Informatieveiligheid
provincie Limburg

Deel I Bestuurlijk rapport

ZUIDELIJKE REKENKAMER

Inhoudsopgave

ZUIDELIJKE REKENKAMER

1. Over dit onderzoek

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

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

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

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

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

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

Om voornoemde redenen heeft de rekenkamer een onderzoek uitgevoerd naar de informatieveiligheid van de provincie Limburg. Informatieveiligheid wordt bepaald door ten minste de volgende twee zaken:
1. de sterkte van de informatiesystemen (techniek) en
2. het gedrag van degenen die uit hoofde van hun functie toegang hebben tot die systemen.
Om informatieveiligheid te waarborgen, wordt gebruik gemaakt van informatiebeveiliging (maatregelen).

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

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

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

Ons onderzoek richtte zich op de periode vanaf 1 juli 2014 (vaststelling informatiebeveiligingsbeleid) tot april 2018. Voor de beantwoording van de onderzoeksvragen hebben we gegevens verzameld uit documenten, mondelinge interviews met en schriftelijke vragen aan betrokkenen binnen de provinciale organisatie. Een uitgebreide beschrijving van de onderzoeksopzet en van de onderzoeksresultaten hebben we opgenomen in ons rapport van bevindingen (deel II van deze publicatie). Dit kunt u lezen op de website van de rekenkamer www.zuidelijkerekenkamer.nl. Voorliggend rapport bevat de conclusies en aanbevelingen van de rekenkamer, de reactie van Gedeputeerde Staten (GS) en het nawoord van de rekenkamer. Deze worden in hoofdstuk 2 weergegeven. Daarnaast bevat voorliggend rapport een samenvatting van de bevindingen op basis waarvan de rekenkamer haar conclusies en aanbevelingen heeft geformuleerd. Deze wordt, de onderzoeksvragen volgend, gegeven in hoofdstuk 3 (ingericht op papier), 4 (in de praktijk) en 5 (PS en informatieveiligheid).

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

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

2.1 Conclusies

De rekenkamer concludeert op basis van haar onderzoek dat informatieveiligheid de afgelopen jaren in toenemende mate aandacht heeft gekregen binnen de provincie Limburg. De provincie heeft dan ook al verschillende maatregelen getroffen om te borgen dat haar informatie goed beveiligd is. Vooral in de opzet is de informatiebeveiliging, op enkele punten na, goed ingericht. De uitvoering vindt ook voor een groot deel conform deze opzet plaats, maar het tempo van de implementatie van de voorgenomen beveiligingsmaatregelen is voor verbetering vatbaar. De provincie is de afgelopen jaren (mede) daardoor op punten nog kwetsbaar gebleken in de beheersing van informatieveiligheidsrisico's. In een aantal gevallen was dat niet nodig geweest. Gezien de risico's en mogelijke gevolgen van inbreuken op de informatieveiligheid is het dan ook van belang dat de provincie haar handelen intensief voortzet, zodat informatieveiligheid een vanzelfsprekende voorwaarde wordt in alle geledingen van de provinciale organisatie.

Provinciale Staten hebben tot nu toe een beperkte rol gehad bij de totstandkoming en uitvoering van het informatiebeveiligingsbeleid. Gedeputeerde Staten zien het onderwerp primair als een bedrijfsvoeringskwestie. Sinds 2017 worden PS actief geïnformeerd over informatieveiligheid. Daarvoor schoot de informatievoorziening over de uitvoering tekort.

Uitgebreidere beschrijving van de conclusies

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

1. De provincie Limburg heeft in de periode 2014 tot begin 2018 vooruitgang geboekt in de wijze waarop de informatiebeveiliging in opzet en praktijk is ingericht. De informatiebeveiliging is in *opzet* (beoogde invulling) grotendeels goed ingericht. Er zijn kaders, richtlijnen en een uitvoeringsplan met een overzicht van de beoogde maatregelen opgesteld. Deze zijn helder/navolgbaar en sluiten goed op elkaar aan. De documentatie en beschrijving van procedures, processen en maatregelen schieten echter op punten nog te kort en blijven daarmee een aandachtspunt. De *uitvoering* verloopt eveneens voor een groot deel zoals voorgenomen. Echter de voorgenomen beveiligingsmaatregelen zijn te veelomvattend gebleken om uit te voeren in de looptijd die in de opzet wordt gemeld: het tempo van de implementatie van deze maatregelen gaat (veel) langzamer dan voorzien. Dit als gevolg van gebrek aan voldoende capaciteit en de impact van sommige maatregelen binnen de organisatie (door de natuurlijke spanning tussen het niveau van beveiliging en het gebruikersgemak/openheid). De provincie moet nog het nodige werk verzetten om te voldoen aan het door haar, samen met de andere provincies, gekozen basisambitieniveau (implementatie van de Interprovinciale Baseline Informatiebeveiliging (IBI)). Volgens een interprovinciale monitor over 2016 behoorde de provincie namelijk, samen met enkele andere, tot één

van de laagst scorende provincies.

Een cruciale voorwaarde voor effectieve informatiebeveiliging is dat de gehele organisatie zich bewust is van het belang ervan. Men dient zich gedrag eigen te maken waardoor de informatieveiligheid wordt bewaakt. Informatieveiligheid betreft een proces dat niet vanzelf komt. Het is iets waar je bekwaam in moet worden en wat als vanzelfsprekende voorwaarde moet groeien binnen een organisatie. Een bekend model over bewustwording en leren komt van de hand van Maslow. Hij ziet 'leren' als een patroon waarbinnen vier fases onderscheiden kunnen worden. Als we naar de provincie kijken door de bril van het model van Maslow, dan heeft de provincie zich over het geheel genomen reeds ontwikkeld van *onbewust onbekwaam* en *bewust onbekwaam*, naar *bewust bekwaam*. Dit houdt in dat de provincie bezig is met de gewenste competenties eigen te maken om zo 'bekwaam' te worden. Daar dit overall nog zeker 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.

2. Dat de provincie kwetsbaar is, is onder andere gebleken uit een penetratietest die door de rekenkamer is uitgevoerd. Tijdens deze test is zowel digitaal (via onder andere 'ethisch hacking' en een phishingmail), als fysiek ongeautoriseerde toegang verkregen tot (vertrouwelijke) informatie waarover de provincie beschikt. Opmerkelijk hierbij is dat soortgelijke typen bevindingen naar voren kwamen als bij een penetratietest die de provincie zelf in 2015 liet uitvoeren. Een aantal bevindingen hiervan had niet opnieuw naar voren moeten zijn gekomen, omdat de maatregelen daarvoor al getroffen hadden kunnen zijn (zie onder 1).
3. Provinciale Staten hebben tot nu toe geen kaderstellende rol gehad bij het informatie(beveiligings)beleid. Wel zijn ze actief geïnformeerd over de totstandkoming van het informatiebeleid waar informatiebeveiliging onderdeel van uit maakt. In 2011 en 2016 zijn ze via het overkoepelende strategisch informatiebeleid (SIBL) op hoofdlijnen geïnformeerd over de opzet van informatieveiligheid. Over de uitvoering van het informatiebeveiligingsbeleid zijn PS tot 2017 nauwelijks tot niet geïnformeerd. Dit komt het uitvoeren van hun controlerende rol niet ten goede. Begin 2017 zijn ze via een mededeling portefeuillehouder voor het eerst uitgebreid geïnformeerd over de voortgang van het informatiebeveiligingsbeleid, de in 2016 uitgevoerde acties en over beveiligingsincidenten. PS hebben overigens zelf ook alleen in 2017 aandacht gevraagd voor het onderwerp. Destijds vroegen ze om informatie naar aanleiding van verschillende (inter)nationale beveiligingsincidenten en naar aanleiding van bevindingen van de accountant. De aandacht van PS voor informatieveiligheid lijkt tot nu toe dan ook niet structureel, maar vooral incidentgedreven. Van een structurele dialoog tussen PS en GS over het onderwerp is dan ook nog geen sprake geweest.

