Informatieveiligheid provincie Noord-Brabant

Deel I: Bestuurlijk rapport

ZUIDELIJKE REKENKAMER

ZUIDELIJKE
REKENKAMER

Inhoudsopgave

1. Over dit onderzoek

Hoe heeft de provincie Noord-Brabant haar informatiebeveiliging in opzet en praktijk ingericht en welke kwetsbaarheden kent de beveiliging van de vertrouwelijkheid van de informatie in de praktijk? Dat was de vraag waar wij ons onderzoek mee begonnen in de zomer van 2017.

De ruggengraat van elke organisatie is de informatie waar zij over beschikt, vooral in de huidige informatiesamenleving. Het is belangrijk dat die informatie veilig is.

Onder veiligheid van informatie wordt verstaan dat deze vertrouwelijk, integer en beschikbaar is. De Zuidelijke Rekenkamer heeft de afgelopen jaren geregeld conclusies getrokken over de integriteit[1] en beschikbaarheid van de provinciale informatie. Onderbelicht is de vertrouwelijkheid ervan: in hoeverre is de informatie alleen toegankelijk voor degenen die hiertoe ook daadwerkelijk zijn geautoriseerd?

De provincie beschikt over veel informatie waarvan het niet de bedoeling is dat deze ´op straat komt te liggen´. Te denken valt aan bedrijfseconomische gegevens van de provincie zelf en persoonsgegevens van haar medewerkers, alsook gegevens van bedrijven en organisaties waar de provincie een financiële binding mee heeft. Daarnaast is het niet de bedoeling dat derden onbevoegd toegang hebben tot de informatie(systemen) van de provincie en zo het geheugen van de organisatie kunnen herschrijven of de voortgang van lopende projecten beïnvloeden. Inbreuken kunnen leiden tot financiële en/of materiële schade en tot reputatieschade voor de provincie. De kans dat een organisatie of persoon het slachtoffer wordt van een inbreuk, zoals een cyberaanval of hacktivism, is reëel aanwezig.

De afgelopen jaren hebben er regelmatig informatieveiligheidsincidenten plaatsgevonden, te denken valt aan mei 2017 toen vele slachtoffers wereldwijd getroffen werden door de gijzelingssoftware WannaCry, die computers onbruikbaar maakte. Een maand daarop zorgde een wereldwijde hack wederom voor enorm veel schade.

De beheersing van de informatieveiligheidsrisico's, ook wel aangeduid als cybersecurity-risico's, is daarom van groot belang. Informatieveiligheid richt zich op de beheersing van deze risico's ofwel op de bescherming van informatie tegen dreigingen/inbreuken. Indien de informatieveiligheid onvoldoende is gewaarborgd, kunnen er risico's ontstaan bij/voor de uitvoering van provinciale taken en het functioneren van de organisatie.

Om voornoemde redenen heeft de rekenkamer een onderzoek uitgevoerd naar de informatieveiligheid van de provincie Noord-Brabant. Informatieveiligheid wordt bepaald door ten minste de volgende twee zaken:

1. de sterkte van de informatiesystemen (techniek) en
2. het gedrag van degenen die uit hoofde van hun functie toegang hebben tot die systemen.

[1] De rekenkamer hanteert in haar onderzoeken in het algemeen de term 'betrouwbaarheid'. In deze rapportage spreken we van 'integriteit' omdat deze term bij informatieveiligheid gebruikelijk is.

Om informatieveiligheid te waarborgen, wordt gebruik gemaakt van informatiebeveiliging (maatregelen).

Daar 100% veiligheid niet bestaat, is het doel van informatieveiligheid de risico's tot een voor de provincie vastgesteld acceptabel niveau terug te brengen. De maatregelen die daarvoor genomen worden, moeten in verhouding staan tot de grootte van het risico.

Onze drie onderzoeksvragen volgend, hebben we in kaart gebracht hoe de provincie Noord-Brabant haar informatiebeveiliging op dit moment heeft ingericht en op welke onderdelen er ruimte voor verbetering is. Daarbij hebben we ook gekeken naar de mate waarin de *systemen* in de praktijk voor onbevoegden toegankelijk zijn en anderzijds de mate waarin de *medewerkers* in de praktijk handelen op een manier die de informatieveiligheid bewaakt. Hiervoor is een zogenaamde penetratietest uitgevoerd. Deze test vereist specifieke kennis/deskundigheid welke we hebben ingehuurd bij een bureau dat ervaren en gespecialiseerd is in onder andere het uitvoeren van dit soort testen. Daarnaast hebben we gekeken naar hoe Provinciale Staten (PS) zijn betrokken bij en geïnformeerd over de opzet en invulling van informatieveiligheid.

Ons onderzoek richtte zich op de periode vanaf september 2012 (bespreking startnotitie ICT-beleid in de commissie Economische Zaken en Bestuur) tot eind 2017. Voor de beantwoording van de onderzoeksvragen hebben we gegevens verzameld uit documenten en mondelinge interviews met betrokkenen van de provinciale organisatie. Een uitgebreide beschrijving van de onderzoeksopzet en van de onderzoeksresultaten hebben we opgenomen in ons rapport van bevindingen (deel II van deze publicatie). Dit kunt u lezen op de website van de rekenkamer www.zuidelijkerekenkamer.nl. Voorliggend rapport bevat de conclusies en aanbevelingen van de rekenkamer, de reactie van Gedeputeerde Staten (GS) en het nawoord van de rekenkamer. Deze worden in hoofdstuk 2 weergegeven. Daarnaast bevat voorliggend rapport een samenvatting van de bevindingen op basis waarvan de rekenkamer haar conclusies en aanbevelingen heeft geformuleerd. Deze wordt, de onderzoeksvragen volgend, gegeven in hoofdstuk 3 (ingericht op papier), 4 (in de praktijk) en 5 (PS en informatieveiligheid).

Bevoegdheden Provinciale Staten
De conclusies, aanbevelingen en bevindingen van de rekenkamer raken in algemene zin de volgende bevoegdheden van Provinciale Staten: budgetrecht en kaderstellende en controlerende rol.

2. Conclusies en aanbevelingen, reactie Gedeputeerde Staten en nawoord Zuidelijke Rekenkamer

2.1 Conclusies

De rekenkamer concludeert op basis van haar onderzoek dat de provincie Noord-Brabant al een aantal jaren (pro)actief bezig is met het waarborgen van een goede beveiliging van haar informatie. Ze heeft al veel goede stappen gezet. In *opzet* is de informatiebeveiliging voldoende ingericht, maar in de *uitvoering* is de provincie de afgelopen jaren op enkele punten nog wel kwetsbaar gebleken in de beheersing van informatieveiligheidsrisico's. Dit komt voornamelijk doordat kaders, richtlijnen, procedures en andere gemaakte afspraken nog niet altijd worden nageleefd. Gezien de risico's en mogelijke gevolgen van inbreuken op de informatieveiligheid is het dan ook van belang dat de provincie haar proactieve handelen voortzet, zodat informatieveiligheid als vanzelfsprekende voorwaarde wordt gezien in alle geledingen van de provinciale organisatie.

Provinciale Staten zijn de afgelopen jaren grotendeels voldoende, maar niet structureel geïnformeerd over informatieveiligheid.

Uitgebreidere beschrijving van de conclusies

In aansluiting op onze onderzoeksvragen geeft een uitgebreidere beschrijving van bovenstaande conclusies het volgende beeld:

1. De provincie Noord-Brabant heeft in de periode eind 2012 tot eind 2017 duidelijk vooruitgang geboekt in de wijze waarop de informatiebeveiliging in opzet en in de praktijk is ingericht. De informatiebeveiliging is in *opzet* (beoogde invulling) voldoende ingericht. Er zijn kaders en richtlijnen opgesteld, maar er is verbetering mogelijk in de duidelijkheid over de samenhang en in de overzichtelijkheid van het informatiebeleid. Van dit bredere beleid vormt ook informatiebeveiliging een onderdeel. Daarnaast dient het informatiebeveiligingsbeleid geactualiseerd te worden. Op dit moment is de provincie daar overigens al mee bezig.
   De maatregelen omtrent informatiebeveiliging worden voor een groot deel zoals voorgenomen uitgevoerd. In interprovinciaal verband hebben de provincies gezamenlijk een basisambitieniveau gekozen waaraan ze willen voldoen, de Interprovinciale Baseline Informatiebeveiliging (IBI). De provincie Noord-Brabant is hierin verder dan andere provincies. Uit monitoring blijkt dat ze daarbij namelijk tot een van de best presterende provincies behoort. Op het gebied van digitale/technische beveiliging is een inhaalslag gemaakt (techniek, systemen) en het informatieveiligheidsbewustzijn is in de loop der jaren gegroeid (mens). Een aantal zaken blijkt echter nog voor verbetering vatbaar: bij het beheersen van informatieveiligheidsrisico's is de provincie de afgelopen jaren namelijk op enkele punten kwetsbaar gebleken. Dit wordt voornamelijk veroorzaakt doordat kaders, richtlijnen, procedures en andere gemaakte afspraken nog niet altijd worden nageleefd. In een aantal gevallen gebeurt dat onbewust, maar soms ook bewust. Ook wordt er niet genoeg gestuurd op de naleving van de richtlijnen en afspraken.

Het doorzetten van voorgenomen acties en vooral het naleven van afspraken, vraagt aandacht. De provincie zet steeds weer in op verbeteringen, maar deze komen in de praktijk soms langzaam van de grond. Het is hierbij vooral moeilijk gebleken om te sturen op gedrag. Dit is ook lastig, maar het is wel een cruciale factor in het ondervangen van kwetsbaarheden (zie kader).

Een cruciale voorwaarde voor effectieve informatiebeveiliging is dat de gehele organisatie zich bewust is van het belang ervan. Men dient zich gedrag eigen te maken waardoor de informatieveiligheid wordt bewaakt. Informatieveiligheid betreft een proces dat niet vanzelf komt. Het is iets waar je bekwaam in moet worden en wat als vanzelfsprekende voorwaarde moet groeien binnen een organisatie. Een bekend model over bewustwording en leren komt van de hand van Maslow. Hij ziet 'leren' als een patroon waarbinnen vier fases van elkaar onderscheiden kunnen worden. Als we naar de provincie kijken door de bril van het model van Maslow, dan heeft de provincie zich over het geheel genomen reeds ontwikkeld van *onbewust onbekwaam* en *bewust onbekwaam*, naar *bewust bekwaam*. Dit houdt in dat de provincie bezig is met de gewenste competenties eigen te maken om zo 'bekwaam' te worden. Daar dit overall nog geen 'onbewust' of vanzelfsprekend proces is, heeft de provincie *als organisatie* de laatste fase nog niet bereikt. Wel blijkt uit het onderzoek van de rekenkamer dat zij voornemens is acties te blijven ondernemen om de bekwaamheid en onbewustheid/vanzelfsprekendheid verder te vergroten.

