Vervolgonderzoek Informatieveiligheid

Provincie Noord-Brabant

Rapport van bevindingen

16 juni 2022

ZUIDELIJKE REKENKAMER

Inhoudsopgave

1 Over dit onderzoek

De Zuidelijke Rekenkamer heeft in de periode januari 2022 – mei 2022, in vervolg op haar onderzoek uit 2018, een onderzoek uitgevoerd naar informatieveiligheid van de provincie Noord-Brabant. Dit rapport van bevindingen bevat het feitencomplex daarvan.

1.1 Aanleiding

Het staat buiten kijf dat het zeer belangrijk is dat de informatie waarover de provincie beschikt veilig is. Onbevoegd toegang tot informatie(systemen) van de provincies is ongewenst, want dat kan leiden tot financiële, materiële en/of reputatieschade (bijvoorbeeld als (vertrouwelijke) informatie in 'de verkeerde handen terecht komt').[1] De kans om slachtoffer te worden van bijvoorbeeld cyberaanvallen is reëel aanwezig. Denk onder andere aan de massale cyberaanval uit juli 2021 die wereldwijd tussen de 800 en 1.500 bedrijven trof en waarbij via gijzelsoftware computers of gegevens werden versleuteld en informatie daardoor niet meer beschikbaar was. Of de cyberaanval uit oktober 2021 waarbij de productie bij de VDL-groep tijdelijk (deels) stil kwam te liggen en daardoor ook partners werden geraakt. In 2021 registreerde de politie 14.000 gevallen van cybercrime. Dit betekende een toename van bijna een derde vergeleken met een jaar eerder en drie keer meer dan in 2019.[2] De verwachting is dat deze trend zich doorzet in 2022 en dat cyberaanvallen de grootste bedreiging zijn voor bedrijven.[3]

Met het oog op deze ontwikkelingen heeft de rekenkamer een vervolgonderzoek uitgevoerd naar informatieveiligheid van de provincie Noord-Brabant. In 2018 publiceerden we voor zowel de provincie Limburg als de provincie Noord-Brabant de uitkomsten van onze onderzoeken naar informatieveiligheid. Na bijna 3,5 jaar hebben we in vervolg daarop gekeken naar enerzijds de stand van zaken op dit moment en anderzijds naar de doorwerking van onze aanbevelingen uit 2018. In hoeverre hebben Gedeputeerde Staten (GS) en Provinciale Staten (PS) voldaan aan de opdrachten zoals geformuleerd in het PS-besluit 56/18 Rapport Zuidelijke Rekenkamer Informatieveiligheid, van 14 september 2018. Zie onderstaand kader voor een korte weergave van deze opdracht.

[1] Enkele voorbeelden van mogelijke consequenties zijn: het kan gevaar opleveren voor de continuïteit van de bedrijfsvoering van de provincie, inbreuk op het vertrouwen van burgers, partners, leveranciers en medewerkers, overtredingen van wet- en regelgeving, gevolgen voor het democratische proces en het betalen van losgeld bij een gijzelsoftware-aanval om weer toegang te krijgen tot eigen systemen, bestanden e.d.
[2] www.rtlnieuws.nl, 17 januari 2022. Ook andere bronnen melden dat het jaar 2021 een grote toename kende. Bijvoorbeeld www.winmagpro.nl: in 2021 wekelijks 446 getroffen bedrijven in Nederland, een stijging van maar liefst 86 procent ten opzichte van 2020.
[3] www.managementimpact.nl, 3 maart 2022, www.consultancy.nl onderzoek PWC, 30 maart 2022 en Cyber Security Predictions rapport van Check Point.

Kader 1. Opdrachten PS-besluit 56/18 naar aanleiding van het rekenkameronderzoek Informatieveiligheid.

Aan GS:

- Op de kortst mogelijke termijn een samenhangende informatie(beveiligings)visie en bijbehorend beleidsplan ter vaststelling aan PS aanbieden, waarbij de insteek is de informatieveiligheid daadwerkelijk naar een hoger niveau te tillen.
- Daarbij versplintering over meerdere documenten voorkomen en in de documenten duidelijkheid te geven over de status ervan en de samenhang met andere relevante documenten.
- In de uitvoering voor voldoende continuïteit in de ingevulde verruimde capaciteit te zorgen.
- Daadwerkelijk en voortvarend de voorgenomen (verbeter)acties door te zetten en strakker te sturen op naleving van kaders, richtlijnen, procedures en werkafspraken.

