# Informatieveiligheid provincie Noord-Brabant

Deel II: Rapport van bevindingen

ZUIDELIJKE REKENKAMER

ZUIDELIJKE
REKENKAMER

# Leeswijzer

De Zuidelijke Rekenkamer heeft in de periode juni 2017 – januari 2018 onderzoek verricht naar de informatiebeveiliging van de provincie Noord-Brabant.

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 Noord-Brabant haar informatiebeveiliging in opzet heeft ingericht. Onze bevindingen over de uitvoering van het beleid in de praktijk 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.

.

# 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 Noord-Brabant. 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 informatie-veiligheid 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 doen die bijdragen aan een verbetering van de informatieveiligheid van de provincie Noord-Brabant: 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'. In deze rapportage spreken we van 'integriteit' omdat deze term bij informatieveiligheid gebruikelijk is.

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 Noord-Brabant 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?

We beschrijven het *beleid* en de *organisatie* van de informatiebeveiliging/veiligheid in opzet en praktijk (vraag 1 en 3). Daarnaast rapporteren we 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).

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 september 2012 (bespreking startnotitie ICT-beleid in de commissie Economische Zaken en Bestuur) tot eind 2017.

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 en gesprekken met betrokkenen van 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 raken in algemene zin met name de volgende bevoegdheden van PS: budgetrecht en kaderstellende en controlerende rol. 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

In dit hoofdstuk geven we inzicht in hoe de provincie Noord-Brabant de informatiebeveiliging in opzet heeft ingericht (beoogde invulling).

## 2.1 Context: I(CT)-beleid

### Startnotitie ICT-beleid (2012)

Informatiebeveiliging maakt deel uit van het ICT-beleid van de provincie Noord-Brabant. In de zomer van 2012 stelde de provincie een startnotitie ICT-beleid op.[3] Deze werd opgesteld mede naar aanleiding van het in februari 2012 gepubliceerde rekenkamerrapport over het strategisch informatiebeleid van de provincie Noord-Brabant. Daarin werd onder andere aanbevolen een strategische (informatie)visie op te stellen. In september 2012 besprak de commissie Economische Zaken en Bestuur (EZB) de startnotitie en werd aan GS gevraagd een kadernota op te stellen.

### Kadernota ICT-beleid 2013-2015 (2013)

Op 22 maart 2013 stelden PS de *Kadernota ICT-beleid 2013-2015* vast (inclusief uitvoeringsplannen). De nota geeft de provinciale ICT-ambitie voor de periode 2013 tot en met 2015: eerst de basis op orde en dan (deze op orde houden en) actief volger van ICT-ontwikkelingen mits onderbouwd door een goede businesscase. Als speerpunten zijn benoemd: de technische basis op orde (via een routekaart) en digitaal werken. Ook geeft het de I-visie: “ex- en interne ontwikkelingen worden continu verkend en gewogen op hun waarde voor de informatievoorziening zodat de ICT aangesloten is op (toekomstige) taken en processen van de provinciale organisatie.” Daarnaast worden in de nota de belangrijkste sturingskaders gegeven voor architectuur, projecten, beheer ICT-voorzieningen en beveiliging. Ook worden de beoogde middelen, organisatiestructuur en besturing omschreven. De nota beperkt zich tot ICT-beleid in het volle besef, zo wordt gesteld, dat dit beleid deel uitmaakt van het grotere geheel van informatiebeleid en bedrijfsvoering. Daarbij wordt informatiebeleid gedefinieerd als toekomstige informatiebehoefte welke op jaarbasis wordt vastgelegd in de I-agenda (I-projectenportfolio).

Zoals voorgenomen zijn de kadernota en de uitvoering daarvan in 2014 tussentijds intern, en in 2015 extern geëvalueerd. Tijdens het op orde brengen van de basis was er beperkte aandacht voor een organisatiebrede informatiestrategie (I-visie), zo wordt in de eindevaluatie gesteld. En er is dringend behoefte aan kaders met een meer informatiestrategische insteek. GS geven aan ook na 2015 de koers van de kadernota vast te houden (het op orde houden van de basis). De kaders daaruit blijven geldig, maar zijn ook van toepassing op de informatie die met de ICT wordt beheerd.

### Informatievisie Samen, Slim en Innovatief (juni 2015)

In juni 2015 stelde de directie een I-visie vast die nog tactisch moest worden uitgewerkt: *Informatievisie Samen, Slim en Innovatief*. Het betreft, zo wordt daarin gesteld, een lange

[3] De rekenkamer constateert dat de naamgeving die de provincie voor dit document hanteert varieert. Op het document zelf wordt gesproken van *Startnotitie strategisch IT-beleid*, maar al snel spreekt de provincie steeds van *startnotitie ICT-beleid*. In lijn daarmee zullen we in dit rapport ook deze laatste benaming hanteren.