De conclusies worden in onderstaande paragrafen 2.1.1 – 2.1.3 nader onderbouwd:

2.1.1 Beoogde invulling en uitvoering

Na het mislukken van een aantal ICT-projecten van de provincie zijn GS begin 2011 gestart met de herijking en herpositionering van de ICT-functie. De afgelopen jaren heeft (onder andere) deze herijking geleid tot verschillende beleidskaders en richtlijnen waarbinnen informatieveiligheid als prioriteit naar voren komt. Deze kaders verhouden zich op een logische manier tot elkaar en overige plannen en statuten volgen logisch uit de beleidskaders. Zo beschikt de provincie over een overkoepelend strategisch informatiebeleidskader, waarbinnen informatieveiligheid als een van de belangrijkste thema's is aangemerkt. Op een lager, tactisch, aggregatieniveau is medio 2014 het geactualiseerde informatiebeveiligingsbeleid door GS vastgesteld. Hierin zijn de uitgangspunten opgenomen voor de te nemen maatregelen betreffende informatieveiligheid. In dit kader geeft de provincie onder andere aan zich te committeren aan de IBI. Als uitwerking van het informatiebeveiligingsbeleid is een uitvoeringsplan opgesteld. Dit plan bevat 27 maatregelen die in de periode 2015-2016 uitgevoerd zouden worden.

De uitvoering van het beleid heeft de afgelopen jaren voor een groot deel plaatsgevonden conform de beleidskaders, richtlijnen en het uitvoeringsplan. Het tempo van de implementatie van de voorgenomen maatregelen is echter wel een stuk minder hoog dan gepland. Het in 2015 uitgewerkte uitvoeringsplan was bijvoorbeeld bestemd voor de periode 2015-2016, maar thans lijken de maatregelen zelfs te ambitieus om binnen een periode van vier jaar uit te voeren. Vanuit de provincie is aangegeven dat dit komt vanwege een gebrek aan capaciteit en de impact en inspanning die gepaard gaan met de uitvoering van de maatregelen. Ook de documentatie en beschrijving van procedures, processen en maatregelen schieten op punten nog te kort. De provincie is bezig met de implementatie van een nieuw managementsysteem waarin deze zaken worden opgenomen. Onder andere doordat deze en andere maatregelen meer tijd vergen dan gepland voldoet de provincie Limburg in vergelijking met andere provincies nog in mindere mate aan het nagestreefde basisbeveiligingsniveau (de IBI), waaraan de provincie zich echter wel heeft gecommitteerd.

2.1.2 Penetratietesten

In de periode van 27 juli tot en met 9 oktober 2017 heeft de rekenkamer een zogenaamde penetratietest laten uitvoeren. Daarmee zijn zowel de systemen van de provincie als het gedrag van de medewerkers getoetst. De rekenkamer concludeert dat de provincie op een aantal punten kwetsbaar is gebleken. Enkele opvallende bevindingen uit onze tests zijn:

- Tijdens de test van het interne netwerk van de provincie zijn binnen korte tijd beheerdersrechten verkregen op een groot aantal systemen, zodat er toegang was tot *vrijwel alle* gegevens en systemen van de provincie.
- Tijdens de test vanaf het internet kon toegang worden verkregen tot systemen in de zogenaamde demilitarized zone (DMZ) van de provincie. Daarbij konden databases worden bevraagd en (met gelimiteerde privileges) de systemen worden bestuurd (overgenomen).
- Bij verschillende loginpagina's en enkele systemen van de provincie ontbrak het aan beveiligde verbindingen. Hierdoor is het in slecht beveiligde netwerken voor

kwaadwillenden mogelijk om gebruikersnamen en wachtwoorden (logingegevens) en persoonlijke/gevoelige gegevens te onderscheppen.

- Bij het testen van het veiligheidsbewustzijn van de provinciemedewerkers is onder andere een phishingaanval uitgevoerd op alle emailadressen eindigend op @prvlimburg.nl. Dit waren 1.398 emailadressen. De aanval heeft er toe geleid dat 171 ontvangers van de email hun gebruikersnaam en wachtwoord invulden op een, voor dit onderzoek geprepareerde website.

In 2015 heeft de provincie Limburg zelf al eens een penetratietest en een “passive audit” laten uitvoeren. Zij wenst dit in de toekomst periodiek te herhalen. De provincie heeft destijds naar aanleiding van de bevindingen een aantal maatregelen versneld ingevoerd. De rekenkamer merkt op dat tijdens haar tests op een aantal punten vergelijkbare typen bevindingen[2] naar voren kwamen als in 2015. Het gaat hierbij (ook) om bevindingen die in principe al opgelost hadden kunnen zijn. De directie heeft opgeroepen om ditmaal ook deze quick-wins op te pakken, ook al worden de risico’s van deze kwetsbaarheden door de provincie als laag ingeschat.

2.1.3 PS en informatieveiligheid

PS zijn actief geïnformeerd over de totstandkoming van het informatiebeleid waar informatiebeveiliging onderdeel van uit maakt. De rekenkamer constateert dat PS via het SIBL in 2011 en 2016 op hoofdlijnen zijn geïnformeerd over de kaders, uitgangspunten en governance voor het informatiebeleid en informatiebeveiliging. Het (specifiekere) informatiebeveiligingsbeleid hebben ze niet ontvangen. De verantwoordelijke gedeputeerde ziet het onderwerp primair als bedrijfsvoering, maar benadrukt wel te hechten aan een proactieve communicatie van GS naar PS over het onderwerp informatiebeveiliging. De aandacht van PS voor informatiebeveiliging kan structureel worden bevorderd, onder meer door een nog systematischere informatievoorziening vanuit GS.
Via de begrotingen en jaarstukken krijgen PS nagenoeg geen inzicht in (de stand van zaken/implementatie van) informatieveiligheid, omdat daarin veelal niet specifiek wordt ingegaan op informatieveiligheid. PS zijn (pas) via een mededeling portefeuillehouder van januari 2017 voor het eerst écht inhoudelijk geïnformeerd over de uitvoering van informatiebeveiliging. Deze mededeling werd opgesteld naar aanleiding van enkele informatieveiligheidsincidenten die bij een routine overleg naar voren kwamen. In dit stuk én in de stukken uit de P&C-cyclus wordt echter niet ingegaan op de kosten van informatieveiligheid. De aandacht vanuit PS zelf leek in het verleden voornamelijk incidentgestuurd te zijn. Er ontstaat echter steeds structurelere aandacht voor het onderwerp.

[2] Voorbeelden hiervan zijn: websites die kwetsbaar zijn voor SQL-injectie, systemen die verouderd zijn doordat beschikbare beveiligingsupdates niet waren gedraaid, onvoldoende filtering tussen client- en serversegmenten, ontbreken sterk wachtwoordbeleid, het bestaan van zwakke wachtwoorden en het onveilig opslaan van wachtwoorden.

