Beoordeel uiterlijk na een jaar met een nieuwe externe penetratietest of er nog kwetsbaarheden in de beveiliging tegen cyberaanvallen zitten en neem eventuele passende maatregelen.

9 Verbeter de informatiebeveiliging van de onderzochte applicaties. Realiseer daartoe in ieder geval het volgende:
   a Richt volwassen contractmanagement in, inclusief een Service Level Agreement met de leverancier en een periodieke verantwoording over de afspraken die daarin zijn vastgelegd.
   b Zorg voor actieve betrokkenheid van het management als (gemandateerde) eigenaars van de gegevens bij het toezicht op de beveiliging en het beheer van gegevens.
   c Laat regelmatig onafhankelijke audits uitvoeren op de kwaliteit van de dienstverlening rond het technisch beheer van de applicaties.
   d Maak bij testwerkzaamheden gebruik van geanonimiseerde data.


LAHSINGERLAND

Rekenkamer
LANSINGERLAND

3 reactie college en nawoord

3-1 reactie college

Op 23 november 2017 ontvingen wij de bestuurlijke nota en de nota van bevindingen naar aanleiding van uw onderzoek 'informatiebeveiliging'. Hierna treft u onze reactie aan. De reactie is gesplitst in een algemeen deel en een reactie bij een aantal conclusies en aanbevelingen.

Algemene reactie

De Rekenkamer concludeert op basis van haar onderzoek dat de informatiebeveiliging in Lansingerland (nog) onvoldoende is. Dit beeld is herkenbaar voor het college en ook vergelijkbaar met andere gemeenten (recente Rekenkamer onderzoeken in Rotterdam en Dordrecht geven hetzelfde beeld) en waarschijnlijk met heel veel andere organisaties. De pen-testen en de 'social engineering' testen leveren een aantal nieuwe bruikbare en waardevolle inzichten op die het college meeneemt bij de verdere ontwikkeling van de informatiebeveiliging. De meest acute veiligheidsrisico's zijn als incidenten aangemerkt en zijn of worden op korte termijn opgelost.

Het college onderkent al langer de noodzaak van het verbeteren van de informatieveiligheid. We werken daarom ook al gestructureerd aan het verbeteren van de informatiebeveiliging door de implementatie van de BIG en hebben daar ook middelen voor gereserveerd. De praktijk laat zien dat het verbeteren wel een proces van 'lange' adem is. Waarbij dit eerder een proces van een paar jaar is dan een paar maanden. Enerzijds gaat het om de 'governance' die op orde moet zijn, maar ook vergt het een stuk organisatieontwikkeling en zullen technische en fysieke maatregelen genomen moeten worden. Daar komt bij dat de afgelopen periode er ook personele wisselingen hebben plaatsgevonden die gevolgen hadden voor de 'slagkracht' van de implementatie van de BIG. In 2017 is hierop gereageerd door de implementatie van de BIG te beleggen bij een projectleider en de implementatie los te koppelen van de CISO-functie. Hierdoor kon de projectleider zich volledig richten op de implementatie en werd niet 'opgeslokt' door de 'going concern' activiteiten in het kader van informatiebeveiliging. Dit leidde ertoe dat in 2017 opnieuw stappen zijn gemaakt.

Jaarlijks herijken we de prioriteiten voor de implementatie. Het Rekenkamer rapport zien wij als een belangrijke input voor de komende periode. Op basis van de bevindingen van de Rekenkamer en de aanbevelingen gaan we daarom een aantal zaken anders/sneller aanpakken. De meer 'compliance based' aanpak van de BIG zullen we aanvullen met de door u geadviseerde 'risk-based' aanpak. Beide aanpakken gaan wat ons betreft prima samen. Zo gaan we een aantal risicoanalyses op applicatieniveau en hieraan te koppelen beheersmaatregelen eerder uitvoeren dan gepland. Met name voor de applicaties/processen binnen het sociale domein. Ook zien we een raakvlak met de organisatieontwikkeling. De kennis en kunde op het gebied van de informatiebeveiliging zal naar een hoger niveau moeten. We hebben daar, met

name op het niveau van individuele applicaties, nog een profesionaliseringsslag te maken.

Hierna volgt onze reactie per hoofdconclusie. Een aantal conclusies zijn gebaseerd op testen die uitgevoerd zijn door een door de Rekenkamer ingeschakeld extern bureau. Zonder afbreuk te doen aan de bevindingen, die wij zeer serieus nemen zoals hierna blijkt, benadrukken we dat de testen uitgevoerd zijn in een 'geconditioneerde' omgeving. Zo heeft het externe bureau twee dagen met gemeentelijke toestemming op een werkplek gezeten en als enige doel gehad binnen te komen in het gemeentelijke netwerk en applicaties. In de dagelijkse praktijk zal deze situatie zich niet zo snel voordoen. Daarnaast vernamen wij van zowel uw medewerkers die betrokken waren bij dit onderzoek als van de medewerkers van het externe bureau dat het hen (veel) meer moeite kostte om 'in te breken' in onze systemen dan dat dit bij andere gemeenten/organisaties het geval is. Aan de ene kant een positief signaal, aan de andere kant, gegeven het feit dat bij onze gemeente gegevens nog onvoldoende in veilige handen zijn een zorgwekkend signaal voor de staat van informatiebeveiliging in het land.

Reactie per hoofdconclusie
1. Over het algemeen is gevoelige informatie, zoals (bijzondere) persoonsgegevens, bij de gemeente Lansingerland onvoldoende in veilige handen. Er is namelijk sprake van een combinatie van:
a. een tekortschietende beveiliging van digitale informatiesystemen voor aanvallen van binnenuit,
b. falende fysieke beveiliging van de kantoorlocatie en
c. een tekort aan benodigde 'social & security awareness' bij medewerkers.

Bovenstaande conclusie baseert de Rekenkamer op de beveiligingstesten die door een extern bureau zijn uitgevoerd. Het periodiek uitvoeren van dergelijke testen is ook een maatregel die in de BIG staat en dus ook de komende jaren in opdracht van het college herhaald zal worden. De nu uitgevoerde test was ook de eerste test en heeft daarmee waardevolle informatie opgeleverd. De bevindingen inzake punt 1a. zijn intern als (beveiligings)incidenten aangemerkt en worden conform de procedure 'beveiligingsincidenten' afgehandeld en opgelost.

Voor wat betreft de falende fysieke beveiliging merken we op dat de gemeente Lansingerland als uitgangspunt heeft dat het gemeentehuis een 'huis van de gemeente' is met een dito deels open karakter (van met name het bestuursgebouw). Dit betekent dat de fysieke beveiliging altijd minder zal zijn dan een gebouw met een gesloten karakter (met bijvoorbeeld toegangspoortjes en afgesloten vergaderruimten). De als 'falende' aangemerkte fysieke beveiliging heeft vooral een relatie met punt 1c. Bij de inlooptest kon de 'mystery guest' zonder pasje meelopen of snel doorlopen nadat medewerkers de deuren met een pas hadden geopend. Dat is natuurlijk niet de bedoeling. De geldende instructie is dat medewerkers mensen aanspreken die ze niet kennen en vragen naar hun toegangspas. Bezoekers horen zich te melden bij de receptie en opgehaald te worden door of namens een medewerker met wie ze een afspraak hebben. Deze instructies zullen we de komende periode weer frequenter onder de aandacht gaan brengen bij onze medewerkers. Positief punt vinden wij wel dat tijdens de inlooptest niet is gebleken dat medewerkers gevoelige dossiers met persoonsgegevens onbeheerd op hun bureau hadden laten liggen of hun computers

ongegrendeld hadden achtergelaten. Dit beeld past bij het beleid dat we voeren van ‘clear desk’.

De afgelopen jaren zijn er diverse workshops geweest om de ‘social & security’ awareness te vergroten en via afdelings- en teamoverleggen wordt ook geregeld aandacht besteed aan informatiebeveiliging. Daarnaast worden via Intranet regelmatig berichten/waarschuwingen geplaatst. De test laat zien dat desondanks deze maatregelen het bewustzijn van in ieder geval een deel van de organisatie nog laag lijkt te zijn.

Als onderdeel van de implementatie van de BIG stond al in de planning (ook voor het onderzoek Rekenkamer) om een nieuwe bewustwordingscampagne te starten. Gezien de uitkomsten van het onderzoek overwegen wij de vrijblijvendheid van de campagne te beperken door medewerkers een verplichte training en digitale toets te laten uitvoeren. Door het zelf periodiek (laten) uitvoeren van de genoemde testen meten we of de campagnes effect hebben en het bewustzijn toeneemt. Dit sluit ook aan bij aanbeveling 2 uit uw nota van bevindingen. In de nieuwe bewustzijnscampagne betrekken wij ook nadrukkelijk de uitkomsten van uw rapport. Het rapport zelf zullen wij ook beschikbaar maken voor de organisatie inclusief een overzicht van de ‘lessons learned’.

2. De gemeentelijke informatiesystemen zijn in technische zin beter beveiligd tegen cyberaanvallen van buiten dan tegen aanvallen van binnenuit, onverlet kleinere kwetsbaarheden.

Bovenstaande conclusie baseert de Rekenkamer op de beveiligingstesten die door een extern bureau zijn uitgevoerd. Het periodiek uitvoeren van dergelijke testen is ook een maatregel die in de BIG staat en dus ook de komende jaren in opdracht van het college herhaald zal worden. De nu uitgevoerde test was ook de eerste test en heeft daarmee waardevolle informatie opgeleverd. De bevindingen zijn intern als (beveiligings)incidenten aangemerkt en worden conform de procedure ‘beveiligingsincidenten’ afgehandeld en opgelost. Wij verwachten dat het daarna een stuk moeilijker zal zijn om van binnen uit onrechtmatig toegang te krijgen tot de gemeentelijke systemen, applicaties en data (ook al is fysiek toegang verkregen tot een werkplek binnen het gemeentehuis).

3. Door de tekortschietende informatiebeveiliging bestaan er reële risico’s op identiteitsfraude, misbruik van publieke middelen en ‘datalekken’. Het optreden van deze risico’s kan ten koste gaan van de effectiviteit van gemeentelijk beleid en het vertrouwen in de overheid.

Ons college is zich bewust van de risico’s die verbonden zijn aan tekortschietende informatiebeveiliging en investeert daarom in de implementatie van de BIG. De voorbeelden die u noemt zijn reële risico’s maar hebben zich in Lansingerland nog niet voorgedaan. Ook met stevige beveiligingsmaatregelen zijn datalekken niet uit te sluiten. Daarom heeft het college ook een ‘procedure melden van datalekken’ vastgesteld zodat, mocht er sprake zijn van een datalek, deze ook daadwerkelijk wordt gemeld bij het juiste orgaan en de op grond van de AVG noodzakelijke acties kunnen worden ondernomen. Enerzijds is het dus een zorg dat er een aantal datalekken zijn geweest, anderzijds is het ook een bevestiging van het feit dat onze medewerkers alert zijn op het signaleren van dergelijke datalekken zodat ook richting betrokkenen de

juiste acties kunnen worden ondernomen om eventuele negatieve gevolgen van een datalek te beperken.

4. Er zijn maatregelen genomen die kunnen bijdragen aan effectieve informatiebeveiliging, maar het ontbreekt aan passende maatregelen die volgen uit systematische en actuele risicoanalyses. Deze laatste worden namelijk niet integraal en volledig uitgevoerd, ondanks het juiste voornemen van het college dit wel te doen.

Zoals in de inleiding aangegeven werkt het college aan de implementatie en borging van de BIG. Door de BIG als uitgangspunt te nemen geeft het college invulling aan de resolutie van de VNG over informatiebeveiliging. De implementatie van de BIG is aan te merken als een 'compliance based' aanpak. Het college ziet dit echter breder. Onderdeel van de BIG is de baselinetoets. Daarbij stellen we vast per applicatie/dataverzameling/gegevensverwerking of maatregelen van de BIG alleen voldoende zijn. Is dat niet het geval dan volgt een specifieke risicoanalyse op de applicatie/dataverzameling en worden specifieke op de risico's gerichte maatregelen genomen of wordt bewust de keuze gemaakt dit niet te doen (bijvoorbeeld in verband met de kosten of de praktische uitvoerbaarheid). De baseline toets is recent afgerond en er is een prioritering aangebracht in de uitvoering van risicoanalyses. Binnenkort voert de organisatie een dergelijke analyse uit op de applicaties en processen in het sociale domein. Daarna volgt implementatie van eventuele aanvullende beheersmaatregelen. Daarmee wordt het beleid van het college wel degelijk uitgevoerd, maar de implementatie van de BIG was ten tijde van uitvoering van het Rekenkamer onderzoek nog niet in deze fase beland.

5. De gemeente beschikt over een register van verwerkingen van persoonsgegevens, maar er ontbreken diepgaande risicoanalyse per verwerking van persoonsgegevens. Hierdoor kan de gemeente niet vaststellen of de beveiliging van persoonsgegevens toereikend is.

Zie onze reactie bij conclusie 4. De implementatie van de AVG en de BIG werken daarin samen op.

6. De kwaliteit van de beveiliging van drie specifieke applicaties, die veelvuldig worden gebruikt voor verwerkingen van (bijzondere) persoonsgegevens in het sociaal domein, schiet tekort.

Zie onze algemene reactie. Met name op afdelingsniveau/applicatieniveau is nog een grote professionaliseringsslag te maken op het gebied van informatiebeveiliging. Binnen het sociale domein pakken we dit met voorrang op. Uw conclusie dat informatiebeveiliging klaarblijkelijk niet vanzelfsprekend prioriteit heeft bij het management herkennen wij niet helemaal. Over het algemeen hecht het management waarde aan informatiebeveiliging, maar loopt daarbij wel soms aan tegen financiële kaders en praktische beperkingen. Op onderdelen is dit ook een kwestie van prioriteiten stellen geweest (dus management herkent de prioriteit wel, maar er zijn ook andere prioriteiten). Zo lag bij de implementatie van de drie decentralisaties in 2015/2016 het accent op de continuïteit van de zorg aan cliënten en de financieel administratieve verwerking (berichtenverkeer, facturen en controle en verantwoording). Nu deze fase voorbij is wordt prioriteit gegeven aan de informatiebeveiliging. Een aantal elementen uit de hoofdconclusies heeft ook betrekking op 'contractmanagement'. Voor het professionaliseren van

contractmanagement loopt al een apart verbetertraject. De bevindingen uit uw rapport die hierop betrekking hebben nemen we daarin mee.

Reactie op de aanbevelingen van de Rekenkamer
Uw aanbevelingen zijn duidelijk en passen ook bij de stappen die ons college zelf moet laten zetten in het kader van de verdere implementatie van de BIG en de AVG. Wij nemen uw aanbevelingen dus over.

Tensloten merken wij nog op, en dat hebben we ook eerder naar de Raad gecommuniceerd, dat het een utopie is te veronderstellen dat informatie volledig veilig kan zijn in een organisatie. We onderkennen onze verantwoordelijkheid om, binnen het praktisch uitvoerbare, er alles aan te doen dat informatie in zo veilig mogelijke handen is. Daarbij zal constant een afweging gemaakt worden tussen risico en kosten. De menselijke factor is daarbij ook zeer bepalend, waarbij wij het als onze verantwoordelijkheid zien dat de organisatie een dusdanig instrumentarium ter beschikking heeft die ervoor zorgt dat eventuele inbreuken op de informatiebeveiliging tijdig worden gesignaleerd en de benodigde acties worden ondernomen.

De bestuurlijke nota en de nota van bevindingen zijn in principe openbare stukken. Op pagina 49 onder het kopje ‘een self service portaal is toegankelijk vanaf internet (gemiddeld risico)’ wordt met naam en toenaam vermeld om welke serviceportaal dit gaat. Gezien de openbaarheid van het rapport en met het oog op eventuele beveiligingsrisico’s verzoeken wij u te volstaan met de constatering dat een serviceportaal via internet benaderbaar is, zonder vermelding van de naam van het portaal.

Wij danken u voor het uitgevoerde onderzoek en de prettige samenwerking daarbij.

3-2 nawoord rekenkamer

De rekenkamer dankt het college voor zijn reactie. Het geeft daarin aan de conclusies te herkennen en alle aanbevelingen over te nemen. In dit nawoord zal de rekenkamer nog nader ingaan op enkele opmerkingen van het college bij de hoofdconclusies en aanbevelingen.

hoofdconclusies
Het college onderschrijft op hoofdlijnen de conclusies van de rekenkamer. Wel plaatst het college een aantal kanttekeningen. In algemene zin merkt het college op dat de pen-testen in een geconditioneerde omgeving zijn uitgevoerd en dat het relatief lang duurde voordat de onderzoekers zich toegang verschaften tot het interne netwerk. Volgens het college is de staat van de informatiebeveiliging vergelijkbaar met andere gemeenten.

Met deze opmerkingen lijkt het college de ernst van de bevindingen enigszins te relativeren. Het college lijkt er aan voorbij te gaan dat ‘hacks’ ook van binnenuit kunnen worden uitgevoerd door een medewerker of infiltrant met voldoende tijd tot zijn of haar beschikking. De relatieve score op dit onderdeel zegt bovendien, zoals de gemeente zelf ook opmerkt, meer over de landelijke staat van de informatieveiligheid dan over de situatie in Lansingerland.

Dezelfde toonzetting meent de rekenkamer te bespeuren in de reactie op hoofdconclusie 3. Daar noemt het college de risico's op identiteitsfraude, misbruik van publieke middelen en 'datalekken' weliswaar reëel, maar stelt dat deze zich in Lansingerland nog niet hebben voorgedaan. Vervolgens wordt echter opgemerkt dat datalekken wel degelijk zijn opgetreden. Hoewel de rekenkamer met het college concludeert dat datalekken niet volledig uit te sluiten zijn, dient het risico op deze lekken wel geminimaliseerd te worden. Een risicogerichte inrichting van informatiebeveiliging (aanbeveling 1) is hierbij van groot belang, alsmede voldoende financiële en personele capaciteit (aanbeveling 2).

aanbevelingen
De rekenkamer constateert met het college dat informatiebeveiliging een zaak van de lange adem is, waarbij de menselijke factor zeer bepalend is. In de 'notiebrief informatiebeveiliging' van 3 oktober 2016 is reeds opgemerkt dat de vereiste verandering van houding, gedrag en cultuur een langdurige en actieve inzet vanuit het management vergt. Informatieveiligheid dient daarom vanzelfsprekend de aandacht te hebben van het management. De rekenkamer neemt met instemming kennis van het voornemen om informatiebeveiliging de komende periode een hogere prioriteit toe te kennen.

De rekenkamer heeft verder geen opmerkingen naar aanleiding van de reactie van het college op de aanbevelingen.

