Informatieveiligheid
provincie Limburg

Deel II Rapport van bevindingen

ZUIDELIJKE REKENKAMER

Leeswijzer

De Zuidelijke Rekenkamer heeft in de periode juni 2017 - april 2018 onderzoek verricht naar de informatiebeveiliging van de provincie Limburg.

De resultaten van het onderzoek worden in twee deelrapporten weergegeven. Deel I, het bestuurlijk rapport, bevat de onderzoeksbevindingen op hoofdlijnen, de conclusies en aanbevelingen, de bestuurlijke reactie van Gedeputeerde Staten (GS) op het onderzoek en het nawoord van de rekenkamer. Voorliggend rapport van bevindingen (Deel II) bevat een uitgebreide weergave van de onderzoeksresultaten. In hoofdstuk 1 beschrijven we de aanleiding van het onderzoek en de onderzoeksopzet. In hoofdstuk 2 beschrijven we hoe de provincie Limburg haar informatiebeveiliging in beleid, kaders en richtlijnen heeft vormgegeven. Onze bevindingen over de uitvoering van het beleid komen in hoofdstuk 3 aan bod. In hoofdstuk 4 rapporteren we over in de praktijk aangetroffen kwetsbaarheden in de informatiebeveiliging. De informatievoorziening over informatiebeveiliging aan Provinciale Staten (PS) beschrijven we in hoofdstuk 5.

ZUIDELIJKE REKENKAMER

Inhoudsopgave

1. Over dit onderzoek

1.1 Aanleiding

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. Denk aan de vele slachtoffers die bijvoorbeeld in mei 2017 wereldwijd werden getroffen door de gijzelingssoftware WannaCry, die computers onbruikbaar maakte, en de wereldwijde hack die een maand later weer voor enorm veel schade zorgde. 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 twee zaken: de sterkte van de informatiesystemen en 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). 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.

1.2 Doelstelling, onderzoeksvragen, afbakening, aanpak

Doel van ons onderzoek is aanbevelingen te doen die bijdragen aan een verbetering van de informatieveiligheid van de provincie Limburg: dit doen we door op zoek te gaan naar kwetsbaarheden in de verdediging van de vertrouwelijkheid van de informatie waar de

[1] De rekenkamer hanteert in haar onderzoeken in het algemeen de term 'betrouwbaarheid'.

provincie over beschikt. Zo willen we ook bijdragen aan een actueel beeld van de informatieveiligheid voor de leden van PS.

De volgende onderzoeksvragen vormen daarbij het uitgangspunt:

1. Hoe heeft de provincie Limburg haar informatiebeveiliging in opzet en praktijk ingericht?
2. Welke kwetsbaarheden kent de beveiliging van de vertrouwelijkheid van de informatie in de praktijk?
3. Op welke wijze worden Provinciale Staten geïnformeerd over informatieveiligheid?

In antwoord op vraag 1 beschrijven we het *beleid* en de *organisatie* van de informatiebeveiliging/veiligheid, zowel hoe deze formeel zijn ingericht (hoofdstuk 2), als hoe deze in de praktijk zijn ingevuld (hoofdstuk 3). Daarnaast rapporteren we (in hoofdstuk 4) onze bevindingen over enerzijds 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 (vraag 2). Tot slot gaan we (in hoofdstuk 5) in op de informatievoorziening aan PS en hoe PS daar zelf hun rol in hebben genomen.

Bij de beantwoording van de onderzoeksvragen 1 en 3 zijn de van toepassing zijnde wet- en regelgeving en algemeen aanvaarde uitgangspunten voor beleids- en verantwoordingsinformatie (zoals leesbaarheid, aansluiting, begrijpelijkheid, bruikbaarheid en transparantie) gehanteerd. Voor onderzoeksvraag 2 hebben door ons ingehuurde specialisten gebruik gemaakt van gangbare standaarden en onderzoeksmethoden voor de daarbij uitgevoerde test.[2]

Het onderzoek richt zich op de periode 1 juli 2014 (vaststelling informatiebeveiligingsbeleid) tot en met april 2018. Voor de beschrijving van het beleid en informatie aan PS wordt soms iets verder terug gegaan in de tijd.

Voor de beantwoording van onderzoeksvraag 1 hebben we in kaart gebracht in hoeverre de provincie de sturing op, de beheersing van en de verantwoordelijkheid voor informatieveiligheid heeft verankerd. Voor onderzoeksvraag 3 hebben we gekeken op welke wijze PS zijn geïnformeerd over informatieveiligheid. Voor de beantwoording van deze onderzoeksvragen hebben we gegevens verzameld uit documentanalyse, schriftelijke vragen en gesprekken met betrokkenen binnen de provinciale organisatie. Een overzicht van de geraadpleegde documenten is opgenomen in bijlage 1. Voor de beantwoording van onderzoeksvraag 2 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. In hoofdstuk 4 geven we een beschrijving van de uitgevoerde test.

1.2.1 Bevoegdheden PS

De bevindingen van de rekenkamer over informatieveiligheid raken in algemene zin met name aan het budgetrecht en de kaderstellende en controlerende rollen van PS. Zie verder paragraaf 5.1.

[2] Als leidraad voor het proces van testen is gebruik gemaakt van de Penetration Testing Execution Standard (PTES: www.pentest-standard.org).

2. Beleid, kaders en richtlijnen

In dit hoofdstuk geven we inzicht in hoe de provincie Limburg de informatiebeveiliging in opzet heeft ingericht (beoogde invulling). De provincie Limburg heeft twee beleidskaders die informatiebeveiliging omvatten. Het in 2015/2016 geactualiseerde *Strategisch Informatiebeleid Limburg* (SIBL) is het overkoepelende document (SIBL 2016-2019). 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 opgestelddat in 2015 is opgevolgd door het document *Werkwijze vraaggerichte informatievoorziening*, ook wel I-Kompas genoemd. Deze documenten geven de belangrijkste inhoudelijke en procedurele spelregels met betrekking tot de provinciale informatievoorziening.
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 mondde vervolgens in januari 2016 als uitwerking van één van de maatregelen het *programma Bewustwording informatieveiligheid 2016-2017*.

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

In dit hoofdstuk worden de inhoud van deze documenten en enkele (externe) ontwikkelingen uiteengezet.

2.1 Context: Strategisch Informatiebeleid Limburg (SIBL), informatiestatuut en I-Kompas

SIBL (2011 en 2016)

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. De falende informatievoorziening zou op twee fronten aangepakt worden, te weten door (1) het opstellen een plan van aanpak voor een strategisch informatiebeleid en (2) een projectplan om ICT-knelpunten op te lossen om te voorkomen dat er weer projecten mislukken.

Eind 2011 hebben GS vervolgens het eerste strategische informatiebeleid vastgesteld: het *Strategisch Informatiebeleid Limburg (SIBL) 2011-2015*. Van dit SIBL maakte

informatiebeveiliging onderdeel uit. Uitgangspunten van het SIBL waren onder andere, zo is vanuit de ambtelijke organisatie aangegeven: moraliteit, awareness, integriteit, WOB en afleggen van de eed. In 2015 is het SIBL 2011-2015 intern geëvalueerd. Op 13 september 2016 hebben GS vervolgens het geactualiseerde SIBL 2016-2019 vastgesteld. Naast de resultaten van de evaluatie zijn ook relevante wettelijke, bestuurlijke en organisatorische ontwikkelingen meegenomen in de totstandkoming van het nieuwe document. Het SIBL is na de vaststelling door GS ter kennisname aan PS aangeboden.

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 informatiebeleid is, volgens het SIBL, het geheel van visies, kaders en richtlijnen dat richting geeft aan de ontwikkeling en inrichting van de informatievoorziening voor de komende vier jaar, gegeven de strategie, ambities, behoeften en ontwikkelingen van de provincie.[3] Het hoofddoel van, en visie op de informatie(voorziening) wordt omschreven:

Hoofddoel en visie informatie(voorziening)
Hoofddoel: de informatievoorziening is erop gericht dat de juiste informatie van de juiste kwaliteit op het juiste moment en 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.

Het SIBL bestaat uit twee pijlers, te weten:

- A: Interactie met de samenleving verbeteren.
- B: Groeien naar een zakelijke en professionele organisatie.

Informatiebeveiliging

Aan de twee pijlers zijn verschillende actiepunten gekoppeld waarin prioriteiten worden gelegd ter invulling van het SIBL. Informatiebeveiliging/Cybersecurity is één van de speerpunten en komt naar voren onder pijler B. De ambitie van de provincie bij pijler B luidt: streven naar een professionele interne dienstverlening naar PS, GS, haar medewerkers en (keten)partners. Informatiebeveiliging is vervolgens belegd in actielijn B2, waarin de doelstelling wordt 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 2.2).

Aangegeven wordt dat GS en PS in aansluiting op de bestaande planning- en controlcyclus

[3] In het Informatiestatuut uit 2011/2012 en het I-Kompas uit 2015 geeft de provincie aan dat “het SIBL het kader vormt voor de richting, inrichting en verrichting met betrekking tot de toekomst voor de informatievoorziening”.

(P&C; begroting en jaarstukken) periodiek geïnformeerd zullen worden over de voortgang van de activiteiten en projecten van het SIBL en dat het SIBL in principe elke vier jaar opnieuw opgesteld en indien nodig jaarlijks geactualiseerd wordt.

Informatiestatuut provincie Limburg (2011/2012) en I-Kompas (2015)

Gelijktijdig met het SIBL 2011-2015 heeft de provincie een informatiestatuut opgesteld: *Informatiestatuut, Inhoudelijke en procedurele afspraken voor een toekomstvaste informatievoorziening in Provincie Limburg (2011-2015)*. Het informatiestatuut vloeit voort uit het SIBL en geeft de belangrijkste inhoudelijke en procedurele 'spelregels' voor informatievoorziening inclusief informatiebeveiliging. Zo wordt bijvoorbeeld 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 die gekarakteriseerd wordt door 1) planmatig, 2) projectmatig, 3) procesgericht en 4) programmatisch werken en portfoliomanagement, 5) werken met businesscase en 6) werken onder architectuur. Deze zes thema's worden ook, al dan niet expliciet, in het SIBL genoemd. De voorschriften voor informatiebeveiliging, die deels ook in het SIBL en/of het informatiebeveiligingsbeleid zijn opgenomen, worden opgesomd en er wordt ingegaan op de financiën.
In 2015 worden de spelregels uit het informatiestatuut op enkele punten nader ingevuld en aangescherpt in het document *Werkwijze vraaggerichte informatievoorziening provincie Limburg*, het I-Kompas. De provincie wil via accountgericht werken invulling geven aan vraaggericht en planmatig werken. Ze 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, waaraan de vraaggerichte component is toegevoegd. Eén van de onderwerpen die niet (expliciet) terug komt, zijn de voorschriften voor informatiebeveiliging. De rekenkamer constateert verder dat het document nog niet helemaal is ingevuld. Zo zijn bijvoorbeeld beschrijvingen van verschillende processen nog niet opgenomen, daarbij staat alleen "verder uitwerken".

Vigerend informatiebeleid

Het vigerende *informatiebeleid* staat beschreven in de SIBL 2016-2019. PS zijn over de inhoud geïnformeerd.

2.2 Informatiebeveiliging

Informatiebeveiligingsbeleid provincie Limburg (2008)

In 2008 stelde de provincie haar eerste informatiebeveiligingsbeleid op.[4]

Externe ontwikkeling: landelijke taskforce (februari 2013)

Naar aanleiding van een aantal landelijke informatiebeveiligingslekken stelde de Minister van Binnenlandse Zaken en Koninkrijkrelaties (BZK) in februari 2013 de Taskforce Bestuur en Informatieveiligheid Dienstverlening (BID) in. Onder andere om binnen de overheid het bewustzijn op het gebied van informatieveiligheid te verhogen en het onderwerp hoog op de (bestuurlijke) agenda te krijgen (zie kader).

[4] Vanuit de ambtelijke organisatie is aangegeven dat er geen formeel informatiebeveiligingsbeleid is van een eerdere datum.

Interprovinciaal beleid en landelijke aandacht voor informatieveiligheid
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. Het doel is om provincies op een vergelijkbare manier te laten werken aan informatieveiligheid; om op basis van kwalitatief uitgevoerde risicoanalyses een basis beveiligingsniveau vast te stellen voor de gehele organisatie. De IBI geeft een standaardwerkwijze waarmee per bedrijfsproces of informatiesysteem bepaald wordt welke beveiligingsmaatregelen getroffen moeten worden. Eind 2014 is op zowel ambtelijk als bestuurlijk niveau door alle provincies het Convenant *Interprovinciale Regulering Informatieveiligheid* opgesteld. Dit is een afsprakenkader waarmee provincies verantwoordelijkheid nemen voor het opstellen, uitvoeren en handhaven van het informatieveiligheidsbeleid. Het is de bedoeling dat de provincies op deze manier één standaard ontwikkelen en behouden waardoor informatieveiligheid geen vrijblijvend proces is. Daarnaast bestond van 2013 tot 2015 de Taskforce Bestuur en Informatieveiligheid Dienstverlening (BID), waarin het Rijk, het IPO, de Vereniging Nederlandse Gemeenten en de Unie van Waterschappen waren vertegenwoordigd. Doel van de Taskforce BID was om informatieveiligheid op de bestuurlijke agenda te zetten, om het bewustzijn van informatieveiligheid te vergroten en om instrumenten te ontwikkelen om sturing op informatieveiligheid door bestuur en management mogelijk te maken. De IBI is door de taskforce bekrachtigd als vigerend beleid voor de provincies. Verder is er op landelijk niveau het Nationaal Cyber Security Centrum (NCSC). Dit is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland en internationaal het Nederlandse aanspreekpunt op het gebied van ICT-dreigingen en cybersecurity-incidenten.

Informatiebeveiligingsbeleid provincie Limburg (2014)

Zoals reeds eerder gemeld maakt informatiebeveiliging deel uit van het SIBL en zijn de uitgangspunten en kaders voor informatiebeveiliging zowel in het SIBL als in het informatiebeveiligingsbeleid verwoord. Het SIBL vormt het algemene uitgangspunt voor informatiebeveiliging. Het SIBL positioneert informatie als *strategisch bedrijfsmiddel* waarbij informatiebeveiliging wordt gezien als proces om op een passende manier de beschikbaarheid, integriteit en vertrouwelijkheid te waarborgen. Een betrouwbare informatievoorziening is namelijk essentieel voor het goed functioneren van de processen van de provincie en helpt bij een goede invulling van haar maatschappelijke taken; het bereiken van haar doelen, zo wordt gesteld. Daarnaast heeft de provincie een maatschappelijke verantwoordelijkheid: van de provincie mag verwacht worden dat zij zorgvuldig omgaat met de gegevens die zij beheert, en dat de gegevens die zij levert juist, accuraat en tijdig zijn. De provincie, zo wordt gesteld, neemt ook op het gebied van informatievoorziening steeds meer een rol als partner op zich, waardoor de informatievoorziening niet meer als op zichzelf staand kan worden beschouwd, maar veel meer vanuit een ketenbenadering zal moeten worden opgepakt en beveiligd.

Informatiebeveiliging is geen doel op zich, maar dient een integraal onderdeel 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. Door onder andere de huidige informatiesamenleving zijn er vele bedreigingen en risico's voor de betrouwbaarheid van informatie. Het beheersen van deze risico's en daarmee ook het implementeren van geschikte maatregelen vereist zorgvuldige planning en aandacht

vanuit een daartoe ingericht proces informatiebeveiliging, zo wordt gesteld. Informatiebeveiliging dient dan ook structurele aandacht te krijgen. Daarbij dient rekening te worden gehouden met eisen vanuit wet- en regelgeving, contractuele verplichtingen alsmede de resultaten van een globale risicoanalyse en eventuele beveiligingsincidenten die zich in de praktijk hebben voorgedaan.

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. In het SIBL 2016-2019 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.

In het informatiebeveiligingsbeleid worden de kaders voor, de organisatie van, de verantwoordelijkheden, rollen en het proces voor en de (beleids)uitgangspunten en principes van informatiebeveiliging beschreven.

In 2014 is het informatiebeveiligingsbeleid uit 2008 geactualiseerd. Dit mede naar aanleiding van een aanbeveling van de externe accountant van de provincie. In 2014 verscheen het geactualiseerde informatiebeveiligingsbeleid dat op 1 juli 2014 door GS werd vastgesteld. De visie voor informatiebeveiliging luidt:

Visie informatiebeveiliging
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 integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

Informatiebeveiliging wordt gedefinieerd als:

Definitie informatiebeveiliging(sproces)
Het definiëren, implementeren, onderhouden, handhaven en evalueren van een samenhangend stelsel van maatregelen[5] 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.

De provincie wil voldoen aan de wet- en regelgeving die eisen stelt aan informatiebeveiliging, zoals de Wet bescherming persoonsgegevens (Wbp), de Wet Computercriminaliteit en de archiefwet en aan de afspraken die daarvoor op landelijk en

[5] Op de provinciale website staat: “het opstellen van een geheel van maatregelen, richtlijnen en procedurs die gericht zijn op het waarborgen (….)”.

interprovinciaal niveau zijn gemaakt, zoals de Interprovinciale Baseline Informatiebeveiliging (IBI). De wet- en regelgeving en afspraken zijn dan ook medebepalend voor de maatregelen die genomen worden in het kader van informatieveiligheid.

De IBI vormt de basis voor de set aan beveiligingsmaatregelen (ISO 27002). 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. Een voorbeeld is het uitgangspunt ‘Anoniem gebruik, gebruikersnaam en wachtwoord’, waarbij onder andere de volgende twee principes behoren:

- gebruikersnaam en wachtwoord zijn strikt persoonlijk;
- toegang tot de gesloten ICT-infrastructuur van buiten het gouvernement vindt plaats met twee-factor-authenticatie (iets wat je weet in combinatie met iets dat je bezit).

Een ander voorbeeld is het uitgangspunt dat het gebouw en de ICT-infrastructuur in zones zijn ingedeeld (op basis van een risico-inschatting). Bij het uitgangspunt ‘Locatie gegevens/beschikbaarheid’ is één van de principes het toepassen van ‘clear desk’. En bij het uitgangspunt ‘Personele beveiligingseisen’ is één van de principes dat autorisatie van gebruikers tot applicaties en gegevens plaats vindt op basis van functionele noodzaak; alleen die rechten worden verstrekt die voor de uitvoering van de taak nodig zijn (least privileged). Een laatste voorbeeld is het uitgangspunt ‘Beheer informatievoorziening’ waarbij één van de principes is dat de uitvoering van beheer- en gebruikerstaken wordt gescheiden op basis van specifieke authenticatie en autorisatie.