2.2 Aanbevelingen

De rekenkamer beveelt Gedeputeerde Staten aan om, gezien de risico's en mogelijke gevolgen van beveiligingsinbreuken voor de provincie, haar toenemende aandacht voor informatieveiligheid voort te zetten, in lijn daarmee haar inspanningen op dit gebied te intensiveren en daarbij:

- met kracht in te zetten op het voldoen aan het gekozen basisambitieniveau; de IBI, onder ander door de procedures, processen en maatregelen op korte termijn te verwerken in het nieuwe managementsysteem en de andere voorgenomen maatregelen voortvarender te implementeren en te sturen op de realisatie daarvan.
- de voorgenomen periodieke penetratietesten uit te voeren en op basis daarvan, samen met de aandachtpunten uit de jaarlijkse IBI-analyse, informatiebeveiligingsincidenten en dergelijke, de te nemen maatregelen vast te stellen met inschatting van de daarvoor benodigde capaciteit en financiële middelen, deze te prioriteren en te sturen op realisatie daarvan.

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

2.3 Reactie Gedeputeerde Staten

We hebben Gedeputeerde Staten van Limburg gevraagd om een bestuurlijke reactie op ons conceptrapport. Op 3 juli 2018 ontvingen wij onderstaande reactie.

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

Informatiebeveiliging vraagt onze continue aandacht en alertheid. Ondanks alle inspanningen die wij hier tot nu toe aan geleverd hebben en ook in de toekomst gaan leveren, realiseren wij ons dat 100% veiligheid niet bestaat.
In zekere zin is er sprake van een afruil tussen beveiligingsvereisten enerzijds en de noodzakelijke transparantie en efficiency anderzijds. Absolute veiligheid is daarbij onhaalbaar. Meer veiligheidsmaatregelen zetten spanning op efficiency en transparantie. Om deze reden zullen wij voortdurend afwegingen en (risicogedreven) keuzes moeten maken. Informatiebeveiliging gaat daarbij verder dan alleen techniek en het doorvoeren van technische maatregelen. Er is een minstens zo belangrijke organisatorische component, bestaande uit afspraken en structuren, maar ook uit bewustzijn, houding en gedrag van bestuur en medewerkers.

Wij herkennen ons in de conclusies die de Zuidelijke Rekenkamer heeft getrokken in het conceptrapport. Het onderzoek van de Zuidelijke Rekenkamer biedt ons aanknopingspunten voor het verder en continu verbeteren van de informatiebeveiliging. De conclusies en aanbevelingen sluiten goed aan bij de ontwikkeling en het toenemende belang van Informatiebeveiliging binnen onze Provincie.

Wij zijn verheugd met de bevestiging door de Zuidelijke Rekenkamer dat de opzet van onze informatiebeveiliging goed is ingericht. De conclusie van de Rekenkamer dat deze op onderdelen nog verder verbeterd dient te worden biedt ons een extra stimulans om deze verbeteringen verder door te voeren.
Ondanks de, ook door de Rekenkamer geconstateerde, verhoogde inspanningen van de afgelopen jaren, dient ook naar onze mening nog meer aandacht uit te gaan naar het executietempo. Dit rapport is voor ons mede aanleiding om hier versnelling in aan te brengen. Hierbij moet onder andere worden gedacht aan het doorvoeren van maatregelen, het documenteren van processen, procedures en maatregelen en aan het werken aan een verdere bewustwording voor de gevaren van inbreuken op de informatiebeveiliging bij bestuur en medewerkers.
In lijn met de ingezette ontwikkelingen op het gebied van informatiebeveiliging kan naar onze mening, mede gezien de toenemende dreiging van cyberaanvallen, ook de communicatie met Provinciale Staten, waartoe ons college in 2017 het initiatief heeft genomen, worden geïntensiveerd.”

2.4 Nawoord Zuidelijke Rekenkamer

Met waardering hebben we kennis genomen van de reactie van Gedeputeerde Staten. De rekenkamer constateert met genoegen dat Gedeputeerde Staten zich herkennen in onze conclusies en dat zij, in lijn met onze aanbevelingen, voornemens zijn om op het gebied van informatieveiligheid tot een verdere verbetering en versnelling te komen van maatregelen binnen de eigen organisatie en intensiever te communiceren met Provinciale Staten. We zullen deze ontwikkelingen met belangstelling volgen.

Vastgesteld door de Zuidelijke Rekenkamer op 5 juli 2018.

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

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

3. Beleid, kaders en richtlijnen informatieveiligheid

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

3.1 Beleid, kaders en richtlijnen in het kort

Informatiebeveiliging maakt in Limburg onderdeel uit van twee beleidskaders. Het maakt zowel deel uit van het algemenere, overkoepelende strategische informatiebeleid, als van beleid dat specifiek is gericht op informatiebeveiliging. Deze kaders vormen de *opzet* van het informatiebeveiligingsbeleid en komen in dit hoofdstuk aan de orde. Op hun beurt mondden deze kaders de afgelopen jaren uit in concretere plannen en programma's.

- Het in 2015/2016 geactualiseerde *Strategisch Informatiebeleid Limburg, het SIBL 2016-2019,* is het overkoepelende vigerende kader. Hierin is op concernniveau vastgelegd hoe de provincie omgaat met informatie(voorziening) en de organisatie daarvan. Voortvloeiend uit het SIBL 2011-2015 is in 2011 een informatiestatuut opgesteld. Het *Informatiestatuut* geeft de belangrijkste inhoudelijke en procedurele 'spelregels' met betrekking tot de provinciale informatievoorziening inclusief informatiebeveiliging. Deze spelregels zijn in 2015 op enkele punten nader ingevuld en aangescherpt. Dit is vastgelegd in het document *Werkwijze vraaggerichte informatievoorziening*, ook wel I-Kompas genoemd. Zie verder paragraaf 3.2.
- Naast het SIBL is er het *Informatiebeveiligingsbeleid provincie Limburg*. Dit kader is in 2014 door GS vastgesteld en wordt in 2018 geactualiseerd. Op basis van dit kader volgde in 2015 een uitvoeringskader, het *Uitvoeringsplan Informatiebeveiliging provincie Limburg 2015-2016*. Hieruit volgde vervolgens in januari 2016 als uitwerking van één van de maatregelen het *programma Bewustwording informatieveiligheid 2016-2017*. Zie verder paragraaf 3.3.

Document	Vastgesteld
SIBL 2016-2019 (vervolg op geëvalueerde en geactualiseerde SIBL 2011-2015).	Door GS, september 2016
Informatiestatuut (2011-2015)	Op clusterniveau, 2011/2012
Werkwijze vraaggerichte informatievoorziening (I-Kompas)	Op clusterniveau, augustus 2015
Informatiebeveiligingsbeleid	Door GS, 1 juli 2014
Uitvoeringsplan Informatiebeveiliging 2015-2016	Door GS, december 2015
Programma Bewustwording Informatieveiligheid 2016-2017	Door directie, januari 2016

3.2 Overkoepelend beleid: Strategisch Informatiebeleid, Informatiestatuut en I-Kompas

3.2.1 Strategisch informatiebeleid

Na het mislukken van een aantal ICT-projecten van de provincie, waaronder Aristoteles, gaven GS begin 2011 aan te zijn gestart met een herijking en herpositionering van de ICT-functie. Eind 2011 hebben GS vervolgens het eerste strategische informatiebeleid vastgesteld: het *Strategisch Informatiebeleid Limburg (SIBL) 2011-2015*. Van dit SIBL maakte informatiebeveiliging onderdeel uit. In 2015 is het SIBL 2011-2015 na een interne evaluatie geactualiseerd. Op 13 september 2016 hebben GS het hernieuwde SIBL 2016-2019 vastgesteld. Het SIBL is na de vaststelling door GS ter kennisname aan PS aangeboden. Het SIBL wordt in principe elke vier jaar opnieuw opgesteld en indien nodig jaarlijks geactualiseerd.