Naar aanleiding van het verzoek van het college om de self service portaal niet met naam en toenaam te noemen is de tekst aangepast.

nota van bevindingen

Rekenkamer LANSINGERLAND

1 inleiding

1-1 aanleiding

Gemeenten hebben als gevolg van de decentralisaties in het sociaal domein steeds meer (bijzondere) persoonsgegevens in beheer. Ook wordt steeds meer informatie digitaal opgeslagen en overgedragen en worden systemen en data steeds vaker aan elkaar gekoppeld. Het belang van gemeenten om de informatiebeveiliging op orde te hebben en weerbaar te zijn tegen dreigingen als cybercrime is als gevolg van deze ontwikkelingen aanzienlijk toegenomen. Het belang van dit onderwerp bleek ook uit de uitslag van de zogeheten stemkastsessie op 9 december 2015 met de gemeenteraad, waarbij het onderwerp informatiebeveiliging als zeer relevant werd benoemd.

De Rekenkamer Lansingerland heeft op 15 december 2015 aangegeven een onderzoek te willen starten naar de informatiebeveiliging in de gemeente Lansingerland. Naar later bleek was de timing van dit onderzoek naar informatiebeveiliging niet ideaal, zoals vervolgens is aangegeven in een brief van 25 mei 2016 aan de raad. Dit had er mee te maken dat binnen de gemeente Lansingerland veel ontwikkelingen gaande waren op het gebied van informatiebeveiliging.

De Rekenkamer Lansingerland heeft daarom besloten om het onderzoek naar informatiebeveiliging op een later moment voort te zetten. Wel heeft de rekenkamer door middel van een tussentijdse rapportage de eerste bevindingen van haar onderzoek gedeeld met de raad.[9]

In de onderzoeksprogrammering voor 2017 heeft de rekenkamer aangegeven dit jaar het eerder geplande onderzoek uit te voeren.

1-2 beveiliging van persoonsgegevens

Bedrijven en overheden die persoonsgegevens gebruiken hebben een wettelijke plicht om deze goed te beveiligen. Artikel 13 van de Wet bescherming persoonsgegevens (Wbp) schrijft voor dat organisaties hiertoe passende technische en organisatorische maatregelen nemen.

artikel 13 Wet bescherming persoonsgegevens (Wbp)

De tekst van artikel 13 Wbp luidt als volgt: “De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De

9 Rekenkamer Lansingerland, ‘Notiebrief informatiebeveiliging’, 3 oktober 2016.

maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen."

In de 'Richtsnoeren beveiliging persoonsgegevens' heeft de Autoriteit Persoonsgegevens (AP) nader toegelicht wat onder een passend niveau van beveiliging wordt verstaan.[10] Uitgangspunten die de AP hanteert zijn onder andere dat:

- beveiliging van persoonsgegevens gedurende de hele levensduur van een informatiesysteem punt van aandacht moet zijn, van het eerste ontwerp tot het wissen van het laatste back-up bestand;
- beveiliging ingebed moet zijn in een plan-do-check-act cyclus waarin risico's worden beoordeeld, gebruik wordt gemaakt van algemeen geaccepteerde beveiligingsstandaarden en regelmatig controle en evaluatie plaatsvindt.

Sinds 1 januari 2016 is de meldplicht datalekken van kracht. Als sprake is van een datalek en uit toetsing door de AP blijkt dat niet is voldaan aan de wettelijke regels, dan kan de autoriteit een boete opleggen die kan oplopen tot maximaal € 810.000.

1-3 context

1-3-1 informatiebeveiligingsbeleid

De gemeente Lansingerland heeft een door het college van B en W vastgesteld informatiebeveiligingsbeleid.[11] De indeling van dit document is gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG). Deze baseline bestaat uit een strategisch deel, gericht op de organisatie en verantwoording van informatiebeveiliging, en een tactisch deel met normen en maatregelen.[12]

Gemeenten zijn niet verplicht de BIG in te voeren, wel heeft de algemene ledenvergadering van de VNG zich gecommitteerd aan de invoering van de BIG.[13] Per onderdeel van de BIG worden in het informatiebeveiligingsbeleid een algemene doelstelling, het beoogde resultaat en de basisnormen beschreven. Tevens is in het beleid de organisatie van de informatiebeveiliging beschreven. Het beleid dient eens in de drie of vier jaar te worden bijgesteld.

Op basis van het informatiebeveiligingsbeleid is in november 2015 een informatiebeveiligingsplan opgesteld.[14] In het informatiebeveiligingsbeleid is bepaald dat dit plan eens in de één of twee jaar wordt opgesteld. Het bevat aandachtspunten die moeten worden verbeterd om aan de doelstellingen van het beveiligingsbeleid, in casu de BIG, te kunnen voldoen. Hierbij waren 42 van de 204 nog te implementeren maatregelen uit de BIG geprioriteerd. Voor de implementatie van de verbeterpunten is een plan van aanpak opgesteld,[15] met een planning van de verbetermaatregelen.

10 Autoriteit Persoonsgegevens, 'Richtsnoeren beveiliging persoonsgegevens', februari 2013.

11 College van B en W, 'Gemeente breed informatiebeveiligingsbeleid', vastgesteld op 26 mei 2015.

12 Tevens zijn er meer operationele handreikingen om de invoer van de BIG te ondersteunen.

13 VNG, resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente', aangenomen op 29 november 2013.

14 Gemeente Lansingerland, 'Informatiebeveiligingsplan', 28 november 2015.

15 Gemeente Lansingerland, 'Plan van aanpak informatiebeveiliging, overzicht van de verbeteracties 2015/2016', 28 november 2015.

In zijn tussentijdse rapportage heeft de rekenkamer opgemerkt dat dit plan van aanpak erg optimistisch is en het niet duidelijk is of, en zo ja, wanneer de gemeente beoogt te voldoen aan alle eisen van het BIG. In een presentatie aan de gemeenteraad, gehouden op 31 januari 2017, is de toenmalige stand van zaken ten aanzien van de implementatie toegelicht. Op dat moment waren de 42 maatregelen met prioriteit nog niet volledig geïmplementeerd. Uit een interne notitie van de gemeente blijkt dat de gemeente in mei 2017 voldoet aan 57% van de maatregelen uit de BIG.[16]

In juni 2017 is een nieuw informatiebeveiligingsplan[17] opgesteld waarin 57 maatregelen uit de BIG zijn geprioriteerd, voor de periode tot en met het tweede kwartaal van 2018. Daar de selectie van te implementeren maatregelen in 2017 is gebaseerd op andere criteria, zijn dit niet noodzakelijkerwijs de maatregelen waaraan in 2015 prioriteit werd toegekend, maar nog niet waren geïmplementeerd.

1-3-2 organisatie informatiebeveiligingsfunctie

taken informatiebeveiliging

Het college van B en W draagt de integrale verantwoordelijkheid voor de beveiliging van informatie binnen de werkprocessen van de gemeente. Binnen de ambtelijke organisatie zijn de verantwoordelijkheden voor informatiebeveiliging verdeeld over de volgende functies:

- De gemeentesecretaris is gemandateerd verantwoordelijk voor informatiebeveiliging.
- De Chief Information Security Officer (CISO) is op organisatieniveau verantwoordelijk voor het actueel houden van het beleid, het adviseren bij projecten en het managen van risico's evenals het opstellen van rapportages. Sinds 1 juni 2017 is deze functie vacant (in de onderzoeksopzet stond abusievelijk 1 juni 2016 vermeld) en op 1 oktober is de functie weer ingevuld.
- De controller informatiebeveiliging is op organisatieniveau verantwoordelijk voor de verbijzonderde interne controle op de naleving van het informatiebeveiligingsbeleid, de controle op de realisatie van voorgenomen veiligheidsmaatregelen en de escalatie van beveiligingsincidenten.
- De beveiligingsfunctionaris rijbewijzen en reisdocumenten is verantwoordelijk voor toezicht op de naleving van de beveiligingsprocedures rond deze documenten.
- Voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid van specifieke gegevensverzamelingen zijn beveiligingsbeheerders aangesteld. Voorbeelden van deze gegevensverzamelingen zijn de Basisadministratie Adressen en Gebouwen (BAG) en SUWINET (het systeem van informatie-uitwisseling in de keten van werk en inkomen).
- De afdelingshoofden zijn verantwoordelijk voor de (informatie)veiligheid en de betrouwbaarheid van de informatieprocessen en systemen binnen hun afdeling.[18]

taken privacy

Vanaf 25 mei 2018 wordt de Algemene Verordening Gegevensbescherming (AVG) van kracht, die iedere overheidsorganisatie verplicht een functionaris

16 Gemeente Lansingerland, 'Informatieveiligheidsanalyse Mei 2017', juni 2017.

17 Gemeente Lansingerland, 'Actieplan informatieveiligheid, overzicht van de verbeteracties voor 2017/2018', juni 2017.

18 College van B en W, 'Gemeente breed informatiebeveiligingsbeleid', vastgesteld op 26 mei 2015.

gegevensbescherming aan te stellen. De Functionaris Gegevensbescherming (FG) houdt binnen de organisatie toezicht op de toepassing en naleving van de Wbp. Er zijn op dit moment reeds twee privacy beheerders die toezicht houden op de toepassing en naleving van de Wbp en adviseren over privacybescherming en bescherming van persoonsgegevens.

overleg en rapportage
Volgens het informatiebeveiligingsbeleid vindt vier keer per jaar een formeel overleg plaats tussen onder andere de CISO, de controller informatiebeveiliging en de beveiligingsfunctionarissen. Hierbij wordt onder meer de uitvoering van het informatiebeveiligingsplan besproken.[19]
De rekenkamer heeft niet geverifieerd of deze overleggen daadwerkelijk plaatsvinden.

Het onderwerp informatieveiligheid is onderwerp van de reguliere planning en control cyclus. In de bedrijfsvoeringsparagraaf van de begroting en de jaarstukken wordt aan de gemeenteraad gerapporteerd over de informatieveiligheid. De controller informatiebeveiliging controleert deze rapportages.[20]

Per 1 juli 2017 zijn gemeente verplicht om de verantwoording over informatieveiligheid in te richten via de ENSIA-systematiek. ENSIA staat voor Eenduidige Normatiek Single Information Audit. ENSIA bestaat uit een zelfevaluatievragenlijst op basis van de normen van de BIG en de specifieke normen voor bijvoorbeeld Suwinet, BRP (Basis Registratie Personen) en DigiD. Deze zelfevaluatie vormt de basis voor horizontale verantwoording naar de gemeenteraad in de jaarstukken en de verticale verantwoording naar de rijksoverheid. Daarnaast stelt het college van B en W vanaf 2018 een verklaring op waarin het aangeeft in hoeverre de gemeente de beheersingsmaatregelen voldoen aan de normen waarin wordt getoetst in de ENSIA systematiek. Een IT-auditor dient te controleren in hoeverre deze verklaring een getrouw beeld geeft.

1-4 doel- en vraagstelling

1-4-1 doelstelling
De rekenkamer beoogt met dit onderzoek na te gaan of (bijzondere) persoonsgegevens en andere gevoelige informatie bij de gemeente Lansingerland in veilige handen zijn.

1-4-2 onderzoeksvragen
De centrale vraag van het onderzoek luidt als volgt:

Zijn (bijzondere) persoonsgegevens en andere gevoelige informatie bij de gemeente Lansingerland in veilige handen?

De centrale onderzoeksvraag is uitgewerkt in de volgende deelvragen:

19 In ambtelijk wederhoor is aangegeven dat er tevens werkgroepen zijn voor de verdere optimalisatie van de informatieveiligheid op verschillende terreinen, waaronder bewustwording, veiligheidsincidenten, autorisatiebeheer en wijzigingsbeheer. Periodiek is er overleg tussen de verantwoordelijken rondom privacy en informatieveiligheid (P&I overleg). Om de maand wordt directie en het managementteam in het managementteamoverleg geïnformeerd over de huidige stand van zaken van de optimalisatie van de informatieveiligheid.

20 In ambtelijk wederhoor is aangegeven dat deze controle in de praktijk nog niet plaatsvindt.

10 Heeft de gemeente Lansingerland in brede zin een goed beeld van de belangrijkste risico's op het gebied van informatiebeveiliging en in het bijzonder de bescherming van (bijzondere) persoonsgegevens en andere gevoelige informatie?
11 Heeft de gemeente Lansingerland adequate maatregelen getroffen om de (bijzondere) persoonsgegevens en andere gevoelige informatie die zij in beheer heeft te beschermen tegen de belangrijkste veiligheidsrisico's?
12 Is het mogelijk om oneigenlijke toegang te krijgen tot (bijzondere) persoonsgegevens en andere gevoelige informatie die de gemeente Lansingerland in beheer heeft? En zo ja, welke gevolgen kan dit hebben voor burgers?

1-5 aanpak

In het kader van deelvraag 2 heeft de rekenkamer zowel maatregelen betrokken die op niveau van het concern zijn getroffen, als maatregelen binnen de individuele afdelingen. Daarbij zijn tevens zowel technische als organisatorische beveiligingsmaatregelen in ogenschouw genomen. In het kader van deelvraag 3 heeft de rekenkamer getest of het mogelijk is oneigenlijke toegang te krijgen tot (bijzondere) persoonsgegevens in systemen van de gemeente Lansingerland en tot andere gevoelige informatie die de gemeente in beheer heeft (onder meer via een zogeheten penetratietest). In de afzonderlijke hoofdstukken wordt voor zover nodig nader ingegaan op de gevolgde methode. In bijlage 1 wordt eveneens ingegaan op de gevolgde onderzoeksmethoden.

1-6 afbakening

Met betrekking tot de afbakening van dit onderzoek zijn de volgende punten relevant:

In het kader van deelvraag 1 beoogt de rekenkamer na te gaan of de gemeente de belangrijkste risico's (met in potentie de grootste impact) in beeld heeft. De rekenkamer zal dus niet beoordelen of de gemeente alle potentiële risico's in beeld heeft.

In het kader van deelvraag 2 neemt de rekenkamer zowel technische als organisatorische (o.a. gericht op de beheersing van het gedrag van medewerkers) beveiligingsmaatregelen in ogenschouw. De rekenkamer beperkt zich hierbij tot de beveiligingsmaatregelen voor (bijzondere) persoonsgegevens die de gemeente beheert als gevolg van de decentralisaties in het sociaal domein. Hierbij zijn drie verwerkingen van (bijzondere) persoonsgegevens geselecteerd, namelijk verwerkingen in het kader van jeugdhulp, regie op zorg en maatschappelijke ondersteuning. Het betreffen gegevens van een groot aantal burgers van Lansingerland. Ter indicatie: in de 2e helft van 2016 waren er 1.468 lopende indicaties op basis van de Jeugdwet en 3.235 op basis van de Wet maatschappelijke ondersteuning (Wmo).[21]

In het kader van deelvraag 3 zal de rekenkamer testen of het mogelijk is oneigenlijke toegang te krijgen tot (bijzondere) persoonsgegevens en andere gevoelige informatie die de gemeente in beheer heeft als gevolg van decentralisaties in het sociaal domein. Door een penetratietest worden de technische beveiligingsmaatregelen van ICT-systemen getest. Een zogeheten 'social engineering'

21 Gemeente Lansingerland, 'Jaarrapportage sociaal domein 2016, bijlage cijfermatige rapportage', 2 juni 2017.

test richt zich op de menselijke kant van de beveiliging; het veiligheidsbewustzijn van medewerkers.

1-7 leeswijzer

In hoofdstuk twee beoordeelt de rekenkamer of de gemeente voldoende zicht heeft op de belangrijkste risico's op het gebied van informatiebeveiliging (onderzoeksvraag 1). In hoofdstuk drie komen de maatregelen aan de orde die de gemeente op het gebied van informatiebeveiliging heeft getroffen (onderzoeksvraag 2). Ten slotte worden in hoofdstuk vier (onderzoeksvraag 3) de resultaten behandeld van de hack die de rekenkamer heeft laten uitvoeren. Hiermee wordt inzicht gegeven in de effectiviteit van de beveiligingsmaatregelen die zijn getroffen om oneigenlijke toegang tot gemeentelijke systemen te voorkomen.

De nota van bevindingen bevat de analyses en feiten die horen bij de onderzoeksvragen. Bij deelvragen één (hoofdstuk 2) en twee (hoofdstuk 3) wordt getoetst in hoeverre wordt voldaan aan normen en criteria. De normen zijn vermeld in de inleiding van deze hoofdstukken. Deelvraag 3 (hoofdstuk 4) is beschrijvend van aard. Hierop zijn geen normen van toepassing.

In bijlage 1 is een onderzoeksverantwoording opgenomen. Bijlage 2 bevat een lijst met aangehaalde documentatie. Bijlage 3 bevat een lijst van veelgebruikte begrippen en bijlage 4 is een toelichting op de implementatie van de BIG. Ten slotte is bijlage 5 een lijst met gebruikte afkortingen.

schuingedrukte teksten

In de nota van bevindingen beginnen paragrafen met een cursieve tekst. Deze cursieve tekst vormt de korte conclusie van de betreffende (sub)paragraaf aan de hand van de gehanteerde normen. Bij afwezigheid van normen vormt de cursieve tekst een samenvatting van de paragraaf.

gekleurde kaders

In de nota zijn geelgekleurde en blauwgekleurde tekstblokken te vinden. De geelgekleurde tekstblokken bevatten aanvullende informatie die voor de oordeelsvorming niet essentieel is, maar een nadere toelichting geeft over bijvoorbeeld gebruikte begrippen en instrumenten. De blauwgekleurde tekstblokken bevatten nadere informatie of uitleg over feiten waarover in het rapport wordt geoordeeld.

2 risicoanalyse

2-1 inleiding

In dit hoofdstuk beoordeelt de rekenkamer de wijze waarop de gemeente Lansingerland risico's op het gebied van informatiebeveiliging in kaart brengt. Daarmee wordt een antwoord gegeven op de volgende onderzoeksvraag:

Heeft de gemeente Lansingerland in brede zin een goed beeld van de belangrijkste risico's op het gebied van informatiebeveiliging en in het bijzonder gevoelige informatie zoals (bijzondere) persoonsgegevens?

Bij de beantwoording van deze vraag hanteert de rekenkamer normen, die in de onderstaande tabel staan weergegeven.

tabel 2-1: normen en criteria risico analyse

normen	criteria	paragraaf
Er worden met voldoende frequentie risicoanalyses en/of dreigingsanalyses gemaakt. In de risicoanalyses en/of dreigingsanalyses zijn de belangrijkste risico's geïdentificeerd.	• het uitvoeren van risicoanalyses is onderdeel van het informatiebeveiligingsbeleid;	2-2
	• het informatiebeveiligingsbeleid (of een aanvullend document) schrijft voor op welke momenten en op welke wijze risicoanalyses uitgevoerd moeten worden;	2-2
	• de risico's op het gebied van informatiebeveiliging en het beheer van vertrouwelijke informatie worden periodiek, met een passende frequentie, in kaart gebracht.	2-3
De risicoanalyses en/of dreigingsanalyses geven inzicht in specifieke risico's m.b.t. het beheer van (bijzondere) persoonsgegevens.	• er is gedocumenteerd welke (bijzondere) persoonsgegevens worden vastgelegd en bewerkt;	2-4
	• risico's ten aanzien van het beheer van (bijzondere) persoonsgegevens zijn in kaart gebracht.	2-4

In de volgende paragraaf wordt de risk-based opzet van het informatiebeveiligingsbeleid toegelicht (paragraaf 2-2). Vervolgens wordt ingegaan op de daadwerkelijke uitvoering van risicoanalyses (paragraaf 2-3). Ten slotte wordt ingegaan op risicoanalyses gericht op het beheer van (bijzondere) persoonsgegevens (paragraaf 2-4).