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. Soms hebben de maatregelen een net iets andere insteek. Drie uitgangspunten komen niet terug in het uitvoeringsplan:

- ‘draadloze internettoegang voor bezoekers van het gouvernement’ omdat dit reeds gerealiseerd was;
- ‘beschikbaar stellen van gebruiksgegevens’ omdat, zo is vanuit de ambtelijke organisatie aangegeven, dit al “common practice” was, en;
- logischerwijs ‘clustermanager Organisatie en Informatie (O&I) stelt maatregelenset vast die invulling geeft aan het informatiebeveiligingsbeleid’, want dit betreft het uitvoeringsplan zelf.

Zie voor de organisatie, verantwoordelijkheden en rollen, waarvoor in het SIBL 2016-2019 en I-Kompas af en toe een aanvulling staat, paragraaf 3.4.

Uitvoeringsplan informatiebeveiliging (december 2015)

In december 2015 verscheen het *Uitvoeringsplan Informatiebeveiliging Provincie Limburg 2015-2016*, dat nog steeds geldig is. 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”, zo wordt gesteld. Voorbeelden zijn het verhogen van de bewustwording rondom informatieveiligheid en maatregelen die vanuit de actualiteit aandacht vragen zoals ransomware en authenticatie.

De te nemen maatregelen kwamen naar voren na een eerste analyse. Daarbij werden als uitgangspunt genomen:

- Het informatiebeveiligingsbeleid.
- De IBI: deze is gebruikt om inzicht te krijgen in de resultaten van de door de provincie reeds ingestelde maatregelen.
- Gebeurtenissen: dit zijn zaken zoals “gecompromitteerde usercodes, ransomware en SSL-problematiek.”

Uit de analyse volgden 27 maatregelen waarbij de volgende onderwerpen/parameters worden onderscheiden:

- Inspanning: heeft betrekking op een inschatting van de inspanning om de oplossing van het probleem c.q. de maatregel te implementeren.
- Risico: daarbij gaat het om het risico (kans x impact) van het probleem dat door de maatregel gemitigeerd wordt.
- Impact: inschatting van de verstoring binnen de organisatie, die het oplossen van het probleem c.q. het uitvoeren van de maatregel met zich mee brengt.
- Baseline: voor het categoriseren van de acties en maatregelen wordt de indeling van de IBI aangehouden.
- Herkomst: op basis waarvan de betreffende acties en maatregelen zijn geselecteerd (beleid, norm (IBI) en/of actualiteit).

Met betrekking tot de realisatie van maatregelen zijn in een bijlage tevens opgenomen:

- Stand van zaken.
- Wanneer oplevering wordt voorzien.
- Welke personen aanspreekpunt zijn.

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

Zoals reeds opgemerkt raken de maatregelen veelal de in het informatiebeveiligingsbeleid omschreven uitgangspunten/principes. Er zijn zeven maatregelen die niet direct zijn te koppelen: organisatie, inkoop, logging, convenant zelfregulering, besturingssoftware up-to-date (beleid vaststellen dat verouderde (niet meer ondersteunde) software wordt verwijderd), (onderzoek naar behoefte aan) beveiligde email en veilig delen bestanden.

Over de uitvoering van de maatregelen wordt in het plan aangegeven: “De hiervoor genoemde acties/maatregelen (27) zijn verschillend van aard. Sommige acties bevinden zich op het niveau van richten en inrichten (9-vlaks model van R. Maas). Dit betekent dat dergelijke acties veelal leiden tot maatregelen die op het niveau verrichten (regulier) uitgevoerd worden. Voorbeeld hiervan is het “maken van beleid” (richten) als maatregel. Dit leidt op zijn beurt tot een aantal (procedurele) maatregelen die genomen dienen te worden om het beleid uit te voeren (inrichten). Dit leidt dan weer tot het daadwerkelijk uitvoeren (verrichten).”

In het uitvoeringsplan wordt verder gesteld dat dit plan een periodiek (jaarlijks) karakter krijgt doordat de risicoanalyse die aan het uitvoeringsplan ten grondslag ligt, wordt verankerd binnen het informatiebeveiligingsproces.[6] In het SIBL 2016-2019 wordt in lijn daarmee aangegeven dat de provincie werkt met een jaarlijks uitvoeringsplan, waarin maatregelen ter bevordering van de informatiebeveiliging worden gepland en geïmplementeerd.

Programma bewustwording informatieveiligheid (januari 2016)

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. De provincie maakt gebruik van de openbare adviezen van het NCSC.
Het bewustwordingsprogramma bestaat uit verschillende onderdelen en deelname hieraan

[6] In het informatiestatuut stond dat het informatiebeveiligingsplan jaarlijks zou worden geëvalueerd en bijgesteld.

vindt in principe op vrijwillige basis plaats:

- Eerst heldere communicatie naar alle medewerkers over bestaan, nut en noodzaak van informatieveiligheid en het bewustwordingsprogramma en onder andere per cluster aankondiging van een te spelen game.
- Beschikbaar stellen van algemene informatie over informatieveiligheid, zodat relevante informatie kan worden geraadpleegd. Voor de herkenbaarheid en voor promotie wil de provincie bij alle publicaties het door het interne grafisch centrum ontworpen logo informatiebeveiliging gebruiken.
  Daarnaast eens per maand of kwartaal informatie via (verwijzingen naar) relevante artikelen of ad hoc naar aanleiding van in- of externe incidenten zoals een phishingmail. Ook wil de provincie een aantal regelingen en gedragscodes samenvoegen.
- Op clusterniveau spelen van een game die deelnemers bewust(er) maakt van informatiebeveiligingsrisico´s en per cluster een terugkoppeling van de resultaten.
- Opzetten en uitvoeren van een introductieprogramma voor nieuwe medewerkers,waarbij onder andere ook aandacht zal worden besteed aan informatieveiligheid en het bewustwordingsprogramma.
- Ongeveer een jaar na implementatie van het bewustwordingsprogramma wil de provincie een evaluatie uitvoeren, waarna indien nodig het programma wordt bijgesteld. Bij de evaluatie wil de provincie gebruik maken van één of meerdere van de volgende instrumenten:
  - intern rondsturen van een phishingmail om medewerkers te verleiden vertrouwelijke gegevens prijs te geven, bijvoorbeeld hun wachtwoord;
  - uitnodigen van een mysteryguest die binnen een vastgestelde periode zoveel mogelijk binnen de organisatie rondloopt en onzorgvuldigheden tracht bloot te leggen;
  - manipulatie via social engineering, waarbij via telefoon of email medewerkers worden verleid om vertrouwelijke informatie te delen;
  - medewerkers verleiden ‘achtergelaten’ USB-gadgets te gebruiken als usb-sticks en lampjes die voorzien zijn van specifieke software.

In het bewustwordingsprogramma zijn in een bijlage tips en richtlijnen opgenomen voor medewerkers voor informatieveilig handelen. Deze zijn, met een enkele kleine aanpassing, ook opgenomen in de brochure *Tips en richtlijnen voor informatieveilig handelen* (zonder datum). Het betreffen onder andere tips en richtlijnen hoe om te gaan met fysieke toegang tot het gouvernement, vertrouwelijke informatie, fysieke werkplek, accountgegevens waaronder wachtwoorden, wifi en phishingmail.

Externe ontwikkeling: ISO 27002 en 27001 (2015-2017)

Zoals reeds eerder aangegeven, bevat de IBI de basisset van beveiligingsmaatregelen (ISO 27002). De provincie heeft zich aan deze baseline gecommitteerd; haar doel is om onder andere hieraan te voldoen. Omdat het noodzakelijk is om op reguliere basis de IBI te herijken, is de IBI 1.0 uit 2010 herijkt op basis van nieuwe risicoanalyses. De uitkomsten hiervan zijn verwerkt en hebben geleid tot de IBI 2.0 die in 2017, zo is vanuit de ambtelijke organisatie aangegeven, in concept is opgesteld door het CIBO, maar nog niet definitief is gemaakt. Verder, zo is aangegeven, hebben de provincies in 2017 met elkaar afgesproken dat ze in 2021 allemaal klaar moeten zijn voor ISO 27001-certificering voor de besturing van de informatieveiligheid; elke provincie stelt dan zijn eigen maatregelenset vast op basis

van een eigen risicoanalyse waarmee dan de IBI kan komen te vervallen. Vooruitlopend hierop wordt de ISO 27002 (maatregelenset) als norm gehanteerd.

Externe ontwikkeling: Wbp (2015 en 2018) en acties provincie daarop

Een van de wetten die eisen stelt aan informatiebeveiliging is de Wbp. In juli 2015 werd deze wet uitgebreid met een meldplicht datalekken: organisaties die persoonsgegevens verwerken werden met ingang van 1 januari 2016 verplicht om inbreuken op de beveiliging te melden die leiden tot bijvoorbeeld diefstal, verlies of misbruik van persoonsgegevens. Deze datalekken dienen bij de Autoriteit Persoonsgegevens (AP) gemeld te worden. De provincie heeft in dit kader een procedure en protocol meldplicht datalekken (januari 2017) opgesteld. Per 25 mei 2018 zal deze Nederlandse privacywetgeving worden vervangen door de Europese Algemene Verordening Gegevensbescherming (AVG). De provincie is sinds 2017 ook bezig met voorbereidingen op deze AVG.

Vigerend informatiebeveiligingsbeleid

Vanuit de ambtelijke organisatie is aangegeven dat het Informatiebeveiligingsbeleid uit 2014 het vigerende beleid is voor *informatiebeveiliging*. PS hebben dit beleid niet van GS ontvangen, maar door het aanbieden van het SIBL 2016-2019 zijn ze via dat document op hoofdlijnen over de kaders en uitgangspunten van informatiebeveiliging geïnformeerd. Conform de uitgangspunten uit het informatiebeveiligingsbeleid zal het beleid, na vier jaar, in 2018 worden geactualiseerd, zo is vanuit de ambtelijke organisatie aangegeven. In de toekomst wordt deze periode waarschijnlijk aangepast naar tweejaarlijks. Dit omdat de veranderingen en ontwikkelingen op het gebied van informatiebeveiliging zo snel gaan en er op deze wijze sneller ingespeeld kan worden op (nieuwe) risico's. Na de zomer zal het geactualiseerde beleid ter vaststelling worden aangeboden aan de directie en GS. Hierna zal het dan ter kennisname aan PS worden gestuurd, zo is daarbij gesteld. Het uitvoeringsplan, bevindingen uit onderzoeken, waaronder het voorliggende rekenkameronderzoek en de invoering van ISO 27001 vormen de basis voor de actualisatie van het beleid en de daaruit voortvloeiende maatregelen (uitvoeringsplan 2019-2020), zo is vanuit de ambtelijke organisatie aangegeven.

3. Uitvoering beleid

In dit hoofdstuk geven we inzicht in hoe de provincie Limburg de informatiebeveiliging in de praktijk heeft ingevuld. Daartoe beschrijven we hoe de beoogde invulling, zoals omschreven in het informatiebeveiligingsbeleid, het uitvoeringsplan 2015-2016 en het bewustwordingsprogramma 2016-2017, in verhouding staat tot de praktijk.

3.1 Jaarlijks uitvoeringsplan en prioritering maatregelen

In het informatiebeveiligingsbeleid wordt gesteld dat informatiebeveiliging een continu verbeterproces is. ‘Plan, do, check en act’ vormen samen het managementsysteem van informatiebeveiliging.
Hoewel in het uitvoeringsplan wordt gesproken over een periodiek (jaarlijks) karakter van dit plan en in het SIBL 2016-2019 wordt aangegeven dat de provincie jaarlijks een uitvoeringsplan opstelt, geldt het ‘uitvoeringsplan 2015-2016’ voor een periode van vier jaar. Uit een gesprek met een bij informatieveiligheid betrokken ambtenaar blijkt dat het te ambitieus is gebleken om jaarlijks een nieuw programma op te stellen en ook voor de periode van vier jaar is het plan te ambitieus, zo wordt gesteld. Het vergt tijd voordat maatregelen zijn geïmplementeerd in de organisatie en er is niet voldoende capaciteit om alles met zodanige snelheid door te voeren. Er is daarom een prioritering aangebracht in de te nemen maatregelen. Dit is binnen de bestaande I-governancestructuur gebeurd, op basis van de risico’s, de impact en de inspanning om de maatregelen uit te voeren. De rekenkamer constateert dat de prioritering van de maatregelen uit het uitvoeringsplan verder niet heeft geleid tot een concrete tijdplanning.

3.2 Uitvoering maatregelen

In 2014 wordt in het informatiebeveiligingsbeleid gemeld dat er reeds diverse maatregelen zijn genomen om te komen tot een aanvaardbaar niveau van informatieveiligheid. Ook begin 2017 wordt in een mededeling van de portefeuillehouder aan PS gesteld dat in het kader van het informatiebeveiligingsbeleid door de jaren heen diverse maatregelen zijn getroffen om de risico’s op verstoringen van de bedrijfsvoering tot een minimum te beperken. Een aantal van de maatregelen uit het uitvoeringsplan, zo wordt gesteld, was bij de start van 2017 reeds afgerond.[7] De rekenkamer constateert 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.

Hierna wordt per maatregel uit het uitvoeringsplan ingegaan op de stand van zaken. In de mededeling van de portefeuillehouder van januari 2017 wordt ook stilgestaan bij de uitvoering van maatregelen. De rekenkamer heeft deze in onderstaande beschrijving, zo goed als mogelijk, proberen te koppelen aan de maatregelen zoals opgenomen in het uitvoeringsplan.

[7] In het uitvoeringsplan zijn 27 maatregelen opgenomen. In de statenmededeling wordt gesproken van 28 maatregelen.

1. Organisatie informatiebeveiliging

Rollen, verantwoordelijkheden en spelregels/afspraken rondom informatiebeveiliging zijn vastgelegd in beleid en het I-Kompas (tot augustus 2015 het informatiestatuut). Zie paragraaf 3.4 voor uitgebreidere informatie. In de CIBO-monitor 2016 van de provincie wordt vermeld dat de organisatie in 2017 formeel zal worden vastgesteld. De portefeuillehouder geeft in de statenmededeling in januari 2017 aan dat de organisatie verder geformaliseerd zal worden. Als antwoord op schriftelijke vragen van de rekenkamer geeft een bij informatieveiligheid betrokken ambtenaar aan dat een notitie hiertoe nog geformaliseerd dient te worden. Daarnaast zullen processen verder beschreven worden in het Information Security Management Systeem (ISMS) dat de provincie aan het invullen is (zie ook maatregel 15 betreffende documentatie).

2. Business Impact Analyse (BIA (risicoanalyse))

Via een BIA wordt gekeken naar de impact van een wijziging of nieuw systeem op de beschikbaarheid, integriteit en vertrouwelijkheid. Indien de BIA op een hoger niveau uitkomt dan de baseline, dienen aanvullende beveiligingsmaatregelen te worden getroffen. De provincie heeft ervoor gekozen om nieuwe en ingrijpend gewijzigde toepassingen aan een BIA te onderwerpen. Meestal gebeurt dat binnen projecten, zo is vanuit de ambtelijke organisatie aangegeven. Echter, zo is daarbij aangegeven, de business realiseert zich niet in alle gevallen in voldoende mate en tijdig dat het cluster Organisatie en Informatie (O&I) hierin een rol heeft, waardoor het voor kan komen dat O&I pas laat in het proces/project wordt ingeschakeld. O&I adviseert en spreekt de gebruikers indien nodig aan.
Onder het kopje ‘Inbedding informatiebeveiliging in werkwijze O&I’ wordt in de mededeling van de portefeuillehouder gesteld dat in de werkwijze aandacht is voor informatiebeveiliging bij elke majeure verandering in bestaande of aanschaf van nieuwe informatievoorzieningen (‘security by design’). O&I voert een analyse uit die inzicht geeft in de eisen die de proceseigenaar aan de informatiebeveiligingsaspecten stelt (BIA). In aanvulling op het uitvoeringsplan wordt ook gekeken naar de eisen die worden gesteld in verband met privacy (PIA), zo wordt in de mededeling aangegeven. Daarnaast wordt voor de aanschaf van web- en cloudtoepassingen aangesloten bij vragenlijsten die door het NCSC zijn aangeboden.

3. Authenticatie en autorisatie

Er bestaat een natuurlijke spanning tussen het niveau van beveiliging enerzijds en het gebruikersgemak/openheid anderzijds. Tot een aantal jaren geleden moest alle informatie voor iedere medewerker toegankelijk zijn en waren provinciehuizen ook open voor iedereen, zo is vanuit de ambtelijke organisatie aangegeven.Bij de provincie Limburg zijn een aantal jaren geleden, zo is daarbij aangegeven, de eerste stappen gezet naar een andere balans met bijvoorbeeld het plaatsen van toegangspoortjes. In dit kader is in het uitvoeringsplan ook de maatregel opgenomen om de authenticatie en autorisatie aan te scherpen. In een gesprek is tegenover de rekenkamer aangegeven dat naar aanleiding van de aangebrachte prioritering dit met de hoogste prioriteit is opgepakt. In antwoord op schriftelijke vragen is aangegeven dat het proceduredeel van dit project is afgerond. In de mededeling van de portefeuillehouder van januari 2017 werd al aangegeven dat medewerkers in de toekomst gebruik zouden moeten gaan maken van een extra identificatiemiddel voor extern inloggen op de citrix-omgeving. De directie heeft eind 2017 besloten om over te gaan op deze zogenoemde ‘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). Deze extra 'beveiligingsstap' was, zo is vanuit de ambtelijke organisatie aangegeven, voorgesteld vanuit het cluster O&I, nadat er breed met vertegenwoordigers van andere clusters over was gesproken en daaruit bleek dat er ook breed draagvlak voor is. Ook is de provincie nog voornemens het autorisatieproces aan te scherpen waardoor medewerkers alleen toegang krijgen tot de systemen en 'schijven' die voor hun werkzaamheden noodzakelijk zijn ('rolebased access'). De toegevoegde waarde van de inzet van identity access management (IAM) wordt (in het licht van het gebruik van cloudtoepassingen) verder onderzocht, zo is aangegeven. IAM betreft de processen binnen een organisatie die gericht zijn op het veilig administreren en beheren van resources binnen het eigen IT-netwerk. Authenticatie en autorisatie vormen de kern van IAM.
Door deze verschuiving van de balans, zal het gebruikersgemak wel iets afnemen. De vraag die daarbij nu speelt is: wat is een aanvaardbaar niveau van informatieveiligheid? Wanneer is goed, goed genoeg? Deze afweging moet de provincie (steeds) maken.
De komende tijd wil de provincie ook onderzoeken of de procedure rondom privileged accounts verbeterd kan worden. Tevens is begin 2018 besloten om het wachtwoordbeleid aan te passen.