Aan PS:

- De griffie opdracht te geven om in het kader van bewustwording en in samenwerking met de ambtelijke organisatie een informatiesessie over informatiebeveiliging voor PS te organiseren.
- PS op te roepen om, met het oog op hun controlerende rol, alert te blijven op de informatieverstrekking door GS over informatieveiligheid en zelf meer structureel aandacht te vragen voor het onderwerp.

1.2 Doelstelling en onderzoeksvragen

Doel is om PS van de provincie Noord-Brabant inzicht te geven in hoeverre GS en PS de opdrachten uit PS-besluit 56/18 hebben uitgevoerd en wat de huidige stand van zaken op het gebied van informatieveiligheid is. Hiermee willen we een bijdrage leveren aan een verdere verbetering van de informatieveiligheid van de provincie Noord-Brabant.

De onderzoeksvragen zijn:

1. Welke veranderingen hebben er vanaf 2018 bij de provincie Noord-Brabant plaatsgevonden op het gebied van informatieveiligheid qua beleid en uitvoering in de praktijk?
2. In hoeverre hebben GS voldaan aan de opdrachten uit PS-besluit 56/18?
3. In hoeverre hebben PS opvolging gegeven aan de oproepen uit PS-besluit 56/18?
4. Welke lessen volgen hieruit voor de toekomst?

1.3 Aanpak

1.3.1 Normenkader

Het normenkader dat de rekenkamer hanteert is in tabel 1 opgenomen. Dit sluit aan bij de hierboven beschreven doelstelling en vragen van het onderzoek. Het kader heeft als doel een basis te bieden voor de bevindingen en daarop te baseren conclusies (oordelen) en aanbevelingen.

Tabel 1 Normenkader informatieveiligheid.

Thema	Vraag	Normen
Groei informatieveiligheid	1	Er zijn stappen gezet waardoor sprake is van (verdere) verbetering op het gebied van informatieveiligheid.
Opdrachten PS informatieveiligheid	2 en 3	GS en PS hebben de opdrachten van PS uit 2018 uitgevoerd.

1.3.2 Onderzoeksmethodiek

Het onderzoek richt zich op de periode september 2018 tot mei 2022. Via documentanalyse en interviews met ambtelijk betrokkenen is in kaart gebracht welke maatregelen in deze periode zijn genomen en wat de huidige stand van zaken is op het gebied van informatieveiligheid. Ook hebben we een beroep gedaan op enkele externe experts op het gebied van informatieveiligheid en zijn actuele ontwikkelingen meegenomen, zoals het massale thuiswerken dat als gevolg van de coronapandemie in 2020 werd ingevoerd en in de toekomst gedeeltelijk zal worden doorgezet.

In bijlage 1 is een overzicht opgenomen van de geraadpleegde documenten en gebruikte afkortingen. Bijlage 2 bevat een lijst met gesprekspartners. De conceptversie van voorliggend rapport van bevindingen is half mei aangeboden voor ambtelijk wederhoor. Op 7 juni 2022 zijn de ambtelijke reacties ontvangen van de ambtelijke organisatie. Deze zijn door de rekenkamer besproken en verwerkt in voorliggende definitieve versie, die is vastgesteld door het bestuur van de rekenkamer op 13 juni 2022.

2 Informatieveiligheid vanaf 2018

Dit hoofdstuk begint met een overzichtstabel die toont in hoeverre GS en PS van Noord-Brabant hebben voldaan aan de opdrachten uit PS-besluit 56/18. Daarna geven we per opdracht een onderbouwing van onze beoordeling. Tot slot spreken we ons kort uit over de huidige stand van zaken op het gebied van informatieveiligheid en wat eventuele lessen voor de toekomst zijn.

2.1 Uitvoering opdracht van PS uit 2018 in vogelvlucht

PS droegen GS in 2018 op om de aanbevelingen van de rekenkamer op te volgen. Samenvattend constateert de rekenkamer dat GS na ruim 3,5 jaar volledig aan deze opdracht hebben voldaan. Er is voortvarend gewerkt aan een samenhangende informatie(beveiligings)visie en bijbehorend beleidsplan. PS zijn tussentijds geïnformeerd over de voortgang hiervan en met één beleidsplan is niet langer sprake van versplintering over meerdere documenten.

Op het gebied van Informatieveiligheid zijn in korte tijd grote stappen gezet, waarbij informatieveiligheid daadwerkelijk naar een hoger niveau is getild. De provincie heeft een Chief Information Officer (CIO) aangesteld en er is een CIO-office ingericht met onder meer een fulltime Chief Information Security Officer (CISO). Voor het na te streven kader vanuit de rijksoverheid (Baseline Informatiebeveiliging Overheid) en interprovinciale afspraken (NEN-ISO 27001), is Noord-Brabant de eerste en enige[4] provincie die hiervoor is gecertifieerd.