2-2 risk based informatiebeveiligingsbeleid

Het uitvoeren van risicoanalyses is onderdeel van het informatiebeveiligingsbeleid. Deze analyses moeten worden uitgevoerd voor het (minimaal eens per twee jaar) op te stellen

informatiebeveiligingsplan. Verder is in het informatiebeveiligingsbeleid bepaald dat risicoanalyses worden opgesteld voor specifieke (informatie)systemen die vertrouwelijke of privacygevoelige gegevens bevatten. Ten slotte dient de gemeente een business impactanalyse op te stellen in het kader van continuïteitsbeheer. De frequentie van de business impact analyse en de risicoanalyses per systeem is echter niet vastgelegd in het informatiebeveiligingsbeleid.

De manier waarop de risicoanalyses moeten worden uitgevoerd is niet beschreven in het informatiebeveiligingsbeleid of aanvullende documenten. De rekenkamer constateert wel dat in het informatiebeveiligingsbeleid onder risico's ten aanzien van informatieveiligheid wordt verstaan: het niet voldoen aan de normen van de BIG. Risico's ten aanzien van informatieveiligheid worden daarmee gelijkgesteld aan het niet voldoen aan normen voor informatiebeveiliging. Dit is een onjuist uitgangspunt. Een risico is namelijk een potentiële gebeurtenis die het behalen van een bedrijfsdoelstelling negatief kan beïnvloeden. Door dit uitgangspunt kan het informatiebeveiligingsbeleid niet als 'risk-based', maar als 'compliance-based' worden omschreven. Het gevaar van deze benadering is dat de capaciteit voor informatieveiligheid ineffectief wordt ingezet, zonder rekening te houden met daadwerkelijke risico's.

Het uitvoeren van risicoanalyses zou volgens de BIG een standaard onderdeel moeten zijn van informatiebeveiliging door gemeenten. Zo zou het lijnmanagement op basis van een expliciete risicoafweging eisen voor het niveau van de informatiebeveiliging van de informatiesystemen moeten vaststellen.[22] Op basis van deze betrouwbaarheidseisen kunnen de te nemen beveiligingsmaatregelen worden bepaald. In het informatiebeveiligingsbeleid van de gemeente wordt op enkele plekken ingegaan op het uitvoeren van risicoanalyses.

Allereerst wordt in de beschrijving van het informatiebeveiligingsbeleid, aan het begin van het document, het uitvoeren van een risicoanalyse onderkend als belangrijke fase in de beleidscyclus van informatiebeveiliging. De implementatie van het informatiebeveiligingsbeleid zou volgens het beleid moeten beginnen met een risico-inventarisatie en evaluatie (hierna RI&E). Tijdens deze RI & E dienen de uitgangspunten van het gemeentebrede informatiebeveiligingsbeleid te worden getoetst. Deze toetsing zou zowel 'harde aspecten' als techniek en procedures, als 'zachte kanten' zoals menselijk handelen en cultuur moeten betreffen. De risico's worden gewogen, geprioriteerd en eventueel van maatregelen voorzien. De RI & E zou moeten worden uitgevoerd in het kader van het opstellen van het informatiebeveiligingsplan, waarmee de implementatie van informatiebeveiligingsbeleid vorm krijgt. In de paragraaf van het beleidsdocument die het informatiebeveiligingsplan behandelt, staat dat een analyse wordt verricht van de 'bedrijfsprocessen ten opzichte van de ICT-omgeving'. In het plan dienen in ieder geval te worden benoemd:

- risico's die onvoldoende af te dekken zijn door maatregelen;
- risico's die zijn gerelateerd aan de kritische bedrijfsprocessen en/of (informatie)systemen. [23]

In het beleid is verder bepaald dat het informatiebeveiligingsplan eens in de één of twee jaar wordt opgesteld. De rekenkamer constateert derhalve dat het periodiek uitvoeren van risicoanalyses onderdeel is van het beleid.

22 Zie onder andere Informatiebeveiligingsdienst, strategische baseline informatiebeveiliging gemeenten, p.9.

23 College van B en W, 'Gemeente breed informatiebeveiligingsbeleid', vastgesteld op 26 mei 2015.

Het uitvoeren van risicoanalyses komt ook op twee andere plekken in het beleidsdocument terug. Bij het onderdeel verwerving, ontwikkeling en onderhoud van systemen wordt verwezen naar (informatie)systemen die vertrouwelijke of privacygevoelige gegevens bevatten. Voor deze systemen zouden volgens het beleidsdocument, op basis van classificatie en risicoanalyse, aanvullende beveiligingsmaatregelen te worden vastgesteld. Het gaat hierbij dus om *risicoanalyses op systeemniveau* in plaats van gemeentebreed. Uit het beleid blijkt niet op welke momenten en met welke frequentie deze analyses moeten worden uitgevoerd.[24]

Verder is bij het onderdeel continuïteitsbeheer sprake van een *business impactanalyse,* waarin 'gebeurtenissen worden geïdentificeerd die kunnen leiden tot discontinuïteit in het bedrijfsproces. Aan de hand van een risicoanalyse zijn de waarschijnlijkheid en de gevolgen van de discontinuïteit in kaart gebracht in termen van tijd, schade en herstelperiode'. Met discontinuïteit wordt hierbij de onderbreking van activiteiten van de gemeentelijke ICT-infrastructuur als gevolg van storingen en calamiteiten en de gevolgen hiervan voor kritische bedrijfsprocessen bedoeld.[25] Op basis van deze risicoanalyse zouden bedrijfscontinuïteitsplannen moeten worden opgesteld. In het actieplan informatieveiligheid voor de periode 2017/2018 staat overigens dat deze business impact analyse niet is opgesteld, omdat reeds een concernbrede RI & E wordt uitgevoerd.[26] De rekenkamer kan zich vinden in deze redenatie; de RI & E beschrijft namelijk niet alleen de kans en impact van risico's ten aanzien van informatieveiligheid, maar ook ten aanzien van de continuïteit van het bedrijfsproces (bijvoorbeeld het risico op brand, stroomstoringen en explosies).

In het informatiebeveiligingsbeleid is niet helder beschreven op welke wijze de risicoanalyses uitgevoerd moeten worden. De concernbrede RI & E wordt omschreven als een 'toets aan de praktijk op basis van het informatiebeveiligingsbeleid en de normen die hierin zijn vermeld of de normen waar in het beleid naar wordt gerefereerd'.[27] Hoe deze toets precies dient te worden uitgevoerd is echter niet beschreven. De normen waar in het beleid aan wordt gerefereerd zijn vermeld in paragraaf 1-2 van het document:

- de internationale NEN/ISO 27000 standaarden;
- de Baseline Informatiebeveiliging Gemeenten;
- aanvullende richtlijnen en eisen van het Nationaal Cyber Security Centrum (NCSC);
- wettelijke kaders zoals de Wet Basisregistratie Personen (Wet BRP), Wet bescherming persoonsgegevens (Wbp), Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), het DigiD beveiligingsassessment (DigiD audit) en de Wet Openbaarheid Bestuur (Wob).

In het beleidsdocument wordt niet meer specifiek verwezen naar deze normen, zodat niet duidelijk is wat de herkomst is van normen die in het beleidsdocument worden genoemd. In de praktijk blijkt overigens dat in de informatiebeveiligingsplannen die in

24 In ambtelijk wederhoor wordt opgemerkt dat risicoanalyses worden opgesteld als nieuwe systemen worden ontwikkeld of verworven. Het is niet vooraf vast te stellen hoe vaak een dergelijke situatie zich voordoet. De rekenkamer merkt op dat de BIG impliceert dat informatiebeveiligingsbeleid een Plan-Do-Check-Act cyclus kent. Ook de risicoanalyses voor bestaande systemen moeten dus periodiek worden herijkt.

25 College van B en W, 'Gemeente breed informatiebeveiligingsbeleid', vastgesteld op 26 mei 2015, p. 47.

26 Gemeente Lansingerland, 'Actieplan informatieveiligheid', juni 2017.

27 College van B en W, 'Gemeente breed informatiebeveiligingsbeleid', vastgesteld op 26 mei 2015, p. 13.

2015 en 2017 zijn opgesteld, alleen wordt getoetst aan de normen van de BIG en niet aan de andere normen die zijn beschreven in het informatiebeveiligingsbeleid. De werkwijze en de te volgen stappen bij de risicoanalyses op systeemniveau en de business impactanalyse ten behoeve van continuïteitsbeheer zijn niet nader beschreven.

De rekenkamer merkt verder op dat in het beleid risico's ten aanzien van informatieveiligheid worden gelijkgesteld met het niet voldoen aan normen voor informatiebeveiliging. Dit blijkt onder andere uit de volgende toelichting op het informatiebeveiligingsplan: '…bevat de risicoanalyse (de toets aan de praktijk) op basis van informatiebeveiligingsbeleid en de normen die hierin zijn vermeld of de normen waar in het beleid naar wordt gerefereerd'.[28] Dit is echter een onjuist uitgangspunt. Een risico is namelijk een potentiële gebeurtenis die het behalen van een bedrijfsdoelstelling negatief kan beïnvloeden.[29] Het voldoen aan een beveiligingsnorm kan de kans en impact van een risico weliswaar verminderen, maar het is niet zo dat door het naleven van de beveiligingsnormen (bijvoorbeeld uit de BIG) alle risico's ten aanzien van informatieveiligheid worden uitgesloten. Voor sommige informatiesystemen is daarom, gezien het belang van de gegevens die daarin worden verwerkt, een hoger beveiligingsniveau dan de BIG wenselijk. Anderzijds levert het niet naleven van de BIG niet automatisch bij elke applicatie een onacceptabel risico ten aanzien van informatieveiligheid op.

Door dit uitgangspunt kan het informatiebeveiligingsbeleid niet als 'risk-based', maar als 'compliance-based' worden omschreven.[30] Het gevaar hiervan is dat genormeerde beveiligingsmaatregelen worden ondernomen zonder dat er een specifiek risico bestaat of dat de gemeente, noodzakelijke beveiligingsmaatregelen (bovenop de genormeerde maatregelen) niet neemt. Mede gezien het feit dat de gemeente nog niet voldoet aan een deel van de normen uit de BIG, is het gevaar reëel dat de beschikbare middelen niet 'risk-based' worden ingezet.

2-3 uitvoering risicoanalyses

De rekenkamer constateert dat het uitvoeren van risicoanalyses geen wezenlijk onderdeel is van de informatiebeveiligingsplannen. De inzet van de informatiebeveiligingsplannen richt zich op de implementatie van maatregelen uit de BIG, waarbij de prioriteitsstelling is gebaseerd op niet nader uitgewerkte criteria, zoals 'bewustwording of 'hacking'. Er zijn geen diepgaande risicoanalyses per applicatie of proces uitgevoerd. Wel is een classificatie van applicaties gemaakt, waarmee is bepaald of, in aanvulling op de BIG, extra beveiligingsmaatregelen nodig zijn. Voor 75 applicaties, waaronder applicaties die veelvuldig worden gebruikt in het sociaal domein, is dit inderdaad het geval.

28 College van B en W, 'Gemeente breed informatiebeveiligingsbeleid', vastgesteld op 26 mei 2015, p. 13.

29 Committee of Sponsoring Organizations of the Treadway Commission, 'Risico management van de onderneming. Geïntegreerd raamwerk Enterprise Risk Management Integrated Framework (ERM)', 2014.

30 Het voldoen aan normen sluit een risicogerichte benadering overigens niet uit, integendeel: ook het voldoen aan de BIG impliceert dat informatiebeveiligingsmaatregelen gebaseerd worden op risico analyses per proces of systeem. Volgens de Strategische Baseline van de BIG moet er een risicoafweging plaatsvinden. De mogelijke methodes hiervoor zijn een baselinetoets gevolgd door een diepgaande risicoanalyse, certificering of Privacy Impact Assessment (PIA).

In de praktijk blijkt het informatiebeveiligingsbeleid, inclusief de gemeentebrede risicoanalyse (RI&E) en het informatiebeveiligingsplan gericht op de implementatie van de BIG: een set minimum beveiligingsmaatregelen, die geldt voor alle applicaties. Het informatiebeveiligingsbeleid schrijft voor dat tevens risicoanalyses en beveiligingsplannen per applicatie worden opgesteld. Uit deze risicoanalyses kan blijken dat, in aanvulling op de BIG, extra beveiligingsmaatregelen nodig zijn. In de praktijk geeft de gemeente voorrang aan de concernbrede invoering van de minimummaatregelen uit de BIG. Er zijn geen risicoanalyses uitgevoerd per informatiesysteem of applicatie.[31] Het is de bedoeling dat deze worden uitgevoerd op het moment dat de BIG is geïmplementeerd.[32] [33]

In het eerste informatiebeveiligingsplan en plan van aanpak die zijn opgesteld in november 2015 zijn dan ook, in lijn met het 'compliance based' beleid, geen risico's geïnventariseerd, maar is in kaart gebracht in hoeverre aan de normen van de BIG wordt voldaan (een zogeheten GAP-analyse). Dit is een van de stappen die de Informatiebeveiligingsdienst voor gemeenten adviseert bij de implementatie van de BIG. In bijlage 4 wordt dit proces nader toegelicht.

Na de GAP-analyse zijn vier algemene criteria geselecteerd, op basis waarvan de maatregelen worden gekozen die bij implementatie voorrang krijgen. Het gaat om de criteria gedrag en bewustwording, incidentenbeheer, ongeautoriseerd gebruik van systemen en mobile Device Management. Het eerste criterium is gekozen, omdat het volgens de gemeente in de adviezen van de VNG/KING een doorslaggevende rol speelt bij het op orde brengen van de informatiebeveiliging. Tevens bleek volgens de gemeente ook dat het onderdeel 'mensen' een relatief hoog risico zou geven, waarbij met beperkte middelen een relatief groot resultaat zou kunnen worden bereikt. De rekenkamer constateert dat het gangbaar is dat, met maatregelen op het terrein van gedrag en bewustwording, de meeste winst kan worden geboekt vormen bij de verbetering ven informatiebeveiliging. Van de overige criteria voor de selectie van te implementeren maatregelen ontbreekt echter een onderbouwing.

Ten behoeve van het informatiebeveiligingsplan en plan van aanpak voor de periode 2017/2018 is een RI & E uitgevoerd, waarbij kans en impact per risico is bepaald (zie kader).

top vijf risico's informatieveiligheid Lansingerland

De gemeente Lansingerland heeft in mei 2017[34] voor het laatst de risico's ten aanzien van informatieveiligheid in kaart gebracht, waarbij per risico aan de kans en impact een puntenscore is toegekend. De vijf risico's met de hoogste puntenscore zijn: hacking, mensen als risico voor informatieveiligheid, virussen, ongeautoriseerd gebruik van systemen en digitaal phishing.

31 E-mail ambtenaar, 6 september 2017.

32 Interview ambtenaren, 18 september 2017.

33 In ambtelijk wederhoor heeft de gemeente opgemerkt dat in het kader van het implementeren van het logisch toegangsbeleid per applicatie wel wordt besproken welk risico's er rond het autoriseren van personen bestaan en welke maatregelen hierop moeten worden ondernomen.

34 Gemeente Lansingerland, 'informatieveiligheidsanalyse mei 2017', juni 2017.

De rekenkamer constateert dat deze top vijf niet voldoet aan de gangbare definitie van een risico: een potentiële gebeurtenis die het behalen van een bedrijfsdoelstelling negatief kan beïnvloeden.[35] De risico's zijn namelijk te weinig concreet beschreven: het is niet duidelijk welke vorm van hacking of ongeautoriseerd gebruik bedoeld wordt en op welke manier de bedrijfsdoelstellingen daardoor negatief kunnen worden beïnvloed. Als 'risico's' zijn ook bepaalde menselijke handelingen, zoals het uitwisselen van wachtwoorden of het niet afsluiten van werkstations benoemd. Hierbij gaat het dus niet om een specifieke gebeurtenis, maar om het niet voldaan aan een beveiligingsnorm. De risicoanalyse biedt daardoor weinig aanknopingspunten voor het treffen van beveiligingsmaatregelen.

De IBD heeft een aantal concrete voorbeelden van mogelijke risico's geformuleerd per informatiesysteem. Voor via het internet toegankelijke webbased informatiesystemen zijn dat onder andere fraude als gevolg van misbruik van gegevens door hackers, defacement door hackers (vervanging door een eigen website) van de gemeentelijke website en infectie van gebruikers met malware door oneigenlijke installatie hiervan op de website.[36] In het gele kader in paragraaf 4-1 zijn enkele voorbeelden gegeven van risico's die ontstaan, wanneer hackers zich toegang verschaffen tot bijzondere persoonsgegevens in het sociaal domein.

In het plan worden mogelijke maatregelen genoemd om deze risico's af te dekken. De rekenkamer constateert echter geen aantoonbare relatie tussen de risicoanalyse en de maatregelen. In het actieplan zijn namelijk, net als in het 1e plan van aanpak, maatregelen geselecteerd uit de BIG die nog dienen te worden geïmplementeerd. Dit zijn niet noodzakelijkerwijs dezelfde maatregelen als die in de risico-inventarisatie. In het informatiebeveiligingplan wordt hierover het volgende opgemerkt: "De criteria voor te selecteren maatregelen zijn gebaseerd op het rapport 'In onveilige handen' van de Rekenkamer Rotterdam,[37] openstaande maatregelen uit het actieplan informatieveiligheid 2015, de uitkomsten van de risico-inventarisatie en –evaluatie 2017 en algemene adviezen van de Informatie Beveiligings Dienst (IBD)".[38] De criteria zijn in dit geval bewustwording, bedrijfscontinuïteitsbeheer, autorisatiebeheer, in-, door- en uitstroomprocessen, incidentenbeheer en wijzigingsbeheer. Afgezien van de verwijzing naar deze verschillende bronnen is niet duidelijk hoe de criteria tot stand zijn gekomen en in hoeverre sprake is van een rangorde. Twee risico's zijn beoordeeld als 'acceptabel', namelijk de risico's samenhangend met het niet invoeren van periodieke screening van personeel en het niet uitvoeren van een business impact analyse (zie ook paragraaf 2-2).

In 2017 is verder een classificatie gemaakt van de data in ICT-applicaties van de gemeente. Per applicatie is een score toegekend ten aanzien van de aspecten 'beschikbaarheid', 'vertrouwelijkheid' en 'integriteit'. Hierbij is de systematiek van de baselinetoets gebruikt (zie bijlage 4). Deze classificatie is gemaakt om in te kunnen schatten of het beveiligingsniveau van de BIG volstaat, of dat extra beveiligingsmaatregelen moeten worden getroffen. Deze classificatie kan worden beschouwd als een vereenvoudigde vorm van een risicoanalyse. Het is echter niet construeerbaar hoe de classificatie tot stand is gekomen. De classificatie is volgens de

35 Committee of Sponsoring Organizations of the Treadway Commission, 'Risico management van de onderneming. Geïntegreerd raamwerk Enterprise Risk Management Integrated Framework (ERM)', 2014.