2. Dat de provincie kwetsbaar is, is onder andere gebleken uit een penetratietest die de rekenkamer in de tweede helft van 2017 door een extern bureau heeft laten uitvoeren. Hoewel het aantal aangetroffen kwetsbaarheden daarbij *relatief* laag was, is er tijdens de test zowel digitaal als fysiek ongeautoriseerde toegang verkregen tot (vertrouwelijke) informatie waarover de provincie beschikt. Opmerkelijk hierbij is dat enkele soortgelijke typen bevindingen naar voren kwamen als bij de penetratietesten die de provincie zelf in 2014 en begin 2017 liet uitvoeren. Een enkele daarvan had niet opnieuw naar voren moeten zijn gekomen, omdat al afspraken waren gemaakt over het voorkomen daarvan.
3. Provinciale Staten hebben in 2013 kaders vastgesteld voor informatiebeveiliging als onderdeel van het informatiebeleid. Ze zijn daarmee zeer op hoofdlijnen geïnformeerd over de opzet van informatieveiligheid. Over de uitvoering van het informatiebeveiligingsbeleid zijn PS niet via de reguliere planning- en controlcyclus geïnformeerd, zoals was beoogd, maar via enkele onderzoeksrapportages. Via deze documenten zijn PS in de betreffende jaren (2014-2016) voldoende geïnformeerd over de uitvoering. Een uitzondering daarop vormen de financiële middelen/kosten van informatiebeveiliging. Daarover is geen informatie verstrekt. PS hebben met de informatie over de uitvoering inzicht kunnen verkrijgen in zaken die goed gaan en zaken die aandacht behoeven. De aandacht van PS zelf, voor

informatieveiligheid lijkt incidentgedreven. Van een structurele dialoog tussen PS en GS over het onderwerp is dan ook nog geen sprake geweest.

De conclusies worden in onderstaande paragrafen 2.1.1 - 2.1.3 nader onderbouwd.

2.1.1 Beoogde invulling en uitvoering

In de afgelopen jaren heeft de provincie Noord-Brabant verschillende nota's opgesteld, waarin wordt ingegaan op de visie en uitgangspunten van het *informatiebeleid*. Daarnaast heeft ze als verdere invulling daarvan op een lager, tactisch, aggregatieniveau, een specifieke beleidsnota opgesteld voor *informatiebeveiliging*. De rekenkamer constateert dat het niet altijd transparant en duidelijk is wat de samenhang is van de verschillende nota's die afgelopen jaren zijn verschenen. De recentere nota's betreffen op onderdelen actualisaties, maar de oude kaders blijven ook nog geldig. Hierdoor is het niet altijd duidelijk hoe documenten zich tot elkaar verhouden.

Het informatiebeveiligingsbeleid behoeft op enkele punten actualisatie. Zo wordt bijvoorbeeld één van de belangrijk(st)e richtlijnen waaraan de provincie zich in interprovinciaal verband heeft gecommitteerd en welke de basisset van beveiligingsmaatregelen bevat (de IBI) niet genoemd in dit beleidsdocument. Ook is al ruim een jaar sprake van een verouderde beschrijving van de CIO-rol (Chief Information Officer). Ten tijde van het rekenkameronderzoek is aangegeven dat het informatiebeveiligingsbeleid wordt geactualiseerd. Daarnaast zal ook het informatiebeleid worden herijkt in verband met onder andere de inwerkingtreding van de Europese Algemene Verordening Gegevensbescherming (AVG). Deze actualisaties bieden een kans om de samenhang en overzichtelijkheid ten aanzien van het informatiebeleid te verbeteren.

Informatiebeveiliging wordt voor een groot deel conform het informatiebeveiligingsbeleid uitgevoerd. Zo heeft de rekenkamer geconstateerd dat de voorgenomen acties uit het informatiebeveiligingsbeleid zijn opgepakt. Enkele voorbeelden daarvan zijn:

- De verantwoordelijkheden zijn vastgelegd en ingevuld.
- In 2014 en begin 2017 zijn beveiligingsonderzoeken (penetratietesten) uitgevoerd.
- Naar aanleiding van deze beveiligingsonderzoeken en andere analyses zijn maatregelen genomen. Hierdoor zijn er onder andere verbeteringen doorgevoerd in de technische beveiliging en zijn er verschillende acties geweest waarmee het bewustzijn en de vaardigheden van medewerkers op punten zijn vergroot.

Uit een interprovinciale monitor blijkt dat de provincie Noord-Brabant wat betreft het voldoen aan de IBI tot de hoogst scorende provincies behoort. Maar de rekenkamer heeft ook geconstateerd dat de uitvoering van het beleid; de uitgevoerde acties en de invulling van de organisatie niet altijd verloopt zoals door de provincie beoogd. Zo zijn er kwetsbaarheden en daarmee aandachtspunten. Enkele voorbeelden zijn:

- Richtlijnen en afspraken worden niet altijd gevolgd. Soms gebeurt dat onbewust, soms bewust bijvoorbeeld omdat de richtlijnen als te lastig of vertragend worden beschouwd. Daarnaast wordt onvoldoende gestuurd op de naleving ervan. Zo wordt informatieveiligheid vaak niet of te laat betrokken bij de uitvoering van werkzaamheden/projecten. Sinds 2014 wordt bijna jaarlijks aandacht gevraagd voor naleving van afspraken.

- Een aantal voorgenomen acties en maatregelen komen in de praktijk vertraagd tot stand. Onder andere veel persoonswisselingen en beperkte capaciteit op belangrijke functies (vele taken bij een zeer beperkt aantal personen) spelen daarbij een rol. Hierbij dient te worden opgemerkt dat in de loop van 2018 invulling wordt gegeven aan een nieuw ingerichte eigenstandige CIO-functie. Daarnaast is de functie beleidsmedewerker informatiebeveiliging opgesplitst in een afzonderlijke Chief Information Security Officer (CISO) en ISO-functie. Ook is er een Functionaris Gegevensbescherming (FG) aangesteld. Door deze wijzigingen is er meer dan twee fte extra beschikbaar.
- Er zijn tot nu toe geen specifieke budgetten beschikbaar of benoemd voor informatieveiligheid.

2.1.2 Penetratietesten

In de periode van 6 juni tot en met 10 oktober 2017 heeft de rekenkamer een zogenaamde penetratietest laten uitvoeren. Daarmee zijn zowel de systemen van de provincie als het gedrag van de medewerkers getoetst. De rekenkamer concludeert dat de provincie daarbij op een aantal punten kwetsbaar is gebleken. Enkele opvallende bevindingen zijn:

- Tijdens de test van het interne netwerk van de provincie zijn beheerdersrechten verkregen waarmee er toegang was tot vrijwel *alle* gegevens en bestanden van de provincie. Zo was het mogelijk om vertrouwelijke informatie in te zien van onder andere de griffie, de directie en de rekenkamer.
- Tijdens de test vanaf het internet is een web shell aangetroffen die sinds januari 2016 aanwezig was (een al gehackt systeem). Een web shell is een ´achterdeurtje´ waarmee de hacker communiceert met, in dit geval, de server en deze bestuurt. Ook kon toegang worden verkregen tot *alle* (provinciale) gegevens waartoe een betreffende medewerker toegang had.
- Bij het testen van het veiligheidsbewustzijn van de provinciemedewerkers is als eerste een phishingaanval uitgevoerd op alle e-mailadressen eindigend op @brabant.nl. Dit waren 1.791 e-mailadressen. De aanval heeft er toe geleid dat 36 ontvangers van de e-mail hun gebruikersnaam en wachtwoord invulden op een, voor dit onderzoek geprepareerde website. Bij de inlooptest heeft de mysteryguest ongeautoriseerde toegang verkregen tot beveiligde gedeelten van het provinciehuis, systemen en vertrouwelijke gegevens (onder andere op de kamer van de medewerkers van burgemeestersbenoemingen in het bestuurdersgedeelte van het provinciehuis).

Op basis van de onmiddellijk gedeelde uitkomsten van de test heeft de provincie adequate maatregelen genomen. Dit geeft aan de ene kant blijk van alertheid en handelend vermogen. Evenwel roepen de uitkomsten van de tests vragen op over het lerend vermogen. In tests die in 2014 en begin 2017 zijn uitgevoerd in opdracht van de provincie zelf, kwamen namelijk op enkele punten soortgelijke typen bevindingen naar voren. Het gaat hierbij ook om bevindingen die in principe al opgelost hadden kunnen zijn, omdat er maatregelen waren genomen (technische beveiliging). Ook blijkt dat het informatieveiligheidsbewustzijn nog verder kan/moet groeien.

2.1.3 PS en informatieveiligheid

Provinciale Staten hebben in 2013 het (nu nog geldende) kader voor ICT-beleid vastgesteld, waar informatiebeveiliging onderdeel van uitmaakt. Ze zijn daarmee op hoofdlijnen geïnformeerd over de opzet van informatieveiligheid. Als nadere uitwerking van het onderdeel informatiebeveiliging uit de kadernota ICT-beleid heeft de provinciale organisatie het informatiebeveiligingsbeleid vastgesteld. Dit is niet aan Provinciale Staten aangeboden.
Via de begrotingen en jaarstukken dienen PS geïnformeerd te worden over het ICT-beleid. Informatie over de stand van zaken ten aanzien van (de uitvoering/ implementatie van) informatieveiligheid is daarin echter zeer beperkt. PS zijn via de evaluatierapportages van de kadernota eind 2014 en eind 2015 en de boardletters 2014 en 2016 van de accountant wel inhoudelijk geïnformeerd over de uitvoering van informatiebeveiliging binnen het ICT-beleid, maar niet over de kosten daarvan. GS achten de informatie uit de jaarlijkse accountantscontrole voldoende om PS te informeren.