De rekenkamer constateert verder dat PS nagenoeg volledig hebben voldaan aan de oproep die aan hun was gericht. Zo is er niet één, maar zijn er twee themabijeenkomsten georganiseerd. Door een toezegging van GS lijkt ook structurele aandacht voor de nieuwe datavisie geborgd. Hiermee is echter niet automatisch geborgd dat Informatie*veiligheid* structurele aandacht krijgt, aangezien de datavisie over veel meer gaat dan informatieveiligheid. PS dienen dus alert te blijven en zij moeten erop toezien dat de toezegging van GS ook daadwerkelijk wordt ingevuld.

Bij vragen of zorgen over Informatieveiligheid is het stellen van (technische) Statenvragen aan het CIO-office een makkelijke toegang tot meer informatie. Daar is de afgelopen 3,5 jaar echter nauwelijks gebruik van gemaakt door PS.

In onderstaande tabel zijn onze aanbevelingen uit 2018 verkort weergegeven. In de tabel wordt per aanbeveling een overzicht gegeven van de mate van invulling/uitvoering van de opdracht van PS:
Groen: dit deel van de opdracht is volledig uitgevoerd.
Oranje: dit deel van de opdracht is deels uitgevoerd.
Rood: dit deel van de opdracht is niet uitgevoerd.

[4] Peildatum 22 april 2022.

Tabel 2 Mate waarin invulling is gegeven aan de opdrachten in PS-besluit 56/18

Opdrachten aan GS		Uitgevoerd?	Acties GS
1	Op de kortst mogelijke termijn een samenhangende informatie(beveiligings)visie en bijbehorend beleidsplan ter vaststelling aan PS aanbieden, waarbij de insteek is de informatieveiligheid daadwerkelijk naar een hoger niveau te tillen. Daarbij versplintering over meerdere documenten voorkomen en in de documenten duidelijkheid te geven over de status ervan en de samenhang met andere relevante documenten.		✓ 5 februari 2019 Stand van zaken en voortgang van de in voorbereiding zijnde Datavisie provincie Noord-Brabant. ✓ 7 januari 2020 Statenvoorstel Vaststelling Datavisie Provincie Noord-Brabant 2020-2025. ✓ 14 februari 2020 Aangepast Statenvoorstel Vaststelling Datavisie Provincie Noord-Brabant 2020-2025. ✓ 8 mei 2020 Statenbesluit Vaststelling Datavisie Provincie Noord-Brabant 2020-2025.
2	Daadwerkelijk en voortvarend de voorgenomen (verbeter)acties door te zetten en strakker te sturen op naleving van kaders, richtlijnen, procedures en werkafspraken.		✓ CIO aangesteld en CIO-office ingericht. ✓ Noord-Brabant als eerste en enige (peildatum 22 april 2022) provincie BIO en ISO 27001 gecertificeerd. ✓ Gecertificeerd ISMS dat beoordeeld is met de hoogste score qua volwassenheid.
3	In de uitvoering voor voldoende continuïteit in de ingevulde verruimde capaciteit te zorgen.		✓ Geen personeelswisselingen m.b.t. de functies van CIO en CISO. ✓ Uitbreiding van het CIO-office bewerkstelligd.
Opdrachten aan PS		**Uitgevoerd?**	**Acties PS**
4	PS geven de griffie opdracht om in het kader van bewustwording en in samenwerking met de ambtelijke organisatie een informatiesessie over informatiebeveiliging voor PS te organiseren.		✓ 14 februari 2020 Themabijeenkomst over Datavisie Provincie Noord-Brabant 2020-2025. ✓ 6 maart 2020 Vervolg themabijeenkomst Datavisie Provincie Noord-Brabant 2020-2025.
5	PS worden opgeroepen om, met het oog op hun controlerende rol, alert te blijven op de informatieverstrekking door GS over informatieveiligheid en zelf meer structureel aandacht te vragen voor het onderwerp.		• Geen (technische) Statenvragen over Informatieveiligheid in de periode 2021 -maart 2022, m.u.v. een technische vraag PVV i.r.t. Sourcing ICT basisinfrastructuur, 15 oktober 2020. • Bewaak de toezegging van GS.

2.2 Onderbouwing beoordeling opdrachten GS

2.2.1 Op korte termijn een samenhangend beleidsplan voorgelegd

Op 8 mei 2020 stellen PS de Datavisie Provincie Noord-Brabant 2020-2025 vast. De Datavisie vervangt, integreert en consolideert het dan vigerende ICT-beleid (ICT kadernota 2013), het informatiebeleid (Informatievisie 2015) en de nota Digitalisering (2018). Beleid dat over verschillende nota's was verdeeld, komt nu dus samen in één kader. Hiermee is invulling gegeven aan de opdracht uit PS-Besluit 56/18, om versplintering over meerdere documenten te voorkomen.