36 Informatiebeveiligingsdienst, 'Diepgaande risicoanalyse methode gemeenten', augustus 2014.

37 Rekenkamer Rotterdam, 'In onveilige handen, onderzoek informatiebeveiliging van gevoelige informatie', april 2017.

38 Gemeente Lansingerland, 'Actieplan informatieveiligheid', juni 2017, p.5

gemeente gebaseerd op vragenlijsten van de IBD, maar de ingevulde vragenlijsten zijn niet bewaard.[39] Volgens de meest actuele classificatie[40] die de gemeente heeft uitgevoerd, vereisen 75 applicaties een hoger beveiligingsniveau dan de maatregelen uit de tactische baseline. Het gaat hierbij onder meer om applicaties die worden gebruikt in het sociaal domein (Suite voor sociale Regie, Corsa en GWS). Er zijn voor deze applicaties echter geen diepgaande risicoanalyses uitgevoerd en ook geen aanvullende beveiligingsmaatregelen getroffen, zoals wel wordt geadviseerd door de IBD (zie bijlage 4).

2-4 risicoanalyses ten aanzien van bescherming van persoonsgegevens

De gemeente beschikt over een register van verwerkingen van persoonsgegevens. Er ontbreken echter risicoanalyses per verwerking, inclusief een inschatting van de kans op het optreden van een risico en de impact daarvan. Ook zijn geen privacy impact assessments uitgevoerd. Hierdoor kan niet 'risk-based' worden bepaald welke beveiligingsmaatregelen genomen moeten worden om persoonsgegevens te beschermen.

Organisaties die persoonsgegevens verwerken met een hoog risico[41], moeten deze verwerkingen melden bij de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens doet daarom de aanbeveling om een inventarisatie te maken van de verwerkingen van persoonsgegevens.[42] Wanneer de Algemene verordening gegevensbescherming (AVG) op 25 mei 2018 van kracht wordt, is het verplicht om een verwerkingsregister van persoonsgegevens aan te leggen.

De gemeente heeft inderdaad een register[43] aangelegd van (bijzondere) persoonsgegevens die worden vastgelegd en bewerkt. In dit register is onder meer aangegeven welke gegevens worden bewerkt, de wettelijke grondslag, gebruikte ICT-applicatie en een risicoclassificering, variërend van 0 (laag risico) tot 2 (hoog risico). Daarnaast is er zoals eerder opgemerkt een classificatie gemaakt van data in ICT-applicaties van de gemeente. Risicoanalyses per verwerking van persoonsgegevens, inclusief de inschatting van de kans op het optreden van een risico en de impact daarvan, ontbreken echter.

Een Privacy Impact Assessment (PIA) is een instrument om risico's ten aanzien van het beheer van privacygevoelige informatie inzichtelijk te maken. Het gaat dan bijvoorbeeld om het risico op identiteitsdiefstal, waarbij anderen in naam van een betrokkene verplichtingen aangaan, of een inbreuk op de privacy. PIA's kunnen bijvoorbeeld worden uitgevoerd wanneer een nieuwe dienst, een nieuw product of nieuwe regelgeving worden ingevoerd.

Hoewel de hoeveelheid privacygevoelige informatie die de gemeente in beheer heeft de afgelopen jaren sterk is gegroeid door de decentralisatie, de gemeente verschillende nieuwe diensten en producten aanbiedt en nieuwe regelgeving heeft

39 Ambtelijke reactie, ontvangen op 13 november 2017.

40 Gemeente Lansingerland, 'Dataclassificatie 2017', ontvangen op 23 novermber 2017.

41 In artikel 31 van de Wbp is bepaald om welke verwerkingen het gaat.

42 https://autoriteitpersoonsgegevens.nl/nl/melden/melden-verwerking-persoonsgegevens#hoe-meld-ik-mijn-verwerking-bij-de-ap-6206, geraadpleegd op 13 november 2017.

43 Gemeente Lansingerland, 'Register Lansingerland april 2016', ontvangen in het voorjaar van 2016.

opgesteld, zijn nog geen PIA's uitgevoerd. Vanaf 25 mei 2018 zijn gemeenten, op grond van de Algemene verordening gegevensbescherming, verplicht om een PIA uit te voeren bij een gegevensverwerkingen die waarschijnlijk een hoog privacyrisico opleveren voor de betrokkenen.[44]

44 Bron: www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/data-protection-impact-assessment-dpia. Geraadpleegd op 23 oktober 2017.

3 beveiligingsmaatregelen

3-1 inleiding

In dit hoofdstuk beoordeelt de rekenkamer de beveiligingsmaatregelen die de gemeente heeft getroffen en de wijze waarop de gemeente Lansingerland risico's op het gebied van informatiebeveiliging beheerst. Daarmee wordt een antwoord gegeven op de volgende onderzoeksvraag:

Heeft de gemeente Lansingerland adequate maatregelen getroffen om de (bijzondere) persoonsgegevens en andere gevoelige informatie die zij in beheer heeft te beschermen tegen de belangrijkste veiligheidsrisico's?

Bij de beantwoording van de onderzoeksvraag hanteert de rekenkamer de onderstaande normen.

tabel 3-1: normen en criteria beveiligingsmaatregelen

normen	criteria	paragraaf
De maatregelen sluiten aan op de risico's die zijn geïdentificeerd.	• de getroffen maatregelen vloeien logisch voort uit uitgevoerde risicoanalyses; • in ieder geval de belangrijkste risico's zijn voorzien van beveiligingsmaatregelen.	3-2
De gemeente heeft essentiële technische en organisatorische maatregelen getroffen die beveiligingsrisico's doen afnemen.	Voor elke applicatie: • er is een service level agreement opgesteld, inclusief afspraken over informatieveiligheid. Over de uitvoering wordt periodiek gerapporteerd; • er worden back-ups uitgevoerd en er is geborgd dat onbevoegden geen toegang hebben tot de data die in de back-ups zijn opgeslagen; • er is een adequaat gebruikersmanagement, waarbij een gebruikersaccount uniek en persoonsgebonden is, autorisaties worden gecontroleerd op rechtmatigheid, wachtwoorden niet te eenvoudig zijn, en er een periodieke verplichting tot het wijzigen van het wachtwoord is en mutaties in autorisaties worden gelogd; • er is een eigenaar aangewezen die zicht heeft op de getroffen beveiligingsmaatregelen en zich laat informeren over de werking van deze maatregelen en over incidenten die zich hebben voorgedaan; • er worden beveiligingsincidenten conform een procedure gemonitord, geregistreerd en opgevolgd; • er wordt zekerheid verkregen over de opzet en werking van beveiligingsmaatregelen door middel van interne (of externe) controles; • er wordt bij het testen gebruik gemaakt van geanonimiseerde gegevens.	3-3-2 3-3-3 3-3-4 3-3-5 3-3-6 3-3-7 3-3-8

De volgende paragraaf gaat in op maatregelen die de gemeente heeft genomen in het kader van informatiebeveiliging. Daarna richt de rekenkamer zich op drie specifieke verwerkingen van (bijzondere) persoonsgegevens in het sociaal domein: jeugdhulp, regie op zorg en maatschappelijke ondersteuning. Hiervoor worden onder andere drie ICT-applicaties gebruikt: Corsa, GWS en Suite voor sociale regie (hierna S4SR). De rekenkamer beoordeelt in paragraaf 3-3 voor deze drie applicaties of de informatiebeveiliging op acht aspecten op orde is.

3-2 maatregelen op basis van risicoanalyses

Er is geen koppeling tussen risico's en de getroffen beveiligingsmaatregelen. Hierdoor is niet goed te beoordelen of altijd de juiste maatregelen zijn genomen. Ook is onduidelijk hoe de kosten van de maatregelen zich verhouden tot de risico's.

In hoofdstuk 2 is vastgesteld dat de gemeente haar beleidsvoornemen om risicogebaseerd beveiligingsmaatregelen te treffen, niet uitvoert. Omdat zowel gemeentebreed als op applicatieniveau geen adequate risicoanalyses worden uitgevoerd, ontbreekt de koppeling tussen risico's en de getroffen maatregelen. Wel is een classificatie gemaakt van de data in ICT-applicaties van de gemeente, welke kan worden beschouwd als een vereenvoudigde risicoanalyse. Voor de 65 applicaties, die volgens deze analyse een hoger beveiligingsniveau vereisen dan BIG, zijn echter geen diepgaande risicoanalyses uitgevoerd en ook geen aanvullende beveiligingsmaatregelen getroffen. Ook hier ontbreekt dus de koppeling tussen de risicoanalyse en de getroffen beveiligingsmaatregelen.

Dit laat onverlet dat er binnen de gemeente allerlei technische en organisatorische maatregelen zijn genomen om informatie te beveiligen. Hierbij is de BIG leidend. Voorbeelden van maatregelen uit de BIG zijn:

- een clean desk policy;
- de inrichting van een proces voor het rapporteren van beveiligingsincidenten;
- het beschrijven van de beveiligingsorganisatie;
- een automatische vergrendeling van de computer (screensaver) bij inactiviteit;
- regels over het gebruik van e-mail en internet door medewerkers;
- procedure voor screening van nieuwe medewerkers;
- gebruik van voldoende sterke wachtwoorden.

Deze maatregelen dragen onmiskenbaar bij aan effectieve informatiebeveiliging, maar vloeien niet voort uit een risicoanalyse. Omdat risico's niet systematisch in kaart zijn gebracht, is niet goed te beoordelen of altijd de juiste maatregelen zijn genomen. Ook is onduidelijk hoe de kosten van de maatregelen zich verhouden tot de risico's.

De gemeente maakt periodiek een overzicht van de invoering van de beveiligingsmaatregelen ten opzichte van BIG: de GAP-analyse. De laatste GAP-analyse is uitgevoerd in mei 2017 en vastgelegd in een excelsheet die de rekenkamer ontvangen heeft. De gemeente heeft door de GAP-analyses op gemeentebreed niveau een beeld van de technische en organisatorische beveiligingsmaatregelen.

3-3 informatiebeveiliging sociaal domein

De beveiliging van drie applicaties is beoordeeld op acht verschillende aspecten. Ten aanzien van alle acht aspecten zijn tekortkomingen gesignaleerd bij een of meerdere applicaties.

Bij alle drie applicaties ontbreekt een ondertekende service level agreement (SLA). Bij één applicatie is informatiebeveiliging wel onderwerp van de (nog niet ondertekende) SLA. Er vindt derhalve geen periodieke monitoring op de SLA afspraken plaats.

Er is geen formeel vastgestelde procedure voor het maken van back-ups. Back-ups worden wel periodiek uitgevoerd. Ook is voorzien in een uitwijkmogelijkheid bij calamiteiten. Deze is echter niet getest voor één van de twee onderzochte applicaties die de gemeente beheert. De toegang tot de back-ups is beveiligd. Ten aanzien van één applicatie, die door Centric wordt gehost, heeft de gemeente geen zicht op de beveiliging van de back-ups.

Alle applicaties hebben de functionaliteit om rechten toe te kennen op basis van rollen die zijn afgeleid van de functies van medewerkers. Er wordt echter geen toezicht gehouden op het gebruik van autorisaties. De gebruikte wachtwoorden zijn wel voldoende sterk en worden periodiek gewijzigd.

Het eigenaarschap van de applicaties en de data wordt onvoldoende betekenisvol ingevuld door het management: er ontbreekt actief toezicht op de beveiliging en het beheer van gegevens. De systeemeigenaren steunen op gemeentebrede maatregelen op het gebied van informatiebeveiliging, interne werkafspraken en afspraken met derden (bijvoorbeeld zorgaanbieders) over het niveau van informatiebeveiliging.

Bij geen van de applicaties is een recente risicoanalyse aangetroffen. Wel is een classificatie gemaakt van de betrouwbaarheidseisen ten aanzien van de data in de drie applicaties. Deze classificatie kan worden beschouwd als een vereenvoudigde vorm van een risicoanalyse.

Onafhankelijke assurance over de kwaliteit van de dienstverlening rond het technisch beheer van de applicaties ontbreekt bij alle applicaties.

De gemeente maakt bij testwerkzaamheden niet gebruik van geanonimiseerde data. Bij de twee applicaties die gemeente beheert is wel een aparte testomgeving. Bij de applicatie die wordt beheert door Centric heeft de gemeente geen zicht op de beveiliging bij testwerkzaamheden.

3-3-1 beschrijving applicaties

De rekenkamer heeft in het kader van dit onderzoek de beveiliging beoordeeld van een aantal applicaties waarin de gemeente (bijzondere) persoonsgegevens verwerkt of opslaat. Zoals aangekondigd in de onderzoeksopzet zijn hierbij drie verwerkingen van (bijzondere) persoonsgegevens geselecteerd, namelijk verwerkingen in het kader van jeugdhulp, regie op zorg en maatschappelijke ondersteuning. Voor deze verwerkingen worden (onder andere) de drie applicaties GWS[45], S4SR en Corsa gebruikt. GWS is het systeem is waarin alle cliënt-informatie, inclusief bijzondere persoonsgegevens, wordt bijgehouden, beschikkingen worden aangemaakt en gearchiveerd en van waaruit ook betalingen aan cliënten worden geïnitieerd en geadministreerd. S4SR is een applicatie die uitsluitend wordt gebruikt om informatie over cliënten te delen met andere

45 Vanaf 2015 heet deze applicatie: 'Suites voor sociaal domein'.

toegangspartijen. Het gaat hierbij om enkele tientallen cliënten met problemen op meerdere leefgebieden.[46] Corsa is een documentsysteem waarin de dossiervorming plaatsvindt om bijvoorbeeld het recht op uitkering of een voorziening te onderbouwen. Het raadplegen van documenten in Corsa vindt plaats via de documentviewer in GWS (Dis4GWS). GWS en S4SR zijn beide producten van het bedrijf Centric. S4SR is een SAAS (software as a service) applicatie die de gemeenten niet zelf beheert maar waartoe ze online toegang heeft. Het beheer van deze applicatie wordt uitgevoerd door Centric. Corsa is een product van het bedrijf BCTsoftware.

registratie van persoonsgegevens in ICT-applicaties sociaal domein

De registratie van de naam en het adres in GWS en S4SR vindt plaats door koppeling met de Basisregistratie Personen via de applicatie Key2Burgerzaken. Op basis van het Burger Service Nummer (BSN) van de cliënt dat door de administratief medewerkers van Publiekszaken wordt ingevoerd worden de naam en adresgegevens opgehaald. Deze gegevens zijn ook raadpleegbaar voor consulenten van andere domeinen, dan het domein waarvoor melding (bijvoorbeeld een WMO-aanvraag) wordt geregistreerd. Bijzondere persoonsgegevens worden in aparte dossiers in Corsa bijgehouden, waarin het onderzoek en het besluit over een indicatie en toe te kennen voorziening(en) zijn vastgelegd. Deze dossiers zijn alleen raadpleegbaar voor de consulenten van het betreffende domein.

De rekenkamer heeft de beveiliging van deze drie applicaties beoordeeld op verschillende beveiligingsaspecten, die later in deze paragraaf nader worden toegelicht. Hierbij heeft de rekenkamer de opzet en (wanneer dat, bijvoorbeeld door het maken van screenshots, mogelijk was) ook het bestaan van de beveiligingsmaatregelen beoordeeld. Hierbij worden tevens de bevindingen gepresenteerd die uit de beoordeling van de rekenkamer naar voren zijn gekomen.

Tabel 3-2 geeft een overzicht van de uitkomsten van de beoordeling. De legenda bij de tabel is:
- rood: beveiliging is niet op niveau;
- oranje: beveiliging is gedeeltelijk op niveau;
- groen: beveiliging is grotendeels op niveau

tabel 3-2: beoordeling beveiligingsmaatregelen applicaties

applicatie	service level agreement	backups	gebruikers-management	eigenaar-schap	incident management	risico-management	onafhankelijke assurance	anoniem testen
Corsa S4SR GWS								

46 Gesprek ambtenaren, 18 september 2017.

3-3-2 service level agreement

Service level agreements (SLA's) zijn dienstverleningsovereenkomsten tussen de gebruiker van de applicatie en de organisatie die de applicatie aanbiedt en beheert (in de meeste gevallen een externe leverancier). In deze overeenkomst zijn bijvoorbeeld afspraken vastgelegd over beschikbaarheid van de applicatie, afhandeling van wijzigingsverzoeken, responsetijd[47] en dergelijke. De rekenkamer heeft ten aanzien van de geselecteerde applicaties onderzocht of er SLA's zijn afgesloten en zo ja, of het naleven van het gemeentelijke IB-beleid en melden van beveiligingsincidenten onderdeel uitmaken van de afspraken in de SLA's. Ook is de rekenkamer nagegaan of in het kader van de SLA's verantwoording wordt afgelegd over de naleving van het IB-beleid en beveiligingsincidenten die hebben plaatsgevonden.

Het risico van het ontbreken van informatiebeveiliging als onderwerp in de SLA is dat afspraken rond de beveiliging van een applicatie niet duidelijk zijn en, als er rapportages ontbreken, geen inzicht bestaat bij de gebruiker in hoeverre het IB-beleid van de gemeente wordt nageleefd door de leverancier.

Van geen van de drie applicaties is een getekend contract, inclusief SLA aangetroffen. Voor Corsa is volgens de gemeente een hardcopy contract, waarin de aanschaf van deze applicatie in 2003 is overeengekomen, aanwezig in het archief. Dit contract heeft de rekenkamer niet ontvangen. Het is dus niet mogelijk om vast stellen of een SLA onderdeel is van dit contract. Voor de applicatie GWS is eveneens geen SLA ontvangen. Voor S4SR is een niet ondertekende en dus niet rechtsgeldige overeenkomst[48] ontvangen voor een licentie van deze applicatie. Een SLA en bewerkersovereenkomst[49] zijn onderdeel van deze overeenkomst. De gemeente merkt op dat wel wordt gewerkt conform het contract. De rekenkamer heeft dit echter niet kunnen vaststellen, doordat er geen zichtbare monitoring plaatsvindt op de naleving (bijvoorbeeld door rapportages).

Het contract is begin maart 2017 ontvangen en volgens betrokken ambtenaren nog niet getekend omdat men het contract nog een laatste keer wilde controleren, maar door capaciteitsgebrek en personele wisselingen daar nog niet aan was toegekomen. In deze SLA zijn geen afspraken ten aanzien van het naleven van het gemeentelijke IB-beleid en het melden van beveiligingsincidenten opgenomen. Wel is in de SLA vermeld dat de leverancier zich verplicht te voldoen aan de ISO27001, een internationale norm voor informatiebeveiliging. Het informatiebeveiligingsbeleid van de leverancier is gebaseerd op deze norm en relevante wet –en regelgeving, waaronder de Wbp. Het voldoen aan de ISO 27001 wordt volgens het conceptcontract getoetst door een periodieke externe audit.[50]

De rekenkamer constateert verder dat er geen structurele of periodieke monitoring op de SLA-afspraken plaatsvindt. De gemeente acteert naar aanleiding van incidenten. Ook de performance van de applicaties, inclusief de beveiliging, is geen punt van

47 De tijd die een applicatie, computer, server, helpdesk of iets anders nodig heeft om te reageren op een actie van een gebruiker.