De door Gedeputeerde Staten en de accountant in 2014-2016 verstrekte informatie is, voor zover is vast te stellen, niet besproken in PS. PS hebben zelf ICT-beveiliging aangewezen als speerpunt voor de accountantscontrole 2013. Verder hebben statenleden in 2014 en 2017 vragen gesteld over informatieveiligheid, welke vooral gekoppeld waren aan grootschalige beveiligingsincidenten die in dat jaar in onder andere Nederland plaatsvonden. Van een structurele dialoog tussen PS en GS over het onderwerp is nog geen sprake. Najaar 2017 boden GS aan PS aan om een toelichting te geven op informatieveilgheid.
De rekenkamer merkt op dat door de gehanteerde werkwijze van PS in 2016 en 2017 om geen (audio)verslagen te maken van informatie- en platformbijeenkomsten van PS, voor deze bijeenkomsten voor niet-deelnemers onduidelijk blijft wat besproken is en het proces niet geheel herleidbaar is (of er moet navraag worden gedaan bij deelnemers).

2.2 Aanbevelingen

De rekenkamer beveelt Gedeputeerde Staten aan om, gezien de risico’s en mogelijke gevolgen van beveiligingsinbreuken voor de provincie, op de ingeslagen weg verder te gaan en daarbij wat betreft:

- Kaders en richtlijnen: voorkom bij de op handen zijnde actualisatie van het informatie(beveiligings)beleid, zoveel als mogelijk, versplintering over meerdere documenten en geef in de documenten duidelijkheid over de status ervan en de samenhang met andere documenten.
- Uitvoering: zorg voor voldoende continuïteit in de ingevulde verruimde capaciteit, daadwerkelijk en voortvarend doorzetten van voorgenomen (verbeter)acties (waaronder bewustwording, zie paragraaf 4.3 voor aandachtspunten) en strakkere sturing op naleving van kaders, richtlijnen, procedures en werkafspraken.

Provinciale Staten roepen we op, mede met het oog op hun controlerende rol, om alert te blijven op de informatieverstrekking door Gedeputeerde Staten over informatieveiligheid en/of zelf meer structureel aandacht te vragen voor het onderwerp.

Ook bevelen we PS aan om gebruik te maken van het aanbod van Gedeputeerde Staten om een sessie te organiseren voor PS in het kader van bewustwording.

2.3 Reactie Gedeputeerde Staten

We hebben Gedeputeerde Staten van Noord-Brabant gevraagd om een bestuurlijke reactie op ons conceptrapport. Op 4 juli 2018 ontvingen wij onderstaande reactie.

“Op 12 juni 2018 ontvingen wij het concept bestuurlijk rapport ‘Informatieveiligheid provincie Noord Brabant’. In uw onderzoek bent u nagegaan hoe de provincie Noord-Brabant haar informatiebeveiliging in opzet en praktijk heeft ingericht en welke kwetsbaarheden de beveiliging kent. Wij zijn content te lezen dat u concludeert dat de provincie Noord-Brabant al een aantal jaren (pro)actief bezig is met het waarborgen van een goede beveiliging van haar informatie en dat wij vele goede stappen hebben gezet. Het College heeft met veel belangstelling kennis genomen van de conclusies en aanbevelingen en zal hieronder daarop reageren.

Reactie op de conclusies
U concludeert dat wij in de periode eind 2012 tot eind 2017 een duidelijke vooruitgang hebben geboekt in de wijze waarop de informatiebeveiliging in opzet en in de praktijk is ingericht. Wij zijn verheugd met uw constatering dat onze organisatie tot een van de best presterende provincies behoort met betrekking tot de toepassing van het basisbeveiligingsniveau. We zijn er ons terdege van bewust dat we op dit onderwerp nooit klaar zullen zijn en voortdurend alert moeten zijn op actuele ontwikkelingen en tekortkomingen. Wij herkennen dan ook uw conclusie dat er bewustwording en naleving van groot belang is. Daarom hebben we bijvoorbeeld in de week van de integriteit (december 2017) aandacht besteed aan informatieveiligheid en is het voor iedere medewerker verplicht om een 'e-learning module' te doorlopen over informatieveiligheid. Er wordt ook aandacht besteed aan informatiebeveiliging (en data privacy/AVG) tijdens bijeenkomsten voor nieuwe medewerkers. Informatieveiligheid maakt integraal onderdeel uit van het in de perspectiefnota 2018 aangekondigde nieuwe informatiebeleid (in ontwikkeling) waarin al het beleid op het gebied van informatie in samenhang gepresenteerd zal worden. Het opstellen van dit beleid zal als momentum worden benut om (wederom) aandacht te vragen voor het belang van informatieveiligheid om zo de bewustwording en naleving bij iedereen die werkzaam is in onze organisatie te stimuleren. Wij zullen dit soort activiteiten blijven ondernemen om de bekwaamheid en bewustwording/ vanzelfsprekendheid verder te vergroten.

Uw onderzoek heeft een beperkt aantal kwetsbaarheden aan het licht gebracht. De rekenkamer constateert dat 100% veilig niet haalbaar is. Wij vinden elke kwetsbaarheid er een te veel. Omdat ook wij vonden dat sommige bevindingen uit eigen provinciale onderzoeken sneller opgepakt hadden moeten worden, hebben we de sturing en governance op het terrein van informatieveiligheid inmiddels versterkt. Zowel door meer aandacht voor het thema in de directie alsmede door het aantrekken van een onafhankelijke CIO die onlangs is aangetreden.

U constateert dat Provinciale Staten voldoende geïnformeerd zijn over de kaders en de uitvoering van de informatiebeveiliging. Ook wij vinden een structurele dialoog belangrijk. Net als bij integriteit gaat het naast het communiceren van het beleid en uitvoeringsinformatie daarover, over het goede gesprek in het kader van bewustwording

en naleving. We bieden daarom aan om een sessie in het kader van bewustwording niet alleen voor de huidige maar ook voor de toekomstige staten te houden. Tevens bieden wij aan PS de mogelijkheid om gebruik te maken van de e-learning faciliteit om ook hun kennis over informatieveiligheid up-to-date te houden.

Reactie op de aanbevelingen
Wij nemen uw aanbevelingen mee in zowel de actualisatie van het informatiebeleid alsmede in de uitvoering.

Ter afsluiting
We bedanken de rekenkamer voor het onderzoek en daarmee ook hun bijdrage in het bevorderen van het bewustzijn over informatieveiligheid."

2.4 Nawoord Zuidelijke Rekenkamer

Met belangstelling hebben we kennis genomen van de reactie van Gedeputeerde Staten. De rekenkamer constateert met genoegen dat Gedeputeerde Staten zich herkennen in ons rapport. Daar de provincie op punten nog kwetsbaar is gebleken, waarderen we de reeds genomen stappen naar aanleiding van ons onderzoek (blijvende aandacht voor bewustwording, versterking van de sturing (op naleving) en governance, en verdere beheersing van de risico's). Datzelfde geldt voor de toezegging van Gedeputeerde Staten om onze aanbevelingen mee te nemen in zowel de actualisatie als de uitvoering van het informatiebeleid. Wel vraagt de rekenkamer aandacht voor meer structurele informatie richting Provinciale Staten. We zullen de ontwikkelingen op deze gebieden met belangstelling volgen.

Vastgesteld door de Zuidelijke Rekenkamer op 12 juli 2018.

prof. dr. M.J.M. (Marc) Vermeulen
voorzitter

dr. N.A.C. (Ard) Schilder
directeur-secretaris

3. Beleid, kaders en richtlijnen

In dit hoofdstuk geven we een samenvatting van de bevindingen over hoe de provincie Noord-Brabant haar informatiebeveiliging in opzet heeft ingericht (eerste deel van onderzoeksvraag 1).

3.1 Overkoepelend beleid: informatiebeleid

Informatiebeveiliging maakt deel uit van het I(CT)-beleid van de provincie Noord-Brabant. De rekenkamer constateert dat het vigerende *informatiebeleid* beschreven staat in de *Kadernota ICT-beleid 2013-2015* uit 2013 in combinatie met de *nota Digitale Duurzaamheid* uit 2015 en de *Visie en hoofdlijnen informatiebeleid* uit 2016. De kadernota is door PS vastgesteld, de andere twee documenten zijn voor kennisgeving aan PS aangeboden.

Sinds 2012 is op verschillende momenten door verschillende partijen aanbevolen om een strategische visie op informatiebeleid vast te stellen (I-visie). Hierna zijn verschillende documenten verschenen waarbij de provincie bij allen aangaf dat het de I-visie omvat. In de zomer van 2012 stelde de provincie een startnotitie ICT-beleid op.[2] Daarna werd op 22 maart 2013 de *Kadernota ICT-beleid 2013-2015* door PS vastgesteld. De nota geeft de provinciale ICT-ambitie voor de periode 2013 tot en met 2015: eerst de basis op orde en dan (deze op orde houden en) actief volger van ICT-ontwikkelingen mits onderbouwd door een goede businesscase. In de kadernota worden de belangrijkste sturingskaders gegeven waaronder voor beveiliging. Ook worden een I-visie, de beoogde middelen, organisatiestructuur en besturing omschreven. Na de eindevaluatie van de nota stelden GS vast dat de kaders uit de nota ook na 2015 geldig blijven. Daarbij werd medegedeeld dat deze ook van toepassing zijn op de informatie die met de ICT wordt beheerd. In juni 2015 stelde de directie de *Informatievisie Samen, Slim en Innovatief* vast. De visie, zo wordt aangegeven, is integraal onderdeel van het informatiebeleid en kan gebruikt worden om het vigerende informatiebeleid bij te stellen of aan te vullen. De inhoud ervan komt terug in de door GS vastgestelde *nota Digitale Duurzaamheid* van eind 2015 en de notitie *Visie en hoofdlijnen informatiebeleid* uit juni 2016. GS geven aan dat het ICT-beleid met deze twee laatste documenten is geactualiseerd en ‘verbreed’ naar informatie. Het eigenaarschap van de informatie wordt gelegd bij de inhoudelijke beleidsprogramma’s. Informatiebeveiliging/veiligheid komt niet expliciet aan de orde in deze twee documenten. Op hoofdlijnen worden in alle drie de documenten de uitgangspunten uit de kadernota gevolgd; in de notitie Visie en hoofdlijnen wordt expliciet gesteld dat de kaders uit de kadernota van toepassing blijven; de visie bevat geen beleidswijzigingen, zo wordt gesteld.