In het SIBL wordt aangegeven dat het een “kaderdocument” betreft waarin op concernniveau wordt vastgelegd hoe de provincie omgaat met informatie(voorziening) en de organisatie daarvan (gebruik, beheer, vernieuwing): “Het geeft de uitgangspunten en randvoorwaarden voor de gewenste informatievoorziening weer en moet zijn afgestemd op het strategisch beleid van de organisatie.”

Het hoofddoel van, en de visie op informatie(voorziening) zijn volgens het SIBL:
Hoofddoel: De informatievoorziening is erop gericht dat de juiste informatie van de juiste kwaliteit op het juiste moment op de juiste plaats aanwezig is, tegen aanvaardbare kosten om zo PS, het bestuur, de medewerkers en (keten)partners optimaal te ondersteunen in het realiseren van de maatschappelijke opgaven.
Visie: Informatie is een strategisch bedrijfsmiddel voor de provincie.

Informatiebeveiliging/Cybersecurity is één van de speerpunten uit het SIBL, en komt naar voren onder de pijler met de naam “Groeien naar een zakelijke en professionele organisatie”. De ambitie van de provincie hierbij luidt: streven naar een professionele interne dienstverlening naar PS, GS, haar medewerkers en (keten)partners. Met betrekking tot informatiebeveiliging wordt de doelstelling geuit om “informatiebeveiliging een integraal onderdeel te maken van de bedrijfsprocessen en informatievoorziening”. Daarbij wordt onderscheid gemaakt tussen (a) informatiebeveiliging is prioriteit (belang van en structureel aandacht voor informatiebeveiliging), en (b) aandacht voor cybersecurity (risico’s en bedreigingen; bewustwording). Deze elementen zijn in het SIBL verder uitgewerkt. De informatie uit het SIBL over informatiebeveiliging komt (in het algemeen) overeen met informatie daarover in het informatiebeveiligingsbeleid (zie paragraaf 3.3).

Aangegeven wordt dat informatiebeveiliging een integraal onderdeel behoort te zijn van de bedrijfsvoering (alle processen en informatievoorziening). Het heeft betrekking op het treffen van maatregelen om binnen deze processen beschikbare informatie te beschermen.

3.2.2. Informatiestatuut en I-Kompas

Gelijktijdig met het SIBL 2011-2015 heeft de provincie een informatiestatuut opgesteld. Het informatiestatuut vloeit voort uit het SIBL en geeft de belangrijkste inhoudelijke en procedurele ‘spelregels’ met betrekking tot de provinciale informatievoorziening inclusief informatiebeveiliging. Zo wordt ingegaan op de organisatie met rollen en

verantwoordelijkheden van de verschillende actoren. Ook wordt stilgestaan bij de werkwijze voor beheer en vernieuwing van de informatievoorziening en de financiën. Veel informatie uit het statuut komt deels terug in het SIBL en/of het informatiebeveiligingsbeleid.
In 2015 zijn de spelregels op enkele punten nader ingevuld en aangescherpt in het I-Kompas. De provincie wil proactief en vanuit een vraaggestuurde houding nieuwe informatievoorzieningen plannen, ontwerpen, realiseren, implementeren, volgen en beheren. Veel elementen uit het informatiestatuut komen terug in het I-Kompas, maar de voorschriften voor informatiebeveiliging niet. De reden voor het ontbreken van deze voorschriften is dat in 2014 inmiddels het informatiebeveiligingsbeleid was verschenen. De rekenkamer constateert verder dat in het I-Kompas bijvoorbeeld procesbeschrijvingen nog niet zijn opgenomen, daarbij staat “verder uitwerken”.

3.3 Specifiek beleid: Informatiebeveiligingsbeleid, Uitvoeringsplan en Bewustwordingsprogramma

3.3.1 Informatiebeveiligingsbeleid

In 2014 is het informatiebeveiligingsbeleid uit 2008 geactualiseerd. Op 1 juli 2014 is het beleid door GS vastgesteld. Het informatiebeveiligingsbeleid is het kader voor (verdere) passende technische en organisatorische maatregelen om de informatie van de provincie te beschermen en te waarborgen, zodat de provincie voldoet aan de relevante wet- en regelgeving en aan landelijk en interprovinciaal gemaakte afspraken. In het SIBL staat dat bij cybersecurity niet alleen technische maatregelen een rol spelen, maar minstens zo belangrijk de aandacht is voor de houding en het gedrag van de individuele medewerker en de organisatorische component in de zin van het benoemen van rollen en verantwoordelijkheden binnen de organisatie. Deze elementen komen ook terug in het informatiebeveiligingsbeleid.

De provincie streeft er naar om ‘in control’ te zijn en daarover op passende wijze verantwoording af te leggen.

De **visie** voor informatiebeveiliging luidt:
De komende jaren zet de provincie in op het verhogen van de informatieveiligheid en verdere professionalisering van de informatiebeveiligingsfunctie binnen de organisatie. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de provincie en de basis voor het beschermen van rechten van bedrijven en burgers. Dit vereist een integralere, aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

Informatieveiligheid wordt **gedefinieerd** als:
Het definiëren, implementeren, onderhouden, handhaven en evalueren van een samenhangend stelsel van maatregelen gericht op het waarborgen/garanderen van de beschikbaarheid, de integriteit en de vertrouwelijkheid van de (handmatige en geautomatiseerde) informatievoorziening.

Beschikbaarheid: het waarborgen dat geautoriseerde gebruikers toegang hebben tot informatie en dat de benodigde bedrijfsmiddelen voorhanden zijn.
Integriteit: het waarborgen van de juistheid, de volledigheid en tijdigheid van informatie en verwerking.
Vertrouwelijkheid: het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn.

Provincies werken samen in het Centraal Informatiebeveiligingsoverleg (CIBO), een onderdeel van het Interprovinciaal Overleg (IPO). In 2010 heeft het CIBO de Interprovinciale Baseline Informatiebeveiliging (IBI) opgesteld. Deze is afgeleid van de internationale norm ISO 27001/27002 en alle provincies moeten hieraan voldoen. De IBI vormt het formele basisnormenkader voor provincies en bevat richtlijnen op het gebied van informatieveiligheid. De IBI vormt de basis voor de set aan beveiligingsmaatregelen voor de provincie Limburg. Eerst dient voor elk proces/systeem op basis van een Business Impact Analyse (BIA) een inschatting te worden gemaakt van de impact op het proces als de informatiebeveiliging van het systeem niet is gewaarborgd. Dit resulteert in een classificatieniveau. De baseline geeft vervolgens op basis van de classificatie de minimale set aan maatregelen waaraan de provincie moet voldoen. Hieraan wordt getoetst en als er meer maatregelen nodig zijn dan wordt een risicoanalyse uitgevoerd om de benodigde maatregelen te bepalen.

In het informatiebeveiligingsbeleid worden 24 uitgangspunten van informatiebeveiliging geformuleerd. Bij elk uitgangspunt horen één of meer principes. De rekenkamer merkt op dat de meeste uitgangspunten/principes geheel of deels terug komen in de uit te voeren maatregelen uit het Uitvoeringsplan informatiebeveiliging 2015-2016 dat ongeveer anderhalf jaar na het informatiebeveiligingsbeleid, in december 2015 werd vastgesteld.

3.3.2 Uitvoeringsplan informatiebeveiliging

In december 2015 verscheen het *Uitvoeringsplan Informatiebeveiliging Provincie Limburg 2015-2016*. Dit plan komt voort uit het informatiebeveiligingsbeleid en bevat conform dat beleid de te nemen maatregelen op het gebied van informatiebeveiliging. Het plan werd opgesteld omdat naast het informatiebeveiligingsbeleid behoefte was aan een planmatige implementatie van het kaderstellende beleid. De maatregelen uit het uitvoeringsplan dienen het doel om te komen tot een aanvaardbaar niveau van informatieveiligheid. De provincie komt dan “in control”.