4. Inkoop van software, hardware en informatievoorzieningsdiensten

Vanuit de ambtelijke organisatie is aangegeven dat inkooptrajecten door I-adviseurs van het cluster O&I worden begeleid en dat er structureel rekening wordt gehouden met beveiligingsaspecten. Richtlijnen hiertoe zijn overgenomen uit het NCSC. Zie voor een uitgebreidere beschrijving hiervoor onder maatregel 2 BIA.

5. Bewustwording (informatiebeveiligingsbewustzijn/awareness)

In het informatiebeveiligingsbeleid wordt, zoals reeds eerder gesteld, het belang en inzet op bewustwording beschreven. In het uitvoeringsplan dat in 2015 is opgesteld is het vergroten van de awareness een van de belangrijkste voorgestelde maatregelen, zo wordt aangegeven. Daaruit voortvloeiend verscheen in januari 2016 de nota *Programma Bewustwording Informatieveiligheid 2016-2017*. Omdat de mens het grootste risico/zwakste schakel is bij informatieveiligheid is de provincie in 2016 gestart met het uitvoeren van het bewustwordingsprogramma.
De rekenkamer constateert dat conform het bewustwordingsprogramma:

- het bewustwordingsprogramma onder de aandacht is gebracht van de medewerkers en de brochure *Tips en richtlijnen informatieveilig handelen* verspreid is. Leden van PS volgen het bewustwordingsprogramma op basis van vrijwilligheid.
- op het intranet van de provincie op de 'homepagina' onder het kopje 'Services' en vervolgens onder 'Informatieveiligheid' informatie over informatieveiligheid is opgenomen: het informatiebeveiligingsbeleid 2014, het uitvoeringsplan informatiebeveiliging 2015-2016, het programma bewustwording informatieveiligheid 2016-2017 en het document met tips en richtlijnen informatieveilig handelen. Deze documenten zijn daarmee voor alle medewerkers raadpleegbaar. Voor meer informatie wordt verwezen naar de information security officer (ISO) van de provincie. Daarnaast verschenen op intranet enerzijds artikelen/informatieve berichten over (mogelijke)

dreigingen en het daarbij gewenst informatieveilig handelen en anderzijds incidenten die het gevolg waren van niet informatieveilig handelen.

- bij het introductieprogramma voor nieuwe medewerkers in de module 'digitaal werken' aandacht wordt besteed aan informatieveiligheid. Gelet op het belang van informatieveilig handelen is het volgen van deze module ondertussen verplicht gesteld.Het introductieprogramma werd in de afgelopen jaren drie tot vijf keer per jaar gegeven. In 2018 zal het vier keer plaatsvinden, zo wordt aangegeven.
- de provincie een game heeft laten ontwikkelen welke bewust maakt van eigen handelen ('Are you secure?') en zijn in de zomer 2016 uitnodigingen uitgestuurd om deze game te spelen. Daartoe is een uitnodiging verstuurd aan alle in- en externe medewerkers die op dat moment geregistreerd stonden binnen een cluster. De game is ook gespeeld door directieleden. GS hebben destijds geen uitnodiging ontvangen, zo is vanuit de ambtelijke organisatie aangegeven. Ruim de helft van de uitgenodigde personen heeft de game gespeeld, zo wordt gesteld. De game bevat vragen en uitleg over digitale veiligheid, social engineering, social media en fysieke veiligheid. De ISO heeft in alle clusteroverleggen een terugkoppeling gegeven over hoe het cluster het heeft gedaan, heeft afwijkingen gemeld, vragen beantwoord en gezorgd voor nazorg. De opkomst van interne medewerkers daarbij was hoger dan 50%, zo is aangegeven. Eind 2017 werd over het spelen van de game en de terugkoppeling daarvan een rapportage gemaakt voor het directieteam die als nulmeting kan worden gehanteerd, zo wordt gesteld.
- op initiatief van de griffie is tijdens de introductie van een digitaal vergadersysteem in 2015 en bij een vervolgsessie in het voorjaar van 2017 aandacht besteed aan informatieveiligheid. Deelname aan deze sessies vond plaats op basis van vrijwilligheid. Aan de initiële sessie namen circa 25 PS-leden deel[8], aan de vervolgsessie namen circa 10 PS-leden deel.
- een aantal regelingen en gedragscodes is samengevoegd in het document *Tips en richtlijnen informatieveilig handelen*.

De provincie was van plan om eigen social engineeringacties uit te laten voeren (evaluatie) en daarover een actieve terugkoppeling te geven, maar daar de rekenkamer dat in 2017 al deed, is afgezien van het uitvoeren van deze acties.

Via het bespreken van tactisch/operationele informatiebeveiligingskwesties in de I-adviesgroep (zie paragraaf 3.4) is, conform een van de doelen van deze adviesgroep, ook gewerkt aan het vergroten van de awareness van de mensen uit de business die daaraan deelnemen.

In de mededeling van de portefeuillehouder van januari 2017 wordt het gebruik van het provinciaal emailaccount als een van de maatregelen genoemd. Gesteld wordt dat medewerkers zelf verantwoordelijk zijn voor emailafhandeling, inclusief oog voor veiligheid en betrouwbaarheid van externe adressen. Ook wordt opgemerkt dat in 2017 een herijking zal plaatsvinden van de regelingen gebruik internet, smartphones, social media etc.

In 2016 en 2017 heeft de provincie daarmee op verschillende wijze aandacht besteed aan bewustwording. In de mededeling portefeuillehouder van januari 2017 wordt ook kort op enkele van de hierboven beschreven uitgevoerde acties ingegaan. De gebruikers,

[8] In de mededeling portefeuillehouder van januari 2017 wordt gesteld dat informatieveilig handelen ook voor leden van PS van groot belang is.

waaronder ook de beheerders vallen die bijvoorbeeld tijdig patches (beveiligingsupdates) moeten draaien, zijn de meest kwetsbare schakel, daar blijven de grootste risico's liggen, zo wordt gesteld. Het bewustwordingsprogramma wordt dan ook geactualiseerd en gecontinueerd. De provincie is voornemens een nieuwe bewustwordingscampagne te starten waarin medewerkers in een aantal rondes bekwamer worden gemaakt inzake informatiebeveiliging, zo is aangegeven. En, zo is vanuit de ambtelijke organisatie aangegeven, als er extra budget beschikbaar zou zijn voor informatiebeveiliging dan zou ook met name worden ingezet op het vergroten van de alertheid (awareness) bij de gebruikers. Bewustwording is gezien de risico's en met het oog op de toekomst een kwestie die de meeste aandacht vergt. Daarnaast zou ook worden ingezet op meer aandacht voor technische oplossingen, want ook dat kan uiteraard altijd beter.

6. Gegevens

Volgens het uitvoeringsplan zijn de gegevens die binnen processen en toepassingen verwerkt worden tot informatie en kennis "een van de belangrijkste productiemiddelen binnen de provincie". Met de eigenaar van de gegevens dienen afspraken gemaakt te worden over onder andere de classificatie van de gegevens. De eigenaar bepaalt wie toegang heeft tot de betreffende gegevens. Vanuit de ambtelijke organisatie is aangegeven dat classificatie voor een deel is meegenomen binnen het project digitalisering dossiervorming (DDI). Voor persoonsgegevens vindt in het kader van de implementatie van de AVG een inventarisatie plaats.

7. Logging van mutaties

Met betrekking tot logging van mutaties zijn er na de vaststelling van het uitvoeringsplan geen verdere acties ondernomen.

8. Wetten en richtlijnen

In het informatiebeveiligingsbeleid en het uitvoeringsplan staat dat de provincie wil voldoen aan wet- en regelgeving. In het uitvoeringsplan is de maatregel opgenomen dat de eisen uit wet- en regelging in maatregelen worden vertaald en de consequenties worden bepaald van veranderingen in wet- en regelgeving. Door de betrokken ambtenaar wordt aangegeven dat het monitoren en volgen van wetten en richtlijnen een continu proces betreft. Zoals reeds eerder gemeld, zijn organisaties met ingang van 1 januari 2016 verplicht om inbreuken op de beveiliging te melden (datalekken). De provincie heeft 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 AP en de betrokkenen. Ook wordt het proces, de te volgen routing beschreven. Dit alles om te waarborgen dat een datalek op correcte wijze wordt afgedaan. Vermeende datalekken moeten binnen 24 uur aan de directie/chief information officer (CIO) worden gemeld. Daarna worden ze geanalyseerd en wordt deze analyse voorzien van een advies of het lek aan de AP moet worden gemeld, ter besluitvorming voorgelegd aan de directie/CIO.
In 2017 en begin 2018 was de provincie ook bezig met voorbereidingen in verband met de vervanging van de Wbp door de AVG per 25 mei 2018. Om de inwerkingtreding van de AVG in goede banen te leiden, is het kwartiermakerschap bij de ISO en een collega van Juridische Zaken belegd. Op de stand van zaken van deze ontwikkelingen werd ook in januari 2017 stilgestaan in de mededeling portefeuillehouder.

9. Zakelijk gebruik privé-apparatuur

Door het gebruik van privé-apparatuur voor zakelijke doeleinden wordt het risico gelopen dat vertrouwelijke zakelijke gegevens die zich op het apparaat bevinden door derden kunnen worden ingezien, misbruikt en/of ontvreemd. In antwoord op schriftelijke vragen van de rekenkamer heeft een bij informatieveiligheid betrokken ambtenaar aangegeven dat in 2018 met de implementatie van het CISCO-ISE maatregelen worden getroffen om de toegang tot het netwerk met 'vreemde' apparatuur te regelenbij.
Uit de mededeling portefeuillehouder van januari 2017 blijkt dat er op *provinciale* smartphones en tablets mobile device managementsoftware is geïnstalleerd, waarmee in geval van diefstal of verlies een zogenaamde wipe op afstand kan worden uitgevoerd om alle provinciale informatie en apps van het apparaat te verwijderen. Daarnaast wordt een zescijferige persoonlijke toegangscode afgedwongen op deze apparaten, zodat bij diefstal of verlies derden geen toegang kunnen krijgen tot de informatie en apps op het apparaat.

10. Convenant zelfregulering

Eind 2014 is, zoals reeds eerder gemeld, door alle provincies gezamenlijk het convenant *Interprovinciale Regulering Informatieveiligheid* opgesteld. Het convenant dient door de provincies te worden vastgesteld. In het uitvoeringsplan uit december 2015 staat dat dit moet gebeuren. Vanuit de ambtelijke organisatie is aangegeven dat het convenant nog niet door GS is vastgesteld.

11. Functiescheiding beheer (rechten)

In het uitvoeringsplan wordt vermeld dat het belangrijk is dat de 'beheerdersplek' is afgeschermd van de 'individuele werkplek'. Daarbij wordt aangegeven dat destijds binnen I-Services een bepaalde vorm van scheiding reeds was doorgevoerd en deze op sommige punten verder moest worden aangescherpt. Vanuit de ambtelijke organisatie is gemeld dat de noodzakelijke beheerrechten aan de betreffende beheerders zijn toebedeeld (eigen beheerdersaccount).

12. Gebruik USB

In het bewustwordingsprogramma wordt aandacht gevraagd voor het veilige gebruik van USB's, zo is aangegeven vanuit de ambtelijke organisatie. In de mededeling portefeuillehouder werd gesteld dat het beperken van de risico´s van het gebruik van USB-devices worden doorgevoerd in de geplande reguliere vernieuwing van infrastructuurcomponenten van de provincie.

13. Niet gecertificeerde toepassingen/programmatuur

Bij deze maatregelen gaat het volgens het uitvoeringsplan om het "treffen van voorzieningen om alleen gecertificeerde software uit te kunnen voeren. Niet-gecertificeerde software dient geblokkeerd en gemeld te worden". In schriftelijke antwoorden vanuit de ambtelijke organisatie wordt gemeld dat het voor gebruikers niet mogelijk is om in de virtuele desktop infrastructuur (VDI)-omgeving software te installeren. De maatregel gaat niet zover dat enkel goedgekeurde programmatuur uitgevoerd *kan* worden. zo wordt daarbij gesteld.

14. Externe expertise informatiebeveiliging

In 2015 heeft de provincie voor het eerst een penetratietest en passive audit laten uitvoeren door een externe deskundige partij (toets op kwetsbaarheden in systemen). Dit met

als doel de IT-infrastructuur te toetsen op informatieveiligheid. Er heeft toen geen social engineering plaatsgevonden (waarbij bijvoorbeeld personen worden verleid om gevoelige informatie prijs te geven). Het cluster O&I heeft de bevindingen verwerkt. In de mededeling van de portefeuillehouder werd aangegeven dat een aantal bevindingen in samenhang met de geplande vernieuwing van onderdelen van het netwerk zou worden opgepakt.
Vanuit de ambtelijke organisatie is aangegeven dat in een werkafspraak tussen de CIO en de clustermanager O&I is afgesproken om deze testen periodiek te laten uitvoeren. Daar de rekenkamer in 2017 deze testen ging uitvoeren, heeft de provincie ervan afgezien om deze zelf ook in 2017 uit te voeren.

De “passive audit”-test is tussen 1 november 2015 en 11 december 2015 uitgevoerd door het plaatsen van een sensor in het netwerk. In totaal zijn er in die periode vijf incidenten aangetroffen. Eén daarvan had een laag risico, één een hoog en drie een medium risico. Bij deze bevindingen was twee maal sprake van schendingen van het beleid, één keer van misconfiguratie, één keer van kwaadaardige activiteiten en één keer van het gebruik van gedateerde software (Windows XP). De conclusie van de passive audit is vervolgens vertaald naar drie pijlers:

1. *De overall conditie* gaat over de volwassenheid van het netwerk. De provincie scoort hier gemiddeld.
2. Op basis van het *aantal incidenten* scoort de provincie ‘medium’.
3. De *hevigheid van de bedreiging* vanuit deze incidenten is eveneens ‘medium’.

Tijdens de penetratietest in 2015 kon volledige toegang tot het netwerk, systemen en (gevoelige) informatie van de provincie worden verkregen. Van de 50 bevindingen hadden er 3 een zeer hoog en 12 een hoog risico. Geconcludeerd werd dat de beveiligingsmaatregelen die de provincie destijds had, onvoldoende bescherming boden tegen cyberaanvallen op de IT-infrastructuur van de provincie. Er was sprake van onder andere:

- onvoldoende hardening en, niet of onvoldoende valideren van gebruikersinvoer waardoor webapplicaties kwetsbaar zijn voor SQL en Cross-site Scripting (XSS);
- onvoldoende filtering tussen netwerksegmenten en op systemen zelf, waardoor gebruikers toegang hebben tot onnodig veel systemen en services;
- kwetsbare systemen door gebruik van verouderde software (niet alle beschikbare updates zijn geïnstalleerd, patchmanagement is voor verbetering vatbaar);
- gebruik van standaard inloggegevens voor geprivilegieerde gebruikers, zwakke, eenvoudig te raden wachtwoorden ook bij accounts met hoge privileges, zwak wachtwoordbeleid en wachtwoorden worden onveilig opgeslagen.

Deze bevindingen hebben geleid tot een versnelde invoering van een aantal maatregelen, tegelijkertijd hebben sommige bevindingen niet geleid tot maatregelen terwijl die wel (sneller) getroffen hadden kunnen worden (zie paragraaf 4.3). De rekenkamer constateert dat een aantal van deze bevindingen ook in het uitvoeringsplan als maatregel naar voren komt.

15. Documentatie processen en procedures

Op basis van de eerste analyse van de baseline door de provincie Limburg, is gebleken dat met name de documentatie van (werk)processen en procedures in relatie tot beheer van ICT-voorzieningen tekort schiet of ontbreekt. In reactie op schriftelijke vragen van de rekenkamer is vanuit de ambtelijke organisatie aangegeven dat deze eerste analyse begin 2014 is uitgevoerd en 2013 betrof (zie ook maatregel 16 Analyse baseline). In de

Monitoringtool baseline informatiebeveiliging 2014 van het CIBO over 2014 worden deze kritische kanttekeningen over het ontbreken van eenduidige documentatie bij de provincie Limburg herhaald. Verder wordt daarbij gesteld dat dit aandachtspunt in 2015 opgepakt zal worden. In het daarna verschenen uitvoeringsplan van de provincie worden deze kanttekeningen ook genoemd. Daarbij wordt gesteld dat is gebleken dat het grootste deel van de reeds ingestelde maatregelen niet of te globaal gedocumenteerd was, waardoor een analyse op basis van de gedocumenteerde maatregel versus de geïmplementeerde maatregel vrijwel onmogelijk wordt. In het uitvoeringsplan is documentatie als een uit te voeren maatregel opgenomen. De documentatie van maatregelen blijft een kritiek punt, zo is aangegeven in een gesprek met een provinciale medewerker. Om deze kwestie op te vangen wordt binnen de provincie het ISMS geïmplementeerd. Hierin zullen de maatregelen (ISO 27002) worden gedocumenteerd en geregistreerd. Het wordt hierdoor makkelijker om maatregelen terug te vinden en inzicht te krijgen in maatregelen. Ook worden de maatregelen voor een breder publiek transparanter. De huidige maatregelen zijn voornamelijk vanuit een beheeroptiek ingericht, zo wordt gesteld.

16. Analyse Baseline

Dit betreft het inzicht in de stand van zaken met betrekking tot de implementatie en werking van maatregelen zoals aangegeven in de IBI. Vanuit de ambtelijke organisatie is aangegeven dat dit zal worden meegenomen bij het beschrijven van de maatregelen met de implementatie van het ISMS.

De rekenkamer constateert dat er in de praktijk, conform interprovinciale afspraken, door de provincie Limburg rapportages/memo´s zijn opgesteld waarin verantwoording wordt afgelegd over de voortgang en volwassenheid van informatiebeveiliging. Hiervoor zijn via analyses door de ISO, 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. Interprovinciaal is afgesproken om jaarlijks een analyse en daarbij behorende rapportage aan het CIBO op te stellen. In reactie op schriftelijke vragen is vanuit de ambtelijke organisatie aangegeven dat de eerste gezamenlijke rapportage van begin 2014 is en 2013 betreft. De provincie Limburg heeft ook een rapportage opgesteld over 2014 en 2016. Conform afspraken binnen het CIBO is er over 2015 geen rapportage opgesteld in verband met een update van de baseline. In het CIBO werkt de provincie samen met de andere provincies op het gebied van informatieveiligheid. Ook zijn er reguliere contacten met de beveiligingsfunctionarissen van de Zuid-Limburgse centrumgemeenten, zo wordt in de mededeling van de portefeuillehouder van januari 2017 gesteld onder de maatregel ´Samenwerking met andere overheden´.

