Vervolgonderzoek Informatieveiligheid

Provincie Limburg

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 Limburg. Dit rapport van bevindingen bevat het feitencomplex daarvan. Het bestuurlijk rapport geeft de bestuurlijke hoofdpunten, de bijbehorende conclusies en onderbouwing daarvan, aanbevelingen, bestuurlijke reactie en nawoord van de rekenkamer.

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 Limburg. 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 opdracht die PS gaven naar aanleiding van ons onderzoek?

Heel in het kort kwam deze opdracht erop neer dat GS de toenemende aandacht voor informatieveiligheid moesten voorzetten en inspanningen moesten intensiveren om onder andere aan het basisambitieniveau te voldoen. PS werden opgeroepen om alert te blijven op de informatieverstrekking door GS over informatieveiligheid en/of zelf meer structureel aandacht te vragen voor het onderwerp. In het vervolg van dit rapport komt de opdracht uitgebreid aan de orde.

[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. En www.autoriteitpersoonsgegevens.nl (mei 2022): aantal meldingen van datalekken veroorzaakt door cyberaanvallen in 2021 bijna verdubbeld ten opzichte van het jaar daarvoor.
[3] www.managementimpact.nl, 3 maart 2022, www.consultancy.nl onderzoek PWC, 30 maart 2022 en Cyber Security Predictions rapport van Check Point.

1.2 Doelstelling en onderzoeksvragen

Doel is om PS van de provincie Limburg inzicht te geven in hoeverre GS en PS de opdracht van PS naar aanleiding van het rekenkameronderzoek Informatieveiligheid uit 2018 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 Limburg.

De onderzoeksvragen zijn:

1. Welke veranderingen hebben er vanaf 2018 bij de provincie Limburg plaatsgevonden op het gebied van informatieveiligheid qua beleid en uitvoering in de praktijk?
2. In hoeverre hebben GS (hiermee) voldaan aan de opdracht die ze in 2018 van PS kregen naar aanleiding van ons onderzoek?
3. In hoeverre hebben PS opvolging gegeven aan de oproepen naar aanleiding van ons onderzoek?
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
Opdracht PS informatieveiligheid	2 en 3	GS en PS hebben de opdracht van PS uit 2018 uitgevoerd

1.3.2 Onderzoeksmethodiek

Het onderzoek richt zich op de periode juli 2018 (publicatie rekenkameronderzoek) 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 30 mei en 3 juni 2022 zijn de ambtelijke reacties ontvangen van respectievelijk de ambtelijke organisatie en de griffie van de provincie. 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

In dit hoofdstuk geven we eerst op hoofdlijnen inzicht in hoeverre GS en PS Limburg de opdracht van PS naar aanleiding van ons rapport Informatieveiligheid uit 2018 hebben uitgevoerd. Daarna geven we per onderdeel daarvan een onderbouwing; hoe is de opdracht van PS ingevuld. Daarmee wordt ook antwoord gegeven op de vraag welke veranderingen er na ons eerdere onderzoek hebben plaatsgevonden en wat de huidige stand van zaken is.

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 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.[4] De bevindingen daarvan laten een duidelijke verbetering zien ten opzichte van ons eerdere onderzoek. Daarnaast is het bewustwordingsprogramma 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.[5]

[4] Hierbij worden de systemen van de provincie in opdracht van de provincie door ethisch hacker getoetst op risico's en kwetsbaarheden. Tijdens de test worden de eventuele kwetsbaarheden ook werkelijk gebruikt om in de systemen in te breken. Er wordt daarmee dus getoetst of de informatie van de provincie in de praktijk voldoende beschermd is tegen toegang door onbevoegden en kwaadwillenden.
[5] Bron Stateninformatiesysteem (www.limburg.bestuurlijkeinformatie.nl): aanbevelingen rekenkameronderzoek (nummer 1482) afgedaan (deadline 21-6-2019).

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.

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.

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.

2.2 Nog niet op basisambitieniveau informatieveiligheid

Begin 2022 voldeed de provincie nog niet aan het basisambitieniveau voor informatieveiligheid en was ze nog niet klaar certificering op de ISO27001-norm. Dit blijkt uit een audit die eind 2021 is uitgevoerd en andere door de rekenkamer bestudeerde documenten en gevoerde gesprekken.

De Baseline Informatiebeveiliging Overheid (BIO) is een normenkader voor informatiebeveiliging en geeft het basisniveau voor informatiebeveiliging. Het omvat een standaardwerkwijze om te bepalen welke maatregelen getroffen moeten worden. Deze nieuwe overheidsbrede baseline verving eind 2018 de Interprovinciale Baseline Informatiebeveiliging (IBI).[6] Het basisambitieniveau is hetzelfde gebleven; vanuit de BIO zijn alleen enkele maatregelen scherper gedefinieerd. Verder hebben de provincies in 2017 gezamenlijk besloten binnen vijf jaar, uiterlijk 1-1-2023, klaar te willen zijn voor ISO27001-certificering.

[6] Daartoe is besloten op 13 september 2018 in IPO-verband in de Bestuurlijke Adviescommissie Financiën en e-Provincies. Vervolgens is de BIO in december 2018 vastgesteld door de ministerraad (rijksoverheid).

Daadwerkelijke certificering is echter niet verplicht. De hierbij behorende maatregelenset (ISO27002) is het fundament onder de BIO.

ISO27001 is de standaard/normering voor het proces van informatiebeveiliging. De basis voor deze norm is het managementsysteem voor informatiebeveiliging. Dit ISMS is een instrument om informatiebeveiliging te waarborgen en te besturen en wordt ondersteund door software. Het 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. Het vaststellen, implementeren, uitvoeren, controleren, beoordelen, onderhouden en voortdurend verbeteren gebeurt via een Plan-Do-Check-Act (PDCA-)cyclus. PDCA vormen daarmee samen het ISMS. Voldoen aan ISO27001 betekent dat het informatiebeveiligingsproces op uniforme wijze wordt uitgevoerd en de overheden op uniforme wijze kunnen aantonen hoe hun informatiebeveiliging ervoor staat.

De provincie Limburg geeft aan dat ze hiermee ook een interne professionaliseringsslag maken op het gebied van informatieveiligheid en ze als organisatie aantoonbaar meer 'in control' komen wat betreft informatiebeveiliging. Het basisbeveiligingsniveau wordt ermee op het gewenste niveau gehouden, wat inhoudt dat de informatiebeveiligingsrisico's ermee tot een acceptabel niveau worden beperkt (beheerst).

Informatieveiligheidsbeleid 2019 provincie Limburg:
Informatieveiligheid heeft betrekking op het garanderen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Het proces informatiebeveiliging geeft daar invulling aan.
Informatiebeveiliging betreft het definiëren, implementeren, onderhouden, handhaven en evalueren van een samenhangend stelsel van maatregelen gericht op het waarborgen van de beschikbaarheid, de integriteit, vertrouwelijkheid en controleerbaarheid van de (handmatige en geautomatiseerde) informatievoorziening. Het is een continu (verbeter)proces om de risico's tot een acceptabel niveau te reduceren.