In het uitvoeringsplan wordt aangegeven dat de maatregelen aan de hand van de parameters ’risico’, ‘inspanning’ en ‘impact’ zijn gewaardeerd om te komen tot een prioritering. Verder wordt de werkwijze beschreven die de provincie wil aanhouden voor (verdere) besluitvorming rondom prioritering en het al dan niet uitvoeren/implementeren van de maatregelen.

De 27 maatregelen betreffen de volgende onderwerpen:

Organisatie informatiebeveiliging	Gegevens	Functiescheiding beheer (rechten)	Analyse Baseline	Inzet externe medewerkers	Veilig delen bestanden
Business Impact Analyse (risico-analyse)	Logging van mutaties	Gebruik USB	Netwerk-segmentering	Continuïteit informatie-voorziening	Veilige toepassing services
Authenticatie en autorisatie	Wetten en richtlijnen	Niet gecertificeerde toepassingen/ programmatuur	Responsible Disclosure	Personele beveiligings-eisen	
Inkoop van software, hardware en informatie-voorzieningsdiensten	Zakelijk gebruik prive-apparatuur	Externe expertise IB*	Besturings-software up-to-date	Gebruik van Cloud toepassingen	
Bewustwording	Convenant zelfregulering	Documentatie processen en procedures	IB* in Service Level Agreement	Beveiligde email	

* IB = informatiebeveiliging

3.3.3 Bewustwordingsprogramma

Eén van de speerpunten uit het uitvoeringsplan is het opstellen en uitvoeren van een bewustwordingsprogramma informatieveiligheid om de awareness van medewerkers te vergroten/verhogen rondom informatieveiligheid. In januari 2016 verscheen in dat kader het *Programma Bewustwording Informatieveiligheid 2016-2017*. Daarin wordt, zo is vanuit de ambtelijke organisatie aangegeven, expliciet aandacht besteed aan cybersecurity en de 'best practices' die daarvoor landelijk dan wel internationaal ontwikkeld zijn.
Het bewustwordingsprogramma bestaat uit verschillende onderdelen en deelname hieraan vindt in principe op vrijwillige basis plaats.

4. Uitvoering beleid

Met betrekking tot de *uitvoering* van het in het vorige hoofdstuk behandelde beleid, constateert de rekenkamer dat, na drie jaar, begin 2018 het grootste deel van de maatregelen uit het uitvoeringsplan is opgepakt, maar dat de provincie met de meeste daarvan nog bezig is; deze zijn nog niet (volledig) afgerond/geïmplementeerd. Het uitvoeringsplan is, zowel voor een periode van één als vier jaar, te ambitieus gebleken.

In dit hoofdstuk geven we een samenvatting van de bevindingen over hoe de provincie Limburg haar informatiebeveiliging in de praktijk uitvoert (tweede deel van onderzoeksvraag 1 en onderzoeksvraag 2).

4.1 Uitgevoerde acties

De rekenkamer constateert dat voor enkele acties uit het uitvoeringsplan geldt dat ze zijn geïmplementeerd. Voorbeelden daarvan zijn:

- Rollen, verantwoordelijkheden en spelregels/afspraken rondom informatiebeveiliging zijn vastgelegd in beleid, het informatiestatuut en I-Kompas. De organisatie rondom informatiebeveiliging zal in 2018 verder worden geformaliseerd.
- Het vergroten van bewustzijn geldt als één van de belangrijkste voorgestelde maatregelen. In 2016 en 2017 heeft de provincie op verschillende wijze aandacht besteed aan bewustwording. Zo is een bewustwordingsprogramma opgesteld en onder de aandacht gebracht van medewerkers. Conform dit programma heeft de provincie bijvoorbeeld een game laten ontwikkelen welke bewust maakt van eigen handelen. In 2016 zijn alle medewerkers uitgenodigd om deze game te spelen. Daarnaast wordt bij het introductieprogramma voor nieuwe medewerkers in de module ‘digitaal werken’ aandacht besteed aan informatieveiligheid.
- De provincie maakt in het kader van digitale toegangsbeveiliging gebruik van authenticatiesystemen. De directie heeft eind 2017 besloten om voor extern inloggen op de citrix-omgeving (virtuele werkplek) over te gaan op ‘twee-factor authenticatie’ (via een token). Begin 2018 is het ingevoerd. Authenticatie houdt in dat de gebruiker van een systeem, programma of applicatie moet kunnen aantonen dat hij daadwerkelijk is wie hij zegt dat hij is. Meestal wordt daarbij gebruik gemaakt van een combinatie van een gebruikersnaam en wachtwoord om de identiteit van de gebruiker te verifiëren. Bij twee-factor authenticatie wordt het ‘te onthouden iets’, in dit geval het wachtwoord, gekoppeld aan een fysiek object (in dit geval een token).
- De provincie heeft, in het kader van veranderde wet- en regelgeving, een protocol meldplicht datalekken opgesteld dat in januari 2017 is verschenen. Het protocol helpt medewerkers te bepalen of sprake is van een datalek en zo ja, of deze gemeld moet worden bij de Autoriteit Persoonsgegevens (AP) en de betrokkenen. Ook wordt het proces, de te volgen routing beschreven. In 2017 en begin 2018 heeft de provincie ook voorbereidingen getroffen in verband met de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) op 25 mei 2018.
- De rekenkamer constateert dat er in de praktijk, in lijn met interprovinciale afspraken, door de provincie Limburg rapportages/memo´s zijn opgesteld waarin

verantwoording wordt afgelegd over de voortgang en volwassenheid van informatiebeveiliging. Hiervoor is via analyses, vanuit een professionele kijk, bepaald in hoeverre aan de gestelde afspraken/eisen (van de IBI) wordt voldaan. In de rapportages wordt per IBI-hoofdstuk aangegeven hoe de provincie er voor staat en welke aandachtsgebieden er zijn. Sinds 2011 is sprake van rapportages van provincies aan het CIBO over de door henzelf uitgevoerde (risico)analyses informatiebeveiliging.

- Om het gebruik van verouderde software te vermijden zijn verschillende maatregelen getroffen. Vanuit de ambtelijke organisatie is aangegeven dat eind 2017 een hulpmiddel is aangeschaft voor de signalering van kwetsbaarheden in componenten van de informatievoorziening. Sinds begin 2018 is dit operationeel en op basis hiervan kunnen gericht updates worden doorgevoerd
- De Chief Information Officer (CIO) is op verschillende manieren en langs verschillende kanalen geïnformeerd over informatieveiligheid. De meeste zaken over het informatiebeleid worden besproken in het CIO-overleg dat centraal staat in de I-governance (zie hierna).
- Vastgestelde rollen en verantwoordelijkheden zijn, conform de kaders en richtlijnen, ingevuld:

GS

Gedeputeerde Koopmans is portefeuillehouder informatiebeveiliging. GS zijn bestuurlijk verantwoordelijk voor het informatiebeveiligingsbeleid. De ambtelijke organisatie geeft invulling aan de uitvoering.

Ambtelijke organisatie

Directie/CIO: De directie (sturende rol) is, namens GS opdrachtnemer en ambtelijk eindverantwoordelijk voor de totstandkoming en de uitvoering van het informatiebeveiligingsbeleid en wordt ter zake geadviseerd door het cluster Organisatie en Informatie (O&I). Het directielid met de portefeuille informatievoorziening is binnen de provincie de CIO. De CIO is namens de directie opdrachtgever en op strategisch niveau verantwoordelijk. Binnen de directie is de CIO het eerste aanspreekpunt met betrekking tot alle I-zaken, dus ook informatiebeveiliging. Dat geldt op zowel strategisch, tactisch als operationeel niveau.