In de *Monitoringtool baseline informatiebeveiliging 2014* van het CIBO, met het interprovinciale beeld van de implementatie/toepassing van de IBI, werd gesteld dat de monitor van de provincie Limburg laat zien dat deze eind 2014 op de onderdelen: organisatie, beheer van bedrijfsmiddelen, beveiliging van personeel, bedrijfcontinuïteitsbeheer, beheer van informatiebeveiligingsincidenten en naleving wat achter blijft. De score wordt deels verklaard door het ontbreken van eenduidige documentatie rondom de maatregelen en dat dit ook betekent dat diverse

maatregelen moeten worden genomen of aangescherpt. Gesteld wordt dat deze aandachtspunten in 2015 worden opgepakt. Conform het gestelde in de monitoringtool is in 2015 een uitvoeringsplan opgesteld. In het uitvoeringsplan wordt gesteld dat omdat het niveau van documentatie te laag is, een diepgaande analyse van de baseline ten opzichte van de genomen maatregelen niet mogelijk is.

In de *Monitoringtool baseline informatiebeveiliging 2016* van het CIBO werd gesteld dat de scores van 2014 en 2016 in principe niet te vergelijken zijn omdat de geactualiseerde IBI strengere en meer detaileisen stelt. Gesteld wordt dat de provincies nog lang niet voldoen aan het door henzelf opgelegde ambitieniveau en dat er nog veel werk verzet moet worden om het basisniveau te halen. Verantwoordelijkheden dienen verder belegd te worden en sturing dient strakker plaats te vinden. Daarnaast wordt gesteld dat de provincies geen richtdatum hebben afgesproken wanneer moet worden voldaan; dit zou provincies kunnen aansporen om sneller groei door te maken. Provinciebreed bezien blijft op de volgende onderdelen laag worden gescoord danwel blijven deze achter: bewustwording, naleving en bedrijfscontinuïteitsbeheer. Uit de monitor blijkt dat Limburg samen met enkele andere provincies tot de minst scorende provincies behoort. De monitor van de provincie Limburg laat zien dat deze eind 2016 op de onderdelen: cryptografie, veilig personeel, acquistitie, ontwikkeling en onderhoud van informatiesystemen, en leveranciersrelaties achter blijft. Het achterblijven heeft, zo wordt gesteld, te maken met de aantoonbaarheid van het volledige bestaan en de volledige werking. Limburg geeft een uitgebreide toelichting. In 2017 zullen richtlijnen voor cryptografie worden opgesteld, additionele afspraken worden gemaakt voor de acquistitie e.d. van informatiesystemen, met leveranciers zullen afspraken over informatieveiligheid nadrukkelijker worden vastgelegd en gemonitord.

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. De uitgevoerde analyse is meer theoretisch van aard en omvat drie onderdelen. Als eerste zijn digitale assets (hardware, applicaties en data) geselecteerd die essentieel zijn voor het behalen van de organisatiedoelstellingen, zoals de netwerkschijven en basis ICT-infrastuctuur. Daarna is middels een zelfanalyse door enkele provinciale ICT-ambtenaren, onafhankelijk van elkaar, de huidige staat van de informatieveiligheidsmaatregelen inzichtelijk gemaakt. Voorbeelden van maatregelen zijn: informatiebeveiligingsbeleid en toegangsbeveiliging. De staat kan variëren van ad hoc tot geoptimaliseerd. Als derde is een inschatting gemaakt van de impact van de meest bedreigende digitale risico's (bijvoorbeeld bewust lekken) voor de provincie, gerelateerd aan de meest essentiële assets en rekening houdend met de huidige maatregelen. Dit resulteerde in een digitaal risicoprofiel: zes toprisico's. Voor deze toprisico's is ten slotte bekeken welke van de huidige maatregelen relevant zijn en welke status deze hebben. In januari 2018 zijn PS via een statenmededeling geïnformeerd over de uitkomsten van de analyse.

17. Netwerksegmentering

Dit betreft het doorvoeren van (organisatie)scheiding binnen de infrastructuur. In een gesprek met een bij informatieveiligheid betrokken ambtenaar is aangegeven dat voor wat betreft de scheiding tussen het gebruikerssegment en het beheerderssegment de maatregelen het eerste kwartaal van 2018 zullen worden ingevoerd.

18. Responsible disclosure

Personen die gebreken/zwakke plekken ontdekken in de informatieveiligheid van de provincie kunnen dit via een speciaal emailadres (cert@prvlimburg.nl) melden zonder dat dit eventuele strafrechtelijke gevolgen voor de melder zal hebben. Dit staat vermeld op de website (disclaimer) van de provincie, evenals het daarbij behorende beleid.[9] In de mededeling van de portefeuillehouder wordt bij deze maatregel vermeld dat in 2016 twee meldingen zijn binnengekomen: VPN-software (ondernomen actie: zogenaamde patch geïnstalleerd die leverancier daarvoor heeft aangeleverd) en ten onrechte gebruik kunnen maken van het domein limburg.nl als email-domein (probleem is verholpen).

19. Besturingssoftware (technische levensduur)

Om het gebruik van verouderde software te vermijden zijn verschillende maatregelen getroffen. De provincie gebruikte eind 2015 nog het niet meer ondersteunde Windows XP. Dit is inmiddels uitgefaseerd. In de in 2015 uitgevoerde penetratietest bleek dat beveiligingsupdates (patches) niet altijd waren geïnstalleerd. Het niet of te laat doorvoeren van deze wijzigingen brengt een beveiligingsrisico met zich mee, omdat ontdekte kwetsbaarheden dan nog in de software aanwezig zijn en kwaadwillenden daar misbruik van kunnen maken. 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, zo is aangegeven. Zie ook paragraaf 4.3.

20. Service Level Agreement (SLA)

Volgens het uitvoeringsplan gaat dit over het: “Opstellen van eisen/richtlijnen die als praktische vertaling van het informatiebeveiligingsbeleid en de baseline opgenomen dienen te worden in de SLA’s die afgesloten worden met derden die diensten leveren c.q. derden die diensten afnemen.” Vanuit de ambtelijke organisatie is aangegeven dat dit nog niet is geformaliseerd. Dit zal met name actueel worden naarmate meer toepassingen buiten de infrastructuur van de provincie worden geplaatst (cloud/hosting), zo wordt daarbij gesteld. Bij de inrichting van de nieuwe governance wordt er expliciet over deze vraagstukken gedacht.

21. Inzet externe medewerkers

Vanuit de ambtelijke organisatie is aangegeven dat externe medewerkers die worden ingehuurd binnen O&I een geheimhoudingsverklaring ondertekenen. Bij de inzet van externe medewerkers binnen de rest van de organisatie wordt dit nog niet uniform toegepast. Het in het uitvoeringsplan beoogde protocol inzet externe medewerkers in relatie tot informatieveiligheid is nog niet opgesteld.

22. Continuïteit van de informatievoorziening

In het uitvoeringsplan wordt gesteld: “Het waarborgen van de continuïteit van de informatievoorziening heeft tot doel het onderbreken van bedrijfsactiviteiten tegen te gaan en het beschermen van (kritische) bedrijfsprocessen tegen de gevolgen van omvangrijke

[9] Beleid Responsible Disclosure Provincie Limburg. In de notitie staat ook wat de provincie doet als zij bij anderen lekken of kwetsbaarheden aantreft. Ze meldt deze onder andere bij het Nationaal Cyber Security Center van de Nederlandse overheid. Op website van het ministerie (van Veiligheid en Justitie) aangeduid als het Nationaal Cyber Security Centrum.

storingen of rampen.” Streven is om een bedrijfcontinuïteitplan op te stellen (vanuit het aspect informatiebeveiliging). In de CIBO-monitor 2016 wordt deze maatregel ook genoemd.

In de mededeling portefeuillehouder van januari 2017 wordt onder de maatregel ´uitwijkvoorziening´ gesteld dat de provincie geen uitwijkvoorzieningen heeft voor haar (centrale) ICT-infrastructuur; bij een zware externe calamiteit (aardbeving, brand e.d.) kan continuïteit niet gegarandeerd worden. Er zijn geen externe werkplekken. In een extern datacenter staat wel een (nachtelijke) kopie, maar er is geen serverpark waarop applicaties kunnen doordraaien. Gesteld wordt dat hiervoor gekozen is op basis van een calamiteitenonderzoek uit 2011, waarbij de kosten van een volledige uitwijkvoorziening zijn afgezet tegen de kans op daadwerkelijk gebruik daarvan. In het informatiestatuut uit 2011/2012 staat dat er maatregelen dienen te zijn getroffen om verstoringen als gevolg van calamiteiten het hoofd te kunnen bieden; bedrijfszekerheid van ICT-infrastructuur moet via serviceovereenkomsten met leveranciers worden gegarandeerd.

Vanuit de ambtelijke organisatie is aangegeven dat het bedrijfcontinuïteitplan met de afdelingen Juridische Zaken en Facilitaire Zaken wordt opgepakt. Dit vraagstuk verhoudt zich eveneens tot de te ontwikkelen sourcingstrategie, zo wordt gesteld. Sourcingstrategie: “de strategische, tactische en operationele activiteit die resulteert in het vinden, contracteren en evalueren
van de juiste leverancier voor de gewenste IT-diensten. Dit leidt tot keuzes die kunnen bestaan uit het zelf aanbieden van diensten (insourcen), het samen met anderen aanbieden van diensten (co-sourcen) of het door derden laten aanbieden van diensten (outsourcen)”.

23. Personele beveiligingseisen

Dit betreffen de procedurele maatregelen in het kader van medewerkers die werkzaamheden gaan verrichten voor de provincie Limburg, zoals screening en geheimhoudingsverklaringen. Afgezien van de maatregelen die zijn getroffen voor externe medewerkers (zie maatregel 21), dienen maatregelen hiertoe nog te worden opgepakt, zo is vanuit de ambtelijke organisatie aangegeven.

24. Gebruik van cloud-toepassingen

Het laagdrempelige gebruik van cloud-toepassingen brengt het risico met zich mee dat informatie makkelijker lekt. Ten tijde van de vaststelling van het uitvoeringsplan diende het gebruik van cloud-toepassingen geïnventariseerd te worden waarbij inzicht zou worden verkregen in de informatieveiligheid van de gebruikte toepassingen. Vanuit de ambtelijke organisatie is aangegeven dat in het kader van de te ontwikkelen sourcingstrategie expliciete aandacht zal worden besteed aan de informatieveiligheid van cloud-toepassingen. Monitoring van netwerkverkeer vanuit de infrastructuur en de cloud-omgeving vindt nog niet plaats, zo is daarnaast gemeld.

25. Beveiligde email

In het uitvoeringsplan wordt aangegeven dat ‘afhankelijk van de behoefte’ maatregelen getroffen moeten worden voor het versturen en ontvangen van vertrouwelijke email. Volgens een bij informatieveiligheid betrokken ambtenaar neemt de vraag naar beveiligde email steeds meer toe. Op korte termijn zal daarom onderzocht worden hoe een en ander kan worden vormgegeven.

26. Veilig delen van bestanden

In het uitvoeringsplan is opgenomen dat werknemers van de provincie een mogelijkheid geboden dient te worden om op een veilige manier bestanden te delen. In reactie op schriftelijke vragen is vanuit de ambtelijke organisatie gemeld dat voor het uitwisselen van bestanden gebruik kan worden gemaakt van een transfersite. Het delen van bestanden kan daarnaast ook via de PLEIO-omgeving (een online platform van overheden). Ook worden in het kader van het DDI-project de mogelijkheden onderzocht om op een veilige manier samen te werken, ook met externe partijen.

27. Veilige toepassing van services

In het uitvoeringsplan wordt gesteld dat de uitwisseling tussen applicaties steeds vaker verloopt via services (service georiënteerde architectuur) die zich niet enkel beperken tot de infrastructuur van de provincie. Zoals beoogd in het uitvoeringsplan is voor het veilig (geautoriseerd) gebruik van services de enableU-@secure-omgeving geïmplementeerd.

Andere genoemde onderwerpen uit mededeling portefeuillehouder

In de mededeling van de portefeuillehouder van januari 2017 worden nog enkele onderwerpen genoemd die niet direct te koppelen zijn aan de maatregelen zoals opgenomen in het uitvoeringsplan. Zo wordt aangegeven dat er tijdens de interim-controle jaarlijks een toets door de externe accountant wordt uitgevoerd op de interne beheersingsomgeving en daarin opgenomen maatregelen onder andere toegang financiële systemen. De rekenkamer heeft in de rapportages van de accountant in het algemeen geen opmerkingen over informatieveiligheid aangetroffen, uitgezonderd in 2017 (zie paragraaf 5.2).

In de mededeling van de portefeuillehouder wordt ook ingegaan op de prioriteiten bij de afhandeling van informatiebeveiligingsincidenten. Daarnaast wordt ingegaan op de informatiebeveiligingsincidenten uit 2016. In 2016 was sprake van twintig geregistreerde informatiebeveiligingsincidenten. Een overzicht van deze incidenten is opgenomen in de bijlage van de statenmededeling. De helft daarvan is aan te merken als een beveiligingsincident in de zin van een dreiging die daadwerkelijk heeft geleid tot schade voor de provincie. De helft daar weer van heeft betrekking op zogenaamde ransomware en de andere helft op verlies of diefstal van een smartphone of iPad. Er zijn, zo wordt aangegeven, geen gevallen bekend waarin als gevolg van deze incidenten vertrouwelijke of privacygevoelige informatie van de provincie in handen van derden terecht is gekomen. De schade beperkte zich tot de inzet van capaciteit voor het herstellen van de situatie van voor het incident. Voor de ransomware incidenten betekende dit enkele dagen extra inzet van een medewerker van het cluster O&I. Daarnaast wordt geschat dat het verlies aan data mogelijk ook enkele dagen werk betekend heeft voor de getroffen clusters. In de CIBO-monitor 2016 staat dat in 2017 een systematiek zal worden opgesteld om op een structurele manier te rapporteren over incidenten. De portefeuillehouder is voornemens om ook begin 2018 PS weer te informeren over onder andere de informatiebeveiligingsincidenten. In reactie op schriftelijke vragen is vanuit de ambtelijke organisatie aangegeven dat er in 2017 140 meldingen zijn geweest die in eerste instantie betrekking hadden op een beveiligingsincident. Een groot deel daarvan (61) had betrekking op meldingen van spam. Deze waren daadwerkelijk doorgedrongen tot de mailbox van medewerkers. Van phishing-mail zijn zes meldingen geweest. Van cryptolockers/ransomware zijn twee gevallen geregistreerd. Van diefstal of verloren mobile devices waren 13 meldingen en er zijn

13 gevallen gemeld van geblokkeerde mail. Overige meldingen waren divers van aard. Er zijn geen kritieke meldingen geweest ten aanzien van de beschikbaarheid, integriteit of vertrouwelijkheid. De resultaten uit het technische onderzoek van de rekenkamer (zie hoofdstuk 4) zijn niet als beveiligingsincident gemeld, echter wel als zodanig behandeld, zo is vanuit de ambtelijke organisatie aangegeven.

Evaluatie beleid

Het SIBL is conform het beleid en als onderdeel van de planning- en controlcyclus na vier jaar geëvalueerd en bijgesteld, op basis van de relevante interne en externe ontwikkelingen.

3.3 Middelen

Financiële middelen

Er is geen afzonderlijk budget voor informatieveiligheid, 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. Het lokale netwerk, de communicatievoorzieningen, de standaard werkplekapparatuur en de centrale computers, alsmede de informatiesystemen op concernniveau (inclusief informatiebeveiliging) worden als basisvoorziening beschouwd en op concernniveau gefinancierd. De clustermanager O&I is budgethouder van alle budgetten die betrekking hebben op de exploitatiekosten. Projectleiders worden op basis van goedgekeurde projectvoorstellen door de directie aangewezen als budgethouder voor de aan de betreffende projecten toegekende budgetten.

Het is dan ook moeilijk inzicht te geven en krijgen hoe hoog de kosten zijn voor informatiebeveiliging. Vaak zijn de kosten voor informatiebeveiliging één van de kostenposten bij een project. Dit geldt niet voor zaken die direct zijn toe te wijzen aan informatiebeveiliging, zoals het bewustwordingsprogramma of penetratietesten. Deze kosten zijn relatief eenvoudig te traceren. Zo worden de kosten van de uitvoering van het bewustwordingsprogramma bijvoorbeeld gedekt uit de bestaande middelen van het cluster O&I, zo wordt in het bewustwordingsprogramma gesteld.

In het SIBL 2016-2019 wordt opgemerkt dat het niet naleven van de meldplicht datalekken uit de Wbp forse boetes tot gevolg kan hebben en tot grote imagoschade kan lijden. Ditzelfde geldt voor het niet naleven van de AVG die op 25 mei 2018 in werking treedt.

Personeel

De ISO richt zich als enige ‘exclusief’ op informatiebeveiliging. Vanuit de ambtelijke organisatie is aangegeven dat de ISO-functie de eerste jaren ongeveer een halve dag per week vroeg en nu 0,8 fte betreft. Daarnaast zijn ook andere medewerkers deels bezig met

informatiebeveiliging. Bijvoorbeeld de beheerders, de I-adviseurs, de clustermanager O&I en de CIO (zie paragraaf 3.4). Deze inzet tezamen wordt ingeschat op 0,8 fte. Als de ISO afwezig is dan neemt, indien nodig/noodzakelijk, één van de I-adviseurs zijn taken over.

In een gesprek is tegenover de rekenkamer aangegeven dat informatiebeveiliging steeds meer aandacht vergt en krijgt. Met het oog op onder andere deze ontwikkeling en dat de ontwikkelingen op IT-gebied zo enorm snel gaan, zal een verschuiving plaatsvinden van een meer beheersmatige optiek en het inbedden van de juiste functies en processen binnen de organisatie, naar een meer strategische optiek. De provincie wil van reageren naar anticiperen, zo wordt gesteld. Hiertoe dient inzichtelijk te worden gemaakt of de provincie voldoende is geëquipeerd om deze uitdagingen op te pakken: bevinden de mensen met de juiste vaardigheden zich op de juiste plek en zijn er voldoende middelen, zo wordt daarbij opgemerkt.