In mei 2019 bleek uit een door een extern bureau uitgevoerde audit (0-meting) dat op nagenoeg alle onderscheiden punten het gewenste niveau niet werd gehaald door de provincie. Vervolgens is gestart met voorbereidingen voor implementatie van de ISO27001- en BIO-eisen. De focus lag daarbij eerst nog op het treffen van technische maatregelen en het wegnemen van geconstateerde kwetsbaarheden. In maart 2021 werd door de directie een projectplan/plan van aanpak vastgesteld dat vervolgens in uitvoering is genomen. De processen rondom informatiebeveiliging worden (her)ingericht conform de ISO-norm. De provincie wordt daarbij ondersteunt door een externe partij. Na voorbereidende activiteiten zijn de feitelijke werkzaamheden in september 2021 gestart.

In november 2021 kon op basis van een tweede, door een extern bureau uitgevoerde, audit (1-meting) niet in alle gevallen de compliance met de normering (ISO27001/BIO) worden aangetoond. De audit leidt tot een negatief advies voor certificering op de ISO27001- en BIO-eisen. Tijdens de audit zijn er 81 niet-kritieke afwijkingen vastgesteld en 1 kans voor verbetering. Het ISMS voldeed nog niet aan eisen. Ook was het nog niet doeltreffend; de PDCA was nog niet aantoonbaar aanwezig. Gesteld werd dat het belangrijk is dat beleidsregels en procedures worden geformaliseerd en het belang van goede

informatiebeveiliging aantoonbaar wordt uitgedragen. Enkele andere voorbeelden van afwijkingen zijn: verantwoordelijkheden zijn nog wat versnippert en nog niet helemaal compleet, er is nog geen auditprogramma en vaak ontbreekt het aan formeel beleid, plannen, procedures.

Op 31 januari 2022 is de eerste fase van het project afgesloten met het formeel vaststellen door het directieteam (DT) van de beschrijving van het ISMS: de high level structure (HLS). Hiermee zijn vastgelegd: de werkwijzen binnen de provinciale organisatie met betrekking tot het beheersen van informatiebeveiligingsrisico's en de verantwoordelijkheid van de directie hierin. Daarnaast is vastgelegd welke informatie binnen de organisatie wordt beveiligd. Daarmee is de scope bepaald, de reikwijdte waarbinnen het ISMS wordt toegepast. Het betreft:

- het proces serviceverlening van de informatievoorziening (organisatorisch)
- en daarmee de gehele digitale infrastructuur van de provincie voor zover die centraal door het cluster Organisatie en Informatie (O&I) geserviced c.q. ondersteund wordt; dit omvat ook de koppelingen met eventuele externe gehoste omgevingen zoals de cloud (informatietechnisch: deze informatie wordt beveiligd)
- fysiek betekent dit alle locaties waar gebruik wordt gemaakt van voornoemd proces en/of waar informatiecomponenten van de provincie aanwezig zijn.

In een gesprek is tegenover de rekenkamer aangegeven dat in 2022 de meeste aandacht zal uitgaan naar de implementatie van het ISMS. De tweede fase is gestart en afronding is voorzien voor juli 2022. Het betreft het beschrijven en formaliseren van de reeds getroffen en nog aanvullend te treffen maatregelen; deze worden afgestemd op de BIO. De derde fase, die na de zomer van 2022 zal starten, heeft betrekking op het implementeren van de nieuwe en aangescherpte maatregelen; het werken met het ISMS. Ook is de provincie voornemens om in het najaar van 2022 een externe proefaudit uit te laten voeren, waardoor duidelijk wordt op welke onderdelen mogelijk nog een extra inspanning geleverd moet worden. De laatste fase betreft dan een eventuele certificering. In Limburg is in dat kader externe certificering nog geen uitgemaakte zaak: ingegeven door de structurele kosten en administratieve last die dat met zich meebrengt. De rekenkamer constateert dat de provincie nog stappen moet zetten om vóór 2023 te voldoen aan de ISO27001- en BIO-norm.

2.3 Procedures, processen en maatregelen nog niet in ISMS

Zoals uit de vorige paragraaf blijkt, was de provincie begin 2022 nog bezig met de implementatie van het ISMS. In een gesprek met ambtelijk betrokkenen is aangegeven dat in de eerste jaren na het rekenkameronderzoek de focus vooral heeft gelegen op het implementeren en verbeteren van technische maatregelen en het wegnemen van geconstateerde kwetsbaarheden. Dit om een betere beveiliging te realiseren. De provincie heeft er bewust voor gekozen om het formaliseren van processen en procedures later in het proces op te pakken. In 2020 werd gekozen voor een nieuwe ISMS-applicatie omdat een verdere uitrol van de bestaande applicatie gepaard zou gaan met forse licentiekosten. De verwachting is dat de procedures, processen en maatregelen in juli 2022 in het managementsysteem zijn opgenomen.

2.4 Voorgenomen maatregelen i.h.a. voortvarend gerealiseerd

De provincie heeft de afgelopen vier jaar vele maatregelen geïmplementeerd om risico's en kwetsbaarheden weg te nemen en een betere beveiliging te realiseren. (Bij)sturing vond plaats in een tweewekelijks overleg dat is ingesteld. Daarbij is de provincie gestimuleerd door het rekenkameronderzoek uit 2018 van reactief naar proactief gaan handelen en heeft meer geld, tijd en capaciteit ingezet.

Onderstaand worden voorbeelden gegeven van maatregelen die na het rekenkameronderzoek genomen zijn om informatieveiligheid op een hoger niveau te brengen. Meerdere daarvan zijn genomen naar aanleiding van de bevindingen uit de penetratietest van het rekenkameronderzoek. Met implementatie daarvan zijn alle geconstateerde kwetsbaarheden uit die pentest opgelost.

