Vervolgonderzoek Informatieveiligheid

Provincie Limburg

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 Limburg. 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 Limburg na ons vorige onderzoek goede en flinke stappen heeft gezet waardoor sprake is van een duidelijke verbetering op het gebied van informatieveiligheid. Het rekenkameronderzoek blijkt daarbij een flinke stimulans te zijn geweest, waardoor de provincie van reactief naar proactief is gaan handelen bij het waarborgen van een goede beveiliging van haar informatie.

De provincie moest van ver komen. De opdracht van PS om onze aanbevelingen op te volgen is serieus opgepakt en er is flinke beweging geweest. Het is echter nog niet gelukt om de opdracht helemaal uit te voeren. Er wordt namelijk nog niet voldaan aan het nagestreefde basisniveau voor informatiebeveiliging en het is niet gelukt om op korte termijn procedures, processen en maatregelen in het managementsysteem te verwerken. De provincie Limburg is daarmee nog niet klaar voor certificering op de nagestreefde ISO27001-norm en de eisen uit de Baseline Informatiebeveiliging Overheid (BIO) welke het basisniveau voor informatiebeveiliging geeft. In 2022 moeten dus nog stappen worden gezet om uiterlijk 1 januari 2023

[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.

klaar te zijn voor voornoemde certificering, zoals afgesproken in interprovinciaal verband.
Ook PS hebben niet geheel voldaan aan de opdracht. Structurele aandacht voor informatieveiligheid blijft voor PS een aandachtspunt.

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 intensief voort te blijven zetten. Daarbij te zorgen:

- dat de provincie op 1-1-2023 ook daadwerkelijk klaar is voor certificering;
- dat een nieuw bewustwordingsprogramma voor medewerkers en bestuurders wordt opgesteld en uitgevoerd; nu het oude programma dit jaar wordt afgerond en de mens doorgaans de zwakste schakel van elk beveiligingssysteem is;
- dat ze PS jaarlijks blijven informeren over ontwikkelingen en de uitvoering van het informatieveiligheidsbeleid;
- voor voldoende capaciteit op kwetsbare functies die nu door één persoon (gaan) worden ingevuld, waaronder voor de verplichte audits door het cluster Concern.

Provinciale Staten roepen we op om:

- GS financieel in staat te blijven stellen om de ingeslagen weg voort te kunnen zetten;
- mede met het oog op hun controlerende rol, zelf meer structureel aandacht te vragen voor het onderwerp. Grijp bijvoorbeeld de werkgroep Versterking Positie PS aan om de dialoog met GS aan te gaan over informatieveiligheid en de verkiezingen 2023 om in het introductieprogramma voor (nieuwe) Statenleden ook 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 deels aan deze opdracht hebben voldaan. De toenemende aandacht voor informatieveiligheid is voortgezet, de inspanningen zijn geïntensiveerd en te nemen maatregelen zijn gerichter gekozen, vastgesteld en voortvarender geïmplementeerd. Verder zijn periodiek de voorgenomen penetratietesten uitgevoerd.[2] De bevindingen daarvan laten een duidelijke verbetering zien ten opzichte van ons eerdere onderzoek. Daarnaast is het bewustwordingsprogramma voor medewerkers en bestuurders voortgezet, dat in 2022 wordt afgerond. Ook zijn PS jaarlijks actief en uitgebreid geïnformeerd over de uitvoering.

Het is echter nog niet gelukt om te voldoen aan het nagestreefde basisniveau voor informatiebeveiliging en het op korte termijn verwerken van procedures, processen en maatregelen in het Information Security Management Systeem (ISMS), zo constateert de rekenkamer. De provincie Limburg is daarmee ook nog niet klaar voor certificering op de nagestreefde ISO27001-norm en de eisen uit de Baseline Informatiebeveiliging Overheid (BIO) welke het basisniveau voor informatiebeveiliging geeft. Wel zijn daartoe stappen gezet. Zo zijn er naar aanleiding van het rekenkamerrapport en een eind 2017 uitgevoerd onderzoek naar de risico's op het gebied van cybersecurity diverse maatregelen getroffen die een positief effect hebben gehad op de scores met betrekking tot het nagestreefde niveau. Het rekenkameronderzoek heeft de provincie gestimuleerd om op het gebied van informatiebeveiliging van reactief, proactief te gaan handelen en om meer geld, tijd en capaciteit in te zetten. Dit heeft er onder andere in geresulteerd dat ook in de jaren daarna de nodige aanvullende technische maatregelen zijn geïmplementeerd en vooruitgang is geboekt. Maar de provincie moet in 2022 nog stappen zetten om uiterlijk 1 januari 2023 klaar te zijn voor voornoemde certificering, zoals afgesproken in interprovinciaal verband.