Clustermanager O&I: De clustermanager O&I (uitvoerende rol) is ambtelijk verantwoordelijk voor informatievoorziening waaronder ook informatiebeveiliging valt. Hij is eerste adviseur van de CIO en operationele CIO. De CIO neemt formeel de besluiten.

ISO: De provincie heeft geen CISO (Chief Information Security Officer) die op strategisch niveau opereert. Ze heeft wel een Information Security Officer (ISO). Het betreft de enige echte informatiebeveiligingsfunctie (rol) binnen de organisatie en betreft 0,8 fte. De ISO ondersteunt de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover aan de directie. Extern neemt hij deel aan het interprovinciaal platform informatiebeveiliging (CIBO). Het betreft een niet-technische functie op zowel operationeel, tactisch als strategisch niveau.

I-adviseurs: Hoewel niet expliciet genoemd in het informatiebeveiligingsbeleid zijn er binnen het cluster O&I acht I-adviseurs die zijn gekoppeld aan één of meerdere clusters. De ISO is één van deze acht. Als de clusters aanpassingen of nieuwe systemen of dergelijke willen

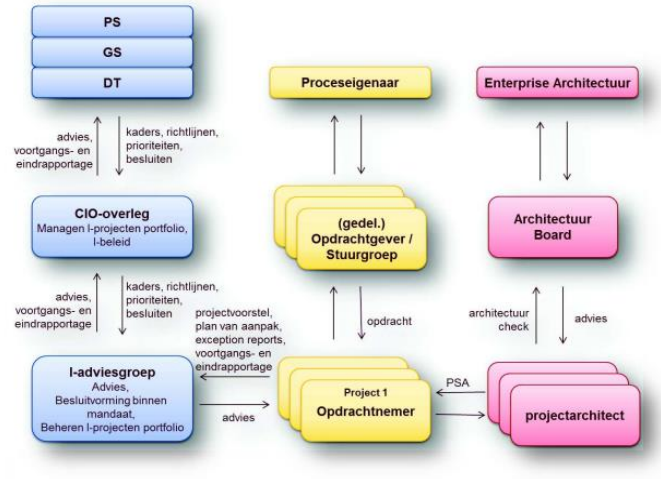
doorvoeren, dan moeten ze O&I hierbij betrekken. Vanzelf wordt hierbij dan ook naar de informatiebeveiligingsaspecten gekeken. De I-adviseurs adviseren hun clusters in deze gevallen. Als de ISO afwezig is, dan neemt, indien nodig, één van de I-adviseurs zijn taken over.

Clustermanagers en medewerkers: Elke clustermanager (vragende rol) is verantwoordelijk voor de processen (gegevens) binnen zijn/haar cluster en derhalve ook verantwoordelijk voor de aan deze processen gerelateerde informatiebeveiliging, met name voor wat betreft (het toezien op) de uitvoering van de daarop afgestemde informatiebeveiligingsmaatregelen. De medewerkers zijn hierbij een belangrijke factor: samen wordt invulling gegeven aan de informatiebeveiliging.

Er is een I-governancestructuur opgezet (zie kader) die borgt dat de informatievoorziening in lijn wordt gebracht en blijft met de strategie, ambities en behoeften van de organisatie.

I-governance richt zich specifiek op besluitvorming omtrent de informatievoorziening. Onderdeel van de I-governance vormt de interface tussen vraag- en aanbodzijde. Dit alles komt bijeen in het I-projectenportfolio: het centrale overzicht van goedgekeurde en nog niet goedgekeurde I-projecten van de provincie Limburg. Het CIO-overleg en de I-adviesgroep vormen de I-governancestructuur:

- ***Het CIO-overleg*** staat centraal in de I-governance. Het bewaakt op strategisch-tactisch niveau dat de juiste projecten worden uitgevoerd en borgt de efficiënte en effectieve inzet van de beschikbare middelen (managen I-projectenportfolio; monitoren en besluit over starten en stoppen I-projecten). De CIO is voorzitter en daarnaast nemen de clustermanager O&I en een medewerker vanuit de concernstaf, één vanuit strategie en een vertegenwoordiger vanuit het beleid zitting in het overleg.
- De ***I-adviesgroep*** heeft een adviesfunctie aan het CIO-overleg en (deels) ook een voorbereidende rol daarvoor. De clustermanager O&I zit de I-adviesgroep voor en is lid van het CIO-overleg. Binnen zijn mandaat als clustermanager en operationele CIO kan hij binnen de I-adviesgroep zelfstandig besluiten nemen over tactisch-operationele informatievraagstukken. De I-adviesgroep heeft een vaste en een deels (afhankelijk van de te bespreken onderwerpen) wisselende samenstelling.



Figuur 7: I-governance

Bron: I-Kompas/SIBL provincie Limburg

Functionaris gegevensbescherming: Met inwerkingtreding van de AVG op 25 mei 2018 is de provincie verplicht tot het instellen van een FG. In een gesprek is door een betrokken ambtenaar aangegeven dat, zoals het er in april 2018 naar uitzag, de FG een onafhankelijke rol wordt binnen de organisatie.

4.2 Aandachtspunten uitvoering

Naast de hiervoor beschreven uitgevoerde acties, is er ook een aantal aandachtspunten in de uitvoering van het Limburgse beleid:

- De rekenkamer constateert dat in haar testen (zie 'Kwetsbaarheden in de praktijk' hieronder) op een aantal punten vergelijkbare bevindingen naar voren kwamen als twee jaar daarvoor bij eerdere penetratietesten. Voorbeelden daarvan zijn: websites die kwetsbaar zijn voor SQL-injectie, systemen die verouderd zijn doordat beschikbare beveiligingsupdates (patches) niet waren gedraaid, onvoldoende filtering tussen client- en servernetwerksegmenten, gebruik zwakke wachtwoorden, ontbreken sterk wachtwoordbeleid en wachtwoorden die onveilig worden opgeslagen. In 2015 zijn risicoafwegingen gemaakt en als het risico laag werd ingeschat is er niets mee gedaan. Nu is vanuit de provincie aangegeven dat deze zaken gewoon sneller hadden moeten worden opgelost, ook al worden de risico's laag ingeschat.
- Vanwege een gebrek aan voldoende capaciteit en vanwege de impact die sommige maatregelen binnen de organisatie hebben, is het te ambitieus gebleken om het uitvoeringsplan jaarlijks te actualiseren, zoals eigenlijk was voorgenomen. De periode van het uitvoeringsplan bedraagt nu vier jaar. Het is daarbij zelfs niet zeker of de maatregelen binnen vier jaar opgepakt en/of gerealiseerd kunnen worden. Zoals reeds eerder opgemerkt zijn nog niet alle maatregelen uit het uitvoeringsplan opgepakt en zijn de meeste van de wel opgepakte maatregelen nog niet (volledig) afgerond/geïmplementeerd. Hoewel binnen de I-governancestructuur een prioritering is aangebracht in de maatregelen, constateert de rekenkamer dat dit niet heeft geleid tot een planmatige aanpak waarop wordt gebaseerd wat, wanneer, en waarom maatregelen worden opgepakt.
- Op basis van verschillende analyses is gebleken dat met name de documentatie van (werk)processen en procedures in relatie tot beheer van ICT-voorzieningen tekort schiet of ontbreekt. Dit blijkt ook uit het I-Kompas waarin een aantal procedures nog moet worden uitgewerkt. Hoewel ook de documentatie van maatregelen een kritiek punt blijft, is aangegeven dat er binnenkort een nieuw systeem wordt geïmplementeerd.
- Uit de *Monitoringtool baseline informatiebeveiliging 2016* blijkt dat Limburg, samen met enkele andere provincies, tot de minst scorende provincies behoort in het voldoen aan de IBI. De monitor van de provincie Limburg laat zien dat deze eind 2016 op de onderdelen: cryptografie, veilig personeel, acquisitie, ontwikkeling en onderhoud van informatiesystemen, en leveranciersrelaties achter blijft.
  Eind 2014 hebben de provincies het Convenant Interprovinciale Regulering Informatieveiligheid opgesteld. Het convenant dient door de provincies te worden vastgesteld. GS Limburg hebben dit nog niet gedaan.
- Interne analyses van de risico´s rondom informatiebeveiliging maken geen onderdeel uit van het interne controlesysteem van de provincie Limburg. Eind 2017 lieten GS in opdracht van PS wel een risicoanalyse uitvoeren naar de risico´s en risicobeheersing

rondom cybersecurity.