- Fysieke toegangsbeveiliging en zonering gebouw.
- Uitgebreide authenticatie en autorisatie in combinatie met 2-factor authenticatie voor externe toegang tot de provinciale informatievoorziening (2018). Deze is in 2021 vernieuwd.
- Aangescherpt wachtwoordbeleid geïmplementeerd (moeilijk te raden wachtwoord, in 2018 10 en later minimaal 8 karakters, bestaande uit minimaal een hoofdletter, kleine letter, getal en leesteken en maximaal 6 maanden geldig).
- Standaard monitoring op kwetsbaarheden in hard- en software via signaleringssoftware (2018). Deze is in 2021 aangevuld met een gezamenlijk interprovinciaal Security Operations Center (SOC).
- Verscherpte controle op binnenkomende e-mail (geautomatiseerde centrale spamfilter), waarmee verdachte e-mails automatisch geblokkeerd en verwijderd worden (2018). In 2020 en 2021 betrof dit bijvoorbeeld 60 à 65% (resp. 7,5 en 4,9 miljoen) van het totaal aan ontvangen externe e-mails.
- Endpointsecurity tegen virussen en malware. Betreft automatische screening door een externe partij van bijvoorbeeld laptops. Bij dreigingen worden deze apparaten direct uitgeschakeld (2019).
- Vervanging firewall (digitale sluis tussen internet en interne netwerk). Dit betreft de eerste verdedigingslinie infrastructuur tegen misbruik van buitenaf (2018-2020).
- Vastgesteld patchbeleid waarin beschreven staat hoe moet worden omgegaan met het doorvoeren van software (beveiligings)updates (2018-2019). Uitvoering van dit patchbeleid.
- Netwerksegmentering (optimalisatie netwerkinrichting): door netwerk onder te verdelen in gescheiden kleinere deelnetwerken, wordt de reikwijdte van een mogelijke inbraak beperkt en daarmee de beveiligingsrisico's verkleind.
- Beveiligde internetverbindingen.
- Beveiligde e-mail (e-mail standaarden, vertrouwelijke email kan via ZIVVER versleuteld verstuurd worden en de ontvanger dient zich te identificeren).
- Actief gebruik van standaarden voor email en alle websites waarvan de provincie geregistreerd eigenaar is. Dit betreft richtlijnen van Forum voor standaardisatie dat onderdeel is van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Dit met oog op gebruik van moderne en betrouwbare internetstandaarden waardoor internet toegankelijker, veiliger en betrouwbaarder wordt. Een ieder kan dit zelf toetsen via de algemeen geaccepteerde Nederlandse controlewebsites internet.nl (voor e-mail en websites) en basisbeveiliging.nl (voor websites). De provincie stuurt actief op een 100% score. De rekenkamer constateert dat deze score ook daadwerkelijk wordt gehaald. Op 30 maart 2022 scoorde

zowel de email @prvlimburg.nl als de website www.limburg.nl 100% op internet.nl. En van alle provincies scoorden alleen de provincie Limburg en Zeeland goed (groen) op basisbeveiliging.nl.

- Provinciale WiFi-omgeving zijn in 2019-2020 geschikt gemaakt voor govroam ontsluiting.
- In 2020 is een nieuwe veilige mobiele werkplek uitgerold voor alle medewerkers. Het betreft een centraal beheerde laptop met vooraf centraal geïnstalleerde software waarmee adequaat en veilig gebruik kan worden gemaakt van de informatievoorziening van de provincie. Corona heeft er toe geleid dat alle provinciale medewerkers versneld over deze beveiligde laptop en smartphone van de provincie beschikten (mobile device management). Tot dat moment werkten medewerkers thuis met eigen apparatuur. Voor het thuiswerken zijn ook MS Teams en Webex uitgerold. In die fase is ook de serious game gespeeld (bewustwordingsprogramma: zie later in deze paragraaf). In 2021 is een maatregel doorgevoerd waarbij enkel de door de provincie uitgegeven en geautoriseerde laptops connectie kunnen maken met het netwerk in het Gouvernement.
- In 2021 is gestart met het opzetten van een centraal interprovinciaal informatieknooppunt informatiebeveiliging. Dit richt zich op het vroegtijdig signaleren en voorkomen van informatiebeveiligingsincidenten. Dit maakt onderdeel uit van de binnen het IPO gepositioneerde Interprovinciale Digitale Agenda (IDA).
- Continuïteitsplan (herstel informatievoorziening na calamiteit).
- Periodiek uitvoeren van penetratietesten (zie paragraaf 2.5) .
- Aangescherpte inkoopvoorwaarden en selectie-eisen bij aanbestedingen hard- en software.

De rekenkamer constateert dat de provincie hiermee ook actie heeft ondernomen op alle drie de elementen die door een expert werden benoemd als de ‘heilige driehoek’ en die tijdens ons onderzoek uit 2018 nog niet goed geregeld waren: patches (beveiligingsupdates), sterke wachtwoorden en netwerksegmentatie. Als zelfs al één van de drie goed is geregeld, dan is er direct minder risico op heel grote schade. Hackers kunnen namelijk relatief eenvoudig een netwerk binnendringen als sprake is van:

- ontbrekende patches[7]
- zwakke wachtwoorden
- ontbrekende netwerksegmentatie.[8]

Naast bovenstaande veelal technische maatregelen is het informatiebeveiligings-, privacy- en informatiebeleid geactualiseerd en is in de periode 2018 tot en met 2022 een nieuw bewustwordingsprogramma uitgevoerd.

- **Informatiebeveiligingsbeleid (2018)**
  Het Informatiebeveiligingsbeleid uit 2014 is geactualiseerd en eind 2018 door GS vastgesteld. Het bevat de visie, missie, doelstelling, beleidsuitgangspunten en organisatie van de informatiebeveiliging. Resultaten van het rekenkameronderzoek uit 2018 en een risicoanalyse cybersecurity uit 2017 dienden

[7] Een patch is een aanpassing/verbetering (update) van bestaande software om de fouten of bugs eruit te halen.
[8] 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.

daarvoor als input. Het Informatiebeveiligingsbeleid richtte zich op 2019-2020. De rekenkamer constateert dat dit beleid sinds 2021 dus al niet meer actueel is. Vanuit de provinciale organisatie is aangegeven dat het nog wel vigerend is. De provincie heeft er bewust voor gekozen om eerst een nieuw bovenliggend en kaderstellend strategisch informatiebeleid door GS te laten vaststellen (zie drie bullits hierna). Echter door de bestuurscrisis heeft dit proces in 2021 een half jaar vertraging opgenomen. De provincie is voornemens om het informatiebeveiligingsbeleid in het tweede kwartaal van 2022 te actualiseren en in het derde kwartaal te laten vast stellen door GS. Het zal vooral gebaseerd zijn op de eerder genoemde begin 2022 vastgestelde HLS-documenten.