De Datavisie is een overkoepelende visie, voor de komende vijf jaar, waarin de provincie in acht leidende principes omschrijft hoe zij wil omgaan met digitalisering, het gebruik van data en de bijkomende risico's.

Informatieveiligheid is één van de acht richtinggevende principes in de Datavisie. Conform de opdracht uit PS-Besluit 56/18 wordt hierbij gestreefd om informatieveiligheid daadwerkelijk naar een hoger niveau te tillen (zie kader 2). Paragraaf 2.2.2. laat zien dat dit streven zich ook daadwerkelijk heeft vertaald in verbeteracties.

Kader 2. Insteek Informatieveiligheid in de Datavisie Provincie Noord-Brabant 2020-2025 [5]

Informatiebeveiliging voorop

We werken continu aan het waarborgen dat de juiste informatie op het juiste moment door (alleen) de juiste personen gebruikt kan worden. We streven naar beveiliging van onze informatie en alle daaraan gerelateerde aspecten die aansluiten bij het ambitieniveau van onze organisatie, met een acceptabele balans tussen kosten en baten. De laatste jaren zijn hier al stevige stappen op gezet, zowel in fysieke beveiliging als digitaal. De komende tijd implementeren we daarnaast onder meer de Baseline Informatieveiligheid Overheid (BIO) en de daaraan gekoppelde ISO 27000 serie. Op deze manier is onze informatie zowel intern goed beveiligd als tegen externe ongewenste invloeden (zoals hackers).

2.2.2 Daadwerkelijk voorgenomen verbeteracties doorgevoerd

Bij het vaststellen van de Datavisie (8 mei 2020) waren twee verbetertrajecten voor Informatieveiligheid reeds (grotendeels) voltooid:

1. Inrichten en faciliteren van een organisatiestructuur met als kerntaak Informatiebeveiliging.
2. Certificering op basis van de NEN-ISO 27001 waarin ook de Baseline Informatiebeveiliging Overheid (BIO) is opgenomen.

Met deze twee verbetertrajecten is voldaan aan de opdracht uit PS-Besluit 56/18 om informatieveiligheid daadwerkelijk naar een hoger niveau te willen tillen. Hieronder wordt deze conclusie nader onderbouwd.

[5] Datavisie Provincie Noord-Brabant 2020-2025, blz. 12.

2.2.2.1 Organisatiestructuur

In juni 2018 is een Chief Information Officer (CIO) aangesteld. De CIO is verantwoordelijk voor de informatievoorziening. Strategie, ICT en de organisatie zijn belangrijke aandachtsgebieden voor de CIO. Ter ondersteuning van de CIO heeft de provincie ook direct een CIO-office ingericht, met een Chief Information Security Officer (CISO) en een Functionaris Gegevensbescherming[6] (FG).

De CISO is verantwoordelijk voor de dagelijkse gang van zaken op het gebied van informatiebeveiliging. De provinciesecretaris/ algemeen directeur is eindverantwoordelijk. Deze taak- en rolverdeling wordt voorgeschreven door de circulaire BIO[7]:

- Het lijnmanagement is verantwoordelijk voor de beveiliging van informatie(systemen).
- De secretaris/algemeen directeur van een organisatie is eindverantwoordelijk voor deze beveiliging en voor de inrichting en werking van de beveiligingsorganisatie.

De CISO vertegenwoordigt de provincie in het Interprovinciaal CIBO Overleg van de provinciale CISO's, waarin Noord-Brabant een voortrekkersrol vervult. De CISO van Noord-Brabant is gedurende een jaar, 2 dagen per week voor BIJ12 werkzaam.[8] Deze detachering is het gevolg van zeer ernstige beveiligingsrisico's (eind 2020) in de gezamenlijke provinciale systemen die in beheer zijn bij BIJ12.

In de werkgroep *Samen Slimmer Sterker* van BIJ12, trekken vijf provincies (Gelderland, Zeeland Flevoland, Groningen en Noord-Brabant) en BIJ12 samen op. Deze zes partijen willen meer integreren en van elkaar leren.