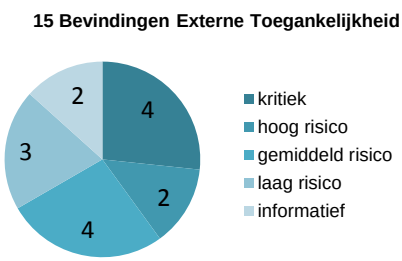
- Tot op heden is er geen budget (financiële middelen) specifiek voor informatiebeveiliging. Hierdoor is het ook moeilijk om inzicht te geven en krijgen in de kosten van informatiebeveiliging. Het wordt bekostigd uit de reguliere middelen. In het informatiestatuut staat dat voor de uitvoering van het informatiebeleid (waar informatiebeveiliging onderdeel van uitmaakt) in principe bij de vaststelling van een nieuw coalitieakkoord een investeringskrediet wordt opgenomen. De directie is budgethouder van dit investeringsbudget. Voor de dekking van de kosten voor de exploitatie en het beheer van de ICT-voorzieningen (structurele kosten voor onderhoud en vervanging van de bestaande hard- en software) wordt een budget opgenomen en door PS eenmalig door middel van het meerjaren-investeringsprogramma vastgesteld.
- Bij nieuwe of wijziging in informatievoorzieningen dient het cluster O&I betrokken te worden, onder andere voor informatiebeveiliging. In de praktijk, wordt ondanks de spelregels uit het I-Kompas, O&I nog niet in alle gevallen in voldoende mate en tijdig betrokken door de business.

Kwetsbaarheden in de praktijk

In de periode van 27 juli tot en met 9 oktober 2017 heeft de rekenkamer een zogenaamde penetratietest laten uitvoeren. Daarmee zijn zowel de systemen van de provincie als het gedrag van de medewerkers getoetst: is informatie van de provincie in de praktijk voldoende beschermd tegen toegang door onbevoegden en kwaadwillenden via het internet en het interne netwerk van de provincie (“hacking”) en via zogenaamde social engineering-aanvallen als phishingmail en een inlooptest; waar liggen de risico’s en kwetsbaarheden? Hierbij dient te worden aangegeven dat 100% veiligheid niet bestaat en de provincie bij het nemen van informatiebeveiligingsmaatregelen een risicoafweging maakt.

De rapportage met bevindingen over dit deel van het onderzoek is al tijdens het onderzoek aan de provincie gestuurd, zodat zij, indien gewenst, naast de ten tijde van de testen onmiddellijk gemelde bevindingen al een slag konden maken met de aangetroffen kwetsbaarheden. Hierna gaan we ter illustratie in op enkele van de aangetroffen kwetsbaarheden.

Externe toegankelijkheid vanaf het internet



De eerste *kritieke* kwetsbaarheid werd aangetroffen op een website die in eigendom van de provincie Limburg is. Deze kwetsbaarheid gaf onder andere toegang tot bestanden in het bestandsuitwisseling/transfer-systeem van de provincie. Hierbij konden onder andere emailadressen worden ingezien van zowel verstuurders als ontvangers, de begeleidende tekst aan de ontvanger en het bestand zelf. Een andere *kritieke* kwetsbaarheid[3] werd aangetroffen op een andere website en gaf toegang tot systemen in de zogenaamde demilitarized zone (DMZ) van de provincie.

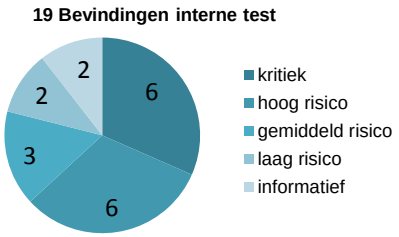
[3] De website bevatte een beheerinterface die niet was afgeschermd voor buitenstaanders.

Daarbij konden databases worden bevraagd en (met gelimiteerde privileges) de systemen worden bestuurd. Hoewel het hier ‘slechts’ twee kritieke kwetsbaarheden betrof, kan een aanvaller zichzelf hiermee toegang verschaffen tot andere systemen. Gezien het risico van deze bevindingen zijn deze na ontdekking direct gemeld aan de provincie. De provincie heeft vervolgens meteen de betreffende systemen uitgeschakeld. Vanuit de provincie is aangegeven dat het om “verweesde” websites ging die al uitgefaseerd hadden moeten zijn

Opvallend is het ontbreken van beveiligde verbindingen bij verschillende loginpagina’s en enkele systemen van de provincie. Hierdoor is het in slecht beveiligde netwerken voor kwaadwillenden mogelijk om gebruikersnamen en wachtwoorden (logingegevens) en persoonlijke/gevoelige gegevens te onderscheppen. Zo wordt een aantal invulformulieren waarin persoonsgegevens worden gevraagd, onversleuteld verstuurd over het internet. Ook loginschermen zijn vaak niet versleuteld.

Interne test/toegankelijkheid

Tijdens de test zijn binnen korte tijd beheerdersrechten verkregen op een groot aantal systemen, zodat er toegang was tot vrijwel alle gegevens en systemen van de provincie. Met dergelijke privileges is het namelijk mogelijk om onder andere emailboxen, bestanden op afdelingsschijven en persoonlijke mappen in te zien, mee te kijken op schermen, keyloggers te installeren of virtuele servers eenvoudigweg te kopiëren, uit te schakelen of te verwijderen. Deze privileges konden onder andere verkregen worden via systemen die niet waren voorzien van recente beveiligingsupdates (patches).



Bij een aantal systemen kunnen wachtwoordhashes[4] worden onderschept. Een aantal van deze hashes kon worden gekraakt, waardoor via de verkregen logingegevens toegang werd verkregen tot een aantal systemen en gedeelde mappen konden worden ingezien. Er zijn bijna 200 wachtwoorden van gebruikers achterhaald. Door het gebruik van zwakke wachtwoorden en het ontbreken van een sterk wachtwoordbeleid kunnen hashes relatief eenvoudig worden gekraakt.

Ten tijde van het onderzoek waren de verkeersstromen tussen client- en servernetwerksegmenten niet voldoende beperkt. Doordat er geen gebruik wordt gemaakt van een vorm van netwerkaccesscontrol (netwerkauthenticatie), kan een ieder die toegang heeft tot de kantoren van het gouvernement, zichzelf toegang geven tot het interne netwerk. En een ieder die deze toegang heeft, kan vervolgens alle systemen aan het interne netwerk bereiken.

Bij het testen van de beveiliging van de draadloze netwerken van de provincie is het niet gelukt om ongeautoriseerde toegang te verkrijgen tot het interne netwerk van de provincie en het is ook niet gelukt om andere systemen op deze draadloze netwerken succesvol aan te vallen.