48 Centric, 'Nader overeenkomst SAAS- Suite voor sociale regie', versie 1.0, 2 maart 2017.

49 Op grond van artikel 14 van de Wbp moet, als een organisatie persoonsgegevens laat bewerken door een derde, een overeenkomst worden gesloten tussen de bewerker en de verantwoordelijke organisatie. In de overeenkomst moet zijn vastgelegd dat de bewerker handelt in overeenstemming met de Wbp. De verantwoordelijke organisatie moet ook toezien op de naleving van de bewerkersovereenkomst.

50 E-mail ambtenaar, 25 september 2017.

aandacht voor de systeemeigenaren. De systeemeigenaren geven aan dat er geen performance problemen zijn geweest in de afgelopen periode. Anderzijds ligt, als een applicatie niet werkt, het werk voor de medewerkers volgens leidinggevenden voor 90% stil. Bij systeemuitval kunnen consulenten wel gesprekken met cliënten voeren. Hun kennis van de situatie van hun cliënten is in veel gevallen toereikend om een dergelijk gesprek op een effectieve manier te voeren.[51] Er zijn geen specifieke uitwijkprocedures voor de sociaal domein applicaties, maar in de praktijk worden er wel volgens leidinggevenden oplossingen gevonden, bijvoorbeeld om toch betalingen te kunnen doen of hulp te bieden aan cliënten. Voor het uitvoeren van betalingen kan een noodprocedure uitgevoerd worden aan de hand van betalingen die in een voorgaande betalingsperiode zijn verricht. Hiermee kan voor een aanzienlijk deel van de cliënten betalingscontinuïteit bewerkstelligd worden.[52] Consulenten weten bijvoorbeeld ook veel uit hun hoofd over bepaalde cliënten. In geval van systeemuitval wordt dan desnoods 'iets georganiseerd' met externe partijen.[53]

3-3-3 back-ups

Ten aanzien van het aspect 'back-ups' beperkt de beoordeling van de rekenkamer zich tot de mate waarin back-ups veilig worden uitgevoerd en geborgd is dat onbevoegden geen toegang hebben tot de data die in de back-ups zijn opgeslagen. Gebruikelijk is dat van de data in systemen en applicaties periodiek (bijv. dagelijks of wekelijks) een kopie in de vorm van een back-up wordt gemaakt. Als gegevens kwijt raken of een database corrupt raakt, kan de meest recente back-up worden teruggeplaatst zodat zo min mogelijk data verloren gaan. Om de vertrouwelijkheid van gegevens te borgen is het noodzakelijk dat rond het maken van back-ups passende beveiligingsmaatregelen worden genomen. Er moet geen onbeperkte toegang tot de back-ups zijn, de back-ups moeten beschermd worden opgeslagen en het terugzetten van kopieën dient gecontroleerd plaats te vinden. Het risico in relatie tot informatiebeveiliging is dat via back-ups vertrouwelijke gegevens onbedoeld toegankelijk zijn voor ongeautoriseerde personen.

Er is geen formeel vastgesteld beleid of procedure voor het maken van back-ups en de uitwijk wanneer het systeem uitvalt. De gemeente beschikt wel over niet-vastgestelde documenten waarin de huidige situatie en werkafspraken ten aanzien van back-ups en de uitwijk zijn beschreven.[54] Voor Corsa en GWS maakt de gemeente zelf back-ups. De back-up wordt continu gemaakt op de hoofdlocatie (het stadhuis). De verzamelde data wordt elk half uur doorgestuurd naar de tweede back-up unit op de nevenlocatie in Bleiswijk. Vervolgens wordt de data op die back-up unit opgeslagen op een tape. De data worden minimaal een jaar bewaard of langer, als de wettelijke bewaartermijn dat voorschrijft.

Op een uitwijklocatie (de nevenlocatie) kunnen de belangrijkste applicaties in productie worden genomen, als de hoofdlocatie uitvalt. Dit is getest voor de basis ICT-voorzieningen en de applicaties waarin de Basisregistratie Personen (BRP) en de Basisregistratie Adressen en Gebouwen (BAG) worden bijgehouden. Ook voor Corsa is

51 Bron: ambtelijke reactie, 13 november 2017.

52 Bron: ambtelijke reactie, 13 november 2017.

53 Gesprek ambtenaren, 18 september 2017.

54 Gemeente Lansingerland, 'Uitwijk en disaster recovery document', 13 januari 2017; gemeente Lansingerland, 'Situatie back-up en uitwijk gemeente Lansingerland', 29 augustus 2017; gemeente Lansingerland, 'Uitwijktest december 2016 versie 2.0', 2 januari 2017.

de uitwijk getest. Het is de bedoeling dat in 2018 de test wordt uitgebreid naar andere belangrijke applicaties, waaronder de applicaties in het sociaal domein. Het testen van de uitwijkprocedure is aan te bevelen, gezien de potentiële complexiteit van dit proces. Het kan immers gebeuren dat een database van een applicatie corrupt raakt. Er moet dan een back-up worden gebruikt van enkele dagen terug. Deze data kunnen dan echter inmiddels zijn bewerkt en/of doorgestuurd naar andere applicaties. Het kan dan erg ingewikkeld zijn om de juiste gegevens te herstellen en de applicaties in productie te nemen; door te oefenen kan de gemeente hier ervaring mee op doen.

De toegang tot de back-ups van S4SR en Corsa is beveiligd: alleen geautoriseerde personeel heeft volgens de gemeente toegang tot de backups.[55] De back-ups voor S4SR worden gemaakt door leverancier Centric. Deze worden dagelijks gemaakt en 30 dagen bewaard.[56] Volgens de gemeente is aan het feit dat Centric voldoet aan ISO27001 enige zekerheid te ontlenen met betrekking tot de beveiliging van back-ups.[57] Dit is echter strikt genomen niet het geval; de ISO 27001 beschrijft immers slechts de proces van de totstandkoming en monitoring van het informatiebeveiligingsbeleid. ISO27001 bevat geen operationele normen voor informatiebeveiliging.

3-3-4 gebruikersmanagement

Bij gebruikersmanagement gaat het om het aanmaken, wijzigen en verwijderen van gebruikersaccounts, verleende autorisaties en wachtwoorden. De beheersing van dit aspect is van groot belang om geautoriseerde toegang tot applicaties te faciliteren en misbruik in de vorm van ongeautoriseerde toegang tegen te gaan.

De rekenkamer is bij de geselecteerde applicaties het proces van het aanmaken van nieuwe accounts en het verlenen van toegang tot gegevens in de applicaties (autorisaties), wijzigingen van autorisaties (bijvoorbeeld bij verandering van functie) en het afsluiten van accounts nagegaan. Belangrijk hierbij is bijvoorbeeld dat een gebruikersaccount uniek en persoonsgebonden is. Tevens moet het management toezicht houden op het geautoriseerd gebruik van applicaties, bijvoorbeeld door het goedkeuren van autorisaties en rapportages over het gebruik van autorisaties (logging) en te checken of iedereen die toegang tot een applicatie heeft daadwerkelijk in dienst is. Een ander aspect van gebruikersmanagement is het beleid ten aanzien van wachtwoorden: wachtwoorden mogen niet te eenvoudig zijn en er dient een periodieke verplichting tot het wijzigen van het wachtwoord te bestaan. Wanneer het gebruikersmanagement niet adequaat wordt uitgevoerd, bestaat het risico dat er gebruikers zijn die onterecht geautoriseerd zijn en daardoor onterecht toegang hebben tot vertrouwelijke gegevens.

Accounts en autorisaties

Voor Corsa, GWS en S4SR dient autorisatie te worden aangevraagd via een formulier, dat wordt ondertekend door de teamleider. Wijzigingen van autorisaties worden in de praktijk doorgaans via e-mail en niet via een formulier doorgegeven.[58] Het komt volgens een betrokken medewerker overigens ook niet heel vaak voor dat er sprake is

55 Gemeente Lansingerland, 'Situatie back-up en uitwijk gemeente Lansingerland', 29 augustus 2017.

56 Centric, 'Service Level Agreement Suite voor sociale regie', versie 1.3, 3 maart 2017.

57 Ambtelijke reactie, ontvangen op 13 november 2017.

58 E-mail ambtenaar, 6 oktober 2017.

van een rolwijziging waardoor autorisaties gewijzigd moeten worden. Deze procedure geldt voor zowel interne medewerkers, externe medewerkers als gebruikers van ketenpartijen. Er is voor de applicaties Corsa en GWS geen vastgestelde 'matrix' met bevoegdheden per functie. De toegang tot applicaties wordt bepaald door de teamleiders. Dit doen zij door te verwijzen naar de toegang tot applicaties van bepaalde andere medewerkers ("zelfde systemen als"). Er is een aparte autorisatieprocedure voor S4SR, inclusief separaat formulier en autorisatiematrix.[59] De rekenkamer heeft enkele voorbeelden van ondertekende formulieren ontvangen. Er zijn geen ingevulde autorisatieformulieren voor S4SR ontvangen. De gemeente heeft in het ambtelijk wederhoor opgemerkt dat zij geen ingevuld formulier kon achterhalen. Klaarblijkelijk wordt het formulier in de praktijk niet gebruikt. Het is niet duidelijk hoe het management, zonder deze vastlegging, controle uitoefent op de bevoegdheden die medewerkers of externen in deze applicatie hebben.

Er worden twee verschillende formulieren gebruikt voor het toekennen van autorisaties: op één formulier van de afdeling Informatievoorziening en Faciliteiten worden de applicaties aangevinkt waartoe de medewerker toegang krijgt. Hiermee wordt het icoon van de applicatie toegankelijk gemaakt. Op een ander formulier van de uitvoerende teams Sociaal domein van de afdeling Publiekszaken, moet voor de applicaties GWS en Suwinet ook een bepaald 'profiel' met bijbehorende toegangsrechten worden gekozen. Beide formulieren worden ondertekend door de teamleider Participatie of de teamleider Maatschappelijke Ondersteuning & Jeugd. Dit doen ze voordat toegang gegeven wordt door de applicatiebeheerder van SUWI-net en Suite4sociale domein (GWS). De rekenkamer constateert dat het management door deze procedure controle heeft op de specifieke bevoegdheden die medewerkers in deze applicaties hebben.[60]

Ten aanzien van de toegang tot persoonsgegevens in de applicaties GWS, S4SR en Corsa wordt opgemerkt dat de basis met cliëntgegevens (adresgegevens) dezelfde is voor consulenten jeugd, wmo en participatie en ook raadpleegbaar is voor consulenten uit andere domeinen. Bijzondere persoonsgegevens (bijvoorbeeld medische informatie) worden in aparte bestanden in de applicaties bijgehouden en zijn alleen raadpleegbaar voor de consulenten van het betreffende domein. De afspraak is dat alleen degene die verantwoordelijk is voor een dossier, het dossier raadpleegt.[61] Deze afspraak is niet schriftelijk vastgelegd.

De rekenkamer constateert dat het management geen controles uitvoert op het gebruik van autorisaties (logging). Voor Suite 4 Sociale Regie (S4SR) kan de gemeente niet zelf loggen (of aan of uitzetten), maar kan dit wel aanvragen bij Centric.[62] De gemeente weet niet in hoeverre de logging daadwerkelijk functioneert. Ten aanzien van GWS wordt de gebruikersactiviteit gelogd (tijdstip van inloggen en mutaties), maar niet het raadplegen van bestanden. Er kan dus achteraf alleen een mutatiehistorie worden opgevraagd indien daar aanleiding toe is.[63] Corsa heeft een

59 Gemeente Lansingerland, 'Memo autorisatieproces S4SR' inclusief Autorisatieformulier Suite voor sociale regie medewerkers, autorisatiematrix en procedure aanvraag/intrekken autorisatie S4SR, 25 juni 2015.

60 Bron: ambtelijke reactie, ontvangen op 13 november 2017 en e-mail ambtenaar, 23 november 2017.

61 Interview ambtenaren, 18 september 2017.

62 E-mail ambtenaar, 26 september 2017.

63 E-mail ambtenaar, 26 september 2017.

aparte module voor logging, Corsa audit, waarin de volgende zaken worden gelogd: wijzigingen in de metadata, het opslaan van een nieuwe versie van een document en het raadplegen van document.

Het management voert geen controles uit op de accounts die 'in omloop zijn', bijvoorbeeld door een vergelijking van accounts en het personeelsbestand. Tot op heden worden de uitgegeven autorisaties in specifieke applicaties niet gestructureerd gecontroleerd. Alleen voor Corsa gebeurt dit ad hoc, op dezelfde wijze als voor de (algemene) netwerktoegang. Doordat Corsa een single sign-on applicatie is, zou dat moeten samenlopen met controles op de autorisaties voor het netwerk. Er is echter geen gestructureerde werkwijze, noch documentatie daarvan. Achteraf is dus niet aan te tonen dat deze controles plaats hebben gevonden.[64] Hierdoor weet de gemeente niet zeker of gebruikersaccounts uniek en persoonsgebonden zijn en iedereen die toegang tot een applicatie heeft daadwerkelijk in dienst is bij de gemeente (of bij een zorgaanbieder of toegangspartij in het geval van S4SR).

Wachtwoorden
Het wachtwoordbeleid van Corsa werkt met single sign-on, dat wil zeggen dat gebruikers die zijn ingelogd in het systeem niet opnieuw hoeven in te loggen in Corsa. Voor het inloggen in het systeem is een wachtwoordbeleid van toepassing. Wachtwoorden voor het systeem hebben volgens de gemeente minimaal 8 karakters, met eisen aan het soort karakters.[65]

Bij GWS en S4SR is er een door de leverancier afgedwongen applicatie-specifiek wachtwoordbeleid. De gemeentelijke applicatiebeheerder kan de wachtwoord instellingen niet wijzigen. De wachtwoordinstellingen betreffen het minimum aantal (8 bij S4SR en 10 bij GWS) en type karakters (een teken, een getal, een hoofdletter). Bij GWS moet een wachtzin worden gebruikt; er moet dus ook een spatie in zitten. Wachtwoorden verlopen na een periode en moeten dan worden gewijzigd. Als een account niet wordt gebruikt, wordt het automatisch geblokkeerd.[66]

De rekenkamer constateert dat het wachtwoordbeleid voldoet aan de minimale eisen die zijn gesteld in de BIG: wachtwoorden zijn voldoende sterk en worden periodiek gewijzigd.

3-3-5 eigenaarschap

In het kader van informatiebeveiliging en de bescherming van (bijzondere) persoonsgegevens is het van belang dat het eigenaarschap van de data in een applicatie betekenisvol wordt ingevuld. De eigenaar dient onder meer zicht te hebben op de getroffen beveiligingsmaatregelen en dient zich te (laten) informeren over de werking van deze maatregelen en incidenten die zich hebben voorgedaan. Het risico van geen of gedeeld eigenaarschap van gegevens is dat bij beveiligingsincidenten onduidelijk is wie waarvoor verantwoordelijk is en dat (daardoor) onvolledige of onjuiste maatregelen zijn getroffen ten aanzien van de beveiliging.

64 E-mails ambtenaren, 27 september en 6 oktober 2017.

65 E-mail ambtenaar, 27 september 2017.

66 Bron: E-mail ambtenaar 26 september. Centric, 'Releasedocumentatie GWS4all versie 17', 1 november 2013 en Centric, 'Suitevoorsocialeregie Accounts en Wachtwoorden', 2016.

De rekenkamer constateert dat er een actueel register bestaat waarin per applicatie is vastgelegd wie eigenaar is van de data in de applicaties.[67] Voor de applicaties Corsa, GWS en S4SR zijn in dit register twee leidinggevenden als eigenaren aangewezen. De gemeente laat weten dat twee andere leidinggevenden (mede)eigenaar zijn van de applicaties Corsa en S4SR.[68] Deze leidinggevenden zijn ook degenen die in de praktijk autorisaties toekennen voor de betreffende applicaties. De rekenkamer merkt op dat deze eigenaren slechts beperkt zicht hebben op de getroffen beveiligingsmaatregelen en zich niet laten informeren over de werking of incidenten. Er bestaat medio 2017 nog geen procedure voor de afhandeling en rapportage van beveiligingsincidenten.[69] Wel houdt de gemeente een register[70] bij waarin beveiligingsincidenten worden geregistreerd waarbij persoonsgegevens verloren zijn gegaan, of wanneer onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kan worden uitgesloten. Dergelijke incidenten heten ook wel 'datalekken'. Het bijhouden van een overzicht is een verplichting op basis van artikel 34a lid 8 van de Wbp. Ook heeft de gemeente sinds 2016 een procedure voor het melden en afhandelen van datalekken ingericht en vastgesteld.[71]

Desgevraagd geven de leidinggevenden aan dat zij ten aanzien van de beveiliging van persoonsgegevens in deze applicaties voornamelijk steunen op de gemeentebrede maatregelen, zoals de Verklaring Omtrent Gedrag (VOG) die nieuwe medewerkers moeten overleggen, de ambtseed en de gedragscode integriteit medewerkers.[72] Om de bewustwording omtrent informatiebeveiliging te vergroten worden volgens de leidinggevenden ook workshops en trainingen georganiseerd. Ook is er aandacht voor informatiebeveiliging tijdens werkoverleggen of overleggen op casusniveau. Daarnaast worden regelmatig onderwerpen die verband houden met informatieveiligheid gedeeld via @Work, het social intranet van de gemeente. De rekenkamer heeft enige documentatie[73] ontvangen waaruit blijkt dat dit gebeurt. Tevens steunen de leidinggevenden op interne afspraken die zijn gemaakt, zoals de afspraak om niet in het ondersteuningsplan van een bepaalde cliënt te kijken als dat niet nodig is. Informatie over cliënten mag niet worden gedeeld, tenzij de betrokken inwoner daarvoor toestemming geeft, of als de veiligheid in het geding komt (bijvoorbeeld als er sprake is van fysieke veiligheidsrisico en als er kinderen bij zijn betrokken). Deze afspraken zijn vastgelegd in het privacy protocol sociaal domein.[74]

In dit protocol is ook vastgelegd dat de verantwoordelijke teamleider toezicht houdt op het tijdig, volledig en correct motiveren en documenteren van afwegingen in het kader van de verwerking van persoonsgegevens (bijvoorbeeld om persoonsgegevens te

67 Gemeente Lansingerland, 'Dataclassificatie 2017', ontvangen op 23 augustus 2017.

68 E-mail ambtenaar, 25 september 2017.

69 Gemeente Lansingerland, 'Gap analyse mei 2017', ontvangen op 10 juli 2017.

70 Gemeente Lansingerland, 'Overzicht meldingen datalekken bij Autoriteit Persoonsgegevens' en 'Overzicht datalekken geen melding bij de Autoriteit Persoonsgegevens', ontvangen op 27 september 2017.