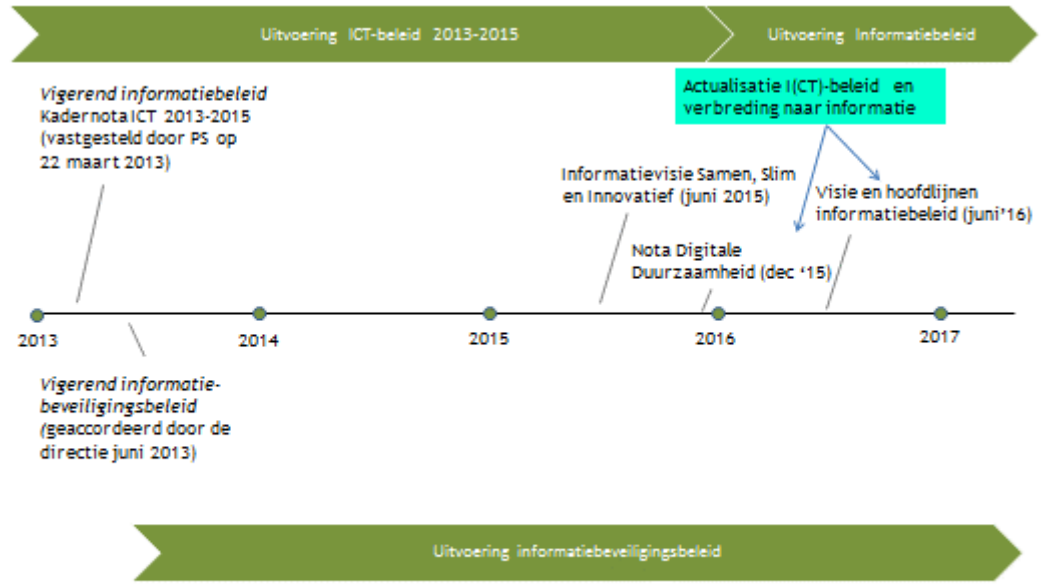
De rekenkamer constateert dat uit de documenten niet duidelijk wordt wat de status is van de door de directie vastgestelde Informatievisie uit 2015. Evenzo is het niet helder hoe deze visie zich verhoudt tot de Kadernota en de Visie en hoofdlijnen

[2] Ook wel *Startnotitie strategisch IT-beleid* genoemd.

informatiebeleid uit 2016. Ze betreffen bijvoorbeeld allemaal visies op informatie. Doordat de recentere nota's actualisaties op onderdelen betreffen, maar de oude kaders ook nog geldig blijven, is het niet altijd duidelijk hoe de documenten zich tot elkaar verhouden.

Missie informatie(voorziening) (Informatievisie Samen, Slim en Innovatief uit 2015)
De informatievoorziening is erop gericht dat de juiste informatie van de juiste kwaliteit, op het juiste moment en op de juiste plaats aanwezig is, tegen zo laag mogelijke kosten om zo de provincie en (keten)partners optimaal te ondersteunen in het realiseren van de maatschappelijke opgaven.

Het totaalbeeld van informatiebeveiligingskaders is als volgt:



3.2 Specifiek beleid: informatiebeveiligingsbeleid

Als nadere uitwerking van het onderdeel informatiebeveiliging uit de kadernota wordt in juni 2013 het *Informatiebeveiligingsbeleid Provincie Noord-Brabant* vastgesteld en door de algemene directie geaccordeerd. Dit is het vigerende beleid voor *informatiebeveiliging*.
In het document beschrijft de provincie:

- wat informatiebeveiliging is;
- waarom ze deze beveiliging noodzakelijk acht;
- wat haar visie en beleid is op dit terrein.

Het document is niet aan PS aangeboden.

De provincie zet in op informatiebeveiliging voor de borging van een betrouwbare informatievoorziening. Een betrouwbare informatievoorziening acht ze essentieel voor het goed functioneren van haar processen en (daarmee) correcte uitvoering van haar

taken. Het uitvallen van informatiesystemen of het door onbevoegden kennisnemen, wijzigen en/of verwijderen van informatie kan verstrekkende gevolgen hebben voor onder andere het imago en de beleidsuitvoering van de provincie, zo wordt in het beleid gesteld.

De provincie definieert informatiebeveiliging als:

Definitie informatiebeveiliging (Informatiebeveiligingsbeleid)
Het kunnen waarborgen dat de juiste informatie op het juiste moment door de juiste personen gebruikt kan worden.

Informatiebeveiliging is daarmee een kwaliteitsaspect van de provinciale bedrijfsvoering, zo wordt in het beleid gesteld, en omvat de drie aspecten die reeds in de kadernota waren opgenomen:

Relevante aspecten informatiebeveiliging (Kadernota ICT-beleid 2013-2015/Informatiebeveiligingsbeleid)
Vertrouwelijkheid/confidentialiteit: de informatie is alleen toegankelijk voor degenen die hiertoe ook daadwerkelijk geautoriseerd zijn. Integriteit: correctheid en volledigheid van de informatie en de informatieverwerking. Beschikbaarheid: geautoriseerde gebruikers hebben op de juiste momenten toegang tot de informatie en de aanverwante bedrijfsmiddelen.

Ook onderstreept de provincie de noodzaak van informatiebeveiliging die voortkomt uit (1) de toenemende digitalisering van de provinciale dienstverlening, (2) de samenwerking met onder andere overheden, (3) wet- en regelgeving die eisen stelt aan informatie, en (4) de maatschappelijke verantwoordelijkheid van de provincie waarbij verwacht mag worden dat zij zorgvuldig omgaat met de gegevens die zij beheert.

In lijn met het doel dat in de kadernota werd gegeven, wordt in het informatiebeveiligingsbeleid gesteld dat:

Visie informatiebeveiliging (Informatiebeveiligingsbeleid)
De provincie streeft met informatiebeveiliging naar beveiliging van haar informatie en alle daaraan gerelateerde aspecten die aansluiten bij het ambitieniveau van haar organisatie met een acceptabele balans tussen kosten en baten, lusten en lasten.

Ofwel zoals in de kadernota wordt gesteld:

Doel informatiebeveiliging
Het naleven van de wetgeving op het gebied van informatiebeveiliging en de afspraken die daarvoor op landelijk en interprovinciaal niveau zijn gemaakt en daarbij steeds de afweging te maken tussen de (kans en) impact van risico's en de kosten van preventiemaatregelen ter voorkoming daarvan.

De informatie(voorziening) dient daarmee afgewogen te worden beveiligd; er dient een beveiligingsniveau te worden gekozen dat passend is bij de risicoafweging. De 'afgewogen beveiliging'/passend beveiligingsniveau komt later ook terug in de I-visie uit 2015 en die uit 2016. De daarbij te hanteren uitgangspunten, die ook al in de kadernota werden genoemd, worden in het informatiebeveiligingsbeleid opgesomd. Deze omvatten procedurele en technische maatregelen. Een voorbeeld daarvan is wetgeving en afspraken die eisen stellen aan informatiebeveiliging zoals de Wet bescherming

persoonsgegevens (Wbp) en de Interprovinciale Baseline Informatiebeveiliging (IBI) van het Centraal Informatiebeveiligingsoverleg (CIBO) van het Interprovinciaal Overleg (IPO).[3] De provincie wil hieraan voldoen.
De IBI bevat de basisset van beveiligingsmaatregelen (NEN/ISO 27002). De provincie heeft zich aan deze baseline gecommitteerd en haar doel is dus om onder andere hieraan te voldoen. De IBI wordt op reguliere basis in interprovinciaal verband herijkt/geactualiseerd.

Er sprake is van een passend beveiligingsniveau als aan de IBI wordt voldaan.

Een ander voorbeeld van een maatregel is het uitzetten van de verantwoordelijkheden in de lijn tot op medewerkersniveau om te bereiken dat bij het dagelijks handelen, bij elke ontwikkeling en elk project aandacht is voor (nut en noodzaak van) informatiebeveiliging; informatiebeveiliging moet een integraal onderdeel gaan uitmaken van de bedrijfsvoering. Daarnaast wordt het belang van bewustwording en bijbehorend gedrag van medewerkers voor informatiebeveiliging onderstreept. De technische maatregelen hebben geen resultaat als het bewustzijn en gedrag van mensen achter blijft; deze zijn noodzakelijk bij het verhogen van de weerbaarheid van de provincie. Door de beveiligingsmaatregelen te implementeren, de verantwoordelijkheden uit te zetten in de lijn en te leren van bevindingen uit evaluaties/audits en incidenten ontstaat, zo wordt gesteld, een basisbeveiligingsniveau en de mogelijkheid om verbeteringen aan te brengen. Veelal als een uitwerking van de kadernota worden verschillende acties opgesomd die de provincie wil uitvoeren om invulling en sturing/beheersing te geven aan het beleid. Daarnaast wordt in aanvulling op de kadernota de organisatie van informatiebeveiliging beschreven.

Het informatiebeveiligingsbeleid werd ten tijde van het rekenkameronderzoek geactualiseerd in verband met de inwerkingtreding van de AVG op 25 mei 2018.
Dit gebeurt, zo is door de provincie aangegeven, op basis van de in de afgelopen jaren uitgevoerde jaarlijkse audits van de accountant, jaarlijkse DigiD-audits van het Rijk en verschillende onderzoeken/scans door externe partijen. De rekenkamer constateert dat het beleid op enkele andere punten ook actualisatie behoefde. Bijvoorbeeld de reeds ruim een jaar verouderde beschrijving van de CIO-rol die niet meer bij de directeur Bedrijfsvoering ligt. Naast een geactualiseerd informatiebeveiligingsbeleid, wordt beleid voor dataprivacy opgesteld. Dit beleid zal slechts op de technische maatregelen ter bescherming van de persoonsgegevens overlappen.

[3] In het Informatiebeveiligingsbeleid ontbreekt de bijlage met kaders en richtlijnen en daarmee inzicht in de inhoudelijke eisen. Ook wordt de IBI niet vermeld bij de voorbeelden van richtlijnen waaraan de provincie zich committeert.

4. Uitvoering beleid

In dit hoofdstuk geven we een samenvatting van de bevindingen over de *uitvoering* van informatiebeveiliging door de provincie Noord-Brabant in de praktijk (tweede deel van onderzoeksvraag 1 en onderzoeksvraag 2).