3.4 Organisatie

Zowel in het informatiebeveiligingsbeleid als in het uitvoeringsplan staat dat regels en verantwoordelijkheden voor het informatiebeveiligingsbeleid worden vastgelegd en vastgesteld.
In de evaluatie van het SIBL wordt gesteld dat in het kader van het aandachtspunt ‘vormgeven en invullen van sturende rollen’ in de periode 2011-2015 opdrachtgever- en opdrachtnemerschap, eigenaarschap, taken en verantwoordelijkheden van de informatievoorziening helder zijn belegd en vastgelegd (directie en clustermanagement). Ook wordt opgemerkt dat in de I-governance de taken, verantwoordelijkheden en bevoegdheden zijn toegewezen.
De rekenkamer constateert dat de rollen en verantwoordelijkheden in het algemeen zijn vastgelegd in het informatiebeveiligingsbeleid en af en toe op punten aangevuld in het SIBL 2016-2019 en het I-Kompas. In januari 2017 geeft de portefeuillehouder in een statenmededeling aan dat de organisatie verder geformaliseerd zal worden, zoals aangegeven in het informatiebeveiligingsbeleid en het uitvoeringsplan. Gesteld wordt dat er een voorstel in voorbereiding is met de rol van onder andere de ISO, clustermanager O&I, directie c.q. CIO en GS.

GS

Het college van GS (sturende rol) is integraal verantwoordelijk voor de beveiliging van informatie binnen de werkprocessen. Zij:

- stelt het informatiebeveiligingsbeleid vast;
- belegt informatieveiligheid als onderdeel van een portefeuille bij een lid.

Conform deze taken hebben GS op 1 juli 2014 het informatiebeveiligingsbeleid vastgesteld en is gedeputeerde Koopmans portefeuillehouder informatiebeveiliging en daarmee politiek/bestuurlijk verantwoordelijk voor de informatiebeveiliging. In de loop van de jaren is de aandacht voor informatiebeveiliging toegenomen en het staat nu hoog op de agenda van de gedeputeerde, zo is vanuit de ambtelijke organisatie aangegeven. Hij ziet informatie als een strategisch bedrijfsmiddel, een instrument dat noodzakelijk is voor de uitvoering van het coalitieakkoord. Deze zienswijze en het belang van informatie(veiligheid) draagt hij proactief uit vanuit gedreven belangstelling, zo wordt gesteld. Zo wil hij een schriftelijk verslag van

incidenten en de maatregelen die naar aanleiding daarvan zijn genomen. Ook wil hij PS proactief informeren over de stand van zaken van de informatiebeveiliging. Zo heeft hij PS begin 2017 via een mededeling portefeuillehouder geïnformeerd over de in 2016 uitgevoerde beveiligingsactiviteiten en incidenten. Intern voert hij ook scherp het debat over dit onderwerp, zo wordt vervolgd. Ook in het debat met PS is het onderwerp in 2017 enkele keren aan de orde geweest.

Directie

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 O&I. De directie:

- stuurt op concernrisico's;
- is verantwoordelijk voor kaderstelling op basis van wet- en regelgeving en landelijke normenkaders;
- is verantwoordelijk voor de controle of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden;
- evalueert periodiek beleidskaders en stelt deze waar nodig bij;
- wordt ondersteund door het cluster O&I.

Ter ondersteuning van de verantwoordelijkheid van de directie heeft het directielid met de portefeuille informatievoorziening, de rol van chief information officer (CIO). De vorming van de CIO-positie was een gevolg van het mislopen van het automatiseringsproject Aristoteles. In 2010 is de functie geïnstitutionaliseerd. De directeur/CFO is CIO en daarmee namens de directie opdrachtgever en op strategisch niveau verantwoordelijk. Zij is bijvoorbeeld (namens de directie) bevoegd om nieuwe I-projecten te starten en stoppen. 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.
De CIO wordt op verschillende wijze en langs verschillende kanalen geïnformeerd over informatiebeveiligingskwesties: via het zeswekelijkse CIO-overleg, regelmatig bilateraal overleg met de clustermanager O&I, direct bij datalekken en op een meer ad hoc wijze bij informatiebeveiligingsissues/incidenten, zo is in een gesprek aangegeven.

Cluster(manager) O&I

De clustermanager O&I (uitvoerende rol) is ambtelijk verantwoordelijk voor informatievoorziening waaronder bijvoorbeeld zowel archief als digitale systemen als informatiebeveiliging vallen. Hij is eerste adviseur van de CIO. De CIO neemt formeel de besluiten. In het I-Kompas en het SIBL 2016-2019 staat aanvullend dat de clustermanager de operationele CIO is. De huidige clustermanager vervult deze functie nu zo'n vijf jaar.
In het informatiebeveiligingsbeleid staat dat het cluster O&I verantwoordelijk is voor de beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen binnen hun verantwoordelijkheidsgebied en voortvloeiend uit de betrouwbaarheidseisen. In het I-Kompas staat dat de I-projectenportfolio de legitimering vormt van de inzet van O&I-medewerkers op provinciale I-projecten en in het SIBL 2016-2019 dat het cluster de projectenportfolio uitvoert. In het informatiestatuut stond dat het cluster het beleid voor informatiebeveiliging opstelt. In het I-Kompas staat dat het cluster meer vraaggericht wil gaan werken en hoe dit zal doorwerken in de werkwijze. Tot het cluster O&I behoren, naast de clustermanager zowel technisch beheerders, functioneel beheerders, informatiebeheerders en -specialisten, archiefmedewerkers, I-adviseurs (waaronder de ISO) als procesarchitecten.

ISO

De provincie heeft geen CISO (chief information security officer) die op strategisch niveau opereert. Ze heeft wel een information security officer (ISO).[10] Deze term is in 2013 bij de provincie geïnstitutionaliseerd. Het betreft de enige echte informatiebeveiligingsfunctie (rol) binnen de organisatie, zo is in een gesprek tegenover de rekenkamer aangegeven.
De rol van ISO is belegd binnen het cluster O&I bij één van de medewerkers in de functie senioradviseur O&I. 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. Hij houdt zich bezig met het stellen en actualiseren van kaders en beleidsmatige zaken (richten) en het voorstellen van maatregelen (inrichten). Hij geeft advies over beheeraspecten van informatiebeveiliging, zoals ICT en securitymanagement, voor het proces informatiebeveiliging, waarbij de risicoanalyse in nauwe samenwerking met businesscontrol en de concernstaf wordt uitgevoerd[11] en hij zorgt voor coördinatie van de afhandeling en het beheer van informatiebeveiligingsincidenten en voor opdrachtverstrekking tot audits en penetratietesten (verrichten), ook verzorgt hij monitoring en rapportage over (compliance) informatieveiligheid. Tevens heeft hij een adviesrol op het gebied van informatiebeveiliging voor de andere clusters en de directie/CIO. De ISO heeft geen formele bevoegdheden in termen van het kunnen beslissen over de inzet van personele resources en financiële middelen; dat loopt via de clustermanager O&I. Alleen bij prangende zaken en/of paniek, zo geeft hij aan, is hij bevoegd om buiten de clustermanager om met zaken naar de directie/CIO te gaan. In de mededeling van de portefeuillehouder van januari 2017 wordt gesteld dat de afhandeling van alle informatiebeveiligingsincidenten door de ISO worden beoordeeld. En dat afhankelijk van de impact van het incident zal worden geëscaleerd langs de lijn clustermanager O&I, proceseigenaar, directie en uiteindelijk de portefeuillehouder in GS.

De ISO heeft geen vaste formatie tot zijn beschikking om werkzaamheden uit te voeren, maar vraagt O&I-resources aan voor het uitvoeren van projecten en maakt gebruik van beschikbare O&I-resources binnen de reguliere beheeractiviteiten en -processen, zo is vanuit de ambtelijke organisatie aangegeven. Als de ISO afwezig is, dienen de I-adviseurs (zie hierna) als achtervang, zo is vanuit de ambtelijke organisatie aangegeven.

I-adviseurs

Hoewel niet expliciet genoemd in het informatiebeveiligingsbeleid zijn er binnen het cluster O&I acht I-adviseurs die zijn gekoppeld aan een 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. Sinds eind 2015 is het cluster O&I daarbij meer vraaggericht gaan werken: proactief vertalen van de behoeften van de organisatie naar informatievoorzieningen (richten, inrichten, verrichten).

[10] De ISO wordt in het SIBL, I-Kompas en informatiebeveiligingsbeleid genoemd, maar niet in het informatiestatuut.
[11] In het SIBL 2016-2019 staat dat de ISO de uitvoering van het jaarlijkse uitvoeringsplan coördineert.

Clustermanagers en medewerkers

Uitgangspunt is dat de verantwoordelijkheid voor informatiebeveiliging bij iedereen belegd is. Elk gegeven, elke gegevensverzameling, elke toepassing (applicatie/informatiesysteem) en elk proces heeft een eigenaar (functioneel verantwoordelijke; opdrachtgever). De eigenaar is verantwoordelijk voor het autorisatiebeheer, het correct gebruik van de gegevens en het systeem en de informatieveiligheid binnen het proces. Hierbij vindt ondersteuning plaats vanuit het cluster O&I.
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.
De clustermanagers:

- zijn verantwoordelijk voor het vaststellen, op basis van een expliciete risicoafweging, van betrouwbaarheidseisen voor de “eigen” informatiesystemen (classificatie);
- zijn verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen voor “hun systemen”;
- sturen op bedrijfscontinuïteit, beveiligingsbewustzijn, en naleving van regels en richtlijnen (eigen verantwoordelijkheid);
- worden bij de informatiebeveiligingsactiviteiten ondersteund door het cluster O&I.

Elke werknemer heeft een eigen verantwoordelijkheid met betrekking tot het beveiligen van informatie; de medewerkers zijn verantwoordelijk voor hun eigen informatieveilig handelen..
De medewerkers:

- zijn verantwoordelijk voor het uitvoeren van de relevante informatiebeveiligings-maatregelen; samen wordt invulling gegeven aan de informatiebeveiliging.

CIO-overleg

In het informatiebeveiligingsbeleid wordt gesproken over een CIO-overleg, maar er wordt verder niet ingegaan op (de inhoud van) dit overleg. In het informatiestatuut stond wel een toelichting. In het I-Kompas en het SIBL 2016-2019 is opgenomen dat de provincie middels een I-governancestructuur (met als dragers het CIO-overleg en de I-adviesgroep) borgt dat de informatievoorziening in lijn wordt gebracht en blijft met de strategie, ambities en behoeften van de organisatie. Het doel van I-governance is om ervoor te zorgen dat de juiste projecten worden uitgevoerd vanuit het perspectief van de verwachte bijdragen aan de organisatiedoelstellingen, door middel van het systematisch betrekken van de juiste stakeholders in het besluitvormingsproces: het bestuur, de directie en het clustermanagement. Om op centraal niveau besluiten te nemen en onderwerpen te agenderen, waaronder over informatiebeveiliging, is het CIO-overleg in het leven geroepen. In het SIBL en het I-Kompas is de rol van het CIO-overleg en samenstelling vastgelegd: 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. Er is bewust gekozen voor deze brede samenstelling om organisatiebreed afwegingen te kunnen maken en op deze manier, naast de techniek ook bijvoorbeeld eventuele strategische, tactische en beleids/gebruikerskwesties te tackelen. Het CIO-overleg 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). Daarnaast worden beleidsmatige onderwerpen met betrekking tot de provinciale informatievoorziening

in het CIO-overleg geagendeerd.
Vanuit de ambtelijke organisatie is aangegeven dat, zoals vastgelegd in het I-Kompas, het CIO-overleg centraal in de I-governance staat en zeswekelijks vergadert. In de mededeling van de portefeuillehouder van januari 2017 wordt aangegeven dat afhankelijk van de impact en kosten, besluitvorming over het doorvoeren van informatiebeveiligingsmaatregelen op het niveau van het CIO-overleg c.q. de directie wordt belegd.
Vanuit de ambtelijke organisatie is aangegeven dat er plannen zijn om, als gevolg van het toenemend belang van informatiebeveiliging, de I-governancestructuur door te ontwikkelen en een separaat informatiebeveiligingsoverleg in het leven te roepen gelieerd aan het CIO-overleg en waarin naast de ISO, ook vertegenwoordigers van P&O, juridische zaken (privacy) en facilitaire zaken deelnemen. Hiermee wordt het onderwerp ook vanuit andere invalshoeken dan primair de I-invalshoek geadresseerd.

I-adviesgroep

Naast het CIO-overleg maakt sinds begin 2014 ook de I-adviesgroep deel uit van de I-governance. Dit overleg heeft een adviesfunctie aan het CIO-overleg en (deels) ook een voorbereidende rol daarvoor. In het I-Kompas worden als doelstellingen voor de I-adviesgroep genoemd: beslissen over tactisch-operationele vraagstukken op het gebied van de provinciale informatievoorziening, advisering en beleidsvoorbereiding voor het CIO-overleg, beheer I-projectenporfolio en bespreken en adviseren over projectvoorstellen..[12] In het SIBL 2016-2019 is opgenomen dat de I-adviesgroep de projectvoorstellen/-plannen meer inhoudelijk zal beoordelen en de beschikbare middelen in kaart zal brengen (input voor prioritering in het CIO-overleg). Vanuit de ambtelijke organisatie is aangegeven dat het overleg zich met name richt op beleidsadvisering (inclusief de set aan beveiligingsmaatregelen) en adviseert over tactisch/operationele informatiebeveiligingskwesties, mede met als doel om de awareness op het gebied van informatiemanagement en -beveiliging te vergroten. Ook, zo wordt gesteld, adviseert de I-adviesgroep het CIO-overleg over het starten (en stoppen) van nieuwe I-projecten.
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, zo wordt in het I-Kompas en SIBL 2016-2019 gemeld. Verder wordt daarin aangegeven dat de I-adviesgroep een vaste en een deels (afhankelijk van de te bespreken onderwerpen) wisselende samenstelling kent. Vanuit de ambtelijke organisatie is aangegeven dat het overleg bestaat uit negen businessvertegenwoordigers en daarmee een brede vertegenwoordiging vanuit de organisatie vormt met gevoel voor de materie. Het overleg vindt conform het informatiebeveiligingsbeleid minimaal een keer per kwartaal plaats. In het I-Kompas staat dat het naar behoefte zal plaatsvinden, maar het uitgangspunt één keer per zes weken is.

Functionaris Gegevensbescherming (FG)

Om de inwerkingtreding van het AVG in goede banen te leiden vormt de ISO samen met een collega van Juridische Zaken (privacy-officer) het kwartiermakerschap voor de AVG, zo is vanuit de ambtelijke organisatie aangegeven. Met inwerkingtreding van de AVG op 25 mei 2018 wordt de provincie verplicht tot het instellen van een FG. In een gesprek is door

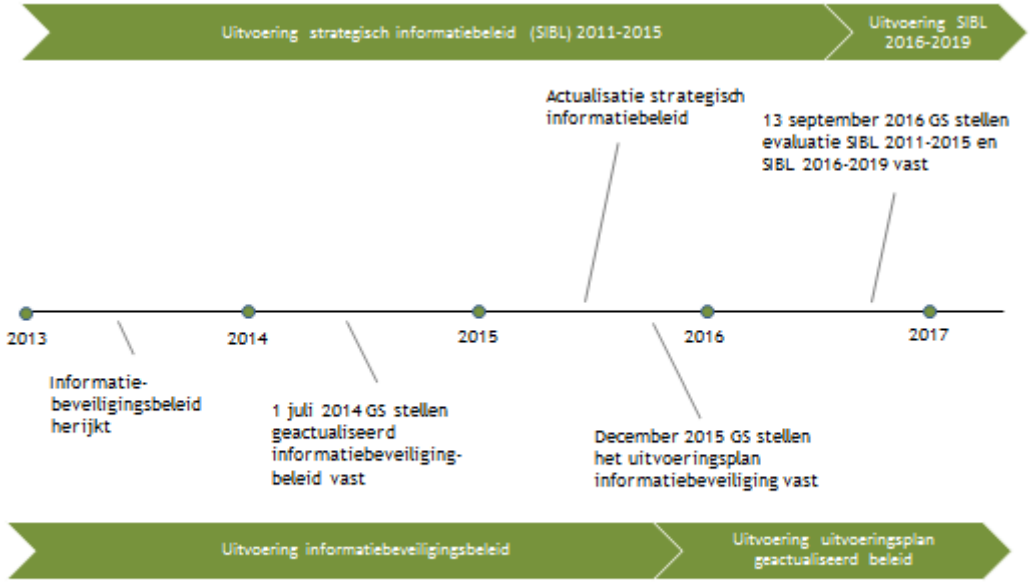
[12] In het informatiestatuut werd de I-adviesgroep niet genoemd, omdat deze pas begin 2014 is opgericht. In het informatiebeveiligingsbeleid wordt in algemene termen gesproken van een adviesgroep en wordt gesteld dat deze zich buigt over tactisch/strategische informatiebeveiligingskwesties.

een betrokken ambtenaar aangegeven dat, zoals het er nu naar uitziet de FG een onafhankelijke rol wordt binnen de organisatie. De provincie wil hiervoor iemand inhuren voor een periode van twee jaar. Hoogstwaarschijnlijk zal het geen fulltime functie zijn, maar 0,2 à 0,4 fte, zo wordt gesteld. Na twee jaar wordt bepaald hoe het daarna zal worden ingevuld. De FG zal een toezichthoudende rol hebben, de strategische, tactische en operationele taken liggen bij de ISO en privacy-officer.

Externe accountant

In het informatiestatuut werd en in het informatiebeveiligingsbeleid, het I-Kompas en het SIBL wordt er geen rol voor de externe accountant beschreven. Vanuit de ambtelijke organisatie is aangegeven dat de externe accountant momenteel ook geen formele rol speelt binnen de informatiebeveiligingsorganisatie, met uitzondering van de jaarlijkse toets op onder andere op algemene IT- en applicatiecontrols. Dit laatste beperkt zich doorgaans tot het financiële domein. De rekenkamer constateert in lijn daarmee dat in de rapportages van de accountant in het algemeen niet wordt ingegaan op informatiebeveiliging/informatieveiligheid (uitgezonderd 2017, zie paragraaf 5.2).

In onderstaande figuur een tijdlijn.



4. Kwetsbaarheden in de praktijk

In dit hoofdstuk beschrijven we de aanpak en zeer op hoofdlijnen de bevindingen van het onderzoek naar de stand van de informatieveiligheid bij de provincie Limburg in de praktijk. Een gedetailleerde beschrijving heeft de rekenkamer tijdens het onderzoek vertrouwelijk aan de provincie aangereikt. Dit deel van het onderzoek is uitgevoerd door een daarin ervaren en gespecialiseerd bureau. Zij toetsten de systemen en gedrag.