- **Strategische Verkenning Digitale samenleving** (februari 2018)
  Een onderdeel van deze verkenning is de impact van digitalisering op de provinciale organisatie. In dat kader wordt gesteld dat digitale vaardigheden bij bestuurders en ambtenaren essentieel zijn voor lagere risico's op het gebied van informatieveiligheid. Er wordt verwezen naar ons onderzoek uit 2018.
- **Privacybeleid** (2018)
  Met invoering van de Algemene Verordening Gegevensbescherming (AVG) is in mei 2018 een Functionaris Gegevensbescherming (FG) aangesteld en in oktober 2018 een geactualiseerd Privacybeleid vastgesteld door GS. In dit beleid wordt uitgesproken dat de provincie een adequaat niveau van privacy- en informatiebeveiliging nastreeft waarbij, voor het reduceren van risico's, voortdurend afwegingen worden gemaakt om de juiste balans te vinden tussen relevante wetgeving, de taakstelling van de organisatie, een praktische manier van werken en de persoonlijke levenssfeer van betrokkenen.
- **Strategisch Informatiebeleid Limburg 2021-2024** (SiBL, 2021)
  In oktober 2021 hebben GS het geactualiseerde SIBL vastgesteld. Het is overkoepelend beleid en kaderstellend voor de doorontwikkeling van onder andere informatiebeveiliging. Informatiebeveiliging heeft binnen het SIBL een hoge prioriteit; het is één van de drie basisonderdelen voor een betrouwbare informatievoorziening. Ook voor dit beleid is gebruik gemaakt van het rekenkameronderzoek uit 2018.[9] Het SIBL omvat ook een (concept)uitvoeringsplan dat planning en uitvoering van projectportfolio beoogt. Het betreffen elementen op hoog/globaal niveau; het zijn geen concrete maatregelen. Voor informatiebeveiliging betreft dit het implementeren en volgen van standaarden en best practices (ISO27001)[10], het versterken van het interne bewustzijn van medewerkers, het samen met ketenpartners bouwen aan kennis en het uitbouwen van de monitoring en rapportagestructuur.
- **Bewustwordingsprogramma** (2018)
  In 2018 is een nieuw bewustwordingsprogramma informatieveiligheid opgestart. Dit bestond uit vijf rondes, waarvan de laatste in het eerste kwartaal van 2022 is opgestart. Alle personen (inclusief leden van GS en PS) die gebruik maken van de infrastructuur van de provincie zijn uitgenodigd deel te nemen aan deze zogenoemde 'serious game'. In 2018 en 2019 lag deelname door de ambtelijke organisatie op 90%, in 2020 en 2021 iets lager waardoor de gemiddelde deelname aan de 1e vier rondes op 80% uitkomt. Dit ondanks het niet vrijblijvende karakter van het programma. De

[9] Ook rekenkameronderzoek naar Papierfabriek Meerssen.
[10] Hierin wordt door interpretatieverschillen nog gesproken van vierde kwartaal 2021 in plaats van 2022. Dit gebeurt ook in enkele andere provinciale documenten.

deelnamegraad van GS, PS en de directie in deze jaren is onbekend, omdat deze informatie niet meer beschikbaar is. De game is door een externe partij gehost en nadat een ronde is afgesloten zijn de detailgegevens niet meer beschikbaar. Alleen de totaalscore van de deelname is nog beschikbaar.
Vanuit de griffie is in het verleden aangegeven om PS en de griffie mee te willen laten doen aan dit spel. De griffie heeft daarom bij elke spelronde een uitnodiging ontvangen om, naast de griffie zelf, ook PS-leden uit te nodigen. Dit heeft volgens de griffie in het verleden ook tot deelname vanuit PS geleid.
De directie heeft deelname aan de 5e ronde verplicht gesteld, waarbij de clustermanagers medewerkers stimuleren om deel te nemen.
Doel is om het bewustzijn te vergroten inzake informatieveilig handelen (personeel is bewust bekwaam). Vragen betreffen informatiebeveiliging, privacy en fysieke beveiliging. Op vragen over privacy, fysieke beveiliging en phishing werd in de eerste spelronden in eerste instantie het laagst gescoord. Doordat vragen correct beantwoord moeten worden om het spel uit te spelen, was op deze onderwerpen het leereffect het grootst. In 2020 werd de game eerder dan gepland gespeeld met het oog op het thuiswerken in verband met corona, wat de mogelijke kwetsbaarheid van medewerkers op het gebied van informatieveilig handelen vergroot. Ondanks de grotere ‘noodzaak’ namen minder medewerkers deel dan in de twee eerdere speelrondes.
Naast de game wordt ook soms op het intranet van de provincie Limburg aandacht gevraagd voor informatieveiligheid. In coronatijd (2020 en 2021) werd meerdere keren extra/nadrukkelijk aandacht gevraagd voor informatieveiligheid. Dit om medewerkers bewust te maken dat men bij thuiswerken nog alerter moet zijn en bij twijfel contact op te nemen met de helpdesk. Ook maakt informatieveiligheid nog steeds onderdeel uit van het verplichte introductieprogramma voor nieuwe medewerkers.

2.5 Voorgenomen penetratietesten uitgevoerd

De provincie heeft, op één jaar na, jaarlijks een penetratietest (pentest) laten uitvoeren door gespecialiseerde externe bureaus met de inzet van ethische hackers. Doel daarvan is de infrastructuur van de provincie door te lichten op mogelijke kwetsbaarheden.

- Eind 2018 liet de provincie de eerste pentest uitvoeren. Dit betrof een externe en interne test: blackbox (toegang proberen te krijgen tot provinciale informatie zonder voorkennis via internet), greybox (toegang proberen te krijgen met minimale voorkennis via het interne netwerk) en whitebox (toegang proberen te krijgen met voorkennis via interne netwerk). Bevindingen laten ten opzichte van de bevindingen van ons eerdere rekenkameronderzoek een duidelijke verbetering zien. Maar een aantal bevindingen gaf aanleiding tot het nemen van aanvullende maatregelen.
- De voor eind 2019 geplande pentest is uitgesteld. Dit in verband met onder andere het doorvoeren van ingrijpende wijzigingen in de netwerkinfrastructuur en de in 2019 geïmplementeerde speciale tooling waarmee proactief kwetsbaarheden worden gesignaleerd in de, in eigen beheer draaiende, systemen (zoals die ook in een pentest naar boven zouden komen).
- In 2020 is onderzoek gedaan naar de buitenste schil van de infrastructuur. De bevindingen die daaruit volgden hebben geleid tot aanpassingen waarmee de geconstateerde kwetsbaarheden zijn weggenomen.
  Ook is een extern onderzoek uitgevoerd naar de in 2020 uitgerolde nieuwe mobiele werkplek. Naar aanleiding daarvan zijn enkele aanpassingen doorgevoerd om de mogelijke risico's van de geconstateerde kwetsbaarheden te mitigeren.
- De pentest 2021 werd in verband met het rekenkameronderzoek begin 2022 uitgevoerd. Het betreft een black- en greyboxtest. De rapportage over deze testen was ten tijde van het opstellen van voorliggend rapport van bevindingen nog niet beschikbaar.

Beveiligingsincidenten binnen de provinciale organisatie

De wereld van de cybercriminelen innoveert continu, en loopt daarmee vaak één stap voor op onder andere de fabrikanten van informatiebeveiligingsoplossingen. Daarnaast is sprake van een toenemend aantal dreigingen. Dit zijn uitdagingen die vragen om blijvende alertheid. Ondanks alle genomen (voorzorgs)maatregelen om incidenten te voorkomen, doen deze zich soms toch voor. De rekenkamer constateert dat de provincie in die gevallen alert heeft gereageerd en indien nodig benodigde en/of verdere (aangescherpte) maatregelen heeft genomen.