4.1 Uitgevoerde acties

Binnen de provinciale organisatie is in 2006 allereerst vanuit de techniek (operationeel) aandacht ontstaan voor informatiebeveiliging. Door verschillende ontwikkelingen binnen en buiten de provinciale organisatie is informatiebeveiliging sinds 2013 hoger op de agenda gekomen en wordt vanuit het dan opgestelde beleid (breder en meer structureel) aandacht besteed aan informatiebeveiliging. Informatiebeveiliging wordt voor een groot deel conform het informatiebeveiligingsbeleid uitgevoerd. Zo heeft de rekenkamer geconstateerd dat de voorgenomen acties uit het informatiebeveiligingsbeleid zijn opgepakt. Voorbeelden daarvan zijn:

- De verantwoordelijkheden zijn vastgelegd en ingevuld. Zo zijn, zoals beoogd, ook de verantwoordelijkheden in de lijn uitgezet: vastgelegd is dat de primaire verantwoordelijkheid voor de informatiebeveiliging bij de eigenaar van de informatie ligt. Projectteams/programma- en proceseigenaren zijn verantwoordelijk voor hun projecten, programma's en processen en de beveiliging daarvan en medewerkers zijn verantwoordelijk voor de informatie en de veiligheid daarvan, waarover zij voor de uitvoering van hun taken beschikken. De namen en functies van alle uitvoeringsverantwoordelijken en verantwoordelijken voor de verschillende processen en de daarbij behorende informatie, en de processen voor de besturing van informatiebeveiliging zijn vastgelegd in het risicomanagementinformatiesysteem (RMIS). De provincie werkt met projectportfoliomanagement voor projecten en een changemanagementproces voor wijzigingen. Bij alle projecten, ontwikkelingen en handelingen dient ook informatiebeveiliging aandacht te krijgen.
- Op basis van de zogenaamde IBI-monitor (spreadsheet/database met zo'n 6.000 maatregelen) bepaalt de provincie in hoeverre ze voldoet aan de gestelde afspraken/eisen (IBI) en welke aandachtsgebieden er zijn op het gebied van informatieveiligheid. In lijn met interprovinciale afspraken stelt de provincie op basis daar weer van een samenvattende rapportage/memo op waarin verantwoording wordt afgelegd over de voortgang en volwassenheid van informatiebeveiliging: hoe staat de provincie er per onderscheiden IBI-hoofdstuk (in opzet) voor en welke aandachtsgebieden zijn er. De provincie Noord-Brabant hoort wat betreft het voldoen aan de IBI interprovinciaal bezien bij de hoogst scorende provincies. Naast deze IBI-monitor en de in principe jaarlijkse rapportages daarover zijn er op reguliere basis risicoanalyses uitgevoerd op diverse processen (die een verhoogd risico lopen vanuit het oogpunt van informatieveiligheid). Voor deze processen is daarbij het risicoprofiel bepaald met de bijbehorende set maatregelen.
- Tweejaarlijks is de implementatie van de maatregelen gecontroleerd via een door een externe partij uitgevoerd beveiligingsonderzoek (penetratietesten en mysteryguestonderzoeken). Deze onderzoeken die in 2014 en begin 2017 zijn uitgevoerd, waren gericht op het toetsen van het beveiligingsbewustzijn van

medewerkers en het identificeren van zwakheden in de digitale en fysieke beveiliging (van het provinciehuis). Naar aanleiding van de bevindingen zijn eveneens, waar nodig, proportionele (afgewogen) maatregelen genomen. In 2017 is voorgesteld om de mysteryguestonderzoeken jaarlijks in plaats van tweejaarlijks te gaan uitvoeren.

- Informatiebeveiligingsincidenten worden centraal geregistreerd in een incidentenregister en volgens de daarvoor geldende procedure afgehandeld.
- De provincie maakt in het kader van toegangsbeveiliging voor mail, webmail en de (virtuele) werkplek gebruik van authenticatiesystemen.
- In de praktijk heeft de provincie verschillende inspanningen verricht om het bewustzijn en de vaardigheden van medewerkers op het gebied van informatieveiligheid te vergroten. Zo is een bewustwordingsplan ‘Bewust veilig digitaal werken’ opgezet en uitgevoerd waarbij gebruik is gemaakt van de bevindingen van het beveiligingsonderzoek uit 2014. Daarnaast zijn bevindingen van het beveiligingsonderzoek uit 2017 bekend gemaakt via intranet en is via banners aandacht gevraagd voor het onderwerp. Veelal zijn naar aanleiding van de onderzoeken ook nog verschillende instruerende en informerende berichten, documenten en een filmpje opgesteld en op intranet geplaatst met betrekking tot onder andere integer handelen, phishingberichten, beveiligingsregels en vertrouwelijke informatie. Tot slot zijn er trainingen en e-learnings aangeboden en is in 2017 in de week van de integriteit een workshop dataveiligheid gegeven. Op intranet staat bijvoorbeeld met betrekking tot informatieveiligheid: ‘Ken je regels’. Voorbeelden daarvan zijn:
  - Kies sterke wachtwoorden voor je apparaten.
  - Berg je vertrouwelijke stukken op (ook tijdens werktijd).
  - Laat geen onbekenden binnen in het beveiligde gedeelte.
  - Spreek onbekenden in het gebouw aan.
- De jaarlijkse audit van de implementatie van het informatiebeveiligingsbeleid is bij de accountant neergelegd. Sinds 2012 beoordeelt de accountant jaarlijks de IT-omgeving. De controles zijn wel voornamelijk op SAP gericht omdat deze van materieel belang is voor de jaarrekeningcontrole en de provinciale processen voor een belangrijk deel worden ondersteund door SAP. Wat informatiebeveiliging betreft kijkt de accountant naar de governance. In de boardletter 2014 en 2016 gaat de accountant het meest uitgebreid in op informatiebeveiliging. In de boardletter 2014 merkt de accountant op dat de provincie diverse acties in gang heeft gezet voor het structureren en daarmee verscherpen van de informatiebeveiliging. In de boardletter 2016 stelt de accountant dat de aandacht van de provincie rondom informatiebeveiliging gepast en de procedures in opzet toereikend zijn.
- De CIO is op verschillende manieren en langs verschillende kanalen geïnformeerd over informatieveiligheid, zoals via een directe lijn bij casuïstiek, via de beleidsmedewerker informatiebeveiliging onder andere naar aanleiding van onderzoeken en via verschillende rapportages zoals de samenvattende rapportages over de IBI-monitor, de evaluaties van de kadernota in 2014 en 2015 en de boardletters van de accountant.

Zoals reeds opgemerkt zijn de verantwoordelijkheden voor informatiebeveiliging ingevuld. In aanvulling op de hiervoor beschreven verantwoordelijkheden, gaan we

hierna kort in op enkele andere. De strategische sleutelposities voor het informatiebeleid (inclusief beveiliging) zijn de CIO en de (strategisch) beleidsmedewerker informatiebeveiliging.

GS

Gedeputeerde Van der Maat is portefeuillehouder informatie(beveiliging). GS zijn verantwoordelijk voor het informatiebeleid. De ambtelijke organisatie geeft invulling aan de uitvoering.

CIO

De CIO is verantwoordelijk voor het informatie(beveiligings)beleid, de uitvoering daarvan en het toezien op de naleving ervan. Tot en met 2017 was de CIO een rol. Deze werd door een directeur ingevuld naast zijn andere taken. Najaar 2017 hebben PS het organisatiekostenbudget (OKB) opgehoogd met 1 fte voor de aanstelling van een nieuwe CIO (een eigenstandige (fulltime) functie). De nieuwe CIO is per 1 juni 2018 in dienst getreden. Het betreft een puur adviserende functie die onafhankelijk zal worden uitgevoerd onder de algemeen directeur; contact met GS dient via de algemeen directeur te verlopen. Eén van de eerste taken van de nieuwe CIO is, de hoofdlijnen van het informatiebeleid en de ICT-strategie in het licht van nieuwe ontwikkelingen te herijken, waaronder de provinciale inzet rondom informatieveiligheid, privacy, gegevensbescherming en e-dienstverlening.

Directie

De directieraad/algemene directie draagt zorg voor het uitdragen van het informatiebeveiligingsbeleid naar alle medewerkers en bestuurders en is eindverantwoordelijk voor handhaving van de kaders.

Beleidsmedewerker informatiebeveiliging (CISO, ISO, FG)

Inhoudelijk wordt de CIO ondersteund door de programmamanager informatiebeleid. Op het gebied van informatiebeveiliging wordt de CIO geadviseerd door de beleidsmedewerker informatiebeveiliging. Het onderhoud/de actualisatie van het beleid is bij hem belegd, hij dient informatiebeveiligingsplannen op te stellen, is verantwoordelijk voor het (laten) registreren van beveiligingsincidenten, coördineert bij nieuwe incidenten de afhandeling, rapporteert over ernstige incidenten onder andere aan de CIO en dient tweemaal per jaar de rapportage informatiebeveiliging op te stellen voor de CIO.
De beleidsmedewerker informatiebeveiliging betreft 1 fte en deze vervulde naast de taken voor informatieveiligheid op alle vlakken (operationeel, tactisch en strategisch), tot begin 2018 ook de taak van Functionaris Gegevensbescherming (FG). In 2017 is ervoor gekozen om de functie van beleidsmedewerker informatiebeveiliging op te splitsen in twee nieuwe functies. Het betreft op strategische niveau de Chief Information Security Officer (CISO)-functie en op operationeel/tactisch niveau de ISO-functie.
Per 1 maart 2018 is de ISO in dienst getreden.
Met inwerkingtreding van de AVG op 25 mei 2018 is de provincie verplicht tot het instellen van een FG. PS hebben najaar 2017 het OKB met 1 fte opgehoogd voor de aanstelling van een FG. De FG zal evenals de CISO aan de directie/CIO rapporteren, maar dan over het dataprivacybeleid in plaats van het informatiebeveiligingsbeleid. De

FG fungeert namens de directie als een onafhankelijk toezichthouder vanuit de Wbp en de Autoriteit Persoonsgegevens (AP).

ICT-beheer e.a.

Naast de voornoemde functies voeren ook andere medewerkers werkzaamheden uit voor informatieveiligheid, bijvoorbeeld ICT-beheer en het dienstenplein. Het is onbekend om hoeveel fte dit gaat, omdat het slechts een klein onderdeel is van de werkzaamheden van deze medewerkers.