De CISO van Noord-Brabant ziet zijn detachering als een meerwaarde voor de provincie. Door met twee benen in twee organisatie te staan, heeft Noord-Brabant een goed beeld van hoe de provincies zich tot elkaar verhouden. Bijvoorbeeld wat betreft uitkomsten van phishing-testen. "Samenwerking is (financieel) doelmatig. Veel processen en uitkomsten zijn identiek. Bijvoorbeeld een risico-analyse BIBOB verschilt nauwelijks per provincie. Dit biedt mogelijkheden voor verregaande samenwerking. Dat is niet alleen financieel gunstig maar je kunt ook veel sneller 'volwassen' worden (synergie) want je kunt in dezelfde tijd veel meer processen op orde brengen."[9]

2.2.2.2 Certificering

De BIO is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). De BIO is in december 2018 vastgesteld door de Ministerraad voor de Rijksoverheid. Daarvoor was door gemeenten, waterschappen en provincies reeds besloten tot invoering van de BIO. In interprovinciaal verband is eind 2017 afgesproken dat alle provincies per 1-1-2023 voldoen

[6] Een FG houdt binnen een organisatie toezicht op de toepassing en naleving van de Algemene verordening gegevensbescherming (AVG).
[7] BIO versie 1.04, blz. 10.
[8] BIJ12 is in 2014 opgericht door de provincies als onderdeel van het IPO en ondersteunt de provincies bij de uitvoering van wettelijke taken.
[9] Interviewverslag CISO.

aan de eisen voor ISO 27001-certificering.[10] Daadwerkelijke certificering is niet verplicht.

De provincie Noord-Brabant heeft invulling gegeven aan deze afspraak door zowel te certificeren op basis van de NEN-ISO 27001 als op basis van de BIO. Op 14 januari 2020 is de provincie Noord-Brabant officieel gecertificeerd voor zowel de NEN-ISO 27001 als de BIO. Noord-Brabant is de eerste en tot nu toe (22 april 2022) de enige provincie die dit heeft bewerkstelligd.

De BIO schrijft voor dat de provincie jaarlijks een In Control Verklaring (ICV) oplevert. Hiermee wordt verklaard dat de eigen bedrijfsvoering aan de BIO voldoet. Wanneer je zowel voor BIO als ISO 27001 bent gecertificeerd dan is zeker gesteld dat je deze verantwoording kunt afleggen.[11]

2.2.2.3 Information Security Management System (ISMS)

Een ISO 27001-certificering gaat hand-in-hand met het gebruik van een Information Security Management System (ISMS). Een ISMS is een managementinstrument om informatiebeveiliging te waarborgen en te besturen en wordt ondersteund door software. ISMS is een ‘manier van werken’ met als basis een systematisch verbeterproces: veiligheidsrisico’s worden in kaart gebracht, beleid wordt opgesteld en taken en verantwoordelijkheden toegewezen.

Om te voldoen aan de ISO 27001 bevat het systeem enkele verplichte activiteiten zoals interne en externe audits. Hiermee wordt aantoonbaar dat de organisatie op de juiste wijze aandacht en opvolging geeft aan informatiebeveiliging. Voor het opzetten en inrichten van het ISMS is de provincie begeleid door het bedrijf Strict.

Met het ISMS anticipeert de provincie op (steeds veranderende) bedreigingen en kansen van buitenaf en organiseert zij de behoefte van binnenuit de organisatie. Op deze manier is haar informatiebeveiliging effectief en up-to-date. Het implementeren, onderhouden en voortdurend verbeteren gebeurt via een Plan-Do-Check-Act (PDCA-)cyclus:

- Plan: Zijn alle potentiële interne én externe bedreigingen en risico’s in kaart gebracht? Eigen richtlijnen, bijvoorbeeld hoe worden risicoanalyses uitgevoerd, wachtwoordenbeleid, telewerken, etc.
- Do: Realiseer maatregelen binnen de organisatie om relevante risico’s te beheersen. De reikwijdte van maatregelen is al vastgesteld, namelijk basisbeveiligingsniveau 2 (BBN 2).
- Check: Heb je gedaan wat je zou doen en hoe kun je dat zien (KPI’s)? Zijn er risico’s die onvoldoende zijn teruggebracht?
- Act: Implementeren jaarplan, verbeteracties en eventuele bijkomende reguliere werkzaamheden (bijvoorbeeld follow-ups uit audits).

[10] https://www.bij12.nl/nieuws/provincies-bereiden-zich-voor-op-iso-27001-in-2023/
[11] Voor meer informatie zie: wetten.nl - Regeling - Circulaire toepassen Baseline Informatiebeveiliging Overheid in het digitale verkeer met het Rijk - BWBR0043146; https://bio-overheid.nl

Het ISMS van de provincie is ondergebracht in een softwarepakket waarin alle processen samen komen. Per proces kan er (op elk moment) een rapportage worden getoond (gegenereerd). Voorbeelden van rapporten zijn: jaarplannen, acties (openstaand/afgerond), uren (geraamd/daadwerkelijk), kosten (geraamd/daadwerkelijk), jaarevaluaties, etc.