Voorbeelden:

- Begin 2019 was sprake van een serieus incident. Door onrechtmatig verkregen toegang tot een provinciale mailbox is in korte tijd een grote hoeveelheid e-mails (waarschijnlijk spam) verzonden. Hierdoor heeft de provincie enkele dagen op een zogenaamde blacklist voor e-mail gestaan en was de mailvoorziening niet beschikbaar. In reactie daarop zijn de maatregelen aangescherpt: verplichte 2-factor authenticatie bij de provinciale webmailvoorziening.
- Eind 2019, begin 2020 zorgde een kwetsbaarheid binnen Citrix wereldwijd voor problemen bij veel organisaties waaronder de provincie. De provincie heeft direct na bekendwording daarvan de

aanwijzingen van de leverancier en het Nationaal Cyber Security Centrum (NCSC) opgevolgd, waarmee de risico's tot een minimum zijn beperkt.

- In 2021 is besloten (voorlopig) geen gebruik meer te maken van drones en software van de Chinese firma DJI. Dit naar aanleiding van berichtgeving over geconstateerde veiligheidsrisico's.
- Eind 2021 heeft een kwetsbaarheid binnen diverse producten, waarbij software aangeduid als "Log4j", bij veel organisaties wereldwijd gezorgd voor de nodige problemen. Onmiddellijk nadat de betreffende kwetsbaarheid bekend werd, zijn de aanwijzingen van o.a. het NCSC opgevolgd. Dit betekende extra alertheid op mogelijke gevolgen van deze kwetsbaarheid.

Kwetsbaarheden in systemen buiten de provinciale organisatie

In 2021 zijn er ook kwetsbaarheden geconstateerd in de beveiliging van een aantal gemeenschappelijke applicaties en informatiesystemen die door de provincies bij BIJ12 zijn ondergebracht.[11] Voorbeelden daarvan zijn databanken en registers voor natuurbeheer, monitoring, subsidieverlening en schade-uitkeringen. Er zijn direct voorzorgsmaatregelen genomen om de kwetsbaarheden op te lossen en de veiligheid te waarborgen. De ICT-systemen zijn tijdelijk offline gezet en er zijn gezamenlijk acties ondernomen om de kwetsbaarheden op te lossen. Het tijdelijk onbereikbaar zijn van de applicaties (websites) betekende dat de informatievoorziening tijdelijk niet beschikbaar was. Overheidsorganisaties en ketenpartners konden redelijk snel wel weer via een speciale constructie op veilige wijze toegang krijgen tot de systemen, zodat de reguliere werkprocessen in een beveiligde omgeving door konden gaan. Binnen twee maanden was het grootste deel van de kwetsbaarheden opgelost en werden deze systemen stapsgewijs weer openbaar toegankelijk. Uit onderzoek bleek dat er geen sporen van inbreuk zijn gevonden op de onderzochte systemen. Enkele applicaties vroegen echter zulke ingrijpende aanpassingen dat op basis van gebruik en kostenoverwegingen wordt gekozen voor herstel, herbouw, uitfasering of gebruik alleen via veilige toegang continueren.

2.6 Gestuurd op realisatie maatregelen

In een gesprek is tegenover de rekenkamer aangegeven dat sinds en naar aanleiding van ons onderzoek uit 2018 'de touwtjes in de uitvoering zijn aangetrokken'. Zo zijn de technische maatregelen flink toegenomen. Ook is een tweewekelijks overleg ingesteld waarin de stand van zaken van de lopende en geplande maatregelen wordt besproken. Daarbij vindt sturing en bewaking van de belangrijkste afspraken, waaronder realisatie, plaats. Dit proces gaat steeds meer vanzelf lopen (het verinnerlijkt), met name door toenemend awareness, commitment (zich verantwoordelijk voelen) en professionalisering bij de meest direct betrokkenen (systeembeheerders/techneuten). Het rekenkameronderzoek uit 2018 heeft hier een impuls aan gegeven. Wat betreft professionalisering geldt dat bijvoorbeeld ook tijdens latere pentesten gesprekken zijn gevoerd met het uitvoerende bureau om leerervaring op te doen.

Er wordt enerzijds gestuurd op basis van reguliere monitoringsactiviteiten als internet.nl, basisbeveiliging.nl waarop via het stoplichtenmodel inzicht wordt gegeven in de stand van zaken van de

[11] BIJ12 werkt als uitvoeringsorganisatie in opdracht van de twaalf provincies.

basisbeveiliging en periodieke interne kwetsbaarheidsrapportages. Anderzijds kunnen ook lopende projecten, incidenten en andere actualiteiten aanleiding geven tot bijsturing of herprioritering van activiteiten. Tevens worden interne beschrijvingen van ISO27001-maatregelen en beleidsdocumenten in dit overleg besproken. Aan dit overleg nemen deel de clustermanager O&I, de Concern Information Security Officer (CISO), de teamleider I-Services (de 'techneuten') en één van de medewerkers van het team I-Services die een interne coördinerende rol vervult op het gebied van informatiebeveiliging.

Personele inspanning

De benodigde capaciteit is mede naar aanleiding van de rekenkameronderzoek in 2018 herijkt. Dat heeft geleid tot de beschikbaarstelling van extra capaciteit. Vanaf 2018 is er ook meer personele inspanning in termen van zowel tijd als aandacht. Zo is de CISO tegenwoordig bijna voltijds bezig met informatieveiligheid. Ook bij de beheerders is deze ontwikkeling zichtbaar. Het is een belangrijk onderdeel van het beheerwerk geworden; het heeft de afgelopen jaren merkbaar meer tijd en aandacht gekregen (o.a. patchen).

Het ISMS omvat audits. Vanaf 2021 geeft het cluster Concern invulling aan het interne toezicht (achteraf) en toetsing (vooraf) om aanwezige risico's zoveel mogelijk te beperken. Dit via het Three lines of defense-model (3LoD). Tot 2022 werden de audits die informatiebeveiliging omvatten extern uitgevoerd. De provincie is bezig met de werving van een Concern Information Governance Specialist (CIGS), maar dit is zeer lastig door de krapte op de arbeidsmarkt. Zodra deze is geworven zal deze de operational audits op het gebied van informatiebeveiliging uitvoeren: beoordeling risicomanagement. Tot die tijd worden de taken van de CIGS waargenomen door het hoofd van het cluster Concern en waar noodzakelijk zal inzet van externen blijven plaatsvinden om de uitvoering van audits en andere noodzakelijke acties mogelijk te maken. Deze situatie illustreert, naar de mening van de rekenkamer, de kwetsbaarheid van de invulling van deze functie door één persoon. De zogenaamde In Control Verklaring van de provincie (bedrijfsvoering voldoet aan BIO) is voorzien in het laatste kwartaal van 2022. Zie bijlage 2 voor een globale beschrijving van de verantwoordelijkheidsverdeling van informatiebeveiliging.