71 Ambtelijke reactie, ontvangen op 13 november 2017.

72 College van B en W, 'Gedragscode integriteit medewerkers', januari 2008.

73 Gemeente Lansingerland, presentatie 'Procesafspraken S4SR', 12 november 2015. Gemeente Lansingerland, presentatie 'Wat heb jij te verbergen', januari 2017. Gemeente Lansingerland, 'Training privacy in het sociaal domein', 25 november en 2 december 2014. Gemeente Lansingerland, 'Hoe werkt het in het nieuwe gemeentehuis', 22 augustus 2012.

74 Gemeente Lansingerland, Privacy Protocol Sociaal Domein Lansingerland, 16 december 2014.

delen). Deze stemt zijn of haar bevindingen met regelmaat af met de Functionaris Gegevensbescherming (FG). De FG dient één maal per jaar verantwoording af te dragen aan het College van Burgemeester en Wethouders over de omgang met persoonsgegevens binnen het sociaal domein.
Zoals eerder is opgemerkt controleren de systeemeigenaren niet in hoeverre medewerkers en teamleiders zich aan de afspraken over de omgang met persoonsgegevens houden; de logging in de applicaties wordt niet geanalyseerd door de eigenaren. De systeemeigenaren zien geen concrete risico's die hiertoe aanleiding geven. Tijdens het gesprek met de systeemeigenaren bleek dat bij hen niet bekend was of de logging überhaupt wel functioneerde. Er is momenteel nog geen FG aangesteld, waaraan teamleiders verantwoording afleggen.

Een andere interne afspraak is volgens leidinggevenden dat medewerkers gebruik maken van beveiligde e-mailkanalen bij uitwisseling van gegevens met derden. Hiervoor wordt Filecap gebruikt, een tool voor encryptie en comprimering van bestanden, die geintegreerd is in Outlook. Voor communicatie met zorgaanbieders wordt ook zorgmail gebruikt, een besloten omgeving waar alleen informatie uitgewisseld kan worden tussen de aangesloten deelnemers. Deze afspraak is echter niet vastgelegd. Bovendien is het gebruik van Filecap pas recent (september 2017) praktijk in contacten met aanbieders, zo blijkt uit een interne e-mail van de gemeente.[75] Filecap is ook gebruikt bij de overdracht van documenten aan de rekenkamer.

Voor de invoering van Filecap werden e-mails inclusief persoonsgegevens onbeveiligd verstuurd.[76] De naleving van deze afspraak door medewerkers wordt ook niet actief gecontroleerd door de eigenaren. Dit geldt overigens niet alleen voor de eigenaren van de betreffende applicaties in het sociaal domein. Volgens het e-mailprotocol[77] kan de directie controles uitvoeren op het e-mailgebruik, o.a. om vertrouwelijkheid van informatie te waarborgen. Van deze bevoegdheid is de afgelopen drie jaar echter geen gebruikgemaakt.[78]

In het sociaal domein wordt samengewerkt met derden, zoals zorgaanbieders en de toegangspartijen. Hierbij deelt de gemeente ook (bijzondere) persoonsgegevens met hen. Ten aanzien van de beveiliging van de persoonsgegevens door deze derden steunt de gemeente primair op bewerkersovereenkomsten die zijn afgesloten met een toenemend aantal partijen, bijvoorbeeld als onderdeel van een inkoopcontract voor de zorg of een subsidiebeschikking. De beveiligingsmaatregelen die bewerkers volgens deze overeenkomsten moeten nemen sluiten aan bij de BIG. De rekenkamer heeft enkele voorbeelden van bewerkersovereenkomsten[79] ontvangen en tevens een register[80] waarin deze overeenkomsten worden bijgehouden. Met 17 van de 60

75 De gemeente merkt in het ambtelijk wederhoor op dat al veel langer gebruik wordt gemaakt van Filecap. De rekenkamer sluit niet uit dat dit inderdaad het geval is voor andere contacten dan de in de e-mail genoemde zorgaanbieders.

76 E-mail ambtenaar, 15 september 2017.

77 College van B en W, 'Privacy reglement e-mail, internet en telefoongebruik Lansingerland 2012', 15 augustus 2012.

78 E-mail ambtenaar, 27 september 2017.

79 Onder andere Gemeente Lansingerland, 'Bewerkersovereenkomst GGZ Delfland uitvoering generalistische basis jeugdggz en/of ernstig enkelvoudige dyslexiezorg', 17 november 2016 en gemeente Lansingerland, 'bewerkersovereenkomst Regionaal Instituut voor Ontwikkelingsproblemen B.V., uitvoering generalistische basis jeugd-ggz en/of en/of ernstig enkelvoudige dyslexiezorg', 16 november 2016.

80 Gemeente Lansingerland, 'Overzicht verwerkersovereenkomst', ontvangen op 4 oktober 2017.

contractanten is een bewerkersovereenkomst gesloten. De rekenkamer merkt in dit kader op dat volgens de Autoriteit Persoonsgegevens zorgaanbieders doorgaans zelf verantwoordelijk zijn voor de beveiliging van persoonsgegevens, conform de Wet bescherming persoonsgegevens.[81] Het vastleggen van verantwoordelijkheden ten aanzien van informatieveiligheid bij de verwerking van persoonsgegevens is overigens wel een good practice.

Naast de bewerkersovereenkomsten kennen zorgaanbieders ook hun eigen beroepscodes (bijvoorbeeld voor Jeugdzorgmedewerker[82]) en regels ten aanzien van privacy en informatiebeveiliging. In subsidiebeschikkingen,[83] convenanten,[84] en contracten met derden wordt afgesproken dat zij zich conformeren aan het privacy protocol van de gemeente. De rekenkamer constateert dat dit is gebeurd in de subsidiebeschikkingen met de toegangspartijen,[85] maar niet in de overeenkomsten met zorgaanbieders die de gemeente aan de rekenkamer heeft overlegd.
De gemeente controleert niet of de externe partijen de afspraken op het gebied van informatiebeveiliging naleven. De gemeente vertrouwt hierbij op de controle van de accountant bij de externe partijen zelf. Dit is de huidige situatie. Volgens een betrokken ambtenaar loopt op dit moment een programma om 'contractmanagement' binnen de gemeente te professionaliseren. Het is de bedoeling dat ook actief de belangrijkste afspraken uit de contracten worden gemonitord (incl. de afspraken over informatiebeveiliging in bewerkersovereenkomsten).[86] Doordat de contracten met zorgaanbieders waar bewerkersovereenkomsten bij horen per 1 januari 2017 ingaan, hebben de zorgaanbieders nog niet hoeven te rapporteren over de resultaten en de naleving van afspraken. Dit gebeurt op jaarbasis.[87]

In het gesprek met de systeemeigenaren zijn twee oorzaken aangewezen, waardoor de beveiliging voor de persoonsgegevens in de onderzochte applicaties nog niet voldoet aan de normen van de BIG. Opgemerkt zijn de beperkte personele capaciteit en het ontbreken van landelijke (dwingende) eisen en ondersteuning. Die eisen en ondersteuning zijn er wel voor landelijke koppelingen die gebruikt worden voor de uitwisseling van persoonsgegevens, zoals bijvoorbeeld SUWI-net en Digid.

3-3-6 incidentmanagement

Bij incidentmanagement gaat het om een goede monitoring, registratie en opvolging van beveiligingsincidenten, bijvoorbeeld het verliezen van een mobiele telefoon. Incidenten die hebben plaatsgevonden dienen adequaat onderzocht te worden en structureel te worden opgelost. Tot slot dient hierover aan het management te worden gerapporteerd. Als beveiligingsincidenten niet worden opgevolgd en niet structureel worden opgelost, bestaat het risico dat incidenten zich herhaaldelijk voor blijven doen en er bijvoorbeeld langdurig sprake is van ongeautoriseerde toegang tot vertrouwelijke gegevens.

81 Bron: www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/gemeente/sociaal-domein?qa=zorgaanbieder&scrollto=1, geraadpleegd op 19 oktober 2017.

82 Beroepsvereniging van professionals in sociaal werk, 'Beroepscode voor de Jeugdzorgwerker', 2015.

83 Interview ambtenaren, 8 augustus 2018.

84 Gemeente Lansingerland, 'Handboek Sluitende Aanpak kwetsbare personen Lansingerland Versie 1.0', 13 februari 2014.

85 College van B en W, beschikking tot verlening van subsidie 2015 Stichting CJG Rijnmond, 4 februari 2015.

86 Interview ambtenaren, 18 september 2017.

87 Interview ambtenaren, 18 september 2017. 28 augustus 2017.

Er ontbreekt, zoals is opgemerkt in de voorgaande paragraaf, een procedure voor de afhandeling van incidenten. Deze is wel in voorbereiding.[88] Verbetering van het beheer van incidenten (hoofdstuk 13 van het operationele normenkader van de BIG) is tevens één van de speerpunten van het Actieplan informatieveiligheid voor de periode 2017/2018. Beveiligingsincidenten worden wel geregistreerd (zie vorige paragraaf).

3-3-7 risicomanagement

Zoals in eerdere hoofdstukken is beschreven gaat het IB-beleid ervan uit dat risicoanalyses worden opgesteld voor specifieke (informatie)systemen die vertrouwelijke of privacygevoelige gegevens bevatten. De rekenkamer is voor de geselecteerde applicaties nagegaan of er risicoanalyses en/of privacy impact analyses zijn uitgevoerd en of deze van goede kwaliteit zijn. Wanneer beveiligingsrisico's onvoldoende in kaart worden gebracht bestaat het risico dat er onvoldoende of niet de juiste maatregelen worden getroffen om de risico's voldoende af te dekken.

De rekenkamer heeft bij geen van de onderzochte applicaties een recente risicoanalyse aangetroffen waarin de kans en impact van beveiligingsrisico's zijn ingeschat en waarbij is aangegeven welke maatregelen worden getroffen om de risico's te mitigeren. Zoals is aangegeven in paragraaf 2-3 is wel een classificatie gemaakt van data in applicaties (inclusief S4SR, Corsa en GWS). Deze classificatie is gemaakt om in te kunnen schatten of het beveiligingsniveau van de BIG volstaat, of dat extra beveiligingsmaatregelen moeten worden getroffen. Deze classificatie kan worden beschouwd als een vereenvoudigde vorm van een risicoanalyse.

Een ambtenaar geeft desgevraagd aan dat het uitvoeren van risicoanalyses pas aan de orde is na de implementatie van de BIG. Er zullen dan risicoanalyses worden uitgevoerd op applicatieniveau en, op basis van deze analyses, maatregelen worden getroffen.[89]

3-3-8 onafhankelijke assurance

Het is een goede praktijk om zekerheid te verkrijgen over de beschikbaarheid, continuïteit en vertrouwelijkheid van gegevens door middel van een onafhankelijk onderzoek (bijvoorbeeld uitgevoerd door een register IT-auditor). Dat geldt voor zowel de interne als externe verwerking van gegevens. De verantwoording hierover vindt zijn weerslag in een zogenaamde third party mededeling ('TPM') of in een International Standard on Assurance Engagements 3402-statement (ISAE-3402). Van belang is dat in het kader van de TPM of ISAE3402 niet alleen wordt vastgesteld dat beveiligingsmaatregelen op papier bestaan, maar dat ook de werking kan worden aangetoond.

Wanneer onafhankelijke assurance ontbreekt, bestaat het risico dat onopgemerkt blijft dat de leverancier ontoereikende maatregelen heeft getroffen voor de beschikbaarheid, continuïteit en vertrouwelijkheid van de gegevens in de applicaties te waarborgen.

88 Gemeente Lansingerland, 'Conceptprocedure voor de melding van incidenten', ontvangen op 23 augustus 2017.

89 Interview ambtenaren, 18 september 2017.

Bevestiging van de kwaliteit van de dienstverlening bij derden in de vorm van een TPM of ISAE3402-statement heeft de rekenkamer bij geen van de onderzochte applicaties aangetroffen.[90] Wel is in de SLA met de leverancier van GWS en S4SR vastgelegd dat deze zich periodiek laat auditen op het voldoen aan de internationale norm voor informatiebeveiliging ISO27001. Deze SLA is echter nog niet ondertekend en dus nog niet rechtsgeldig. Bovendien is ISO27001 slechts een norm voor het proces van de totstandkoming en monitoring van informatiebeveiligingsbeleid.

3-3-9 anoniem testen

In het kader van informatiebeveiliging is het van belang dat bij het testen van nieuwe applicaties of wijzigingen in bestaande applicaties, gebruik wordt gemaakt van geanonimiseerde gegevens. Dit om te voorkomen dat tijdens testwerkzaamheden vertrouwelijke gegevens ten onrechte worden ingezien. Ook voorkomt het testen met geanonimiseerde gegevens dat persoonsgegevens bij het testen onbedoeld verspreid worden. Wanneer voor testwerkzaamheden niet-geanonimiseerde persoonsgegevens worden gebruikt, wordt privacyregelgeving geschonden. Het is namelijk niet toegestaan om persoonsgegevens te gebruiken voor testwerkzaamheden.

Een functionaris van de gemeente heeft aangegeven hoe de testwerkzaamheden worden uitgevoerd.[91] Corsa heeft een aparte testomgeving. Zowel de applicatie als de database zijn gescheiden van de productieomgeving. De persoonsgegevens in de testomgeving zijn niet geanonimiseerd. Alleen de applicatiebeheerder heeft toegang tot de testomgeving. De rekenkamer heeft niet geverifieerd of dit daadwerkelijk het geval is.

Het testen van wijzigingen van S4SR wordt gedaan door Centric. In het contract met Centric is, ten aanzien van het gebruik van persoonsgegevens bij testen, niet specifiek iets geregeld. Wel is een bewerkersovereenkomst gesloten met Centric en staat in het contract dat Centric moet voldoen aan de Wpb. De consequentie van deze (nog niet rechtsgeldige) contracten, is dat Centric voldoet aan de BIG en er wordt getest met anonieme data. Deze afspraak is echter nog niet rechtsgeldig. De gemeente kan bovendien niet verifiëren of Centric daadwerkelijk test met anonieme gegevens in een aparte testomgeving, omdat Centric hier niet over hoeft te rapporteren aan de gemeente.

Voor GWS bestaat een testomgeving die een kopie is van de productie-omgeving. De gebruikers die testen werken ook in de productie met dezelfde data. Het zijn dus geen geanonimiseerde data.[92] Er is wel een test-cliënt (een niet bestaande cliënt en verzonnen gegevens).

90 E-mail ambtenaar, 25 september 2017.

91 E-mail ambtenaar, 25 september 2017.

92 Volgens de gemeente worden bij inhuur van derden voor testen bijzondere afspraken gemaakt in het kader van informatiebeveiliging/privacy, zoals een geheimhoudingsverklaring of bewerkersovereenkomst. Hiervan is een voorbeeld overhandigd aan de rekenkamer. Bron: ambtelijke reactie, ontvangen op 13 november 2017 en e-mail 23 november 2017.

Rekenkamer
LANSINGERLAND

4 resultaten penetratietesten

4-1 inleiding

In dit hoofdstuk staat de volgende onderzoeksvraag centraal:

Is het mogelijk om oneigenlijke toegang te krijgen tot (bijzondere) persoonsgegevens en andere gevoelige informatie die de gemeente Lansingerland in beheer heeft? En zo ja, welke gevolgen kan dit hebben voor burgers?

De rekenkamer heeft deze vraag via drie wegen beantwoord. Ten eerste is een externe penetratietest uitgevoerd. Daarbij is geprobeerd vanuit een niet-gemeentelijke locatie via internet in de gemeentelijke informatieomgeving (de infrastructuur, applicaties en data) door te dringen. Ten tweede is een interne penetratietest uitgevoerd, waarbij vanuit een gemeentelijke locatie (een werkruimte) geprobeerd is oneigenlijke toegang te verkrijgen. Ten slotte is een social engineering test gedaan, waarin de bewustwording van medewerkers ten aanzien van informatiebeveiliging is getoetst. De bevindingen uit de uitgevoerde testen geven inzicht in hoeverre het totaal aan beveiligingsmaatregelen, dat de gemeente heeft getroffen, voldoet om te voorkomen dat onbevoegden kunnen doordringen tot de gemeentelijke informatieomgeving. In het volgende gele kader is een aantal voorbeelden opgenomen van scenario's die kunnen optreden als onbevoegden toegang weten te krijgen tot de gemeentelijke informatieomgeving.

voorbeelden scenario's gevolgen oneigenlijke toegang

- Als een hacker onbevoegd toegang verkrijgt tot de bijzondere persoonsgegevens in het sociaal domein, dan kunnen deze gegevens worden ingezien en gewijzigd. De gevolgen kunnen zijn dat de hacker de gegevens gaat misbruiken voor andere zaken door de identiteit van de burgers over te nemen. Of de gedupeerde burgers krijgen niet meer de dienstverlening waar ze recht op hebben door de mutaties in hun gegevens.
- Als een hacker onbevoegd toegang verkrijgt tot de bijzondere persoonsgegevens in het sociaal domein, zoals bijvoorbeeld het strafrechtelijk verleden, medische indicatie of behandelingstraject van een burger, dan kunnen deze gegevens door de hacker opzettelijk openbaar worden gemaakt. Of de hacker kan de gedupeerde burgers hiermee chanteren.
- De gevolgen van bovenstaande voorbeelden kunnen zijn dat burgers terughoudend worden met het vragen van hulp of het delen van informatie met de gemeente doordat hun privacy is geschaad.
- Als een hacker toegang verkrijgt tot de basisregistratie personen kunnen bijvoorbeeld geboortedata worden aangepast, zodat iemand eerder AOW krijgt. Of iemand kan aangifte doen van de geboorte van meerdere kinderen om zo een hogere kinderbijslag te ontvangen.
- Ook kan een datalek dat het gevolg is van onvoldoende beveiligingsmaatregelen leiden tot een boete van de Autoriteit Persoonsgegevens.

Voor de uitvoering van de testen heeft de rekenkamer gebruikgemaakt van een extern, gespecialiseerd, bureau. Omdat de werkzaamheden – hacks – formeel gezien strafbaar zijn, is tussen de gemeente, dit bureau en de Rekenkamer Lansingerland een vrijwaringsovereenkomst getekend. Daarmee heeft de gemeente toestemming voor de hacks gegeven. Van de zijde van het ingehuurde bureau en de rekenkamer gold onder meer de verplichting de gemeentelijke informatiesystemen niet te ondermijnen en eventueel ontdekte cruciale beveiligingslekken meteen bij de Teamleider Informatievoorziening & Automatisering van de gemeente Lansingerland te melden.

Van de penetratietesten die de rekenkamer heeft laten uitvoeren is een gedetailleerde rapportage gemaakt. Deze rapportage bevat de technische bevindingen die laten zien hoe al dan niet toegang kan worden verkregen tot de gemeentelijke informatiesystemen. Omdat dit gevoelige informatie betreft, is de rapportage als vertrouwelijk aangemerkt. Deze vertrouwelijke rapportage maakt geen onderdeel uit van het openbare rapport van de rekenkamer. De vertrouwelijke rapportage, die ook technische aanbevelingen voor verbetering bevat, is wel toegezonden aan de gemeente.