4.1 Aanpak technisch onderzoek

Voor dit deel van het onderzoek is een zogenaamde penetratietest uitgevoerd, met als doel:

- na te gaan of informatie van de provincie in de praktijk voldoende is beschermd tegen toegang door onbevoegden en kwaadwillenden via het internet en het interne netwerk van de provincie (“hacking”) en via zogenaamde social engineeringaanvallen;
- inzicht te krijgen in de risico’s en kwetsbaarheden met betrekking tot de onderzochte systemen, panden (het gouvernement) en gedragingen van medewerkers;
- handvatten te bieden voor verbetering van de beveiliging op deze vlakken.

4.1.1 De systemen

Er zijn drie manieren getest om in het informatiesysteem van de provincie te komen.

- *Externe toegankelijkheid.* Kunnen kwaadwillenden op afstand in de informatiesystemen van de provincie komen? Zonder enige voorkennis (blackbox) zijn de aan het internet gekoppelde systemen van de provincie onderzocht op kwetsbaarheden en is getracht deze te misbruiken. Aanvallers/kwaadwillenden gaan in het algemeen op deze manier te werk.
- *Interne kwetsbaarheden.* Wat zijn de gevolgen van een aanval op het systeem vanaf het eigen netwerk van de provincie, bijvoorbeeld door medewerkers met slechte bedoelingen of hackers die zich toegang hebben verschaft tot het interne netwerk? Zonder enige voorkennis (blackbox) zijn de interne systemen van de provincie vanaf twee voor dit onderzoek toegewezen werkplekken binnen het gouvernement onderzocht op kwetsbaarheden en is getracht deze te misbruiken. Daarna is hetzelfde geprobeerd via een door de provincie ter beschikking gesteld account (greybox).
- *Wifi.* De provincie heeft een wifi-netwerk voor medewerkers en een wifi-netwerk voor gasten. Hoe stevig is de beveiliging van deze draadloze netwerken?

4.1.2 Het gedrag: social engineering

De mens is doorgaans de zwakste schakel van elk beveiligingssysteem. Er is op drie manieren getest hoe sterk het veiligheidsbewustzijn van de provinciemedewerkers is, en in welke mate er in dit opzicht juist wordt gehandeld.

- *Phishing.* Via een email naar alle emailadressen eindigend op @prvlimburg.nl is geprobeerd mensen naar een geprepareerde website te lokken en te verleiden om daar hun inloggegevens (gebruikersnaam en wachtwoord) in te voeren. Herkennen medewerkers deze mails en gaan ze er goed mee om?

- *Spear phishing*. Aan een select aantal medewerkers is een met malware geïnfecteerd document verstuurd met een gepersonaliseerde boodschap. Ook hier wordt geprobeerd om controle te krijgen over het persoonlijke account of de computer van het slachtoffer. Herkennen de medewerkers spear phishing als het ze overkomt?
- *Oplettendheid*. Provinciehuizen zijn openbare gebouwen waar iedereen naar binnen moet kunnen, maar niet overal bij moet kunnen. In een *inlooptest* is gekeken in hoeverre onbevoegden zich fysieke toegang kunnen verschaffen tot het gouvernement en welke informatie ze daarbij kunnen vinden. De mysteryguest heeft zonder voorkennis en toestemming het beveiligde deel van het gouvernement proberen binnen te komen en daarbij twee met malware geprepareerde USB-sticks achtergelaten. Voor de inlooptest is een vrijwaring van de provincie ontvangen.[13]

De penetratietest heeft plaatsgevonden in de periode van 27 juli tot en met 9 oktober 2017. Om deze fase van het onderzoek zo effectief mogelijk te kunnen uitvoeren (inclusief een 'verrassingseffect'), hebben wij het onderzoek niet, zoals gebruikelijk, voorafgaand aan de start van het onderzoek aangekondigd, en niet in ons Werkprogramma 2017 opgenomen. Wel zijn voorafgaand aan deze penetratietest de algemeen directeur, de commissaris van de Koning en de vaste rekenkamercontactpersoon van de provincie op de hoogte gesteld van het rekenkameronderzoek.
Als onderdeel van de penetratietest is als eerste de externe toegankelijkheid van de systemen getest. Deze test vond plaats in de periode 27 juli tot en met 9 augustus. Tijdens deze test is naar aanleiding van enkele kritieke bevindingen ook de clustermanager O&I van de provincie geïnformeerd over het onderzoek. De bevindingen die een (zeer) hoog risico vorm(d)en voor de provincie zijn ten tijde van het testen met de clustermanager besproken, zodat de provincie (desgewenst) direct actie kon ondernemen om deze problemen te verhelpen. Vervolgens zijn het interne netwerk en de draadloze netwerken van de provincie getest. Deze testen zijn uitgevoerd in de periode 17 tot en met 22 augustus. Tijdens deze testen is er nauw contact geweest met de clustermanager O&I.
Op 21 september heeft het phishingonderzoek plaatsgevonden, op 3 oktober volgde de inlooptest en op 9 oktober het spear phishingonderzoek. Na afronding van de penetratietest hebben wij op 8 november 2017 het onderzoek aangekondigd (bij PS) en opgenomen op onze website. Op 17 november 2017 heeft de provincie een vertrouwelijke rapportage van de rekenkamer ontvangen met alle bevindingen van de penetratietest en screenshots of foto's die daar in het algemeen van zijn gemaakt.[14] Deze rapportage is al tijdens het onderzoek aan de provincie gestuurd, zodat zij, indien gewenst, naast de ten tijde van de testen reeds gemelde bevindingen al een slag konden maken met de aangetroffen kwetsbaarheden.

Opgemerkt dient te worden dat de mogelijkheid bestaat dat het gespecialiseerde bureau niet iedere kwetsbaarheid heeft gevonden, omdat deze gebonden was aan een budget- en tijdslimiet. Daarnaast zijn de bevindingen een momentopname/tijdsgebonden. Na de uitvoering van de penetratietest kunnen nieuwe ontwikkelingen immers nieuwe kwetsbaarheden met zich meebrengen die ten tijde van de uitvoering van de penetratietest nog niet bekend waren danwel nog niet aanwezig waren.

[13] Het bestuursgedeelte van het gouvernement was uitgesloten van de inlooptest, omdat de provincie daartoe geen toestemming had gegeven.
[14] *Rapportage Penetratietest Provincie Limburg* van Hoffmann Cybersecurity.

4.2 Bevindingen/Resultaten technisch onderzoek

4.2.1 De systemen

Externe toegankelijkheid vanaf het internet

Tijdens het externe beveiligingsonderzoek vanaf het internet zijn 15 bevindingen gedaan. Van deze bevindingen heeft het gespecialiseerde bureau er vier als *kritiek* geclassificeerd. Van de overige bevindingen hebben er twee een *hoog* risico, vier een *gemiddeld* risico, drie een *laag* risico en zijn twee ervan *informatief*.

De eerste *kritieke* kwetsbaarheid werd aangetroffen op een website die in eigendom van de provincie Limburg is. Deze kwetsbaarheid[15] gaf onder andere toegang tot bestanden in het bestandsuitwisseling/transfersysteem 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[16] werd aangetroffen op een andere website en gaf toegang tot systemen in de zogenaamde demilitarized zone (DMZ)[17] van de provincie. Daarbij konden databases worden bevraagd en (met gelimiteerde privileges) de systemen worden bestuurd (overgenomen). Gezien het risico van deze bevindingen (ongeautoriseerde toegang tot bestanden/gegevens van de provincie) zijn deze na ontdekking dan ook direct gemeld aan de provincie. De provincie heeft vervolgens meteen de betreffende systemen uitgeschakeld (‘de websites zijn uit de lucht gehaald’). Vanuit de provincie is aangegeven dat het om “verweesde” websites ging die al uitgefaseerd hadden moeten zijn. De rekenkamer constateert dat een van de websites begin 2018 nog steeds wel benaderd kan worden, maar het geen functionele website betreft. Bij openen verschijnt alleen de melding ‘Dit domein is eigendom van de Provincie Limburg’ en met doorklikken kom je op de startpagina van de provinciale website terecht.

Hoewel het hier ‘slechts’ twee kritieke kwetsbaarheden betrof, kan een aanvaller zichzelf hiermee toegang verschaffen tot andere systemen die op zichzelf geen kwetsbaarheden bevatten. Een voorbeeld hiervan is het achterhalen van een aantal gebruikersnamen en wachtwoorden voor de website “gemeentefinanciën”, waarmee vervolgens op deze website kon worden ingelogd. Hetzelfde geldt voor de verkeerskundiginformatiesysteem-website (VISweb).

Naast deze kritieke kwetsbaarheden zijn op andere websites die eigendom zijn van de provincie twee kwetsbaarheden aangetroffen die *van hetzelfde type* zijn als de hiervoor beschreven kwetsbaarheden en twee die van *hoog* risico zijn. Deze zijn tijdens het onderzoek niet geëxploiteerd, maar wel gemeld bij de provincie. Ook hier heeft de provincie in elk geval voor de twee kritieke gevallen actie ondernomen (websites uitgeschakeld, die zoals de provincie aangaf ook “verweesde” websites betroffen).

[15] De website bevatte een zogenaamde ‘SQL-injectie’-kwetsbaarheid in het loginscherm.
[16] De website bevatte een beheerinterface die niet was afgeschermd voor buitenstaanders.
[17] De DMZ is een gescheiden deel binnen een netwerk, bedoeld om bij compromitatie van systemen binnen dat netwerk de aanval tot dat gedeelte van het netwerk te beperken. In een DMZ bevinden zich meestal webservers en hieraan ondersteunende systemen.

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. Uitzonderingen zijn standaard enterprise producten zoals Microsoft webmail, de thuiswerkplekken en bijvoorbeeld het platform voor bestandsuitwisseling. Vanuit de provincie is aangegeven dat deze waarnemingen kloppen, maar de invulformulieren oude, niet meer in gebruik zijnde formulieren betreffen die voor een reguliere bezoeker van de provinciale website niet beschikbaar zijn. Ten tijde van het onderzoek waren deze echter nog wel voor een reguliere bezoeker beschikbaar, zij het via een alternatieve route naar de provinciale website. Vanuit de ambtelijke organisatie is aangegeven dat ze de kans gering achten dat hier misbruik van zou worden gemaakt. Iemand zou dit formulier via internet moeten vinden, vervolgens bewust moeten invullen en verzenden dit zou op hetzelfde moment moeten worden afgevangen door een kwaadwillende die kennis heeft van het bestaan van dit 'uitgefaseerde' formulier, zo wordt gesteld.

De externe IT-infrastructuur van de Innovatoren (pand van de provincie Limburg) is ook onderzocht, zij het terughoudend. Het beheer van deze infrastructuur ligt namelijk niet bij de provincie. Het pand is echter wel van de provincie. Een opvallende bevinding daarbij was dat een beheerinterface voor het fysieke alarmsysteem gekoppeld is aan internet. De logingegevens zijn de fabrieksinstellingen en eenvoudig op te zoeken bij de leverancier.

Interne test/toegankelijkheid

De interne beveiligingstest is uitgevoerd vanaf een kantoor met twee werkplekken in het medewerkersgedeelte van het gouvernement. Deze was door de provincie voor het onderzoek ter beschikking gesteld. Het kantoor gaf toegang tot het netwerk en de aanwezige werkstations/thinclients. Het eerste deel van de interne test is uitgevoerd met meegebrachte systemen en zonder domeinaccount (geen inloggegevens; blackbox), voor het tweede deel (greybox) is gebruik gemaakt van een testaccount (inloggegevens) dat voor dit onderzoek door de provincie ter beschikking was gesteld.

Tijdens de interne test op het interne netwerk van de provincie zijn 19 bevindingen gedaan. Hiervan heeft het gespecialiseerde bureau er zes als kritiek geclassificeerd. Van de overige bevindingen hebben er zes een hoog, drie een gemiddeld en twee een laag risico en zijn er twee informatieve bevindingen.

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.
Het verkrijgen van deze privileges kon via verschillende methoden worden bereikt. Zo zijn systemen die niet voorzien waren van recente beveiligingsupdates (patches), overgenomen

door vrij verkrijgbare exploits[18] uit te voeren.[19] Tevens zijn de logingegevens van een account met beheerderprivileges aangetroffen in een bestand dat voor iedere medewerker inzichtelijk is.[20] Doordat de harddisks van de werkstations/thinclients bij de provincie niet versleuteld zijn, kon het beheerderwachtwoord hiervan verkregen worden door zo'n werkstation te starten van een extern medium, in dit geval een USB-stick. Omdat werkstations onderling met hetzelfde beheerderwachtwoord toegankelijk zijn, kon vervolgens op een groot aantal systemen meegekeken worden en wachtwoorden achterhaald worden.

Bij een aantal systemen kunnen wachtwoordhashes[21] 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. Het wachtwoord hoeft niet aan complexiteitseisen te voldoen, anders dan de minimale lengte van zes karakters, wel dient elke 45 dagen een nieuw wachtwoord te worden gekozen en mag deze niet gelijk zijn aan één van de twaalf laatst gebruikte wachtwoorden. In het document *Tips en richtlijnen voor informatieveilig handelen* wordt daarentegen wel meegegeven om voor wachtwoorden karakters te gebruiken die zoveel mogelijk willekeurig zijn, minimaal acht tekens lang zijn, een combinatie van kleine letters, hoofdletters, leestekens en cijfers zijn en geen persoonlijke informatie bevatten zoals namen en data de gemakkelijk te raden zijn.
Ook blijken kritieke systemen toegankelijk zonder wachtwoord, met een zwak wachtwoord ofwel hebben een default ingesteld wachtwoord. Een daarvan is een server met zowel lees- als schrijfrechten en virtuele disks. Een kwaadwillende zou hierop malware kunnen plaatsen.

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. Dit doordat de genoemde verkeersstromen niet voldoende beperkt zijn. Hierdoor wordt het aanvalsoppervlak voor een kwaadwillende groot. Kwetsbare systemen zijn benaderbaar op netwerkniveau, en het niet tijdig bijwerken van die systemen kan leiden tot de gevolgen zoals die hierboven beschreven zijn.

[18] In deze context is een exploit een voor dit doel ontwikkeld programma of script waarmee een specifieke kwetsbaarheid misbruikt kan worden. Het type misbruik is afhankelijk van het type kwetsbaarheid.
[19] Er zijn een groot aantal systemen en applicaties aangetroffen die niet meer ondersteund worden door de leverancier en/of die verouderd waren (beschikbare beveiligingsupdates bleken niet te zijn toegepast). Deze bevatten vaak bekende en onbekende kwetsbaarheden die in veel gevallen misbruikt kunnen worden om ongeautoriseerde toegang te verkrijgen. Een lijst hiervan is tijdens het onderzoek aan de provincie overhandigd. Deze lijst betreft een momentopname en is naar alle waarschijnlijkheid niet volledig.
[20] Scripts en bestanden bevatten gebruikersnamen en wachtwoorden van onder andere accounts met hoge privileges.
[21] Hash: de versleutelde versie van een wachtwoord zodat deze veiliger kan worden opgeslagen.

Wifi/draadloze netwerken

Het testen van de beveiliging van de draadloze netwerken van de provincie maakte deel uit van de interne beveiligingstest. Het is daarbij 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.

4.2.2 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 de website geblokkeerd. Hoe ging dit in zijn werk?: De phishingmails werden tegelijk verstuurd. De mailservers van de provincie reageerden daar goed op. Omdat er erg veel dezelfde mails binnenkwamen, stuurde de server een deel ervan terug naar de server van de verzender. Vervolgens probeerde die weer de teruggekomen mails te versturen en zo ging het een aantal keer op en neer. Hierdoor kwamen de mails in batches bij de provincie binnen. In de loop van de ochtend, zo is aangegeven, kreeg de helpdesk van de provincie telefoontjes van ongeveer tien mensen die de helpdesk informeerden over de phishingmail. De helpdesk is in deze gevallen het coördinatiepunt. De helpdesk heeft vervolgens, conform procedure, de teamleider van de beheerders ingelicht dat er iets gebeurde dat niet in orde leek. Gezamenlijk is in de avond besloten om de gangbare procedure te volgen. Op het einde van de volgende ochtend is er dan ook een bericht op intranet verschenen over de phishingmail en is de toegang vanuit het provinciaal netwerk tot de phishingsite geblokkeerd. Deze blokkade werkt echter, zo is aangegeven, wel alleen voor de medewerkers die ingelogd zijn op het provincienetwerk en alleen op de browser die daarbinnen wordt gebruikt.

Ook zijn er twee spear phishingaanvallen uitgevoerd, waarbij geselecteerde emailadressen een met malware geïnfecteerde bijlage kregen toegestuurd. De eerste spear phishingaanval via email is niet geslaagd, omdat documenten met macro's die als bijlage werden meegestuurd, correct werden geblokkeerd door de mailserver. De aanval 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 de 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. De rekenkamer constateert dat in het document *Tips en richtlijnen voor informatieveilig handelen* bij 'fysieke toegang' bijvoorbeeld niet is opgenomen dat je geen onbekenden mag laten 'meelopen' naar beveiligde delen van het gouvernement en je waakzaam moet zijn op onbekenden in het beveiligde deel.

4.3 Getroffen maatregelen

Zoals reeds eerder vermeld, heeft de provincie eind november 2017 een rapportage van de rekenkamer ontvangen, waarin niet alleen alle bevindingen van dit deel van het onderzoek zijn beschreven, maar ook de daarbij geformuleerde aanbevelingen.
De rekenkamer constateert dat in haar onderzoek op een aantal punten vergelijkbare bevindingen zijn gedaan als twee jaar daarvoor bij de penetratietesten die destijds in opdracht van de provincie zijn uitgevoerd. 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 worden onveilig opgeslagen. Gevraagd naar redenen voor het aantreffen van vergelijkbare 'problemen'/bevindingen, is vanuit de ambtelijke organisatie aangegeven dat er indertijd risico-afwegingen zijn gemaakt en als het risco laag werd ingeschat is er niets mee gedaan. Maar evengoed hadden deze zaken gewoon sneller opgelost moeten worden, zo wordt aangegeven. De directie heeft nu ook opgeroepen om de quick-wins op te pakken, ook al worden de risico's van deze kwetsbaarheden laag ingeschat.