Financiële middelen

Er zijn meer financiële middelen ingezet voor informatiebeveiliging. Het begrote budget was in de periode 2019 tot en met 2022 iets meer dan € 200.000. De daadwerkelijk ingezette middelen waren in 2018 en 2019, de periode direct na het rekenkameronderzoek, het hoogst. Toen is er respectievelijk € 435.000 en € 280.000 aan informatiebeveiliging uitgegeven. Daarna zijn de uitgaven gedaald naar € 206.000 en € 196.000.

Tabel 3 Begrote en ingezette financiële middelen voor informatiebeveiliging, in € (afgerond)

	2018	2019	2020	2021	2022
Begroot budget	100.000*	202.250	206.100	210.010	213.370
Kosten***	210.000	280.000	206.000	196.000	
Investeringen hard- en software***	225.000*	-	-	-	
Totaal ingezet***	435.000**	280.000	206.000	196.000	

* 2018 was een transitiejaar. In de loop van dat jaar is binnen de financiële administratie een specifieke post informatiebeveiliging opgenomen Ook na 2018 is sprake geweest van investeringen..
** Kosten om informatieveiligheid op een hoger niveau te brengen.
*** Bij de uitgaven dient te worden opgemerkt dat het niet altijd mogelijk is om deze eenduidig aan informatiebeveiliging te koppelen. Wanneer bijvoorbeeld nieuwe netwerkcomponenten worden aangeschaft, bieden deze vaak betere beveiligingsopties. Dit soort uitgaves kunnen zowel gezien worden als geplande reguliere vervangingen alsook als investeringen in het verbeteren van de beveiliging.

Het streven was het SIBL 2021-2024 budgetneutraal uit te voeren. Maar zowel de beschikbare middelen als de capaciteit op tactisch niveau werden daarin ook als risicofactor omschreven. Voor informatiebeveiliging werd gesteld dat het steeds meer capaciteit en financiële middelen vergt om de risico's tot aanvaardbaar niveau te beperken. Inmiddels wordt het streven om het budgetneutraal uit te voeren als niet-haalbaar gezien; ook voor informatiebeveiliging. Dit zal worden meegenomen in de integrale afweging bij de begroting 2023.

2.7 PS uitgebreid geïnformeerd, maar geen (structurele) dialoog

2.7.1 PS jaarlijks uitgebreid Informatie over informatieveiligheid

Zoals toegezegd naar aanleiding van ons eerdere onderzoek hebben GS intensiever gecommuniceerd met PS over (de voortgang en uitvoering van) informatieveiligheid.[12] Via een mededeling portefeuillehouder zijn PS jaarlijks uitgebreid geïnformeerd door GS over de in het voorgaande jaar:

- uitgevoerde werkzaamheden
- belangrijkste ontwikkelingen
- geregistreerde informatiebeveiligingsincidenten (denk aan bijvoorbeeld externe aanvallen zoals spam, phishingmail of verdachte telefoontjes; of aan verlies/diefstal van smartphone of laptop).
- ingezette financiële middelen voor (verbetering) informatiebeveiliging.

Daarnaast wordt in al deze rapportages het belang en de noodzaak van informatieveiligheid onderstreept.

Ook ontvingen PS eind 2018 een mededeling portefeuillehouder met het herijkte Informatiebeveiligingsbeleid 2019-2020. Op deze wijze zijn ze geïnformeerd over de visie, missie, doelstelling, beleidsuitgangspunten, reikwijdte, randvoorwaarden en organisatie van informatiebeveiliging. Verder zijn PS begin 2021 per ommegaande via een mededeling portefeuillehouder geïnformeerd over de

[12] Toegezegd door GS in de bestuurlijke reactie op ons rapport (3 juli 2018), in de mededeling portefeuillehouder van 3 juli 2018 en na verzoek daartoe vanuit PS bij behandeling van ons rapport in de Statencommissie Financiën, Economische Zaken en Bestuur op 2 november 2018 (T8377: PS jaarlijks informeren over informatieveiligheid).

geconstateerde kwetsbaarheden in de beveiliging van een aantal ICT-systemen die de provincies gezamenlijk bij IPO/BIJ12 hebben ondergebracht, de noodzaak van het tijdelijk offline zetten van deze systemen, het oplossen van de kwetsbaarheden om de systemen weer veilig te laten zijn, de zorg voor de continuïteit van de dienstverlening en het onderzoek dat naar aanleiding daarvan werd uitgevoerd naar eventuele inbreuken op de systemen. Twee maanden later werden ze door GS geïnformeerd over de voortgang daarvan.

Van deze mededelingen portefeuillehouder is alleen de mededeling over informatiebeveiliging 2017 besproken in PS. Dit gebeurde tezamen met het rekenkameronderzoek. De andere zijn voor kennisgeving aangenomen en dus niet besproken. Hiermee hebben PS ook geen kaderstellende rol ingenomen bij het informatiebeveiligingsbeleid.

Informatieveiligheid is daarmee sinds juli 2018 alleen in 2018 specifiek aan de orde geweest bij de behandeling van het rekenkameronderzoek. In november 2018 werd het namelijk uitgebreid besproken in de Statencommissie Financiën, Economische Zaken en Bestuur (FEB). Ten behoeve daarvan werden er vanuit één PS-fractie voorafgaand 11 vragen aan de rekenkamer en 7 vragen aan GS gesteld. Er werd tijdens de behandeling onder andere aandacht gevraagd voor beschikbare capaciteit, bewustwording, borgen van incidenten en jaarlijkse informatie aan PS. Op 9 november 2018 werden de aanbevelingen van de rekenkamer in de PS-vergadering zonder beraad overgenomen (hamerstuk).

Zie voor een overzicht en meer informatie onderstaande tabel.

Tabel 4 Mededelingen portefeuillehouder over informatieveiligheid, 1 januari 2018 tot en met maart 2022

Datum	Onderwerp mededeling portefeuillehouder	Behandeling door PS
Juli 2018	Informatiebeveiliging 2017	In november 2018 samen met rekenkameronderzoek besproken in commissie FEB.
December 2018	Informatiebeveiligingsbeleid 2019-2020	Voor kennisgeving aangenomen
Maart 2019	Informatieveiligheid 2018	In april 2019 op de agenda van de Interim Statencommissie naar aanleiding van een ingediende vraag vanuit PS voor de rondvraag: waarom hebben PS al vier weken geen toegang tot de webmail-applicatie? Het antwoord van GS daarop was geagendeerd bij de rondvraag. Het werd echter niet besproken omdat de rondvraag ter vergadering van de agenda werd afgevoerd.
Maart 2020	Informatieveiligheid 2019	Voor kennisgeving aangenomen
Januari 2021	Beveiliging informatiesystemen BIJ12	Voor kennisgeving aangenomen
Maart 2021	Voortgang beveiliging informatiesystemen BIJ12	Voor kennisgeving aangenomen
April 2021	Rapportage informatiebeveiliging 2020	Voor kennisgeving aangenomen
Maart 2022	Rapportage informatiebeveiliging 2021	Voor kennisgeving aangenomen

2.7.2 Schriftelijke vragen vanuit PS

De afgelopen 4 jaar (2018 tot en met 22 april 2022) zijn naar aanleiding van informatiebeveiligingsincidenten in Limburg op twee momenten schriftelijke vragen vanuit PS gesteld die informatieveiligheid raken. Het gaat om vragen die op 10 april 2018 en op 31 december 2019 zijn gesteld en door GS zijn beantwoord. Zie onderstaande tabel voor meer informatie.