Het ISMS wordt jaarlijks getoetst door een officiële externe ISO 27001-auditor. Het ISMS van Noord-Brabant is beoordeeld met de hoogst mogelijke BIO-volwassenheidsscore, level 5.

Tabel 3 BIO-volwassenheid[12]

Level	BIO-volwassendheid
5	Geoptimaliseerd
4	Gelijkwaardig aan gebruik in de branche/voorspelbaar
3	**Vastgesteld op organisatieniveau**
2	Beheerst op afdelingsniveau
1	Ad hoc / infomeel
0	Geen aandacht

2.2.2.4 ISO 27001-cyclus

Een ISO-certificaat is 3 jaar geldig en wordt ieder jaar getoetst. Op 13 mei 2022 is de 2e controle-audit met een positief resultaat afgerond.

Figuur 1 ISO 27001-cyclus.

Bron: Nederlands Certificatie Instituut (NCI)

2.2.3 Voldoende continuïteit in de ingevulde verruimde capaciteit

Verruimde capaciteit

Tot 2018 waren er geen specifieke budgetten benoemd voor informatieveiligheid. De kosten voor informatiebeveiliging werden primair bekostigd uit het ICT-projectenbudget en bij onvoldoende dekking werd geput uit het reguliere budget Basisinfrastructuur. Vanuit het Fit For Future budget (FFF), zijn

[12] Centrum Informatiebeveiliging en Privacybescherming (CIP), Criteria BIO-SA, februari 2021, blz. 5.

informatieveiligheid-projecten gefinancierd tot de vaststelling van de Datavisie. Met de vaststelling van de Datavisie (8 mei 2020) wordt ingestemd met een begrotingswijziging 2020 en aanpassing van de meerjarenraming 2021 tot en met 2023. Het betreft:

- Verhogen van het organisatiekostenbudget (OKB) met 5,6 fte per jaar voor de periode van 2020 t/m 2023 voor de inrichting van het CIO-office.
    - Realiseren CIO office € 2,33 miljoen
    - Ophoging OKB CIO office € 2,5 miljoen

Voldoende continuïteit

In juni 2018 is een Chief Information Officer (CIO) aangesteld, die nog steeds deze functie bekleedt. In de vijf jaar daarvoor was er bewust gekozen om van de CIO géén aparte functie te maken en werd de CIO-rol door vijf verschillende personen, al dan niet tijdelijk, ingevuld.[13]

De taken van een Chief Information Security Officer (CISO) werden tot 2018 uitgevoerd door een medewerker van ICT-beheer. Met de komst van het CIO-office vervult deze medewerker, tot op de dag van vandaag, fulltime de functie van CISO.

2.3 Onderbouwing beoordeling opdrachten PS

2.3.1 Informatiesessies over informatiebeveiliging georganiseerd

Op 14 februari 2020 is er een themabijeenkomst georganiseerd waarin de Datavisie Provincie Noord-Brabant 2020-2025 is besproken. Tijdens deze themabijeenkomst is door GS een inhoudelijke toelichting gegeven over het voorliggende kader. PS hebben een aantal vragen, zorgen en kritiekpunten geuit, waardoor een tweede themabijeenkomst is georganiseerd op 6 maart.[14]

Met het organiseren van twee themabijeenkomsten is voldaan aan de opdracht uit PS-besluit 56/18 om in het kader van bewustwording, in samenwerking met de ambtelijke organisatie, een informatiesessie over informatiebeveiliging voor PS te organiseren.

2.3.2 Alertheid en structurele aandacht voor informatieveiligheid

PS werden in 2018 opgeroepen om, met het oog op hun controlerende rol, alert te blijven op de informatieverstrekking door GS over informatieveiligheid en zelf meer structureel aandacht te vragen voor het onderwerp.

Tijdens de PS-vergadering over de vaststelling van de Datavisie (8 mei 2020), doet de verantwoordelijk gedeputeerde de volgende toezegging: *"*Statenleden periodiek (vaker dan eenmaal per jaar) mee te zullen nemen in de bewustwording van data, dataficering en digitalisering, d.m.v. ondersteuning door het college

[13] Zuidelijke Rekenkamer, Bestuurlijk rapport Informatieveiligheid provincie Noord-Brabant, blz. 22.
[14] Memo van de gedeputeerden over Themabijeenkomst Datavisie, 21 februari 2020 (1029275/4658414).

van GS in werkbezoeken, bijeenkomsten en experts in digitalisering en ethiek."