Na ontvangst van de rapportage 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. Als dat gebeurt, ontstaat een operationeel probleem dat beheerders moeilijk op kunnen pakken, zo wordt gesteld. Met betrekking tot patchmanagement speelt, zo wordt vervolgd, dus vooral de vraag hoe ver je achter mag lopen om zaken zo min mogelijk te ontregelen; wat is acceptabel? In het uitvoeringsplan was ook een maatregel opgenomen die het draaien van updates betreft: maatregel 19 Besturingssoftware. Zoals reeds eerder vermeld is sinds begin 2018 een hulpmiddel operationeel op basis waarvan gericht updates kunnen worden doorgevoerd. Ook zal op de langere termijn lifecyclemanagement stringenter worden uitgevoerd (om uitgefaseerde websites en applicaties uit de lucht te halen), zo is aangegeven.
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, zoals reeds eerder opgemerkt, aangegeven dat dit voor de scheiding tussen het gebruikers- en het beheerdersegment het eerste kwartaal van 2018 zal worden ingevoerd. In het uitvoeringsplan was ook een maatregel opgenomen die filtering betreft: maatregel 17 Netwerksegmenten.
Met betrekking tot netwerkaccesscontrol, heeft de provincie, zoals ook reeds eerder opgemerkt, begin 2018 'twee-factor authenticatie' voor extern inloggen op intranet ingevoerd en zal het autorisatieproces worden aangepast waardoor medewerkers alleen

toegang krijgen tot de systemen en ‘schijven’ die voor hun werkzaamheden noodzakelijk zijn. Mogelijk wordt de twee-factor authenticatie ook ingevoerd voor inloggen als je werkt op het gouvernement, maar, zo wordt aangegeven, daarvoor zijn er ook al de poortjes die mogelijk ook nog verhoogd worden. Tevens is, zoals ook reeds opgemerkt, besloten om het wachtwoordbeleid aan te passen. Sinds begin 2018 dienen wachtwoorden te bestaan uit minimaal tien karakters met verschil in tekens en hoofdlettergebruik. Vanwege deze wijziging dienen de wachtwoorden om het halfjaar te worden gewijzigd. In het uitvoeringsplan was ook een maatregel opgenomen die deze onderwerpen betreft: maatregel 3 Authenticatie en autorisatie.
Ook zal, zoals reeds genoemd, het bewustwordingsprogramma worden geactualiseerd en is de provincie voornemens een nieuwe bewustwordingscampagne te starten (maatregel 5 uit het uitvoeringsplan).

5. Provinciale Staten en informatieveiligheid

In dit hoofdstuk geeft de rekenkamer inzicht in de rollen van PS bij informatiebeveiliging en de informatie aan PS over informatieveiligheid in met name de periode eind 2013 tot en met begin 2018.

5.1 Rollen PS

PS hebben tot nu toe geen kaderstellende rol gehad bij het informatie- en informatiebeveiligingsbeleid. Of PS worden betrokken bij informatiebeveiligingsbeleid is een politieke afweging, zo is vanuit de ambtelijke organisatie aangegeven. De verantwoordelijke gedeputeerde ziet het onderwerp primair als bedrijfsvoering, zo wordt daarbij gesteld, maar hecht aan een proactieve communicatie van GS naar PS over het onderwerp informatiebeveiliging. Tot nu hadden PS op het gebied van informatie(beveiliging), zo wordt gesteld, alleen een controlerende rol: zijn de kaders en normen duidelijk en blijven GS binnen de kaders?
PS zijn in lijn daarmee in 2011 en 2016 geïnformeerd over de kaders van het SIBL. De kaders hiervoor zijn door GS ter kennisname aan PS verstuurd. Het informatiebeveiligingsbeleid uit 2014 en een jaar later het uitvoeringsplan zijn door GS vastgesteld. Deze documenten hebben PS niet ontvangen. PS hebben ook niet om deze documenten gevraagd. Op de momenten dat PS om informatie vroegen over het vigerende beleid en de uitvoering, zijn zij geïnformeerd middels een mededeling portefeuillehouder.

PS kennen elk jaar (via de begroting) middelen toe voor de uitvoering van het IT-beleid (budgetrecht). Het is daarnaast de taak van PS om het door GS gevoerde bestuur te controleren en eventueel bij te sturen met behulp van de kaders. PS zijn via de P&C-cylcus en in 2017 via een mededeling portefeuillehouder geïnformeerd over de uitvoering van het informatie(beveiligings)beleid (zie paragraaf 5.2).

Systemen van PS en fractiemedewerkers maken deel uit van het applicatielandschap van de provincie. Maar de griffie is bijvoorbeeld wel verantwoordelijk voor het stateninformatiesysteem iBabs. Daarbij is gekozen voor een SAAS-oplossing (software as a service). Bij aanschaf is conform de beoogde werkwijze, onder andere op het gebied van informatieveiligheid, begeleiding geweest vanuit O&I. De eigenaar van de onderliggende software is verantwoordelijk voor het systeem. Omdat het systeem onderdeel is van het applicatielandschap, blijft informatieveiligheid een aandachtspunt van de ISO.

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 kennisname integraal aangeboden aan PS. Eind

september 2016 zijn PS geïnformeerd over de evaluatie van dit SIBL. Zij hebben hiervoor van GS de gehele evaluatie ontvangen. Bij dit informatiemoment is ook het nieuwe SIBL 2016-2019 meegezonden. Al de genoemde stukken zijn ter kennisname aangeboden aan PS.
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. De rekenkamer constateert dat PS via de informatie die daarin is opgenomen, in zeer algemene zin zijn geïnformeerd.

In 2014 is het informatiebeveiligingsbeleid en in 2015 is het uitvoeringsplan door GS vastgesteld. PS hebben dit beleidskader en uitvoeringsplan niet ontvangen. Ze zijn via P&C-documenten geïnformeerd over de ontwikkeling en vaststelling daarvan. Begin 2017 zijn PS 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. Hiertoe is door GS aan PS een mededeling portefeuillehouder verstrekt. Dit gebeurde naar aanleiding van rapportages in het routine-overleg (RO) Bedrijfsvoering over enkele informatiebeveiligingsincidenten.

Begrotingen, jaarstukken, vragen
In de begrotingen en jaarstukken wordt als informatiemanagement/ICT aan de orde is vooral gesproken over de algemene vorderingen van het integralere SIBL. Over informatiebeveiliging in het bijzonder is in de jaarstukken en begrotingen weinig informatie opgenomen. In de gevallen dat wordt ingegaan op informatiebeveiliging zijn veelal opmerkingen opgenomen in de trant van dát de provincie werkte aan een uitvoeringskader informatiebeveiliging of dát er binnen de provincie veel aandacht is voor informatiebeveiliging. Zo zijn PS in de begroting 2018 geïnformeerd over het gegeven dat er een nieuw informatiebeveiligingsbeleid in de maak is. Meer inhoudelijk wordt er over de beleidsvoornemens in het algemeen niet uitgeweid.

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, zo is vanuit de organisatie aangegeven. De aandacht van PS leek incidentgestuurd te zijn. Zo zijn er vanuit PS voorjaar 2017 naar aanleiding van de wereldwijde cyberaanvallen vragen gesteld over hoe een en ander bij de provincie geregeld is. Mede daardoor kan informatiebeveiliging inmiddels in meer algemene zin rekenen op een verhoogde aandacht, ook vanuit PS, zo wordt gesteld. Verder wordt gesteld 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. Verschillende scenario's zouden aan GS en PS kunnen worden voorgelegd, zodat zij kunnen aangeven hoe zij staan in de afweging tussen niveau van beveiliging en kosten (inclusief

gebruikersgemak/afname flexibiliteit door barrières) daarvan. Tot nu toe werd de afweging impliciet gemaakt.
Najaar 2017 zijn de restrisico's bepaald, via de eerder genoemde risicoanalyse. PS zouden uitgedaagd moeten worden om mee te praten, over hun rol en de eerder genoemde afweging en daarmee samenhangende risicotolerantie want daarvoor is nu het moment, zo is vanuit de ambtelijke organisatie gesteld.

Onderstaand wordt nader ingegaan op de documenten waarin PS geïnformeerd zijn over informatieveiligheid of beleid dat informatieveiligheid omvat. De informatie wordt chronologisch weergeven. Bij de beschrijving van de aangeboden informatie volgt als eerst een beschrijving van de voorloper van het vigerende informatiebeleid. Het huidige kader kwam daar namelijk uit voort. Omdat het vigerende informatiebeveiligingsbeleid in 2014 is vastgesteld, behandelen we de informatievoorziening aan PS vanaf eind 2013.

De voorloper van het vigerende SIBL: SIBL 2011-2015 en informatiestatuut (febr. 2011 – dec. 2011)

In 2011 zijn PS middels meerdere mededelingen portefeuillehouder geïnformeerd over de stand van zaken van de ontwikkeling van het strategisch informatiebeleid en het informatiestatuut (onder andere in PS 23 mei 2011, de Ad Hoc Commissie 24 juni 2011, de Statencommissie Economie en Bestuur op 23 september 2011 en in november 2011).
Via een informerende brief zijn PS op 22 december 2011 op de hoogte gesteld van het feit dat GS het SIBL 2011-2015 hadden vastgesteld. Bij deze brief is het *Strategisch Informatiebeleid (SIBL) Een toekomstvisie E-Provincie Limburg (2011-2015)* gevoegd.

In 2015/2016 is dit kader geëvalueerd. Het nieuwe SIBL komt voort uit de evaluatie en het oude beleidskader (zie hieronder).

Begroting 2014 (november 2013)

In de verplichte bedrijfsvoeringsparagraaf van de begroting 2014 wordt vermeld "Het strategisch informatiebeleid (SIBL) is eind 2011 vastgesteld en geeft de komende jaren richting aan de veranderingen in de informatievoorziening. 2013 heeft in het teken gestaan van de invoering ervan. In 2014 wordt verder invulling gegeven aan onderstaande aspecten, waarbij het cluster Organisatie en Informatie[22] zich nadrukkelijk zal richten op het verbeteren en optimaliseren van de bedrijfsprocessen van de provinciale organisatie."
Voorts wordt aangegeven dat een deel van de projecten uit het projectenportfolio ook in 2014 gecontinueerd worden: "Daarbij moet onder meer worden gedacht aan de randvoorwaardelijke projecten zoals: Implementatie SIBL, informatiebeveiliging, het werken onder architectuur, de uit wettelijke taken voortvloeiende projecten ProGideon en de implementatie van basisregistraties."
Tot slot wordt ingegaan op het up to date maken en houden van de technische infrastructuur. "In dat kader zijn in 2013 enkele grote infrastructurele projecten gestart (o.a. vervanging netwerk, werkplek in beweging, het vervangen van de centrale storage omgeving) die ook in 2014 een vervolg zullen krijgen."

Jaarstukken 2013 (mei 2014)

In de jaarstukken 2013 wordt onder de programmalijn bedrijfsvoering bij de verschillen tussen de begroting en de realisatie aangegeven dat ter uitvoering van de projectenportfolio

[22] In de begroting wordt per abuis gesproken van 'Informatievoorziening' in plaats van 'Informatie'.

2013-2015 een bedrag van € 0,3 miljoen is overgeheveld naar 2015.
In de paragraaf over het weerstandsvermogen wordt gemeld: “In 2013 is het Informatiebeveiligingsbeleid herijkt en zal in 2014 worden uitgewerkt”.

Onder de verplichte paragraaf Bedrijfsvoering wordt explicieter ingegaan op het informatiebeveiligingsbeleid: “Het Informatiebeveiligingsbeleid van de provincie dateert van 2008 en is gedateerd. In het laatste kwartaal van 2013 is gestart met het actualiseren van het Informatiebeveiligingsbeleid, dat naar verwachting in het eerste kwartaal van 2014 ter besluitvorming aan GS zal worden aangeboden. Interprovinciaal is er veel aandacht voor Informatiebeveiliging. De provincie is hier nauw bij betrokken en conformeert zich aan de landelijke en interprovinciale initiatieven.”

Accountantsverslag 2013 (mei 2014)

In het verslag van de accountant *Provincie Limburg Uitkomsten controle en overige informatie 2013* is over informatieveiligheid geen informatie opgenomen.

Begroting 2015 (november 2014)

In de programmabegroting 2015 wordt onder programmalijn 4.3 Bedrijfsvoering gesteld dat in 2015 het strategisch informatiebeleid wordt geactualiseerd en verder ingevuld. Daarbij, zo wordt opgemerkt, zal de nadruk liggen op het verbeteren en optimaliseren van de bedrijfsprocessen van de provinciale organisatie. Verder zal een deel van de ICT-projecten uit de projectenportfolio gecontinueerd worden. En de huisvesting is erop gericht om een werkklimaat te creëren waarbij plaats- en tijdsonafhankelijker werken wordt gerealiseerd.
In paragraaf 2 Weerstandsvermogen en risicobeheersing wordt gemeld dat één van de activiteiten die afgelopen jaren is ondernomen op het gebied van risicopreventie en -signalering om het bewustzijn binnen de organisatie te stimuleren, is dat in 2013 het informatiebeveiligingsbeleid is herijkt en in 2014 verder is uitgewerkt. Verder zijn onder andere ook conform de uitgangspunten van *Toekomstvast Limburg* in 2013 afspraken gemaakt over taken, bevoegdheden en verantwoordelijkheden van control. Om tot een meer centrale regie te komen op de verschillende initiatieven op het gebied van risicomanagement binnen de provinciale organisatie is eind 2012 gestart met het opstellen van een concernbreed control-raamwerk dat in 2014 is vastgesteld. Dit raamwerk geeft, zo wordt gesteld, een duidelijk kader, is sturingskompas voor de ambtelijke organisatie en moet leiden tot een verbeterd risicobewustzijn binnen de organisatie en een integraal periodiek inzicht in risicobeheersing. Het leidt, zo wordt opgemerkt, tot een meer gestandaardiseerde wijze van het inbedden van risicomanagement in de organisatie, werkprocessen en rapportages. Hiermee wordt invulling gegeven aan het advies van de accountant om risicomanagement verder te verbeteren.
In paragraaf 5 Bedrijfsvoering staat dat bedrijfsvoering erop gericht is om de realisatie van de beleidsdoelstellingen zoals opgenomen in het programmaplan te sturen, beheersen en ondersteunen. En dat het onder meer zaken bevat als informatie(voorziening), communicatie, planning en control en integriteit. Onder informatiemanagement (5.2) worden vergelijkbare zaken genoemd als bij programmalijn 4.3 en paragraaf 2, zoals hiervoor beschreven (strategisch informatiebeleid en informatiebeveiligingsbeleid). Wel staat hier dat in 2015 het in 2014 vastgestelde informatiebeveiligingsbeleid wordt geïmplementeerd in de vorm van het inventariseren, prioriteren en implementeren van uitvoeringsmaatregelen.

Jaarstukken 2014 (mei 2015)

In de jaarstukken 2014 wordt conform de begroting 2015 in paragraaf (5.)2 Weerstandsvermogen en risicobeheersing als één van de activiteiten die afgelopen jaren zijn ondernomen genoemd het in 2013 herijkte informatiebeveiligingsbeleid dat in 2014 verder is uitgewerkt. In paragraaf (5.)5 Bedrijfsvoering staat onder (5.5.2) informatiemanagement: Strategisch Informatiebeleid en Projectenportfolio, conform de begroting 2015, dat in 2014 het Informatiebeveiligingsbeleid van de provincie is geactualiseerd en door GS is vastgesteld. In aanvulling daarop staat, in lijn met de jaarstukken 2013, dat er interprovinciaal veel aandacht is voor informatiebeveiliging, dat de provincie hier nauw bij betrokken is en zich conformeert aan de landelijke en interprovinciale initiatieven. Ook wordt specifieker dan in de begroting 2015 opgemerkt dat dit beleid in 2015 een vervolg krijgt in de vorm van een uitvoeringsplan, waarin concrete maatregelen worden opgenomen teneinde de informatieveiligheid van de provincie te waarborgen. De rekenkamer merkt hierbij op dat er niet op het strategisch informatiebeleid wordt ingegaan (maar ook niet vreemd want dat zou ook pas in 2015 worden geactualiseerd).

Accountantsverslag 2014 (mei 2015)

In het accountantsverslag van 2014 zijn geen opmerkingen opgenomen over informatiebeveiliging.

I-Kompas (augustus 2015)

Het I-Kompas (document Werkwijze vraaggerichte informatievoorziening) is, om reden dat het een intern gericht document is, niet aan PS aangeboden.

Begroting 2016 (november 2015)

In de begroting 2016 wordt bij het begrotingsprogramma 4.2 Bedrijfsvoering onder het kopje bedrijfsvoering gesteld: “Wij bieden flexibele en betrouwbare concernvoorzieningen aan collega’s en het bestuur. We leveren up-to-date managementinformatie, faciliteren diverse activiteiten en zorgen ervoor dat de informatievoorziening en het informatiebeheer zo zijn ingericht dat het zo goed mogelijk bijdraagt aan onze doelstellingen.”
In paragraaf 2 Weerstandsvermogen en risicobeheersing wordt hetzelfde vermeld als in de jaarstukken 2014 en begroting 2015 alleen wordt nu gesteld dat het informatiebeveiligingsbeleid in 2014 is vastgesteld.
In paragraaf 5 Bedrijfsvoering staat onder (5.2) informatiemanagement: Strategisch Informatiebeleid en Projectenportfolio, dienstverlening is leidend. Daarna wordt opgemerkt dat in 2015 het strategisch Informatiebeleid is geactualiseerd waarmee de kaders voor de ontwikkeling van de informatievoorziening voor de komende jaren vastgelegd zijn.
Ook wordt in het kader van dienstverlening gesteld dat de provincie betrouwbaar, veilig en toegankelijk moet zijn en dat is waar het om draait. “Dit vraagt om een professionele, zakelijke en gestroomlijnde organisatie, die klantvriendelijk gericht is op de vraag van haar klanten. ICT-beleid en overige informatiemiddelen zijn hieraan ondersteunend. De implementatie van dit plan moet goed geborgd worden in de organisatie en verbonden worden met (bestaande) systemen.” Ook in deze begroting wordt, evenals in de begroting 2015, aangegeven dat een deel van de projecten uit het I-projectenportfolio gecontinueerd zal worden. Tevens wordt opgemerkt dat de directie heeft besloten om niet tot een organisatiebrede uitrol van de iPads over te gaan, maar te investeren in een nieuw werkplekconcept waarmee in 2015 gestart is en in 2016 verder voorbereid zal

worden en tijd- en plaatsonafhankelijk werken mogelijk dient te maken. Gesteld wordt dat een belangrijk aspect daarbij is de beveiliging van provinciale gegevens. Ook wordt in deze paragraaf genoemd de implementatie van het informatiebeveiligingsbeleid in de vorm van het implementeren van uitvoeringsmaatregelen.