[4] Hash: de versleutelde versie van een wachtwoord zodat deze veiliger kan worden opgeslagen.

Het gedrag: social engineering

Bij het testen van het veiligheidsbewustzijn van de provinciemedewerkers is als eerste een phishingaanval uitgevoerd op alle emailadressen eindigend op @prvlimburg.nl. Dit waren 1.398 emailadressen. De aanval heeft er toe geleid dat 171 ontvangers van de email hun gebruikersnaam en wachtwoord invulden op een, voor dit onderzoek geprepareerde website. De aanval is door de provincie gedetecteerd en deze heeft vervolgens acties ondernomen. Ook een spear phishingaanval met een zogenaamd “Wob-verzoek” via een vragenformulier op de website van de provincie is geslaagd. Hierdoor is toegang verkregen tot de systemen en accounts van twee medewerkers en gevoelige informatie toegankelijk geworden. Tenslotte heeft een inlooptest plaatsgevonden. De mysteryguest heeft daarbij ongeautoriseerd toegang tot werkplekken, systemen en gevoelige gegevens verkregen. Ook is toegang tot systemen en accounts verkregen via de met malware geprepareerde USB-sticks die door de mysteryguest waren achtergelaten.

Getroffen maatregelen

Naast de ten tijde van de testen onmiddellijk gemelde kwetsbaarheden heeft de provincie, zoals reeds eerder vermeld, al direct na het vaststellen van de risico’s in dit deel van het onderzoek een rapportage van de rekenkamer ontvangen, In deze rapportage zijn niet alleen alle bevindingen van dit deel van het onderzoek beschreven, maar ook de daarbij geformuleerde aanbevelingen.

Na ontvangst van de rapportage eind november 2017 is binnen de provinciale organisatie bekeken welke zaken op korte termijn aandacht behoefden en welke structureel opgelost moesten worden, zo is vanuit de ambtelijke organisatie aangegeven. Vervolgens is O&I ermee aan de slag gegaan. Aangegeven wordt dat vanwege de vertrouwelijkheid van de ontvangen rapportage er tijdens het onderzoek nog geen actie is ondernomen naar aanleiding van de phishingmail. Wel zijn naar aanleiding van de bevindingen over patches en patchmanagement direct patches uitgevoerd. Vanuit de ambtelijke organisatie wordt daarbij aangegeven dat patchen altijd al een ´heet hangijzer´ is geweest. Dit wordt veroorzaakt door de snelheid waarmee updates elkaar opvolgen. Als patches worden uitgevoerd, bestaat het risico dat applicaties niet meer goed functioneren. Hierdoor ontstaat een operationeel probleem dat beheerders moeilijk op kunnen pakken, zo wordt gesteld. Zoals reeds eerder opgemerkt, is eind 2017 een hulpmiddel aangeschaft op basis waarvan sinds begin 2018 gericht updates kunnen worden doorgevoerd.

De provincie heeft aangegeven dat zij met weerbaarheidmaatregelen zoals netwerk-segmentatie en een vorm van netwerkaccesscontrol bezig zijn. Met betrekking tot de segmentatie van het netwerk wordt aangegeven dat dit voor de scheiding tussen het gebruikers- en het beheerdersegment het eerste kwartaal van 2018 wordt ingevoerd. Met betrekking tot netwerkaccesscontrol, heeft de provincie, zoals reeds eerder opgemerkt, begin 2018 ‘twee-factor authenticatie’ voor extern inloggen op de citrix-omgeving ingevoerd. Ook zal het autorisatieproces worden aangepast waardoor medewerkers alleen toegang krijgen tot de systemen en ‘schijven’ die voor hun werkzaamheden noodzakelijk zijn. Ook zal het bewustwordingsprogramma worden geactualiseerd en is de provincie voornemens een nieuwe bewustwordingscampagne te starten.

5. Provinciale Staten en informatieveiligheid

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

5.1 Rollen PS

Provinciale Staten hebben tot nu toe geen kaderstellende rol gehad bij het informatie- en informatiebeveiligingsbeleid. De kaders voor informatieveiligheid zijn door Gedeputeerde Staten vastgesteld, omdat de verantwoordelijke portefeuillehouder het onderwerp primair als bedrijfsvoering ziet. PS hebben, eenmalig door middel van het meerjaren-investeringsprogramma, het budget vastgesteld voor het informatiebeleid (SIBL), waar informatiebeveiliging onderdeel van uitmaakt. Daarnaast hebben ze elk jaar (via de begrotingen) middelen toegekend voor de uitvoering van dit informatiebeleid (budgetrecht). Daarnaast is het de taak van PS om het door GS gevoerde bestuur te controleren en eventueel bij te sturen met behulp van de kaders.

5.2 Informatie aangeboden aan PS

Kaders en uitvoeringsplan
Over het proces naar de totstandkoming van het SIBL 2011-2015 zijn PS uitgebreid geïnformeerd door de verantwoordelijke portefeuillehouder. Het SIBL 2011-2015 is vervolgens op 22 december 2011 ter kennisgeving integraal aangeboden aan PS. Eind september 2016 zijn PS geïnformeerd over de evaluatie van dit SIBL. Bij dit informatiemoment is ook het nieuwe SIBL 2016-2019 meegezonden. Al de genoemde stukken zijn slechts ter kennisname aangeboden aan PS.

In 2014 is het informatiebeveiligingsbeleid en in 2015 is het uitvoeringsplan door GS vastgesteld. PS hebben dit beleidskader en uitvoeringsplan niet ontvangen. Via de P&C-documenten zijn ze geïnformeerd over de ontwikkeling en vaststelling daarvan.

Uitvoering
PS zijn zoals opgenomen in het SIBL 2016-2019 in de bestaande P&C-cyclus (begroting en jaarstukken) geïnformeerd over de voortgang van de activiteiten en projecten van het SIBL. Over informatiebeveiliging in het bijzonder is in de begrotingen (voornemens) en jaarstukken (realisatie) echter nauwelijks inhoudelijke informatie opgenomen.
Begin 2017 zijn PS via een mededeling portefeuillehouder voor het eerst extensief geïnformeerd met betrekking tot de definitie, de beleidsvoornemens en de voortgang van het informatiebeveiligingsbeleid, een overzicht van de activiteiten die in 2016 zijn uitgevoerd op het gebied van informatiebeveiliging en een overzicht van de incidenten die in 2016 hebben plaatsgevonden. PS hebben de inhoud van de mededeling niet besproken, deze is

voor kennisgeving aangenomen.

In vergaderingen van PS heeft de afgelopen jaren weinig discussie plaatsgevonden over informatiebeveiliging(sbeleid). Ook zijn er nauwelijks (schriftelijke) vragen ingediend. Naar aanleiding van een opmerking van de accountant bij de jaarstukken 2016 en daarop inhakend een aanbeveling vanuit de statenonderzoeksfunctie, vragen PS op 30 juni 2017 wel aan GS om risico's en risicobeheersing rondom cybersecurity in beeld te brengen. Begin 2018 zijn PS geïnformeerd over de uitgevoerde risicoanalyse.

De aandacht van PS voor informatiebeveiliging kan structureel worden bevorderd, onder meer door een nog systematischere informatievoorziening vanuit GS. De aandacht van PS leek in het verleden incidentgestuurd. Zo zijn er vanuit PS in 2017 naar aanleiding van de wereldwijde cyberaanvallen vragen gesteld over hoe een en ander bij de provincie geregeld is. Vanuit de ambtelijke organisatie is aangegeven dat PS wel betrokken zouden kunnen worden bij de afweging wat een aanvaardbaar niveau van informatieveiligheid is, onder andere vanwege de financiële consequenties die hieruit kunnen voortvloeien.