Gezien voorstaande bevindingen constateert de rekenkamer dat het afdoen van de PS-opdracht in 2020 door GS dan ook voorbarig was.[3]

De rekenkamer stelt verder vast dat PS ook maar deels hebben voldaan aan de oproep die aan hun was gericht. De aandacht vanuit PS voor informatieveiligheid is namelijk nog steeds niet structureel, maar incidentgedreven. Er is (daarmee) ook geen structurele dialoog geweest tussen PS en GS over het onderwerp. De jaarlijkse rapportages van GS sinds 2018 over de uitvoering en het geactualiseerde informatiebeveiligingsbeleid zijn voor kennisgeving aangenomen. Wel is vanuit PS bij bespreking van het geactualiseerde Strategische Informatiebeleid Limburg (SIBL) het belang van informatieveiligheid onderkent en benadrukt. Eind 2021 is vanuit PS een werkgroep Versterking Positie PS gevormd. Deze richt zich onder andere op verbetering van de informatiehuishouding en vraagt daar aandacht voor. Daarnaast is er een kernteam digitalisering opgericht bestaande uit afgevaardigden van de ambtelijke

[2] Hierbij worden de systemen van de provincie in opdracht van de provincie door ethisch hackers getoetst op risico's en kwetsbaarheden. Eventuele kwetsbaarheden worden gebruikt om in de systemen in te breken. Er wordt daarmee getoetst of de informatie in de praktijk voldoende beschermd is tegen toegang door onbevoegden en kwaadwillenden.
[3] Bron: www.limburg.bestuurlijkeinformatie.nl: aanbevelingen rekenkameronderzoek afgedaan (deadline 21-6-2019).

organisatie en de griffie. Via deze werkgroep en kernteam kan aandacht worden gevraagd voor, en de dialoog worden aangegaan met GS over, informatieveiligheid.

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: dit deel is niet uitgevoerd.

Tabel 2 Mate waarin opdracht van PS Limburg naar aanleiding van rekenkameronderzoek 2018 is uitgevoerd (april 2022)

Opdrachten aan GS		Uitgevoerd?	Acties GS vanaf 2018
1	Zet toenemende aandacht voort en intensiveer de inspanningen:		✓ Meer financiële middelen, tijd en capaciteit beschikbaar en ingezet. ✓ Van reactief naar proactief handelen. ✓ Vele maatregelen gerealiseerd die hebben geleid tot betere beveiliging.
2	Zet daarbij met kracht in op voldoen aan basisambitieniveau		• Begin 2022 voldeed de provincie nog niet aantoonbaar aan het nagestreefde niveau voor informatieveiligheid. Daarmee moet de provincie in 2022 ook nog stappen zetten om te voldoen aan de interprovinciale afspraak om uiterlijk 1-1-2023 klaar te zijn voor ISO27001-certificering (processen voldoen aan deze ISO-normen welke alle maatregelen voortkomend uit de BIO omvatten). In 2022 krijgt dat de meeste aandacht. In de eerste jaren heeft de focus vooral gelegen op het implementeren en verbeteren van technische maatregelen.
3	Neem op korte termijn procedures, maatregelen e.d. op in het nieuwe managementsysteem		• De provincie verwacht in juli 2022 klaar te zijn met het ‘invullen’ van het managementsysteem (ISMS) en na de zomer daarmee te gaan werken (zie ook bovenstaande cel).
4	Implementeer maatregelen voortvarender en stuur op realisatie		✓ Meer geld, tijd en capaciteit ingezet. Van reactief naar proactief handelen. ✓ Vele (technische) maatregelen gerealiseerd, waaronder systemen en tools om dreigingen/kwetsbaarheden te kunnen signaleren zoals ransomware. ✓ Bewustwordingscampagne voortgezet (serious game). ✓ Tweewekelijks overleg ingesteld voor o.a. (bij)sturing op realisatie.
5	Voer periodiek penetratietesten uit		✓ Elk jaar een penetratietest laten uitvoeren, waarvan alleen in 2020 onderbouwd is afgeweken

6	Stel maatregelen vast en prioriteer o.b.v. aandachtspunten uit pentesten, incidenten e.d. Schat daarvoor benodigde capaciteit en financiële middelen in en stuur op realisatie maatregelen		✓ Informatiebeveiligingsbeleid herijkt (eind 2019), informatiebeleid welke informatieveiligheid omvat geactualiseerd (SIBL 2021-2024, eind 2021) en bijhorende projectenportfolio daarop aangepast. ✓ In inkoopvoorwaarden aanvullende voorwaarden voor informatieveiligheid bij ICT aanbestedingen. ✓ Tweewekelijks overleg: bespreken stand van zaken maatregelen, bepalen of bijsturen nodig is en indien nodig ook bijsturen. ✓ Jaarlijkse inschatting financiële middelen specifiek voor informatiebeveiliging.
7	Informeer PS actief over uitvoering informatiebeveiligingsbeleid		✓ Jaarlijkse rapportage over uitvoering informatiebeveiligingsbeleid, ontwikkelingen, incidenten. ✓ Eind 2019 geactualiseerd informatiebeveiligingsbeleid ter informatie aan PS. ✓ In 2021 2x mededeling portefeuillehouder over beveiliging systemen BIJ12 (incident).
Opdrachten aan PS		**Uitgevoerd?**	**Acties PS vanaf 2018**
8	Blijf alert op informatieverstrekking door GS en/of vraag zelf meer structureel aandacht voor het onderwerp		• Aandacht vanuit PS nog steeds niet structureel maar incidentgedreven. Nog geen structurele dialoog geweest tussen PS en GS over het onderwerp. - Jaarlijkse rapportages GS en informatiebeveiligingsbeleid niet besproken. - PS zelf maar sporadisch en alleen in 2018 en 2019 na incidenten aandacht gevraagd voor het onderwerp.

