Vervolgonderzoek Informatieveiligheid

Provincie Noord-Brabant

Bestuurlijk rapport

juli 2022

ZUIDELIJKE REKENKAMER

Inhoudsopgave

1 Bestuurlijke hoofdpunten

1.1 Borging informatieveiligheid zeer belangrijk

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 forse toename vergeleken met eerdere jaren. De verwachting is dat deze trend zich doorzet en cyberaanvallen de grootste bedreiging zal zijn voor bedrijven in 2022.

Met het oog op deze ontwikkelingen heeft de rekenkamer een vervolgonderzoek uitgevoerd naar informatieveiligheid van de provincie Noord-Brabant. In 2018 publiceerden we de uitkomsten van onze onderzoeken naar informatieveiligheid. In het eerste kwartaal van 2022 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 opdracht die PS gaven naar aanleiding van ons onderzoek om onze aanbevelingen op te volgen?

1.2 Conclusies

De rekenkamer concludeert dat de provincie Noord-Brabant in korte tijd grote stappen heeft gezet, waarbij informatieveiligheid daadwerkelijk naar een hoger niveau is getild. 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[2] provincie die hiervoor is gecertifieerd.

Ook PS hebben grotendeels voldaan aan de opdracht, maar structurele aandacht voor Informatieveiligheid blijft een aandachtspunt.

[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] Peildatum 22 april 2022.

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. Zoals ook in het onderzoek in 2018 is aangegeven, komt een bekend model over bewustwording en leren van de hand van Maslow. Hij ziet 'leren' als een patroon waarbinnen vier fases onderscheiden kunnen worden. Als we naar de provincie kijken door de bril van het model van Maslow, dan had de provincie zich over het geheel genomen reeds ontwikkeld van *onbewust onbekwaam* en *bewust onbekwaam*, naar *bewust bekwaam*. Binnen bewust bekwaam heeft ze zich afgelopen 3,5 jaar verder ontwikkeld en is ze gegroeid. 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 te vergroten.

1.3 Aanbevelingen

De rekenkamer beveelt Gedeputeerde Staten aan om, gezien de risico's en mogelijke gevolgen van beveiligingsinbreuken voor de provincie, haar handelen op de ingeslagen weg voort te zetten en continuïteit van de ingevulde verruimde capaciteit te waarborgen.

Provinciale Staten roepen we op om:

- GS financieel in staat te blijven stellen om de ingeslagen weg voort te kunnen zetten.
- zelf structureel aandacht te blijven schenken aan informatieveiligheid. Bewaak de toezegging van GS met betrekking tot informatieverstrekking en voorlichting en grijp bijvoorbeeld de verkiezingen 2023 aan om in het introductieprogramma voor (nieuwe) Statenleden aandacht te besteden aan informatieveiligheid.

2 Onderbouwing hoofdpunten

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[3] provincie die hiervoor is gecertificeerd.

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 zelfs 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 een makkelijke toegang tot meer informatie. Daar is de afgelopen 3,5 jaar nauwelijks gebruik van gemaakt.

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 is deels uitgevoerd.
rood: niet uitgevoerd.

[3] Peildatum 22 april 2022.

Tabel 1 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.

Zie voor een uitgebreide onderbouwing van onze bevindingen het rapport van bevindingen van dit onderzoek, Daarin wordt ook een toelichting gegeven op de onderzoeksaanpak.

3 Bestuurlijke reactie GS en nawoord rekenkamer

3.1 Bestuurlijke reactie GS

Op 7 juli 2022 ontving de rekenkamer de bestuurlijke reactie van GS. Deze is hieronder integraal opgenomen.

“Geacht bestuur van de Zuidelijke Rekenkamer,

Graag willen we u hartelijk danken voor de hoeveelheid werk die u verzet heeft om de informatie te bestuderen, te analyseren en er conclusies aan te verbinden. Wij zijn verheugd dat u in lijn met de externe auditor concludeert dat de provincie Noord-Brabant in korte tijd grote stappen heeft gezet op het gebied van informatieveiligheid, waarbij informatieveiligheid ook daadwerkelijk naar een hoger niveau is getild, om zodoende invulling te geven aan het kader vanuit de rijksoverheid (Baseline Informatiebeveiliging Overheid) en interprovinciale afspraken (NEN-ISO 27001).

De door u gedane aanbeveling om, gezien de risico’s en mogelijke gevolgen van beveiligingsinbreuken voor de provincie, haar handelen op de ingeslagen weg voort te zetten en continuïteit van de ingevulde verruimde capaciteit te waarborgen, onderschrijven wij.

Tot slot:
Willen wij onze waardering uitspreken voor het uitgevoerde onderzoek. De uitkomsten van uw onderzoek inspireren ons om op de ingeslagen weg verder te gaan, om zo aan PS, de provinciale organisatie en onze inwoners te laten zien dat wij het onderwerp informatieveiligheid zeer serieus nemen.”

3.2 Nawoord rekenkamer

De rekenkamer bedankt GS voor de bestuurlijke reactie en de waardering voor het uitgevoerde onderzoek. Informatieveiligheid is en blijft een belangrijk vraagstuk voor overheidsorganisaties. De rekenkamer spreekt de hoop uit dat de provincie Noord-Brabant het hogere niveau aan informatieveiligheid dat is bereikt sinds ons onderzoek in 2018 weet vast te houden. Gelet op de vooruitgang die we hebben kunnen vaststellen en de ambities van de betrokken medewerkers, hebben wij er vertrouwen in dat dit komende jaren zal worden gerealiseerd.