Tabel 5 Schriftelijke vragen vanuit PS Limburg, 1 januari 2018 tot en met PM 2022

Vragen naar aanleiding van / over	Datum
Gelekte wachtwoorden provinciale mailaccounts	10 april 2018
Ransomware aanval Universiteit Maastricht	31 december 2019

2.7.3 P&C-documenten, accountantsverslagen en bewustwording

Via de P&C-documenten (begrotingen, jaarstukken en bijbehorende accountantsverslagen) 2018 tot en met 2022 zijn PS zeer op hoofdlijnen geïnformeerd over informatieveiligheid.[13] Het informatiebeveiligings-beleid en belang van informatieveiligheid worden genoemd. Vaak ook het vergroten van bewustwording, het doorvoeren van verbeteringen op het gebied van techniek en/of procedurele afspraken en het streven naar de implementatie van ISO27001.

PS hebben informatieveiligheid niet als speerpunt meegegeven voor de controle van de jaarverslagen door de accountant. De accountant heeft vanaf de controle over 2018 echter wel jaarlijks aandacht besteed aan het onderwerp informatieveiligheid (waarbij de term ‘cybersecurity’ wordt gehanteerd). Dit heeft niet geleid tot bevindingen waarvoor aandachtspunten werden meegegeven.

De uitnodigingen tot deelname aan de ‘serious game’ (bewustwordingscampagne Informatieveiligheid) hebben volgens de griffie in het verleden ook tot deelname vanuit PS geleid.

2.7.4 Overkoepelend en aanpalend beleid dat informatieveiligheid raakt

Naast de mededelingen portefeuilllehouder is informatieveiligheid ook onder de aandacht van PS gebracht via overkoepelend beleid waar informatieveiligheid onderdeel van uit maakt of dat raakt. Het gaat hierbij om het Privacybeleid, de Strategische Verkenning Digitale samenleving en het Strategisch Informatiebeleid provincie Limburg. PS hebben ook hierbij geen kaderstellende rol gehad danwel ingenomen; de documenten zijn sonderend of informerend aan PS voorgelegd en door GS vastgesteld. Zie onderstaande tabel voor een overzicht.

Bij de sonderende bespreking van de conceptversie van het SIBL werd zowel in de presentatie aan PS als in reacties vanuit PS aandacht besteed aan het belang van informatieveiligheid. PS werden gevraagd de

[13] In de betreffende begrotingen en jaarstukken in hoofdstuk 4 Bestuur, hoofdstuk 5 Bedrijfsvoering paragraaf 5.3 Informatiemanagement en paragraaf 5.10 Privacybeleid (vóór begroting 2022 Gegevensbeheer geheten) en in de verplichte paragraaf Weerstandsvermogen en risicobeheersing

onderwerpen uit het SIBL te prioriteren. Dat werd als lastig ervaren, maar vanuit verschillende partijen werd informatieveiligheid wel expliciet als prioriteit genoemd.

Tabel 6 Overkoepelend beleid dat informatieveiligheid omvat of raakt, 1 januari 2018 tot en met PM 2022]

Datum	Document	
Oktober 2018	Privacybeleid (GS)	
Februari 2019	Strategische Verkenning Digitale samenleving Limburg (Hoofdstuk 7 De impact van) digitalisering op de provinciale organisatie	
Februari 2021	Mededeling portefeuillehouder Concept Strategisch Informatiebeleid Limburg 2021-2024 (december 2020)	Sonderend besproken in FEB
Oktober 2021	Mededeling portefeuillehouder Strategisch Informatiebeleid Limburg 2021-2024 (19 oktober vastgesteld door GS)	Voor kennisgeving aangenomen

Alles overziend lijkt de aandacht vanuit PS voor informatieveiligheid, evenals in de periode vóór 2018 nog steeds niet structureel maar incidentgedreven. Er is (daarmee) geen structurele dialoog geweest tussen PS en GS over het onderwerp.

Vanuit PS is een werkgroep Versterking Positie PS (Werkgroep VVPS) gevormd. Deze is sinds 3 december 2021 actief en ziet toe op aspecten van verbetering van de informatiepositie/huishouding/toegankelijkheid en afstemming tussen vraag en aanbod in relatie tot informatievoorziening. Dit alles met het oog op versterking van de positie van PS omtrent kaderstelling, controle en volksvertegenwoordiging. De werkgroep wil op de Statendag van 17 juni 2022 aandacht vragen voor verbetering van de informatiehuishouding door met GS en de directie in overleg te gaan en concrete afspraken te maken.
Ook heeft de griffie een kernteam digitalisering opgericht voor afstemming lopende projecten en trajecten inzake digitalisering en informatievoorziening. Dit kernteam bestaat uit afgevaardigden van de ambtelijke organisatie en de griffie.

2.8 Algemene aandachtspunten

De provincie Limburg zal, zoals reeds aangegeven, in 2022 stappen moeten zetten om vóór 2023 klaar te zijn voor certificering ISO27001 en de eisen uit de BIO. Daarna is het zaak (minstens) dat niveau vast te houden. Informatieveiligheid is ook nooit ‘klaar’. Zoals in paragraaf 2.5 reeds opgemerkt, innoveert bijvoorbeeld de wereld van de cybercriminelen continu, en loopt daarmee vaak één stap voor. Daarbij is ook nog eens sprake van een toenemend aantal dreigingen via onder andere ransomware en phishing. Daarnaast kunnen mensen onbedoeld ‘fouten’ maken. De mens is doorgaans de zwakste schakel in elk beveiligingssysteem. Goede beveiliging en voldoen aan de ISO27001- en BIO-eisen zijn geen garantie dat de provincie bijvoorbeeld niet gehackt kan worden, maar hierdoor is de kans op datalekken of cryptoware wél kleiner en als dit toch gebeurt, dan weet de provincie hoe te handelen omdat daar van tevoren over nagedacht is. 100% veiligheid bestaat niet, maar dit zijn uitdagingen die vragen om blijvende alertheid. Dit werd zowel in gesprekken met de externe experts, als in gesprekken met betrokkenen van de provincie naar voren gebracht.