Jaarstukken 2015 (mei 2016)

In de jaarstukken 2015 wordt onder programmalijn 4.3 Bedrijfsvoering gesteld dat in 2015 het strategisch informatiebeleid 2011-2015 is geactualiseerd en naar verwachting in het voorjaar 2016 vastgesteld zal worden. Hoewel in de jaarstukken bij dit onderdeel 'Facilitair/ICT/Huisvesting' wordt gesteld dat de voor 2015 beoogde resultaten zijn gerealiseerd, wordt op een aantal beoogde resultaten niet ingegaan zodat het voor een lezer onduidelijk blijft of deze ook daadwerkelijk zijn gerealiseerd. Twee voorbeelden daarvan zijn: er wordt niet ingegaan op de verdere invulling van het informatiebeleid in 2015, waar in de begroting 2015/bij beoogde resultaten wel over wordt gesproken en er wordt niet ingegaan op de realisatie van het plaats- en tijdsonafhankelijker werken.
In paragraaf 2 Weerstandsvermogen en risicobeheersing wordt hetzelfde vermeld als in de begroting 2016 (informatiebeveiligingsbeleid in 2014 vastgesteld) en daarmee in lijn met gemelde in de jaarstukken 2014 en begroting 2015.
In paragraaf (5.)5 Bedrijfsvoering staat onder (5.5.2) Informatiemanagement dat in 2015 naast de reguliere beheertaken invulling is gegeven aan een groot aantal projecten die voortkomen uit het centraal gemanagede I-projectenportfolio van de provincie. Gesteld wordt dat de belangrijkste projecten en activiteiten worden genoemd. Vervolgens staat onder Strategisch Informatiebeleid en Projectenportfolio, in lijn met het gestelde in paragraaf 4.3 dat het strategisch informatiebeleid in 2015 is geactualiseerd en dat het begin 2016 zal worden vastgesteld door GS. Onder Uitvoeringsplan Informatiebeveiliging wordt gesteld dat het uitvoeringsplan informatiebeveiliging in 2015 is vastgesteld. "In dit plan zijn de belangrijkste maatregelen geïdentificeerd die de provincie dient te implementeren in het kader van de informatiebeveiliging van de provinciale organisatie. De prioritering van de maatregelen heeft plaatsgevonden op basis van risicoanalyses."

Managementletter 2015 (mei 2016)

In de managementletter van de accountant bij de jaarstukken 2015 zijn geen opmerkingen opgenomen over informatieveiligheid.

Evaluatie SIBL 2011-2015 en nieuwe SIBL 2016-2019 (september 2016)

Op 13 september 2016 sturen GS een informerende brief naar de Statencommissie Financiën, Economische Zaken en Bestuur (FEB). Hierin wordt aangegeven dat GS op basis van artikel 217a van de provinciewet een onderzoek hebben laten verrichten naar de wijze waarop het SIBL 2011-2015 is geïmplementeerd binnen de provinciale organisatie en welke vervolgstappen zijn gezet.
Het intern uitgevoerde onderzoek heeft in 2016 plaatsgevonden, zo wordt gemeld. De uitkomsten hiervan zijn middels het informerende stuk ter kennisname aangeboden aan PS. Tevens wordt het mede op basis van de resultaten van deze evaluatie opgestelde nieuwe SIBL 2016-2019 aan PS ter kennisname aangeboden.

Begroting 2017 (november 2016)

In de begroting 2017 wordt bij het begrotingsprogramma 4.2 Overhead (voorheen was dat onder andere Bedrijfsvoering) alleen inzicht gegeven in de financiën (Wat gaat het

kosten?). Voor 2017 is € 3,2 miljoen voor organisatie- en informatiemanagement begroot.
In paragraaf 2 Weerstandsvermogen en risicobeheersing wordt hetzelfde vermeld als in de jaarstukken 2015 en de begroting 2016 (informatiebeveiligingsbeleid in 2014 vastgesteld) en daarmee in lijn met gemelde in de jaarstukken 2014 en begroting 2015.
In paragraaf 5 Bedrijfsvoering staat dat één van de sleutelbegrippen betrouwbare informatievoorziening is. Onder (5.2) Informatiemanagement: Strategisch Informatiebeleid en Projectenportfolio staat dat in 2016 het geactualiseerde strategisch informatiebeleid van de provincie Limburg (SIBL 2016-2019) door GS is vastgesteld en daarmee de kaders voor de ontwikkeling van de informatievoorziening van de provincie voor de komende jaren vastgelegd zijn. Verder wordt gesteld dat in 2017 langs twee lijnen uitvoering wordt gegeven aan het SIBL 2016-2019: de lijn 'Interactie met de samenleving verbeteren' en de lijn 'Groeien naar een zakelijke en professionele provinciale organisatie'. Beide lijnen zijn vertaald in projecten, waarvan de belangrijkste voor het jaar 2017, zo wordt gesteld, in de begroting worden genoemd. Zo wordt voor de eerste lijn onder andere gemeld dat de website www.limburg.nl in 2017 wordt vervangen. Voor de tweede lijn wordt onder andere gemeld dat er een nieuwe informatievoorziening voor dossier- en archiefvorming zal worden aanbesteed en zal worden geïmplementeerd en in het kader van de geplande vervanging van provinciale werkplekken, implementatie van een nieuw werkplekconcept dat voor die medewerkers die daar functioneel behoefte aan hebben tijd- en plaatsonafhankelijk werken mogelijk maakt, rekening houdend met de beveiliging van provinciale gegevens. De projecten maken deel uit van het I-projectenportfolio. De rekenkamer merkt op dat niet wordt ingegaan op het in 2015 vastgestelde uitvoeringsplan informatiebeveiliging.

Mededeling portefeuillehouder (januari/maart 2017)

Op 3 januari 2017 stemmen GS in met een schriftelijke mededeling van de portefeuillehouder aan de Statencommissie FEB inzake Informatiebeveiliging. Op de agenda van deze statencommissie van 10 maart 2017 staat in de lijst met ingekomen stukken de schriftelijke mededeling met als voorgestelde wijze van afdoen 'voor kennisgeving aannemen'. Uit het vastgestelde verslag van de vergadering blijkt dat de lijst wordt vastgesteld en daarmee de voorgestelde wijze van afdoen.

In de mededeling wordt aangegeven dat naar aanleiding van de rapportages in het RO Bedrijfsvoering over enkele informatiebeveiligingsincidenten en op verzoek van de portefeuillehouder een toelichting wordt gegeven bij de belangrijkste activiteiten en gemaakte keuzes op het gebied van informatiebeveiliging. De mededeling portefeuillehouder bevat informatie over het informatiebeveiligingsbeleid van de provincie, 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.

In het SIBL 2016-2019 is informatiebeveiliging en cybersecurity één van de prioritaire thema's, zo wordt gesteld. Verder wordt vermeld dat in het Informatiebeveiligingsbeleid (GS 2014) een aantal uitgangspunten is benoemd die het kader vormen waarbinnen informatieveiligheid verder vormgegeven wordt. Eén van de uitgangspunten is dat de IBI wordt gevolgd. In 2018 zal het informatiebeveiligingsbeleid wederom worden geactualiseerd, zo wordt gesteld. Ook wordt vermeld dat in het kader van het informatiebeveiligingsbeleid door de jaren heen diverse maatregelen zijn getroffen om de risico's op verstoringen van de bedrijfsvoering tot een minimum te beperken. In 2015

is een uitvoeringsplan opgesteld omdat daarnaast behoefte was aan een planmatige implementatie van het kaderstellende beleid. In dit plan zijn 27 onderwerpen, maatregelen van soms technische en soms organisatorische aard, benoemd die nadere aandacht vragen in het kader van de informatiebeveiliging. Een aantal daarvan was bij de start van 2017 reeds afgerond, zo wordt gesteld. De belangrijkste maatregelen worden vermeld en daarbij wordt ook een inkijkje gegeven in de werkwijze rondom informatievoorziening.

Jaarstukken 2016 (april 2017)

In de jaarstukken 2016 wordt onder 4.2 Bedrijfsvoering voor wat betreft informatievoorziening en informatiebeheer, voor inhoudelijke informatie verwezen naar paragraaf 5.5.2.
In paragraaf 2 Weerstandsvermogen en risicobeheersing wordt hetzelfde vermeld als in de begroting 2017, jaarstukken 2015 en begroting 2016 (informatiebeveiligingsbeleid in 2014 vastgesteld) en daarmee in lijn met gemelde in de jaarstukken 2014 en begroting 2015.
In paragraaf 5 Bedrijfsvoering staat onder (5.5.2) Informatiemanagement, conform de begroting 2017, maar wat niet (expliciet) in de bij de jaarstukken behorende begroting 2016 als beoogde prestatie is genoemd, dat in 2016 het SIBL 2016-2019 door GS is vastgesteld. Ook hier wordt evenals in voorgaande P&C-documenten ingegaan op enkele belangrijke projecten uit het I-projectenportfolio. De rekenkamer merkt hierbij op dat door slechts een aantal projecten te noemen en in de opeenvolgende P&C-documenten niet altijd op dezelfde projecten wordt ingegaan niet altijd inzicht wordt verkregen in of de provincie bereikt heeft wat ze wilde bereiken. Zo is in 2016 voor digitalisering dossiervorming (DDI) een veranderplan opgesteld dat beschrijft op welke wijze de noodzakelijke veranderingen qua kennis, vaardigheden en gedrag kunnen worden bereikt. Maar wordt bijvoorbeeld niet teruggekomen op de in de begroting 2016 vermelde beoogde acties voor het nieuwe werkplekconcept. Ook wordt niet aangegeven/wordt niet duidelijk of de in de begroting 2016 genoemde beoogde implementatie van elektronisch aanvragen van subsidies is gerealiseerd (uit de begroting 2017 blijkt dat deze in 2017 zal worden afgerond). Wel wordt gemeld dat in 2016 invulling is gegeven aan het uitvoeringsplan informatiebeveiliging, dat tal van maatregelen bevat die erop gericht zijn om de risico's op het gebied van informatiebeveiliging te verkleinen. In de begroting 2016 werd het uitvoeringsplan niet expliciet genoemd maar werd gesproken van 'implementeren van uitvoeringsmaatregelen'. Eén van de maatregelen, zo wordt gemeld, betrof een concernbrede campagne gericht op het vergroten van de bewustwording bij de medewerkers. Daarnaast is onder andere gewerkt aan de voorbereiding van de verbetering van de autorisatie en authenticatieprocessen binnen de provincie. Ook is in 2016 gewerkt aan het onderhoud en up to date houden van de technische infrastructuur.

Managementletter 2016 (april 2017)

In de managementletter van de accountant bij de jaarstukken 2016 worden bij de evaluatie van de IT-omgeving substantiële bevindingen gedaan over cybersecurity. In het stuk is opgenomen: "Cyber is een onlosmakelijk onderdeel geworden van onze samenleving. Dagelijks werken we met digitale oplossingen, zowel privé als zakelijk. Door het gebruik van het internet, interne netwerken en bedrijfsapplicaties hebben ook organisaties, ongeacht hun omvang, te maken met aan cyber gerelateerde risico's, zoals cybercrime. Als cyberrisico's zich voordoen, kunnen deze een (significante) impact hebben op de financiële systemen, op uitspraken over de interne beheersing, en ook op de jaarrekeningcontrole.
Tijdens de pre-audit, op 14 november 2016, hebben wij een afvaardiging van de

directie verzocht inzicht te geven in de eigen inschatting van het risico dat de jaarrekening een materiële afwijking zou kunnen bevatten als gevolg van cyberrisico's in het betalingsverkeer, door het onttrekken van persoonsgegevens, vertrouwelijke gegevens of Intellectual Property, of door het verstoren van de bedrijfsvoering. Tijdens deze gesprekken heeft de afvaardiging van de directie aangegeven zich bewust te zijn van cyberrisico's en heeft zij voorbeelden gegeven van de manier waarop zij deze beheerst. Tegelijkertijd stellen wij vast dat een interne analyse van de risico's rond cybersecurity ontbreekt. Uw organisatie loopt hiermee het risico dat de interne beheersing kwetsbare plekken bevat die onopgemerkt blijven. Aangezien iedere organisatie waardevolle informatie heeft te verliezen of ernstige schade kan leiden als de IT-infrastructuur (tijdelijk) niet meer beschikbaar is, attenderen wij u op het belang van een cyberrisicoanalyse als vast onderdeel van het interne controlesysteem dat erop is gericht bedrijfsrisico's te onderkennen en het belang en de waarschijnlijkheid daarvan in te schatten”

Verzoek Provinciale Staten (juni 2017)

Naar aanleiding van een opmerking van de accountant bij de jaarstukken 2016 over het ontbreken van een risicoanalyse en daarop inhakend een aanbeveling vanuit de statenonderzoeksfunctie, vragen PS op 30 juni 2017 aan GS om risico’s en risicobeheersing rondom cybersecurity in beeld te brengen.

Begroting 2018 (november 2017)

In de begroting 2018 wordt in de paragraaf over weerstandsvermogen en risicobeheersing aangegeven dat in 2014 het informatiebeveiligingsbeleid is vastgesteld. Onder informatiemanagement wordt later in de paragraaf over bedrijfsvoering hier verder over gemeld: “Voor een organisatie die informatie als een strategisch bedrijfsmiddel ziet, is continue aandacht voor informatiebeveiliging onontbeerlijk. In 2018 zal een geactualiseerd informatiebeveiligingsbeleid door GS vastgesteld worden. Het huidige beleid dateert uit 2014 en is geoperationaliseerd middels een uitvoeringplan. Belangrijk onderdeel van zowel het oude als het nieuwe beleid vormt het inspringen op ontwikkelingen in de wereld van cybersecurity”.

Risicoanalyse cybersecurity (januari/februari 2018)

Via een statenmededeling van 23 januari 2018 worden PS geïnformeerd over de uitkomsten en aanbevelingen van de uitgevoerde risicoanalyse. Op 6 februari 2018 publiceerde L1 naar aanleiding daarvan een bericht met als kop “Provincie moet informatie beter beveiligen”.

5.3 Informatie op provinciale website

Naast de voornoemde documenten die aan PS zijn aangeboden en die te vinden zijn bij de vergaderstukken van PS en een pagina die ingaat op informatieveiligheid waarbij mensen worden verzocht vermeende ICT-kwetsbaarheden met de provincie te delen, met daarbij een link naar het document met het betreffende beleid (Beleid Responsible Disclosure Provincie Limburg), zijn er geen documenten over informatiebeveiliging/veiligheid aangetroffen op de provinciale website.

Bijlage 1 Geraadpleegde documenten

Centraal Informatiebeveilingsoverleg (IPO) (2010), *Interprovinciale Baseline Informatiebeveiliging 1.0*

Provincie Limburg (mei, juni, september, november 2011), *Mededeling portefeuillehouder Voortgang Strategisch Informatiebeleid*

Provincie Limburg (december 2011), *Strategisch Informatiebeleid Limburg 2011-2015: Een toekomstvaste (E-)Provincie Limburg (2011-2015)*

Provincie Limburg (december 2011), *Informatiestatuut, Inhoudelijke en procedurele afspraken voor een toekomstvaste informatievoorziening in Provincie Limburg (2011-2015)*

Provincie Limburg (december 2011), *Toekomen informerend stuk inzake het strategisch informatiebeleidsplan*

Ernst & Young (april 2014), *Provincie Limburg Uitkomsten controle en overige informatie 2013 Rapportage aan Provinciale Staten*

Provincie Limburg (juli 2014), *Informatiebeveiligingsbeleid Provincie Limburg*

Provincie Limburg (juli 2014), *Openbare besluitenlijst van de vergadering van Gedeputeerde Staten van 1 juli 2014*

Centraal Informatiebeveilingsoverleg (IPO) (september 2014), *Convenant Interprovinciale Regulering Informatieveiligheid*

Centraal Informatiebeveilingsoverleg (IPO) (maart 2015[23]), *Monitoringtool baseline informatiebeveiliging 2014, Rapportage interprovinciale beeld implementatie baseline informatiebeveiliging eind 2014*

Deloitte (mei 2015), *Controleverklaring jaarrekening 2014*

FOX -IT BV (2015), *Passive Audit en penetratietest Provincie Limburg (vertrouwelijk)*

Provincie Limburg (augustus 2015), *Werkwijze vraaggerichte informatievoorzieining provincie Limburg (I-Kompas)*

Provincie Limburg (december 2015), *Uitvoeringsplan Informatiebeveiliging Provincie Limburg 2015-2016*

Provincie Limburg (januari 2016), *Programma Bewustwording Informatieveiligheid 2016-2017*

[23] In het document zelf staat per abuis maart 2014.

Provincie Limburg (2016), *Tips en richtlijnen informatieveilig handelen*

Centraal Informatiebeveilingsoverleg (IPO) (februari 2016), *Interprovinciale Baseline Informatiebeveiliging 2.0*

Provincie Limburg (april 2016), *Evaluatie Strategisch Informatiebeleid 2016-2019*

Deloitte (april 2016), *Accountantsverslag 2015 provincie Limburg*

Provincie Limburg (september 2016), *Openbare besluitenlijst van de vergadering van Gedeputeerde Staten van 13 september 2016*

Provincie Limburg (september 2016), *Strategisch Informatiebeleid Limburg 2016-2019: Dienstverlening is leidend*

Provincie Limburg (januari 2017), *Mededeling portefeuillehouder inzake Informatiebeveiliging Provincie Limburg*

Provincie Limburg (z.d.), *Overzicht CIBO-monitor informatiebeveiliging 2016 (concept)*

Deloitte (mei 2017), *Controleverklaring jaarrekening 2016*

Provincie Limburg (mei 2017), *Analyse Jaarstukken 2016 provincie Limburg*

Centraal Informatiebeveilingsoverleg (IPO) (juni 2017), *Monitoringtool baseline informatiebeveiliging 2016, Rapportage interprovinciale beeld implementatie baseline informatiebeveiliging eind 2016*

Hoffman Cybersecurity (november 2017), *Rapportage Penetratietest Provincie Limburg* (ten behoeve van onderzoek Zuidelijke Rekenkamer)

AON (december 2017), *Cyber Impact Analyse Provincie Limburg* (vertrouwelijk)

Provincie Limburg (februari 2018), *Mededeling portefeuillehouder inzake risico analyse cybersecurity*

Provincie Limburg (2013-2017), *Begrotingen* 2014, 2015, 2016, 2017, 2018 en *Jaarstukken* 2013, 2014, 2015, 2016

Provincie Limburg (2012-2018), *Vastgestelde verslagen en/of audioverslagen relevante bijeenkomsten PS*

Relevante documenten via intranet (citrix-omgeving) van de provincie en www.limburg.nl (geraadpleegd oktober 2017 en april 2018, zoals *Beleid Responsible Disclosure Provincie Limburg*)