ICT-kernteam (IKT)

In 2010 is het ICT-kernteam (IKT) geformeerd dat tot medio 2015 goedkeuring moest geven voor de start van iedere fase van een project en kende budget toe voor de uitvoering van de fase. Het IKT keek vooral naar het tactisch portfoliomanagement en bestond uit een dwarsdoorsnede van de I-kolom. Het IKT is als zodanig niet meer actief. De taken zijn nu belegd via een portfolio- en projectteam. In het portfolioteam zijn architectuur, informatiebeveiliging, I-control, dataprivacy, een adviseur concernteam en demandmanagement vertegenwoordigd. Het portfolioteam adviseert de CIO over de vraag om I-projecten en de behoeften daarbij die worden vastgelegd in een zogenaamd i-OG/ON-formulier.

I-board

Van maart 2015 tot december 2017 werd naast het IKT een I-board geplaatst die een adviesfunctie had richting de CIO over de strategische inzet van I(CT). De I-board bestond uit een dwarsdoorsnede van de organisatie (vanuit de beleidskant twee directeuren, twee lijnmanagers en een programmamanager, de CIO, concerncontroller, IT-controller en afvaardiging MT-I). Doel was om op deze wijze de organisatie te betrekken bij strategische afwegingen (I-projectportfoliomanagement/poortwachter) en de I-board had daarmee een bredere rol dan het IKT.

Sourcing

Mede ingegeven door een krimpopdracht en het feit dat er erg veel ontwikkelingen zijn op IT-gebied en deze te snel gaan voor het beperkte aantal mensen dat daarvoor bij de provincie beschikbaar is, is bepaald welke taken door anderen/externen kunnen worden gedaan en welke expertise de provincie in huis nodig heeft om daarover goed de regie te kunnen houden. De sourcingstrategie is eind 2017 opgesteld. Strategie, dataprivacy en beleid voor informatieveiligheid kan niet worden geoutsourcet, zo is bepaald. De operationele IT-omgeving wordt in drie stappen geoutsourcet.

4.2 Aandachtspunten uitvoering

De rekenkamer heeft geconstateerd dat de uitvoering van het beleid niet altijd verloopt zoals door de provincie beoogd. Zo zijn er kanttekeningen te plaatsen:

- zoals eerder opgemerkt, dient bij alle projecten, ontwikkelingen en handelingen ook informatiebeveiliging aandacht te krijgen. Informatiebeveiliging wordt echter vaak niet of te laat betrokken/geraadpleegd bij de uitvoering van werkzaamheden. Dit doordat medewerkers die primair verantwoordelijk zijn voor de informatiebeveiliging zich onvoldoende bewust zijn dat deze aspecten betrokken moeten worden en/of

doordat de kaders en richtlijnen, het projectportfolio- en changemanagementproces worden gemeden omdat deze als te lastig en vertragend worden beschouwd en er verschillende belangen spelen (beheerbelang versus organisatiebelangen) en/of doordat er niet genoeg gestuurd wordt op de naleving van kaders en richtlijnen. Sinds 2014 is (naar aanleiding van onderzoeken) dan ook bijna jaarlijks aandacht gevraagd voor het naleven van het projectportfolio- en changemanagementproces. Toen begin 2017 bleek dat er op onder andere voornoemde punten weinig was veranderd, heeft de CIO opgedragen dat alles via het portfolioproces moet verlopen en alle projecten langs de CIO moeten; er kwam daarmee meer dwang.

- De beoogde *centrale* informatiebeveiligingsplannen zijn in de praktijk nooit als zodanig opgesteld door de beleidsmedewerker informatiebeveiliging. Hierin zouden de maatregelen/acties moeten worden opgenomen die noodzakelijk worden geacht om de aandachtspunten uit onder andere de risicoanalyses, de samenvattende rapportages die zijn opgesteld op basis van de IBI-monitor en de beveiligingsonderzoeken op een acceptabel niveau te krijgen, In de praktijk zijn de werkzaamheden/acties die voor een lopend jaar werden voorzien, vastgelegd in het persoonlijk werkplan (PWOP) van de beleidsmedewerker informatiebeveiliging. Daarnaast is er een database waarin per informatieproces de te nemen (beheers)maatregelen zijn opgenomen en de implementatie ervan wordt gevolgd tot configuratie.
- Ondanks de inspanningen van de provincie om het bewustzijn op het gebied van informatiebeveiliging te vergroten, is in de afgelopen jaren in de meeste onderzoeken blijvend aandacht gevraagd voor (het ontwikkelen en vasthouden van) bewustwording op het gebied van informatiebeveiliging (en later ook privacy). De oorzaak hiervan is dat het merendeel van de medewerkers niet voldoende op de hoogte is van de risico's op het gebied van informatiebeveiliging. Het beveiligingsbewustzijn is onvoldoende. Naar aanleiding van het tweede beveiligingsonderzoek begin 2017 heeft de CIO besloten dat de trainingen (e-learnings) verplicht moeten worden gevolgd door de medewerkers. De provincie verwacht verder dat de opsplitsing van de H&O-taken van managers ook een positieve bijdrage zal leveren aan het verhogen van het bewustzijn van informatieveiligheid. Zo maken bijvoorbeeld e-learnings nu deel uit van 'het goede gesprek' tussen H-manager en medewerker. De provincie stelt dat het ontwikkelen en vasthouden van bewustwording en vaardigheden op het terrein van informatiebeveiliging een continu proces is en een blijvend aandachtspunt vormt. Het is een lastig traject omdat het gedrag en cultuur betreft en dat is moeilijker te veranderen. Ook is aangegeven dat het belangrijk is dat ook GS, PS en de directie worden meegenomen in het traject van bewustwording op het gebied van informatiebeveiliging en dataprivacy. Zo komt het bijvoorbeeld nog steeds voor dat GS/PS-leden e-mail van het @brabant.nl-account automatisch doorsturen naar een gmail-adres. Naar aanleiding van schriftelijke vragen vanuit PS over informatieveiligheid najaar 2017 geven GS wat betreft bewustwording aan dat indien gewenst de beleidsmedewerker informatiebeveiliging een toelichting kan geven specifiek gericht op PS-leden.
- In het informatiebeveiligingsbeleid staat dat de CIO twee keer per jaar een rapportage ontvangt over informatiebeveiliging en de betrouwbaarheid van de informatievoorziening. In de praktijk is er niet twee keer per jaar een dergelijke

specifieke rapportage informatiebeveiliging aan de CIO gestuurd. De informatievoorziening liep zoals reeds eerder opgemerkt meer naar aanleiding van gebeurtenissen en uitgevoerde onderzoeken en testen. Naar aanleiding van het beveiligingsonderzoek uit 2017 is een nieuwe kwartaalrapportage aan de CIO toegevoegd.

- Tot op heden zijn er geen specifieke budgetten beschikbaar gesteld of benoemd voor informatieveiligheid. Dit is, zo is in een interview gesteld, zeer zeker een punt van aandacht. De kosten voor informatiebeveiliging worden primair bekostigd uit het ICT-projectenbudget en bij onvoldoende dekking wordt geput uit het reguliere budget Basisinfrastructuur. Sinds 2016 is van belang dat de Autoriteit Persoonsgegevens bij een datalek een boete kan opleggen aan de provincie. De Wbp/AVG kan dus (onverwachte) financiële gevolgen hebben voor de provincie.
- De bij informatieveiligheid betrokken actoren hebben invulling gegeven aan hun verantwoordelijkheden. In de praktijk was daarbij echter niet altijd sprake van continuïteit/stabiliteit, waardoor onder meer zaken zijn vertraagd en sommige zaken duurden lang voordat ze tot uitvoer kwamen.

CIO

De CIO-rol is in de afgelopen vijf jaar door vijf verschillende personen, al dan niet tijdelijk, ingevuld. De CIO-rol was aanvankelijk belegd bij de directeur Bedrijfsvoering en Financiën die deze functie en rol van 1 september 2013 tot
1 december 2015 vervulde. Er was bewust gekozen om van de CIO géén aparte functie te maken in het licht van de organisatieontwikkeling en de daarmee gepaard gaande verkleining van de directie(raad) en omdat ervan uit werd gegaan dat het op directieniveau geen fulltime uit te voeren taken vraagt. De rol werd bij deze directeur gelegd, omdat de CIO-rol wel specifieke kennis en competenties vraagt.
In eerste aanleg moest bij de CIO om aandacht worden gevraagd voor informatiebeveiliging, omdat het een nieuw vakgebied betrof. De strategische kant sneeuwde onder, door de vele andere taken van de directeur. Na het vertrek van deze CIO in december 2015 zijn de taken voor een korte periode overgenomen. Doordat deze vervanging slechts een relatief korte periode betrof, heeft het oppakken van onderwerpen als de impact van de uitbreiding van de Wbp (dataprivacy), enige vertraging opgelopen en is het pas najaar 2016 met de benodigde prioriteit en samen met de toekomstige AVG opgepakt door de nieuwe CIO. Eind september 2016 heeft de algemeen directeur de CIO-rol op zich genomen en heeft deze tot december 2017 ingevuld. De algemeen directeur wilde dat de CIO-rol op directieniveau belegd bleef om strategisch te kunnen adviseren over I. Omdat de directie op dat moment maar uit één persoon bestond, heeft de algemeen directeur deze taak opgepakt. De strategische kant kreeg meer aandacht dan bij de 1e CIO, maar het bleef lastig door de vele andere taken van de algemeen directeur. Van december 2017 tot juni 2018 werd de CIO-taak belegd bij de nieuwe algemeen directeur die in december 2017 in dienst trad. In juni 2018 is de nieuwe CIO in dienst getreden.

I-board

In januari 2014 werd al voorgesteld om een I-board op te stellen, maar door verschillende managementwisselingen werd dat een jaar uitgesteld. De impact van de I-board zakte enige tijd weg toen in 2016 de rol van CIO niet werd ingevuld door een

personele wisseling.

Beleidsmedewerker informatiebeveiliging

De functie beleidsmedewerker informatiebeveiliging was lang kwetsbaar doordat veel taken bij één persoon waren belegd, zonder goede achtervang. Al geruime tijd werd, zo is in een interview gesteld, gevraagd om ondersteuning/capaciteit op tactisch-operationeel niveau. De discussie om de functie beleidsmedewerker informatiebeveiliging op te splitsen in twee functies (één op strategisch en één op tactisch-operationeel niveau) loopt sinds 2013. In 2017 is uiteindelijk besloten om de functie op te splitsen en op 1 maart 2018 trad de ISO in dienst.
Het aanstellen van een FG stond al voor eind 2016 op de planning, maar uiteindelijk werden PS pas najaar 2017 gevraagd het OKB daarvoor op te hogen met 1 fte. De werving van de FG startte vervolgens in het voorjaar van 2018.