Met deze toezegging hebben PS structurele aandacht voor de Datavisie geborgd, maar niet specifiek voor informatieveiligheid. Structurele aandacht voor informatieveiligheid is dus niet automatisch geborgd. PS dienen ook alert te blijven of de toezegging van GS wel daadwerkelijk wordt ingevuld. In 2021 heeft (slechts) één bijenkomst[15] plaatsgevonden en in 2022 tot nog toe geen.

2.3.2.1 (Technische) Statenvragen

Na PS-besluit 56/18 (14 september 2018):

- zijn er geen schriftelijke vragen over informatieveiligheid gesteld;
- is er 1 technische vraag over informatieveiligheid gesteld.

Technische vraag

Tijdens de behandeling van de Bestuursrapportage 2020 stelt de PVV de volgende technische vraag over informatieveiligheid (15 oktober 2020): "Op welke wijze wordt de security van de ICT-basisinfrastructuur gewaarborgd?"

Antwoord GS: "De ICT-basisinfrastructuur is na een Europese aanbesteding uitbesteed aan OGD ICT-diensten. Deze leverancier levert, conform contractuele afspraken, haar diensten volgens de eisen vanuit de ISO27001, en sluit aan op de voor provincie Noord-Brabant geldende Baseline Informatiebeveiliging Overheid (BIO). De leverancier verklaart door middel van een extern opgestelde in control verklaring (ICV) jaarlijks dat zij voldoet aan de eisen die door de BIO worden gesteld. Tevens zal de Provincie Noord-Brabant op basis van audits onderzoeken of de compliance van de desbetreffende leverancier voldoet."

2.4 Huidige stand van zaken

2.4.1 Informatieveiligheid

De "heilige driehoek"

Hackers kunnen relatief eenvoudig een netwerk binnendringen als de onderstaande zaken niet goed geregeld zijn:

- ontbrekende patches[16]
- zwakke wachtwoorden
- ontbrekende netwerksegmentatie[17]

[15] Data & Ethiek (17 september 2021): over digitale transformatie, waaronder het gebruik van data, de techniek van het gebruik van algoritmes en bijbehorende ethische vraagstukken. De sessie werd georganiseerd door het CIO-Office.
[16] Een patch is een aanpassing (update) van bestaande software om de fouten of bugs in die software te verbeteren.
[17] Wanneer er geen segmenten zijn, kunnen alle aanwezige devices met elkaar communiceren. Een hacker heeft dan overal toegang toe en virussen kunnen eenvoudig van de ene naar de andere device overspringen. Is er sprake van netwerksegmentatie dan kun je schade bij een hack of besmetting beperken.

Als één van de drie goed is geregeld dan is er direct minder risico op heel grote schade. Optimaal is als alle drie in orde zijn. Dit is het geval bij de provincie.

- ✓ De provincie beschikt over professionele scanapparatuur die niet-gepatchte servers in de netwerkomgeving signaleert.
- ✓ Een sterk wachtwoord heeft een lengte van minimaal 8 posities en is complex van samenstelling. Binnen de provincie moet een wachtwoord bestaan uit minimaal 9 tekens en complex van samenstelling zijn.
- ✓ In 2019 heeft de provincie samen met een externe partij een blauwdruk beveiligingsinfrastructuur ontwikkeld, waardoor is geborgd dat er binnen de organisatie gebruik wordt gemaakt van segmentering.

Forum Standaardisatie

Forum Standaardisatie is een adviescommissie met deskundigen uit diverse overheidsorganisaties, het bedrijfsleven en de wetenschap. De leden worden op persoonlijke titel benoemd door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties Forum Standaardisatie rapporteert halfjaarlijks over het gebruik van informatieveiligheid-standaarden. Voor deze meting maken zij gebruik van Internet.nl. Deze website test de informatieveiligheidsstandaarden volgens de richtlijnen van het Nationaal Cyber Security Centrum. De provincie Noord-Brabant behaalt op deze website een score van 100%.

Bemensing en budget

In 2018 waren de functies van Chief Information Officer, Chief Information Security Officer en Functionaris Gegevensbescherming reeds door de provincie ingevuld. Sindsdien is het CIO-office uitgebreid met de volgende functies:

- Strateeg Digitale transformatie;
- Beleidsmedewerker digitale transformatie (2x);
- Programmabeheerser;
- Lead enterprise architect;
- Projectleider sensordata;
- Beleidscommunicatieadviseur.

In 2021 zijn 5 personen opgeleid tot erkende IS0 27001-auditor. Het betreft 2 personen uit het CIO-office en 3 personen uit het team concern control. Deze auditors gaan vanaf februari 2022 tweewekelijks aan de slag om onderwerpen op het gebied van de ISO 27001 intern te auditen.