In dit hoofdstuk wordt een beeld geschetst van de bevindingen uit de testen. Daarbij wordt in algemene zin een indruk gegeven van de aard van de bevindingen, het daarbij behorende risico en de mogelijke consequenties.

4-2 resultaten externe penetratietest

Het is niet gelukt om binnen de beschikbare tijd van twee dagen via het internet binnen te dringen in systemen van de gemeente Lansingerland. Wel zijn er kwetsbaarheden geconstateerd die aanvallers, die meer tijd tot hun beschikking hebben, in staat stellen om de informatiesystemen van de gemeente binnen te dringen. Bijvoorbeeld door via het internet een self service portaal te benutten om een eigen apparaat toe te voegen en de beheer console te benaderen. Ook zijn er verouderde Javascript bibliotheken aangetroffen met kwetsbaarheden die mogelijk in de toekomst misbruikt kunnen worden. Verder bestaat de kans dat via valse links het uiterlijk van de gemeentelijke website te veranderen is, zodat bezoekers van de website verleid worden een valse link te bezoeken. Vervolgens kan bijvoorbeeld malware worden geïnstalleerd op de computer van de bezoeker.

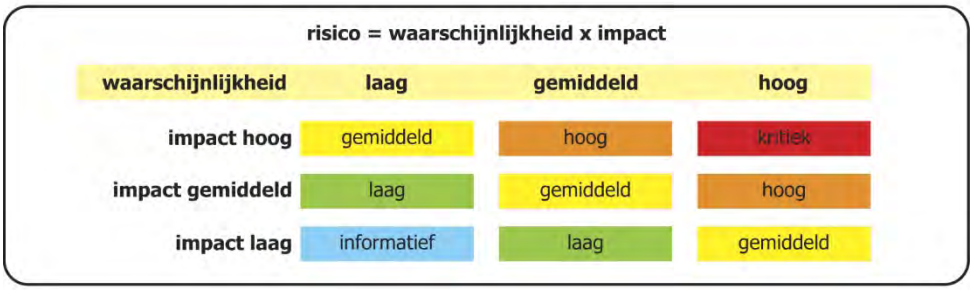
Bij de externe penetratietest is geprobeerd zonder voorkennis via het internet toegang te verkrijgen tot systemen van de gemeente Lansingerland. Omdat zonder voorkennis niet alle systemen en netwerken betrouwbaar gedetecteerd kunnen worden zijn de resultaten mogelijk onvolledig. Binnen de beschikbare tijd van twee dagen is het niet gelukt om deze toegang te verkrijgen. Wel zijn er bij deze externe penetratietest kwetsbaarheden aan het licht gekomen. Tabel 4-1 geeft een overzicht van deze kwetsbaarheden.

tabel 4-1: bevindingen externe penetratietest

kwetsbaarheid	risico
een self service portaal is toegankelijk vanaf internet	gemiddeld
verouderde Javascript bibliotheken	gemiddeld
Cross-Site Scripting aangetroffen	gemiddeld
metadata aangetroffen	laag

Figuur 4-1 licht de verschillende risiconiveaus (laag-gemiddeld-hoog-kritiek) toe die van toepassing zijn op de verschillende kwetsbaarheden die aan het licht zijn gekomen. Hierin wordt geïllustreerd dat bij een kritiek risico zowel de waarschijnlijkheid dat een kwetsbaarheid zal worden uitgebuit, als de impact daarvan (in termen van schade), zijn ingeschat op hoog.

Figuur 4-1 risiconiveaus gedetecteerde kwetsbaarheden



Hierna worden de verschillende geconstateerde kwetsbaarheden[93] nader toegelicht.

een self service portaal is toegankelijk vanaf internet (gemiddeld risico)
Een self service portaal is vanaf het internet benaderbaar. Dit houdt in dat in het geval van een geslaagde (spear, voice of e-mail) phishing actie een kwaadwillende kan inloggen op deze self service portaal en een eigen apparaat kan toevoegen. Daarnaast is de beheer console, de computer waarop de toegang tot het netwerk wordt geregeld, benaderbaar vanaf het internet. Via deze portaal kunnen hackers nieuwe devices configureren. In potentie kunnen hackers hiermee oneigenlijk toegang krijgen tot het netwerk.

verouderde Javascript bibliotheken (gemiddeld risico)
Er is een tweetal verouderde Javascript bibliotheken op de gemeentelijke website aangetroffen. Beide bibliotheken bevatten kwetsbaarheden, die door kwaadwillenden mogelijk in de toekomst kunnen worden misbruikt, door er malware aan toe te voegen.

Cross-Site Scripting aangetroffen (gemiddeld risico)
Op de gemeentelijke website is een zogeheten reflected Cross-Site Scripting als kwetsbaarheid aangetroffen. Het is dan mogelijk het uiterlijk van de website te veranderen door bijvoorbeeld valse login schermen op te zetten op de website of kwaadaardige scripts uit te voeren. Zo kunnen kwaadwillenden betrouwbaar ogende phishing aanvallen opzetten en bezoekers van de website verleiden een valse link te bezoeken waarmee vervolgens bijvoorbeeld malware geïnstalleerd kan worden op de computer van de bezoeker.

93 De kwetsbaarheden met risico gemiddeld zijn gemeld aan betreffende leveranciers. De cross-site scripting bevinding is volgens de leverancier verholpen. De gemeente heeft dit niet kunnen vaststellen omdat deze bevindingen voor ons niet reproduceerbaar zijn.

metadata aangetroffen (laag risico)
Via het downloaden van vijfhonderd PDF-documenten van de gemeentelijke website zijn zogeheten metadata gevonden. Metadata zijn gegevens over gegevens zoals bijvoorbeeld softwareversies en gebruikersnamen. Deze gegevens zijn onnodig inzichtelijk en kunnen door kwaadwillenden gebruikt worden voor doelgerichte aanvallen.

4-3 resultaten interne penetratietest

Uit de interne penetratietest kwamen drie tekortkomingen met een hoog risico en twee met een gemiddeld risico naar voren. Een tekortkoming met een hoog risico is dat het administrator wachtwoord op veel systemen identiek is. Doordat de harde schijven van werkstations niet zijn versleuteld, bleek het mogelijk dit wachtwoord te achterhalen. Hierdoor werd toegang verkregen tot nagenoeg alle applicaties, inclusief ICT-applicaties met bijzondere persoonsgegevens in het sociale domein. Deze gegevens kunnen dan worden geraadpleegd, gewijzigd of verwijderd. Verder bleek een aantal applicaties verouderd, waarbij de beschikbare beveiligingsupdates niet waren toegepast. Hierdoor kon toegang worden verkregen tot twee systemen. Een tekortkoming met een gemiddeld risico is het ontbreken van netwerkauthenticatie. Ook zijn de systemen voor klimaatcontrole en noodstroomvoorzieningen onnodig toegankelijk vanaf het netwerk.

Voor de uitvoering van de interne penetratietest had het externe bureau tijdelijke werkplekken met netwerkaansluiting in het gemeentehuis gekregen. In tabel 4-2 is een overzicht van de gevonden tekortkomingen opgenomen.

tabel 4-2: bevindingen interne penetratietest

kwetsbaarheid	risico
misbruik van beheer wachtwoord	hoog
niet versleutelde werkstations	hoog
ontbrekende beveiligingsupdates	hoog
geen netwerkauthenticatie	gemiddeld
apparaten onnodig benaderbaar	gemiddeld

Hierna worden de vijf geconstateerde tekortkomingen nader toegelicht.

misbruik van beheer wachtwoord (hoog risico)
Het bleek dat het lokale Administator wachtwoord op veel systemen identiek was. Door met dit account vanaf het netwerk in te loggen, heeft het externe bureau via het werkstation van een beheerder volledige toegang gekregen tot Active Directory met beheerrechten door een achterhaalde beheer wachtwoord.[94] Om dit wachtwoord te kunnen achterhalen was fysieke toegang tot een werkstation nodig. Er is gebruik gemaakt van een bekende Windows kwetsbaarheid waarbij hashes van wachtwoorden op de lokale schijf worden opgeslagen. Hierdoor werden nagenoeg alle Windows systemen, accounts en mappen toegankelijk. Door de verkregen

94 Dit is overigens na 1,5 dag gelukt door het externe bureau, wat relatief lang duurde. In de tussentijd werd volgens de gemeente geregistreerd dat pogingen tot inbraak werden ondernomen. Bron: ambtelijke reactie, 13 november 2017.

beheerrechten kan een kwaadwillende zich ook toegang verschaffen tot applicaties in het sociale domein. Dit betekent dus ook ongeautoriseerde toegang tot de bijzondere persoonsgegevens in GWS en Corsa met kans op het kopiëren, wijzigen en verminken van de aanwezige data tot gevolg. Dit geldt niet direct voor SAAS-software zoals S4SR, dat wordt beheerd door Centric.

niet versleutelde werkstations (hoog risico)
De harde schijf van de werkstations is niet versleuteld, waardoor toegang wordt verkregen tot het bestandssysteem en het 'versleutelde' Administrator wachtwoord. Doordat de harde schijven niet versleuteld zijn bestaat het risico op manipulatie van het bestandssysteem en toegang tot het bestandssysteem bij bijvoorbeeld diefstal en/of verlies.

ontbrekende beveiligingsupdates (hoog risico)
Verouderde besturingssystemen en applicaties bevatten vaak kwetsbaarheden doordat beveiligingsupdates ontbreken. In het kader van de test is een scan gemaakt van ontbrekende beveiligingsupdates bij specifieke systemen of applicaties. Er zijn daarbij 1.876 kwetsbaarheden gedetecteerd, waarvan 20 kritiek, 16 hoog, 1.367 medium en 473 met een lage kwetsbaarheidsgraad. Het gaat om 316 unieke kwetsbaarheden, waarvan 8 kritiek en 5 hoog. Het bleek mogelijk om ongeautoriseerde toegang te verkrijgen tot een tweetal systemen doordat beschikbare beveiligingsupdates ontbraken.[95]

Het aantal (unieke) kwetsbaarheden is laag in verhouding tot andere gemeenten waar het externe bureau testen heeft uitgevoerd, waaronder Dordrecht, Breda, Barneveld, Leusden, Haarlemmermeer en Den Helder. Het beheer van updates ('patchmanagement') is in Lansingerland beter op orde. Een één-op-één vergelijking met specifieke andere gemeenten gaat echter mank. Dat het aantal kwetsbaarheden laag ligt, hangt namelijk deels samen met het relatief kleine aantal applicaties dat Lansingerland in beheer heeft en de daarmee samenhangende lagere beheerslasten. Door het lage aantal kwetsbaarheden kostte het de onderzoekers van het externe bureau wel, in verhouding tot de andere gemeenten waar tests zijn uitgevoerd, meer moeite om binnen te dringen in de informatiesystemen van de gemeente Lansingerland.

geen netwerkauthenticatie (gemiddeld risico)
Als sprake is van netwerkauthenticatie krijgt een gebruiker pas toegang tot het bekabelde netwerk nadat de gebruiker is ingelogd. Hiervan wordt binnen de gemeente geen gebruik gemaakt. Hierdoor is het mogelijk om via fysieke toegang tot een netwerkpoort eenvoudig een IP adres te verkrijgen. Kwaadwillenden kunnen dan op deze wijze verkennende scans uitvoeren en zwakheden in kaart brengen en/of misbruiken.

apparaten onnodig benaderbaar (gemiddeld risico)
Een tweetal systemen is onnodig toegankelijk vanuit het deel van het netwerk waar de werkstations zich bevinden die beschikbaar zijn gesteld voor het externe bureau. Dit betreft de systemen voor klimaatcontrole en noodstroomvoorzieningen.

95 In de ambtelijke reactie op deze rapportage heeft de gemeente opmerkt dat het hierbij gaat om twee systemen die niet in beheer van de gemeente zijn. De leveranciers zijn op de hoogte gesteld.

Kwaadwillenden kunnen met netwerktoegang deze systemen manipuleren en de dagelijkse gang in het gebouw ontwrichten.

4-4 resultaten social engineering test

Het bewustzijn met betrekking tot informatieveiligheid van medewerkers van de gemeente schiet te kort. Drie van de vijf benaderde medewerkers probeerden de kwaadaardige bijlagen van zogeheten spear phishing e-mails te openen, ondanks een beveiligingswaarschuwing. Bij voice phishing was het mogelijk om geldige logincombinaties van alle vijf benaderde medewerkers te achterhalen waarmee toegang tot hun systeemaccounts kon worden verkregen. Hierdoor is het mogelijk om toegang te krijgen tot bijvoorbeeld (bijzondere) persoonsgegevens in de ICT applicatie Corsa, Outlook en andere applicaties waarvoor geen extra wachtwoord nodig is.

Het bleek relatief eenvoudig om ongeautoriseerd toegang te krijgen tot het gemeentelijk pand. Eenmaal binnen was er vrije toegang tot diverse ruimtes en aanwezige (vertrouwelijke) informatie.

De social engineering test bestond uit drie componenten: spear phishing e-mails, voice phishing en een inlooptest. In tabel 4-3 geeft de resultaten van deze testen weer.

tabel 4-3: bevindingen social engineering test

kwetsbaarheid	risico
spear phishing mails	gemiddeld
voice phishing	hoog
inlooptest	hoog

Hierna worden per onderdeel de bevindingen toegelicht.

spear phishing mails

Er zijn vijf gerichte spear phishing e-mails verstuurd waarmee geprobeerd is de ontvangers te verleiden om bijgevoegde kwaadaardige bijlagen te openen. Alle spear phishing mails zijn tegengehouden door het spamfilter van de gemeente, maar omwille van de test zijn deze spear phishing e-mails doorgelaten. De technische beveiligingsmaatregelen waren dus effectief. In het geval dat de spear phishing e-mails kwaadaardige links in plaats van bijlages hadden bevat, dan had het spamfilter ze niet tegengehouden.

In de test hebben drie van de vijf medewerkers de bijlage geprobeerd te openen. De macro's met de malware in de bijlage werden door technische beveiligingsmaatregelen geblokkeerd waardoor deze bestanden niet geopend konden worden. Ondanks een beveiligingswaarschuwing bleek een meerderheid van deze medewerkers gevoelig te zijn voor spear phishing. Het bewustzijn met betrekking tot informatiebeveiliging onder medewerkers schiet op dit punt dus nog te kort.

voice phishing
Via voice phishing wordt getracht via telefonisch contact informatie te verkrijgen. In de test zijn vijf voice phishing telefoontjes gepleegd naar willekeurige medewerkers binnen de gemeente. Op deze manier zijn vijf geldige logincombinaties achterhaald die misbruikt hadden kunnen worden. Het was mogelijk om toegang te verkrijgen tot de systeemaccounts van deze medewerkers. Als deze medewerkers werkzaam waren in het sociale domein, dan was ook toegang mogelijk geweest tot de applicaties in het sociale domein. Hierdoor was bijvoorbeeld directe toegang tot Corsa mogelijk omdat daar het single sign-on wachtwoordbeleid geldt: als je inlogt in het systeem ben je ook automatisch ingelogd in Corsa. Om toegang te krijgen tot de applicaties GWS en S4SR is dan nog een aanvullend ander wachtwoord nodig. De medewerkers bleken gevoelig te zijn voor voice phishing. Enkele medewerkers die hun login-gegevens hadden verstrekt, hebben naderhand bij hun leidinggevende aangegeven de situatie toch niet te vertrouwen. Op dat moment was echter al reeds toegang verleend tot de systeemaccount. Het bewustzijn met betrekking tot informatiebeveiliging onder medewerkers schiet ook op dit punt dus nog te kort.

inlooptest
Bij de inlooptest was het de onderzoeker van het externe bureau gelukt om, zonder pas, toegang te krijgen tot werkplekken van ambtenaren. Hierbij worden verschillende tactieken gebruikt, bijvoorbeeld achter medewerkers naar binnen lopen ('tailgating') of bij een deur wachten tot een medewerker naar buiten komt en dan naar binnen gaan. Er is één keer gevraagd of de onderzoeker geen toegangspasje bij zich had, maar verder kon hij zich vrij door het pand bewegen. De sociale controle van medewerkers op elkaar schoot dus nog te kort. Het was mogelijk om bedrijfseigendommen of documenten te ontvreemden en toegang tot het netwerk trachten te verkrijgen in de ruimtes waar de onderzoeker ongeauthoriseerd toegang had verkregen. In één van de ruimtes waar de onderzoeker kwam had hij een reeds aanwezige USB-stick aangetroffen. Hij heeft deze niet onderzocht en laten liggen. Door tevens gebruik te maken van de geconstateerde gebreken in de interne penetratietest en de voice phishing en spear phishing test had een kwaadwillende toegang kunnen krijgen tot ICT applicaties met bijzondere persoonsgegevens, die gebruikt worden in het sociaal domein. Anderzijds is tijdens de test niet gebleken dat medewerkers gevoelige materialen, zoals hardcopy dossiers met persoonsgegevens onbeheerd op hun bureau hadden laten liggen of hun computers onvergrendeld hadden achtergelaten.

4-5 totaalbeeld penetratietesten

Met de interne en externe penetratietest, de social engineering test heeft de Rekenkamer Lansingerland zicht gekregen op de effectiviteit van het IB-beleid van de gemeente Lansingerland. Het kostte relatief meer moeite om binnen te dringen in de informatiesystemen van de gemeente dan bij andere gemeenten. De technische beveiligingsmaatregelen zijn relatief goed op orde in Lansingerland; het aantal technische kwetsbaarheden als gevolg van verouderde software is laag. Dit komt door het goede beheer van updates (patchmanagement) en gedeeltelijk door het kleinere aantal applicaties dat Lansingerland gebruikt in verhouding tot grotere gemeenten, waardoor dezelfde kwetsbaarheid zich minder vaak voordoet. Ook de lagere beheerslasten met betrekking tot informatiebeveiliging kunnen een rol hebben gespeeld.

Ondanks dat het aantal technische kwetsbaarheden relatief laag ligt, is het nog eenvoudig om toegang te verkrijgen tot de informatiesystemen waarin bijzondere persoonsgegevens zijn opgeslagen. De gevolgen van deze oneigenlijke toegang kunnen zeer groot zijn.

Uit de voice phishing en spear phishing test blijkt dat het bewustzijn met betrekking tot informatieveiligheid nog te kort schiet. Hierdoor kan, zelfs wanneer de technische beveiligingsmaatregelen optimaal zijn, toch toegang worden verkregen tot informatiesystemen met bijzondere persoonsgegevens. Daarnaast is er onvoldoende sociale controle; zo werd de onbevoegde onderzoeker slechts één keer aangesproken door medewerkers van de gemeente. Dit alles maakt dat het voor kwaadwillenden relatief eenvoudig is om in de digitale systemen van de gemeente te komen.