Bijlage 1 Geraadpleegde documenten en gebruikte afkortingen

- Zuidelijke Rekenkamer, Informatieveiligheid provincie Limburg, juli 2018
- Provincie Limburg, Mededeling portefeuillehouder inzake informatiebeveiliging (2017), juli 2018
- Zuidelijke Rekenkamer, Antwoorden rekenkamer op PS-vragen n.a.v. rekenkameronderzoek Informatieveiligheid, september 2018
- Provincie Limburg, Antwoorden GS op PS-vragen n.a.v. rekenkameronderzoek Informatieveiligheid, september 2018
- Provincie Limburg, Statenvoorstel van de Statencommissie FEB rekenkameronderzoek Informatieveiligheid, oktober 2018
- Provincie Limburg, Privacybeleid Provincie Limburg 2018, oktober 2018
- Provincie Limburg, Informatiebeveiligingsbeleid Provincie Limburg 2019-2020, december 2018
- Provincie Limburg, Mededeling portefeuillehouder inzake Informatiebeveiligingsbeleid, december 2018
- Hoffmann, Provincie Limburg Rapportage Pentest, februari 2019
- Provincie Limburg, Strategische verkenning Digitale samenleving Limburg , februari 2019
- Provincie Limburg, Mededeling portefeuillehouder inzake informatieveiligheid 2018, maart 2019
- Provincie Limburg, Mededeling portefeuillehouder inzake webmail PS, april 2019
- Provincie Limburg, Nota voor Directieteam, Evaluatie bewustwording informatieveiligheid, april 2019
- Provincie Limburg Nulmeting ISO27001 & Baseline Informatiebeveiliging Overheid, mei 2019
- Provincie Limburg, Antwoorden GS op schriftelijke vragen gelekte wachtwoorden provinciale mailaccounts en status voorbereiding op de AVG, mei 2019
- Provincie Limburg, Antwoorden GS op schriftelijke vragen ransomware aanval Universiteit Maastricht, januari 2020
- Provincie Limburg, Mededeling portefeuillehouder informatieveiligheid 2019, maart 2020
- Provincie Limburg, Stateninformatiesysteem (www.limburg.bestuurlijkeinformatie.nl): aanbevelingen rekenkameronderzoek (nummer 1482) afgedaan (deadline 21-6-2019), 2020
- Provincie Limburg, Mededeling portefeuillehouder concept Strategisch Informatiebeleid Limburg 2021 – 2024, december 2020
- Provincie Limburg, Mededeling portefeuillehouder beveiliging informatiesystemen BIJ12, januari 2021
- Secura, Technisch beveiligingsonderzoek Black Box infrastructuur scan provincie Limburg januari 2021
- Secura, Technical Security Assessment Device onderzoek thuiswerken provincie Limburg, januari 2021
- Provincie Limburg, Mededeling portefeuillehouder Richtinggevende vragen sonderende behandeling concept Strategisch Informatiebeleid Limburg 2021 – 2024, februari 2021
- Provincie Limburg, Mededeling portefeuillehouder Rapportage informatiebeveiliging 2020, februari 2021
- Provincie Limburg, Mededeling portefeuillehouder Voortgang beveiliging informatiesystemen BIJ12, maart 2021
- Provincie Limburg, Nota voor Directieteam, Bewustwording informatieveiligheid, maart 2021
- Provincie Limburg, Nota voor Directieteam, Informatiebeveiliging ISO27001 (projectplan), maart 2021
- Provincie Limburg, Mededeling portefeuillehouder Rapportage informatiebeveiliging 2020, april 2021
- Provincie Limburg, Strategisch Informatiebeleid Limburg 2021-2024, oktober 2021

- DigiTrust, Auditrapport ISO 27001:2017 + BIO 2021 pre-audit (herijking tov 2019 audit), november 2021
- DigiTrust, Overzicht auditrapport herijking 0-meting, november 2021
- Provincie Limburg, Interne nota aan de CIO, Implementatie ISO27001 HLS, december 2021
- Provincie Limburg, Interne nota aan de CIO, Implementatie ISO27001, januari 2022
- Provincie Limburg, Nota voor Directieteam Implementatie ISO27001/BIO (HLS), januari 2022
- Provincie Limburg, Nota voor Directieteam, Weerbaarheid cyberaanval, januari 2022
- Provincie Limburg, Mededeling portefeuillehouder Rapportage informatiebeveiliging 2021, maart 2022
- Begrotingen 2019, 2020, 2021 en 2022, Jaarstukken 2018, 2019 en 2020
- Notulen/bandopname van commissie- en Statenvergaderingen waarin bovenstaande documenten waren geagendeerd.
- Interne website provincie Limburg, www.rtlnieuws.nl (17-1-2022), www.winmagpro.nl, www.managementimpact.nl. www.consultancy.nl, www.rijksoverheid.nl (actieplan ‘Open op Orde’),

Gebruikte afkortingen

- 3LoD: Three lines of defence
- AVG: Algemene verordening gegevensbescherming
- BIO: Baseline Informatiebeveiliging Overheid
- CIO: Chief Information Officer
- CIGS: Concern Information Governance Specialist
- CISO: Concern Information Security Officer
- DT: directieteam
- FEB: Financiën, Economische Zaken en Bestuur
- FG: Functionaris Gegevensbescherming
- GS: Gedeputeerde Staten
- HLS: High Level Structure
- IBI: Interprovinciale Baseline Informatiebeveiliging
- IDA: Interprovinciale Digitale Agenda
- IPO: Interprovinciaal Overleg
- ISMS: Information Security Management Systeem
- NCSC: Nationaal Cyber Security Centrum
- O&I: Organisatie en Informatie
- PDCA: Plan-Do-Check-Act
- PS: Provinciale Staten
- P&C: Planning en control
- SIBL: Strategisch Informatiebeleid Limburg
- SOC: Security Operations Center
- Wob: Wet openbaar bestuur
- Woo: Wet open overheid

Bijlage 2 Lijst gesprekspartners en verantwoordelijkheidsverdeling informatiebeveiliging

Provincie Limburg

- Senior adviseur Organisatie en Informatie / CISO
- Clustermanager Organisatie en Informatie

Niet provincie Limburg

- Senior adviseur en verandermanager bij BMC
- Twee consultants Corporate & Cybersecurity bij Hoffmann
- Senior Security Specialist & Public Speaker bij Secura B.V.

Verantwoordelijkheidsverdeling informatiebeveiliging

Het college van GS is integraal verantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de provincie. De directie is verantwoordelijk voor de totstandkoming en uitvoering van het Informatiebeveiligingsbeleid (dit is belegt bij de CIO zijnde de directeur bedrijfsvoering) en wordt daarbij ondersteunt door het cluster O&I. Cluster O&I is verantwoordelijk voor de beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen. Elke clustermanager is verantwoordelijk voor de informatiebeveiliging van zijn processen. Cluster O&I (CISO) ondersteunt clustermanagers en is verantwoordelijk voor uitvoering van het ISMS (waaronder advies). Het cluster Concern is verantwoordelijk voor het (laten) uitvoeren van audits (3LoD-model). Medewerkers hebben eigen verantwoordelijkheid voor onderkennen informatiebeveiligingsrisico's. De CISO ondersteunt de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert daarover aan directie en GS.