Jaarlijks is er circa € 200.000 beschikbaar voor het (laten) uitvoeren van hele concrete informatieveiligheid acties, zoals: pentesten, audits, het inhuren van mystery guests, bewustwordingsacties, etc.

Conform de ‘Uitvoeringsagenda Digitale Transformatie 2021-2022’ wordt eind juni/begin juli 2022 een evaluatie van de voorgenomen en uitgevoerde activiteiten aan PS gerapporteerd. Bij deze zogenoemde midterm-rapportage ontvangen PS ook de structurele herijking van de budgetten voor CIO-office, ICT en

Informatieveiligheid.[18] Een belangrijk moment dus voor de controlerende taak en het budgetrecht van PS inzake informatieveiligheid.

2.4.2 Aandachtspunten

Informatieveiligheid is nooit ‘klaar’. Het feit dat de provincie gecertifieerd is voor BIO en ISO 27001 betekent niet dat de provincie niet gehackt kan worden. Certificering is geen garantie, maar het geeft aan dat de processen op orde zijn. De rekenkamer heeft enkele externe beveiligingsexperts (zie bijlage 2) gevraagd naar de belangrijkste aandachtspunten als je als organisatie gecertificeerd bent. Hieruit kwamen de volgende aandachtspunten naar voren:

- Gecertificeerd blijven.
- Scope van de certificering: welke informatie en bedrijfsonderdelen maken deel uit van certificering?
- Scope en kwaliteit van uitgevoerde (penetratie)testen.
- Mate waarin je als organisatie in staat bent om proactief op dreigingen te reageren en in een vroeg stadium te stoppen.
- Mate van controle en overzicht van de omgeving.

[18] Begroting 2022 (PS 55/21), blz.98.

Bijlage 1 Geraadpleegde documenten en gebruikte afkortingen

Documenten provincie Noord-Brabant

- Besluit 56/18 Rapport Zuidelijke Rekenkamer Informatieveiligheid, 14 september 2018
- Memo van de gedeputeerde, Maatregelen ter verhoging informatieveiligheid, 17 december 2018
- Statenmededeling Voortgang Datavisie, 5 februari 2019
- Statenvoorstel 09/20a Vaststelling Datavisie Provincie Noord-Brabant 2020-2025, 7 januari 2020
- Waardengedreven digitaal transformeren. Datavisie Provincie Noord-Brabant 2020-2025, 7 januari 2020
- Informatievisie, Samen, Slim en Innovatief, 7 januari 2020
- Aangepast Statenvoorstel Vaststelling Datavisie Provincie Noord-Brabant 2020-2025, 14 februari 2020
- Memo van de gedeputeerden, Themabijeenkomst Datavisie, 21 februari 2020
- Besluit 09/20 Vaststelling Datavisie Provincie Noord-Brabant 2020-2025, 8 mei 2020
- Besluit 58/20 Notulen vergadering Provinciale Staten d.d. 8 mei 2020, 11 september 2020
- Uitvoeringsagenda Digitale Transformatie 2021-2022, 30 maart 2021
- Stand van zaken moties en toezeggingen per 7 april 2021

Overige documenten

- Zuidelijke Rekenkamer, Informatieveiligheid provincie Noord-Brabant, 31 augustus 2018
- Baseline Informatiebeveiliging Overheid, versie 1.04, 4 november 2019
- Circulaire toepassen Baseline Informatiebeveiliging Overheid, 12 februari 2020

Gebruikte afkortingen

AVG: Algemene verordening gegevensbescherming
(Wet) BIBOB: Wet bevordering integriteitsbeoordelingen door het openbaar bestuur
BIJ12: Uitvoeringsorganisatie voor de samenwerkende provincies
BIO: Baseline Informatiebeveiliging Overheid
CIO: Chief Information Officer
CISO: Chief Information Security Officer
FG: Functionaris Gegevensbescherming
GS: Gedeputeerde Staten
ICV: In Control Verklaring
IPO: Interprovinciaal Overleg
ISMS: Information Security Management System
ISO: Internationale Organisatie voor Standaardisatie
NEN: Nederlandse Norm / Stichting Koninklijk Nederlands Normalisatie Instituut
PS: Provinciale Staten

Bijlage 2 Lijst gesprekspartners

Provincie Noord-Brabant

- Chief Information Officer.

Andere organisaties

- Senior adviseur onderzoek, verandermanagement bij BMC
- Consultant Corporate & Cybersecurity bij Hoffmann Bedrijfsrecherche B.V.
- Senior Security Specialist & Public Speaker bij Secura B.V.