- De sourcingstrategie zou naar verwachting najaar 2015 ontwikkeld worden, maar is uiteindelijk pas eind 2017 opgesteld, waarbij begin januari 2018 nog moest worden bepaald op welk niveau een en ander vastgesteld dient te worden.

Kwetsbaarheden in de praktijk

In de periode van 6 juni tot en met 10 oktober 2017 heeft de rekenkamer een zogenaamde penetratietest laten uitvoeren. Daarmee zijn zowel de systemen van de provincie als het gedrag van de medewerkers getoetst: is informatie van de provincie in de praktijk voldoende beschermd tegen toegang door onbevoegden en kwaadwillenden via het internet en het interne netwerk van de provincie (“hacking”) en via zogenaamde social engineering-aanvallen als phishingmail en een inlooptest; waar liggen de risico’s en kwetsbaarheden? Hierbij dient te worden aangegeven dat 100% veiligheid niet bestaat en de provincie bij het nemen van informatiebeveiligingsmaatregelen een risicoafweging maakt.
De rapportage met bevindingen over dit deel van het onderzoek is al tijdens het onderzoek aan de provincie gestuurd, zodat zij, naast de ten tijde van de testen direct gemelde bevindingen, al een slag konden maken met de aangetroffen kwetsbaarheden. De rekenkamer heeft vastgesteld dat hier ook daadwerkelijk werk van is gemaakt.

Externe toegankelijkheid vanaf het internet

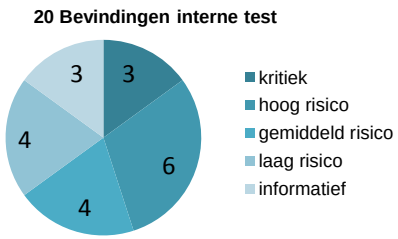
Het aantal kwetsbaarheden dat is aangetroffen tijdens het externe beveiligingsonderzoek vanaf het internet is laag. Twee daarvan zijn echter wel als kritiek geclassificeerd.

11 Bevindingen Externe Toegankelijkheid

De eerste betrof de aanwezigheid van een web shell op één van de servers van de provincie. Een web shell is een “achterdeurtje” waarmee de hacker via een browser communiceert met, in dit geval, de server en deze bestuurt. Er is geconstateerd dat de aangetroffen web shell sinds eind januari 2016 aanwezig was

op het desbetreffende systeem en draaide met dermate hoge privileges dat dit een kritiek risico vormde. Deze bevinding is na ontdekking dan ook direct gemeld aan de provincie. De provincie heeft vervolgens direct acties ondernomen en het betreffende systeem uitgeschakeld (‘uit de lucht gehaald’). De aanwezigheid van deze web shell had tot gevolg dat onbevoegden gebruik konden maken van de rekencapaciteit van de betreffende server (de web shell is gebruikt om een bitcoinminer te installeren) en de informatie konden inzien die op de server stond. Er is, zo stelt de provincie, geen onbevoegde toegang geweest tot vertrouwelijke informatie van de provincie, daar het betreffende systeem alleen openbare informatie bevatte.
De andere kritieke bevinding behelst dat het tijdens het externe onderzoek is gelukt om toegang te krijgen tot alle (provinciale) gegevens waartoe een betreffende medewerker toegang had. Hiertoe zijn eerst uit openbare documenten e-mailadressen van provinciale medewerkers achterhaald (laag risico). Het is vervolgens gelukt om, in een beperkt aantal pogingen, van één van deze e-mailadressen het wachtwoord te achterhalen. Hiervoor is een aantal eenvoudige/voorspelbare wachtwoorden geprobeerd, waarvan er één geldig bleek (eenvoudig/voorspelbaar wachtwoord, hoog risico). Met de betreffende gegevens (e-mailadres en wachtwoord) was het mogelijk om in te loggen op de webmailomgeving van de desbetreffende medewerker (geen two-factor authenticatie op webmail; hoog risico). In de mailbox werden voor deze medewerker ook de SMS-toegangscodes voor de two-factor inlogprocedure voor de thuiswerkplek (Citrix) afgeleverd (in combinatie met voorgaande bevindingen: kritiek risico). Zodoende kon met de inloggegevens van de medewerker op de remote werkplek worden ingelogd en was het mogelijk om gegevens in te zien waartoe deze medewerker toegang had.

Interne test/toegankelijkheid



Tijdens de interne test op het interne netwerk van de provincie is het gelukt om beheerdersrechten te verkrijgen via het achterhalen van accountgegevens (inlognaam en wachtwoord) waarbij een wachtwoord van een beheerdersaccount voorspelbaar en relatief eenvoudig te kraken was omdat het met negen karakters kort is en daarnaast gebaseerd was op een woordenboekwoord. Met de verkregen beheerdersrechten (privileges) was er toegang tot vrijwel alle gegevens en bestanden van de provincie. Zo was het mogelijk om vertrouwelijke informatie in te zien van onder andere de griffie, de directie en de Zuidelijke Rekenkamer. Tijdens dit eerste deel van de interne test is verder bijvoorbeeld ook een groot aantal systemen en applicaties aangetroffen die niet meer ondersteund worden door de leverancier en/of die verouderd waren (beschikbare beveiligingsupdates (patches) bleken niet te zijn toegepast). Deze bevatten vaak bekende en onbekende kwetsbaarheden die in veel gevallen misbruikt kunnen worden om ongeautoriseerde toegang te verkrijgen.
Het aantal kwetsbare systemen dat is aangetroffen, was laag ten opzichte van het

totaal aantal systemen.

Het gedrag: social engineering

Bij het testen van het veiligheidsbewustzijn van de provinciemedewerkers is als eerste een phishingaanval uitgevoerd op alle e-mailadressen eindigend op @brabant.nl.[4] Hierbij 'vulden' 36 van de 1.791 e-mailadressen hun gebruikersnaam en wachtwoord in. De aanval is door de provincie gedetecteerd, er is een waarschuwingsmail verstuurd naar de medewerkers van de provincie en de besmette link in het e-mailbericht is geblokkeerd.
Ook een spear phishingaanval met een zogenaamd "Wob-verzoek" via een vragenformulier op de website van de provincie is geslaagd. Hierdoor is op een tweetal systemen toegang tot het account van een medewerker verkregen en gevoelige informatie toegankelijk geworden.
Op beide dagen dat er inlooptesten zijn uitgevoerd, heeft de mysteryguest ongeautoriseerd toegang tot werkplekken, systemen en vertrouwelijke gegevens verkregen, onder andere op de kamer van de medewerkers van burgemeesterbenoemingen (kamer met de naam "Burgemeesterszaken") die zich bevindt in het bestuurdersgedeelte van het provinciehuis.

Getroffen maatregelen

Zoals eerder vermeld, heeft de provincie eind november 2017 een rapportage van de rekenkamer ontvangen, waarin niet alleen alle bevindingen van dit deel van het onderzoek zijn beschreven, maar ook de daarbij geformuleerde aanbevelingen. Deze zijn vervolgens, binnen de provincie besproken met de betreffende verantwoordelijken (cluster/eenheid Informatievoorziening en ICT (I&I) en de CIO). De bevindingen zijn daarna uitgezet onder de verantwoordelijken en zij hebben deze opgepakt.
De aangetroffen kwetsbaarheden zijn door de provincie daar waar mogelijk direct opgelost en eind januari 2018 was 80-90% opgelost, zo is in een interview gesteld. Daarbij wordt door de provincie aangegeven dat sommige lastiger zijn op te lossen dan anderen en nog tijd vergen. Voor wat betreft two-factor authenticatie voor webmail wordt aangegeven dat naar aanleiding van het beveiligingsonderzoek uit 2014 is overwogen om dit in te voeren. Omdat dit volgens de organisatie een te grote impact had op de gebruiksvriendelijkheid voor de werknemers, is destijds door de CIO besloten om af te zien van invoering. Dit is gebeurd op basis van een zogenoemde risicoacceptatie. Omdat de rekenkamer dit risico nu wederom constateerde, heeft de CIO het advies van de beleidsmedewerker informatiebeveiliging overgenomen om de two-factor authenticatie in te voeren voor webmail.brabant.nl.

De provincie heeft in de loop van de jaren een inhaalslag gemaakt op het gebied van technische informatiebeveiliging en ook het bewustzijn is op punten gegroeid. Toch bleken, bij testen die de provincie begin 2017 zelf had laten uitvoeren naar de toegankelijkheid van haar systemen, veel typen bevindingen hetzelfde te zijn als in de twee jaar daarvoor (2014) uitgevoerde test. Net zoals in ons onderzoek werd begin 2017 geconstateerd dat zowel de technische informatiebeveiliging (systemen en

[4] Een phishingsimultatie bootst een gerichte cyberaanval na om te kijken in hoeverre medewerkers (bewust of onbewust) bereid zijn om potentieel kwaadaardige software (malware) te laten uitvoeren die bijvoorbeeld per e-mailbericht wordt aangeboden.

beheer), als het beveiligingsbewustzijn van de medewerkers, als de fysieke beveiliging van het provinciehuis nog onvoldoende zijn: het was ook toen gelukt om volledige controle te verkrijgen over de technische infrastructuur, waren er niet vergrendelde en/of onbeheerde werkplekken, werd toegang ‘gegeven’ tot (mogelijk) gevoelige informatie van de provincie door het klikken op de link in een phishingmail en onbekenden die in het beveiligde gedeelte van het provinciehuis hun gang konden gaan. Als verklaring voor het aantreffen van vergelijkbare problemen, werd in 2017 onder andere gesteld:

- onvoldoende sturing op het integraal werken binnen het cluster I&I . Dat resulteert in een verkokerde aanpak waardoor er onder andere onvoldoende zicht en controle op de naleving van afgesloten contracten is. Ook is er onvoldoende sturing op operationeel beheer binnen I&I waardoor werkzaamheden niet op een juiste manier geprioriteerd worden. Dit resulteert erin dat het op orde houden van de basisinfrastructuur geen prioriteit heeft waardoor onder andere bevindingen uit eerdere onderzoeken nog niet zijn opgepakt.
  Ook de cultuur van het omzeilen van procedures heeft voor problemen gezorgd.