Tot op heden hebben zich nog geen cyber-incidenten met grote maatschappelijke gevolgen voorgedaan in Lansingerland. De kans dat zo'n incident zich ook in Lansingerland zal gaan voordoen is echter reëel. Er hebben zich namelijk sinds 1 januari 2016 reeds acht datalekken voorgedaan, die ook zijn gemeld bij de Autoriteit Persoonsgegevens en elf beveiligingsincidenten die niet zijn gemeld, waarvan één betrekking heeft op het sociaal domein. Het gaat hierbij voornamelijk om menselijke fouten, waarbij persoonsgegevens per ongeluk zijn verspreid, en diefstal van laptops of tablets.[96]

Menselijke fouten zijn weliswaar niet uit te sluiten, maar met de huidige staat van de informatiebeveiliging en met name het bewustzijn van medewerkers met betrekking tot informatieveiligheid is de gemeente Lansingerland nog niet voldoende weerbaar tegen misbruik of oneigenlijk gebruik van persoonsgegevens.

96 Gemeente Lansingerland, 'Overzicht meldingen datalekken bij Autoriteit Persoonsgegevens' en 'Overzicht datalekken geen melding bij de Autoriteit Persoonsgegevens', ontvangen op 27 september 2017.

bijlagen

bijlage 1 onderzoeksverantwoording

inleiding
Het onderzoek naar informatiebeveiliging Lansingerland is uitgevoerd in de periode van juli 2017 tot en met medio oktober 2017. Het rapport is gebaseerd op een documentstudie, interviews met betrokken ambtenaren van de gemeente, een nadere beoordeling van de beveiliging van drie belangrijke applicaties waarin persoonsgegevens worden verwerkt en een ethical hack.

documentstudie
De rekenkamer heeft onder meer de volgende documenten geraadpleegd:
- documenten die inzicht geven in het beleid van de gemeente op het terrein van informatiebeveiliging;
- rapportages van onderzoeken en penetratietesten die eerder in opdracht van de gemeente zijn uitgevoerd;
- documenten die inzicht geven in de staat van informatiebeveiliging van de drie onderzochte applicaties.

In bijlage 2 staan de documenten opgesomd die in dit rapport staan genoemd.

interviews
De rekenkamer heeft met diverse personen binnen en buiten de gemeente Lansingerland gesproken of per e-mail contact gehad.

Binnen de gemeente Lansingerland is gesproken met:
- drie teamleiders van de afdeling Economische en Maatschappelijke ontwikkeling;
- de controller informatiebeveiliging;
- een applicatiebeheerder;
- de teamleider informatievoorziening en automatisering;
- de projectleider implementatie BIG;

analyse applicaties
De rekenkamer heeft drie applicaties geselecteerd waarin veel persoonsgegevens omgaan en de staat van informatiebeveiliging bij deze applicaties nader onderzocht. De rekenkamer heeft in dit verband gesprekken gevoerd met de systeemeigenaren en een beheerder van deze applicaties. Ook heeft de rekenkamer screenshots van instellingen van het technische beheer en documentatie over de onderzochte applicaties geanalyseerd.

ethical hack
De rekenkamer heeft door een gespecialiseerd bureau een ethical hack laten uitvoeren. Ten eerste is een externe penetratietest uitgevoerd. Daarbij is geprobeerd vanuit een niet-gemeentelijke locatie via internet in de gemeentelijke informatiesystemen door te dringen. Ten tweede is een interne penetratietest uitgevoerd, waarbij vanuit een gemeentelijke locatie (een werkruimte, vergaderzaal) geprobeerd is oneigenlijke toegang te verkrijgen. Ten slotte is een social engineering test gedaan, waarin de “awareness” van medewerkers is getoetst. De social

engineering test bestond uit een inlooptest, het versturen van spear phishing-mails en voice phishing.

procedures
De opzet van het onderzoek is op 20 juli 2017 ter kennisname aan de raad verstuurd. De voorlopige onderzoeksresultaten zijn opgenomen in een concept nota van bevindingen. Deze is op 30 oktober 2017 voor ambtelijk wederhoor voorgelegd. Na verwerking van de op 13 november 2017 ontvangen ambtelijke reactie is een bestuurlijke nota opgesteld. Deze omvat de voornaamste conclusies en aanbevelingen van de rekenkamer. De bestuurlijke nota, met de nota van bevindingen als bijlage, is op XX november 2017 voor bestuurlijk wederhoor voorgelegd aan het college van B en W. Op @@@ heeft de rekenkamer de reactie van het college van B en W ontvangen. De reactie van B en W en het nawoord van de rekenkamer zijn opgenomen in het rapport. Het definitieve rapport wordt door toezending aan de gemeenteraad en B en W openbaar.

bijlage 2 geraadpleegde documenten

In deze bijlage staan de aangehaalde documenten opgesomd, die zijn geraadpleegd voor dit rapport. Dat neemt niet weg dat voor het onderzoek ook andere hier niet aangehaalde bronnen zijn gebruikt, waaronder inzage in vertrouwelijke documenten.

gemeentelijke documenten

- College van B en W, 'Gemeente breed informatiebeveiligingsbeleid', vastgesteld op 26 mei 2015.
- College van B en W, 'gedragscode integriteit medewerkers', januari 2008.
- College van B en W, 'beschikking tot verlening van subsidie 2015 Stichting CJG Rijnmond', 4 februari 2015.
- College van B en W, 'Privacy reglement e-mail, internet en telefoongebruik Lansingerland 2012', 15 augustus 2012.
- Gemeente Lansingerland, 'Actieplan informatieveiligheid, overzicht van de verbeteracties voor 2017/2018', juni 2017.
- Gemeente Lansingerland, 'Bewerkersovereenkomst GGZ Delfland uitvoering generalistische basis jeugdggz en/of ernstig enkelvoudige dyslexiezorg', 17 november 2016.
- Gemeente Lansingerland, 'Bewerkersovereenkomst Regionaal Instituut voor Ontwikkelingsproblemen B.V., uitvoering generalistische basis jeugd-ggz en/of en/of ernstig enkelvoudige dyslexiezorg', 16 november 2016.
- Gemeente Lansingerland, 'Conceptprocedure voor de melding van incidenten', ontvangen op 23 augustus 2017.
- Gemeente Lansingerland, 'Dataclassificatie 2017', ontvangen op 23 augustus 2017.
- Gemeente Lansingerland, 'Gap analyse mei 2017', ontvangen op 10 juli 2017.
- Gemeente Lansingerland, 'Handboek Sluitende Aanpak kwetsbare personen Lansingerland Versie 1.0', 13 februari 2014.
- Gemeente Lansingerland, 'Hoe werkt het in het nieuwe gemeentehuis', 22 augustus 2012.
- Gemeente Lansingerland, 'Informatiebeveiligingsplan', 28 november 2015.
- Gemeente Lansingerland, 'Informatieveiligheidsanalyse Mei 2017', juni 2017.
- Gemeente Lansingerland, 'Jaarrapportage sociaal domein 2016, bijlage cijfermatige rapportage', 2 juni 2017.
- Gemeente Lansingerland, 'Memo autorisatieproces S4SR' inclusief Autorisatieformulier Suite voor sociale regie medewerkers, autorisatiematrix en procedure aanvraag/intrekken autorisatie S4SR, 25 juni 2015.
- Gemeente Lansingerland, 'Overzicht datalekken geen melding bij de Autoriteit Persoonsgegevens', ontvangen op 27 september 2017.
- Gemeente Lansingerland, 'Overzicht meldingen datalekken bij Autoriteit Persoonsgegevens', ontvangen op 27 september 2017.
- Gemeente Lansingerland, 'Overzicht verwerkersovereenkomst', ontvangen op 4 oktober 2017.
- Gemeente Lansingerland, 'Plan van aanpak informatiebeveiliging, overzicht van de verbeteracties 2015/2016', 28 november 2015.
- Gemeente Lansingerland, presentatie 'Procesafspraken S4SR', 12 november 2015.
- Gemeente Lansingerland, presentatie 'Wat heb jij te verbergen', januari 2017.

- Gemeente Lansingerland, Privacy Protocol Sociaal Domein Lansingerland, 16 december 2014.
- Gemeente Lansingerland, 'Register Lansingerland april 2016', ontvangen in het voorjaar van 2016.
- Gemeente Lansingerland, 'Situatie back-up en uitwijk gemeente Lansingerland', 29 augustus 2017.
- Gemeente Lansingerland, 'Training privacy in het sociaal domein', 25 november en 2 december 2014.
- Gemeente Lansingerland, 'Uitwijk en disaster recovery document', 13 januari 2017.
Gemeente Lansingerland, 'Uitwijktest december 2016 versie 2.0', 2 januari 2017.

overige documenten

- Autoriteit Persoonsgegevens, 'Richtsnoeren beveiliging persoonsgegevens', februari 2013.
- Beroepsvereniging van professionals in sociaal werk, 'Beroepscode voor de Jeugdzorgwerker', 2015.
- Committee of Sponsoring Organizations of the Treadway Commission, 'Risico management van de onderneming. Geïntegreerd raamwerk Enterprise Risk Management Integrated Framework (ERM)', 2014.
- Centric, 'Nader overeenkomst SAAS- Suite voor sociale regie', versie 1.0, 2 maart 2017.
- Centric, 'Releasedocumentatie GWS4all versie 17', 1 november 2013.
- Centric, 'Service Level Agreement Suite voor sociale regie', versie 1.3, 3 maart 2017.
- Centric, 'Suitevoorsocialeregie Accounts en Wachtwoorden', 2016.
- Informatiebeveiligingsdienst, 'Baselinetoets', juni 2014.
- Informatiebeveiligingsdienst, 'Diepgaande risicoanalyse methode gemeenten', augustus 2014.
- Informatiebeveiligingsdienst, 'Implementatie BIG', augustus 2016.
- Informatiebeveiligingsdienst, 'Handreiking dataclassificatie', augustus 2016.
- Informatiebeveiligingsdienst, 'Tactische baseline informatiebeveiliging Nederlandse gemeenten', 27 juli 2015.
- Rekenkamer Lansingerland, 'In de groei, de toegang tot jeugdhulp in Lansingerland', 23 februari 2017.
- Rekenkamer Lansingerland, 'Notiebrief informatiebeveiliging', 3 oktober 2016.
- VNG, resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente', aangenomen op 29 november 2013.

websites

- Autoriteit Persoonsgegevens.
www.autoriteitpersoonsgegevens.nl/nl/melden/melden-verwerking-persoonsgegevens, geraadpleegd op 21 augustus 2017.
www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/data-protection-impact-assessment-dpia. Geraadpleegd op 23 oktober 2017.

bijlage 3 lijst met begrippen

back-up	een veiligheidskopie van programma`s en data
persoonsgegevens	elk gegeven dat te herleiden is tot een persoon
bijzondere persoons-gegevens	BSN-nummers en gegevens m.b.t. ras, godsdienst, politieke voorkeur, gezondheid, seksueel leven, lidmaatschap van vakbond en strafrechtelijk verleden
comply or explain	pas toe of leg uit
cross-site scripting	een fout in de beveiliging van een webapplicatie
cybercrime	criminaliteit op of via het internet
datalek	wanneer (persoons)gegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben
hacken	illegaal inbreken op computers
logging	het bijhouden van loggegevens
penetratietest	onderzoek naar kwetsbaarheden in computersystemen
social engineering	een persoon verleiden om informatie vrij te geven die in principe niet toegankelijk zijn voor derden

bijlage 4 implementatie BIG

Voor de implementatie van de BIG adviseert de Informatiebeveiligingsdienst van de VNG een aantal stappen te doorlopen. Deze worden toegelicht in het tactische deel van de BIG[97] en een aantal handreikingen.[98] De stappen worden getoond in figuur A.

Figuur 4-2 implementatie BIG

bron: tactische baseline informatiebeveiliging Nederlandse gemeenten

Allereerst dient een baselinetoets te worden uitgevoerd, waarmee per informatiesysteem en proces kan worden bepaald of het beveiligingsniveau dat wordt geboden door de maatregelen uit de BIG, volstaat. Voor het uitvoeren van de baselinetoets is een instructie beschikbaar. Voor drie aspecten van informatiebeveiliging, namelijk beschikbaarheid, integriteit en vertrouwelijkheid, wordt een puntenscore bepaalt op basis van zeven vragen per onderdeel. Wanneer de baselinetoets resulteert in een bepaalde score, volstaat het niveau van de beveiligingsniveau dat de BIG biedt. Daarboven zijn aanvullende beveiligingsmaatregelen nodig om voldoende bescherming te bieden. Het is dan verstandig om eerst een diepgaande risicoanalyse uit te voeren. Wanneer één of meerdere keren een twee of hoger is ingevuld bij beschikbaarheid en één of meerdere keren een drie of hoger bij integriteit of vertrouwelijkheid, moet ook een diepgaande risicoanalyse worden uitgevoerd om het gewenste niveau van beveiliging te bepalen. Als alternatief voor een baselinetoets, kan een dataclassificatie worden uitgevoerd, waarbij niet het beveiligingsniveau van de informatiesystemen, maar die van data die daarin wordt verwerkt wordt beoordeeld. Hiervoor wordt een vergelijkbaar proces gevolgd met vragenlijsten en puntentelling.[99]

In de handreiking 'Diepgaande risicoanalyse methode gemeenten' van de IBD wordt toegelicht hoe deze analyse in zijn werk gaat. Er worden drie stappen doorlopen:

- Het in kaart brengen van het informatiesysteem, waarvoor de IBD het MAPGOOD-model[100] aanraadt;
- Het inventariseren en classificeren (Laag, Medium, Hoog) van dreigingen, waarbij nog geen rekening is gehouden met beveiligingsmaatregelen;
- Het vertalen van dreigingen naar maatregelen.

97 Informatiebeveiligingsdienst, 'Tactische baseline informatiebeveiliging Nederlandse gemeenten', 27 juli 2015.

98 Onder andere Informatiebeveiligingsdienst, 'Implementatie BIG', augustus 2016; Informatiebeveiligingsdienst, 'Baselinetoets', juni 2014; Informatiebeveiligingsdienst, 'Diepgaande risicoanalyse methode gemeenten', augustus 2014.

99 Informatiebeveiligingsdienst, 'Handreiking dataclassificatie', augustus 2016.

100 MAPGOOD staat voor Mens, Apparatuur, Programmatuur, Gegevens, Organisatie, Omgeving en Diensten.

Nadat zodoende duidelijk is geworden welke beveiligingsmaatregelen passen bij het beveiligingsniveau per informatiesysteem of proces, wordt een GAP-analyse uitgevoerd. Hierbij wordt gekeken welke maatregelen van de BIG zijn geïmplementeerd en welke niet (of niet volledig). Hiervoor heeft de IBD een spreadsheet gemaakt, waarin alle maatregelen uit de BIG zijn opgenomen. Als de spreadsheet is ingevuld, kan in een diagram zichtbaar worden gemaakt welke maatregelen nog ontbreken.

Vervolgens worden op een aantal quick wins geïdentificeerd en een impactanalyse uitgevoerd om te bepalen in welke volgorde de overige te implementeren maatregelen dienen te worden doorgevoerd. Hierbij wordt onder andere rekening gehouden met de beschikbare tijd en budget, technologische ontwikkelingen of uitbesteding en samenwerking met andere partijen. De gemeente kan ook expliciet besluiten het risico van bepaalde niet geïmplementeerde maatregelen te accepteren of zich daarvoor te verzekeren.

Ten slotte besluit het management over de te prioritering van maatregelen en worden de maatregelen onderdeel van het informatiebeveiligingsplan, de uitvoering en de verantwoordingsinformatie.

bijlage 5 lijst met afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BAG	Basisadministratie Adressen en Gebouwen
BIG	Baseline Informatiebeveiliging Gemeenten
BRP	Basisregistratie personen
BSN	Burger Service Nummer
CISO	Chief information security officer
ENSIA	Eenduidige Normatiek Single Information Audit
FG	Functionaris Gegevensbescherming
GBA	Gemeentelijke Basis Administratie
IB	Informatiebeveiliging
IBD	Informatie Beveiligingsdienst
ICT	informatie- en communicatietechnologie
ISMS	Information Security Management System
IT	Informatie Technologie
KING	Kwaliteits Instituut Nederlandse Gemeenten
NCSC	Nationaal Cyber Security Centrum
PDCA	Plan-do-check-act
PIA	Privacy Impact Assessment
RI&E	Risico-inventarisatie en evaluatie
SAAS	Software as a service
S4SR	Suite voor sociale regie
SLA	Service level agreement
SUWI	Structuur Uitvoering Werk en Inkomen
TPM	Third party mededeling
VOG	Verklaring Omtrent Gedrag
VNG	Vereniging Nederlandse Gemeenten
Wbp	Wet bescherming persoonsgegevens
Wmo	Wet maatschappelijke ondersteuning
Wob	Wet openbaarheid van bestuur

de rekenkamer

De gemeenteraad van Lansingerland heeft op 24 mei 2007 de Rekenkamer Lansingerland ingesteld. De gemeenteraad benoemde op 28 mei 2009 Paul Hofstra als directeur van de rekenkamer. Hij is zijn werkzaamheden op 2 juni 2009 begonnen.

doel

De rekenkamer onderzoekt de doelmatigheid, de doeltreffendheid en de rechtmatigheid van het beleid, het financieel beheer en de organisatie van het gemeentebestuur. De rapporten van de rekenkamer zijn een aanknopingspunt voor het bestuur om rekenschap af te leggen aan de burgers.

positie

De rekenkamer is een onafhankelijk orgaan binnen de gemeente. Haar taken en bevoegdheden staan in de Gemeentewet en de verordening Rekenkamer Lansingerland. Zij bepaalt zelf wat en hoe zij onderzoekt en waarover zij rapporteert. Wel kunnen de raad en het college van B en W de rekenkamer om een onderzoek verzoeken. De rekenkamer stuurt hen jaarlijks haar onderzoeksplan en jaarverslag toe.

onderzoek

Het onderzoeksterrein strekt zich uit over alle organen (raad, B en W, commissies en burgemeester) en diensten van de gemeente. Ook kan de rekenkamer onderzoek doen bij gemeenschappelijke regelingen waar de gemeente aan deelneemt, bij NV's en BV's waar de gemeente meer dan 50% van de aandelen in bezit heeft en bij instellingen die een grote subsidie, lening of garantie van de gemeente hebben ontvangen. De onderzoeken worden uitgevoerd door het bureau van de rekenkamer.

publicaties

Het onderzoek resulteert in openbare rapporten die ter behandeling aan de raad worden aangeboden. Zij bevatten tevens de reacties van de onderzochte organen en instellingen op de eerder toegezonden voorlopige onderzoeksresultaten, conclusies en aanbevelingen (wederhoor). Bij kleine onderzoeken of studies met een beperkte reikwijdte doen we de onderzochte organen of instellingen en de raad de conclusies in een openbare brief direct ter kennisname toekomen. Ten slotte publiceert de rekenkamer op basis van haar onderzoek ook handreikingen en worden medewerkers aangemoedigd om artikelen te publiceren.

Rekenkamer Lansingerland
Postbus 70012
3000 KP Rotterdam

telefoon
010 . 267 22 42

info@rekenkamer.rotterdam.nl
www.rekenkamer.lansingerland.nl

fotografie
Gemeente Lansingerland
en Leo Huizinga

basisontwerp
DE WERF.com, Zuid-Beijerland

uitgave
Rekenkamer Lansingerland
december 2017

ISBN/EAN
978-90-79683-09-3