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 5 juli 2022 ontving de rekenkamer de bestuurlijke reactie van GS Limburg. Deze is hieronder integraal opgenomen.

“Met belangstelling hebben wij kennis genomen van het conceptrapport "Vervolgonderzoek Informatieveiligheid Provincie Limburg". Graag maken wij van de geboden gelegenheid gebruik om op het conceptrapport te reageren.

Het groeiende belang van informatiebeveiliging is evident. Bijna dagelijks worden wij via de media geconfronteerd met berichten over cyberaanvallen bij bedrijven en instellingen, vaak met enorme gevolgen. Wij realiseren ons dat, ondanks al onze inspanningen op dit gebied, de kans om slachtoffer te worden van cyberaanvallen ook binnen de Provincie Limburg reëel aanwezig is.

De conclusie van uw rekenkamer dat de Provincie Limburg na het vorige onderzoek goede en flinke stappen heeft gezet, wordt door ons onderschreven. Uw onderzoek uit 2018 is voor ons een stevige stimulans geweest om de gedane aanbevelingen serieus op te pakken. Wij zijn mét u van mening dat hierdoor sprake is van een duidelijke verbetering op het gebied van informatieveiligheid, waardoor de provincie bij het waarborgen van een goede beveiliging van haar informatie van reactief naar proactief is gaan handelen.

U constateert daarnaast terecht dat het nog niet gelukt is om (aantoonbaar) te voldoen aan het nagestreefde basisniveau voor informatiebeveiliging en dat het ons niet gelukt is om op korte termijn procedures, processen en maatregelen in het managementsysteem te verwerken. Wij zijn echter, conform ons vastgestelde implementatieplan, voornemens de noodzakelijke stappen te zetten om uiterlijk 1 januari 2023 klaar te zijn voor certificering op de nagestreefde ISO27001-norm en de eisen uit de Baseline Informatiebeveiliging Overheid (BIO). Daarnaast verwachten wij in de loop van de komende maanden het managementsysteem voor informatieveiligheid formeel in gebruik te nemen, waarmee de opzet en het bestaan van de maatregeĺen, richtlijnen en werkwijze aantoonbaar worden en de door de rekenkamer benoemde aandachtspunten worden opgelost.

De door u gedane aanbevelingen passen naadloos binnen onze eigen plannen en nemen wij dan ook graag over. Wij zijn voornemens, gebaseerd op onze ervaringen van de afgelopen jaren, een nieuw bewustwordingsprogramma voor medewerkers en bestuurders te starten, waarbij wij overwegen ook nieuwe instrumenten in te zetten. Ook zullen wij, zoals we al sinds 2017 doen, PS jaarlijks en indien nodig tussentijds blijven informeren over ontwikkelingen en de uitvoering van het informatieveiligheidsbeleid. Tevens zullen wij zorgen voor voldoende capaciteit op kwetsbare functies, waarbij wij de mogelijkheid om naar behoefte externe deskundigheid in te huren ook in de toekomst open houden.

Wij zullen onze verhoogde aandacht voor informatieveiligheid en onze inspanningen op dat gebied ook in de toekomst voortzetten. De implementatie van de ISO27001-norm biedt ons hierbij een uitstekend kader, dat een risicogerichte PDCA[4]-sturing op onze informatieveiligheid ondersteunt, waardoor informatieveiligheid nog beter ingebed wordt in onze bedrijfsvoering.

Tenslotte merken wij op dat het onderzoek van de rekenkamer zich nadrukkelijk ook richt op de vraag in hoeverre Provinciale Staten zelf voldaan hebben aan de opdracht die PS in 2018 aan zichzelf gegeven hebben. Ons College heeft kennis genomen van uw bevindingen, conclusies en aanbevelingen inzake deze onderzoeksvraag, maar achten het aan de Staten om daar inhoudelijk op te reageren."

3.2 Nawoord rekenkamer

De rekenkamer ziet in de bestuurlijke reactie dat GS het belang van goede informatiebeveiliging onderstrepen en voornemens zijn hun inspanningen op dat gebied te continueren. Het onderzoek van de rekenkamer in 2018 heeft daarbij een impuls gegeven.
De rekenkamer constateert dat GS de conclusies en de aanbevelingen die aan hen gericht zijn, onderschrijven en overnemen. Belangrijk is dat maatregelen die zijn gepland voor de tweede helft van 2022 ook daadwerkelijk tot uitvoering komen. Gelet op de bestuurlijke reactie en de ambities van de betrokken ambtenaren, heeft de rekenkamer vertrouwen dat noodzakelijke en verdere stappen zullen worden gezet.

[4] Plan-Do-Check-Act.