Aanbevelingen die begin 2017 werden gedaan, betroffen onder andere:

- Borgen dat de operationele taken op het gebied van informatiebeveiliging worden belegd en opgepakt.
- Borgen dat voor elk project het projectportfoliomanagementproces en voor elke wijziging het changemanagementproces wordt gevolgd, zodat kaders en richtlijnen juist worden toegepast.
- Zorgen voor inrichting van monitoring en handhaving voor de naleving van contracten en de handhaving van kaders en richtlijnen in het algemeen en te zorgen dat kaders en richtlijnen ook voldoende geborgd zijn binnen het sourcingtraject.

Begin 2017 is een taskforce opgericht om de bevindingen op te lossen en de aanbevelingen op te pakken, waaronder het versterken van wachtwoorden en het draaien van beveiligingsupdates. De rekenkamer constateert dat een half jaar later in haar onderzoek op een aantal punten weer vergelijkbare bevindingen zijn gedaan, zoals beveiligingsupdates (patches) die niet waren gedraaid. Gevraagd naar redenen voor het aantreffen van vergelijkbare ‘problemen’/bevindingen, is vanuit de ambtelijke organisatie aangegeven dat de updates niet gedraaid zijn door achterstallig onderhoud bij ICT-beheer. De follow-up van de bevindingen uit januari 2017 wordt, zo is aangegeven, wekelijks besproken door de verantwoordelijken en de patches zouden eigenlijk één keer per maand moeten worden doorlopen, zoals begin 2017 is afgesproken om te borgen dat de geconstateerde problemen voortaan worden voorkomen. De rekenkamer constateert dat dit laatste niet is gelukt. Het uitvoeren van de betreffende updates en het toezicht daarop valt onder de verantwoordelijkheid van de opdrachtnemer ICT-beheer. De beleidsmedewerker informatiebeveiliging controleert periodiek door middel van externe audits of dit ook daadwerkelijk gebeurt. Op basis van de uitkomsten vindt dan bijsturing plaats.
Begin 2017 werd de provincie geattendeerd op wachtwoorden die niet aan de (inter)provinciale eisen van een wachtwoord voldeden, zoals ‘welkom01’. Deze zijn, zo wordt gesteld, vervangen door complexe wachtwoorden. Ook is het nu zo dat, als een wachtwoord niet voldoet aan de eisen, het wachtwoord bij het wijzigen/instellen niet

wordt geaccepteerd door het systeem en een ander wachtwoord moet worden gekozen dat voldoet aan de eisen. De door de rekenkamer aangetroffen wachtwoorden als ‘Zomer2017!’ voldoen wel aan de provinciale eisen, maar zijn voorspelbaar en relatief eenvoudig te kraken. De rekenkamer constateert dat, ondanks de aandacht die in 2017 onder andere in e-learnings is gevraagd voor het belang van sterke wachtwoorden, er wachtwoorden worden gebruikt die voorspelbaar en relatief eenvoudig zijn te kraken.

Wat betreft de phishingmail constateert de rekenkamer dat 36 ontvangers hun logingegevens ‘weggaven’, ondanks de maatregelen die op technisch gebied zijn genomen en de acties op het gebied van bewustwording die de provincie ongeveer een half jaar voor de aanval uitvoerde na een andere phishingsimulatie. De intentie is om zoveel mogelijk kwaadwillende mails op voorhand te blokkeren. Dagelijks worden zo’n 2.000 tot 3.000 phishingmails uit het mailverkeer gevist, zo wordt aangegeven. Indien er toch kwaadwillende mail in mailboxen wordt afgeleverd, zal deze na een melding via het dienstenplein en beoordeling door ICT-beheer alsnog worden verwijderd zonder tussenkomst van menselijk handelen. De rekenkamer constateert dat conform deze procedure is gehandeld. Nadat de phishingmails waren verwijderd, verscheen er ook nog een prikkelende waarschuwingsboodschap van ICT-beheer op het interne sociale netwerk van de provincie (Yammer). Overigens is de ervaring dat in de loop van de tijd minder mensen op dit soort mails reageren, zo is vanuit de ambtelijke organisatie aangegeven. In een eerste onderzoek waren het er 656, in het tweede 83, in het derde 47 en nu 36. Het kan, zo is in interviews gesteld, iedereen overkomen om op een link in zo’n mail te klikken, maar het wordt als kwalijk ervaren dat er toch nog zoveel mensen hun inlognaam en wachtwoord invulden.

5. Provinciale Staten en informatieveiligheid

In dit hoofdstuk geven we een samenvatting van de bevindingen over hoe Provinciale Staten zijn betrokken bij en geïnformeerd over de opzet en invulling van informatieveiligheid (onderzoeksvraag 3).

5.1 Rollen PS

Provinciale Staten hebben (in 2013) kaders vastgesteld voor informatiebeveiliging als onderdeel van het I(CT)-beleid (kaderstellende rol). Verder hebben ze (in de begrotingen) middelen toegekend voor de uitvoering van dit I(CT)-beleid (budgetrecht). Daarnaast is het de taak van PS om het door GS gevoerde bestuur te controleren en eventueel bij te sturen met behulp van de kaders. In het ICT-beleid (de kadernota) is vastgelegd dat PS toezicht houden op de realisatie van het ICT-beleid.

Systemen van PS en fractiemedewerkers zijn gescheiden van de provinciale systemen. De griffie is bijvoorbeeld verantwoordelijk voor iBabs en de beveiliging daarvan. De eigenaar van de onderliggende software is verantwoordelijk voor het systeem.

5.2 Informatie aangeboden aan PS

De rekenkamer constateert dat PS via de *kadernota*, die door hen is vastgesteld, zeer op hoofdlijnen zijn geïnformeerd over de kaders, uitgangspunten en governance voor informatiebeveiliging. Zo wordt wel gesteld dat de provincie wetgeving en afspraken wil naleven, maar er wordt geen inzicht gegeven in de inhoud daarvan. De twee andere nota's die mede vigerend zijn, de *nota Digitale Duurzaamheid* en de *Visie en hoofdlijnen informatiebeleid*, zijn voor kennisgeving aan PS aangeboden. Het *informatiebeveiligingsbeleid* is niet aan PS aangeboden, omdat het een verdere (tactische) invulling van de kadernota betreft en dit destijds werd gezien als een ambtelijke verantwoordelijkheid en bevoegdheid.

De rekenkamer constateert dat PS daarnaast, zoals vastgelegd in de kadernota, met ingang van 2013 via de reguliere planning & controlcyclus zijn geïnformeerd over de doelstellingen en de uitvoering van het ICT-beleid. Vaak betreft het procesachtige informatie: er wordt bijvoorbeeld melding gemaakt dat er beleid is, de CIO-functie is ingevuld, de governance verder is geprofessionaliseerd met oprichting van de I-board en dat het beleid grotendeels is gerealiseerd, maar er wordt in het algemeen niet aangegeven wat er nog niet is gerealiseerd en wat nog (extra) aandacht vereist. Ook wordt er specifiekere informatie gegeven in de jaarstukken dan in de begroting zodat de aansluiting lastig is te maken (wat is wel/niet gerealiseerd van wat werd beoogd).
Er wordt veelal niet specifiek ingegaan op informatieveiligheid en de kosten daarvan. Alleen in de jaarstukken 2013, 2015 en 2016 wordt heel summier ingegaan op informatieveiligheid (gemeld wordt dat acties zijn uitgewerkt en het onderwerp meer aandacht heeft gekregen).

De accountant heeft, in opdracht van PS en zoals vastgelegd in de kadernota, jaarlijks aan PS gerapporteerd over zijn bevindingen op het gebied van informatieveiligheid.[5]
In de kadernota is eveneens vastgelegd dat PS in 2014 ook buiten de P&C-cyclus zullen worden geïnformeerd over de voortgang, dan een geactualiseerde versie ontvangen en dat er een eindevaluatie als afsluiting van de beleidscyclus zal worden uitgevoerd. De rekenkamer constateert dat PS eind 2014, eind 2015 en in juni 2016 via een statenmededeling en de onderliggende documenten zijn geïnformeerd over respectievelijk de resultaten en aanbevelingen van de tussenevaluatie en de eindevaluatie van het ICT-beleid en de notitie Visie en hoofdlijnen provinciaal informatiebeleid. De rekenkamer constateert verder dat PS via de evaluatierapportages van eind 2014 en eind 2015 en de boardletters 2014 en 2016 van de accountant inhoudelijk zijn geïnformeerd over de uitvoering van informatiebeveiliging binnen het ICT-beleid, maar niet over de kosten daarvan. De informatie in deze documenten is informatief en begrijpelijk. In 2014 hebben PS geen geactualiseerde versie van de kadernota ontvangen, zoals gemeld in de kadernota. De tussenevaluatie gaf daartoe geen aanleiding.
Vanuit de ambtelijke organisatie is aangegeven dat PS via de bevindingen van de jaarlijkse controle door de accountant worden geïnformeerd over de stand van zaken van informatieveiligheid en dat dat wat GS betreft voor nu voldoende informatie is. De bevindingen van de accountant zouden eventueel aanleiding moeten geven voor vervolgvragen: ‘piepsysteem’. Daarnaast worden PS niet geïnformeerd over informatieveiligheid, maar uiteraard wordt er wel op eventuele vragen van PS gereageerd, zo wordt aangegeven.

PS hebben bij de bespreking van de kadernota in 2013 en de jaarstukken in 2015 vragen gesteld over het ICT-beleid, in 2013 ook aandacht gevraagd voor beveiliging en ICT-beveiliging als speerpunt aangewezen voor de accountantscontrole 2013. In 2014 werd naar aanleiding van recente hacks van overheidssites gevraagd naar de stand van zaken van de informatiebeveiliging. In 2017 zijn vanuit PS op verschillende momenten naar aanleiding van gebeurtenissen vragen gesteld die betrekking hadden op informatie-veiligheid. Zo werd ook toen bijvoorbeeld weer gevraagd naar de status van de informatieveiligheid. De rekenkamer merkt op dat door de gehanteerde werkwijze van PS in 2016 en 2017 geen (audio)verslagen beschikbaar zijn van informatie- en platformbijeenkomsten van PS.

[5] Conform een aanbeveling van de rekenkamer uit 2012 (*Strategisch Informatiebeleid provincie Noord-Brabant*).