termijnvisie en -strategie op informatie en legt vast hoe de provincie met informatie(voorziening) omgaat. De visie, zo wordt aangegeven, is integraal onderdeel van het informatiebeleid en zal gebruikt worden om, waar nodig, het vigerende informatiebeleid bij te stellen of aan te vullen. De provincie wil van informatie een strategisch bedrijfsmiddel maken.
De missie luidt:

| Missie Informatie(voorziening) |
| --- |
| 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 zo laag mogelijke kosten om zo de provincie en (keten)partners optimaal te ondersteunen in het realiseren van de maatschappelijke opgaven. |

Er dient gestuurd te worden vanuit de maatschappelijke opgaven. Ook wordt gesteld dat je wat betreft informatie op de provincie moet kunnen vertrouwen en dat informatie afgewogen wordt beveiligd.
Het document is niet aan PS aangeboden.
De rekenkamer constateert dat het document op hoofdlijnen de uitgangspunten van de kadernota volgt, maar 'basis op orde (houden)' en de kaders voor informatiebeveiliging komen niet aan de orde; informatieveiligheid komt in het algemeen indirect aan de orde.

### Nota Digitale Duurzaamheid (eind 2015) en Visie en hoofdlijnen informatiebeleid (2016)

In 2016 geven GS aan dat het ICT-beleid is geactualiseerd en 'verbreed' naar informatie. De basis hiervoor vormde de voornoemde eindevaluatie van de kadernota en het in december 2014 gepubliceerde rekenkameronderzoek *Digitalisering en duurzame toegankelijkheid van informatie*. Hierin werd eveneens aanbevolen een visie op informatiebeleid en -beheer vast te stellen. In februari 2016 is de *nota Digitale Duurzaamheid* van eind 2015 en in juni 2016 de notitie *Visie en hoofdlijnen informatiebeleid* aan PS aangeboden. Het eigenaarschap van de informatie wordt gelegd bij de inhoudelijke beleidsprogramma's en niet bij de centrale ICT-eenheid. In deze documenten komt beveiliging niet expliciet aan de orde. Wel komen in de *nota Digitale Duurzaamheid* de elementen uit de I-visie uit 2015 terug, zij het op informatie gericht in plaats van op informatievoorziening. Ook deze nota volgt daarmee op hoofdlijnen de uitgangspunten uit de kadernota. In de notitie Visie en hoofdlijnen wordt ook gesteld dat de kaders uit de kadernota van toepassing blijven (de visie bevat geen beleidswijzigingen), zij het ook op informatie. De inhoud van de I-visie wordt in de notitie samenvattend gegeven. Daarbij wordt gesteld dat een en ander onder andere vraagt om "een informatievoorziening die niet meer kost dan nodig is en die modern, veilig, transparant en betrouwbaar is". De missie wordt echter niet meer expliciet genoemd. In de (statenmededeling over de) notitie Visie en hoofdlijnen wordt gesproken over een strategisch kader dat is afgeleid van de informatievisie.
De rekenkamer constateert dat de uitgangspunten uit de kadernota van toepassing blijven, maar met de Visie en hoofdlijnen informatiebeleid ook gelden voor informatie.

### Vigerend informatiebeleid

Het vigerende *informatiebeleid* staat beschreven in de *Kadernota ICT-beleid 2013-2015* in combinatie met de *nota Digitale Duurzaamheid* en de *Visie en hoofdlijnen informatiebeleid*. De kadernota is door PS vastgesteld, de andere twee documenten zijn voor kennisgeving aan PS aangeboden.

## 2.2 Informatiebeveiliging

### Kadernota ICT-beleid 2013-2015 (begin 2013)

Zoals eerder gemeld maakt informatiebeveiliging deel uit van het informatiebeleid.
In de kadernota wordt het belang van informatieveiligheid benadrukt en worden kaders voor informatiebeveiliging gegeven. Daarvoor worden drie relevante aspecten (zie onderstaand kader) van informatiebeveiliging benoemd.

| Relevante aspecten van informatiebeveiliging (Kadernota ICT-beleid 2013-2015) |
|---|
| Vertrouwelijkheid/confidentialiteit: de informatie is alleen toegankelijk voor degenen die hiertoe ook daadwerkelijk geautoriseerd zijn. |
| Integriteit: correctheid en volledigheid van de informatie en de informatieverwerking. |
| Beschikbaarheid: geautoriseerde gebruikers hebben op de juiste momenten toegang tot de informatie en de aanverwante bedrijfsmiddelen.[4] |

Het doel van informatiebeveiliging wordt omschreven:

| Doel informatiebeveiliging |
|---|
| Het naleven van de wetgeving op het gebied van informatiebeveiliging en de afspraken die daarvoor op landelijk en interprovinciaal niveau zijn gemaakt en daarbij steeds de afweging te maken tussen de (kans en) impact van risico's en de kosten van preventiemaatregelen ter voorkoming daarvan. |

De informatievoorziening dient daarmee afgewogen te worden beveiligd; er dient een beveiligingsniveau te worden gekozen dat passend is bij de risicoafweging. Het element 'afgewogen beveiliging' komt ook later in de I-visie uit 2015 en die uit 2016 naar voren.

Wetgeving die eisen stelt aan de beveiliging van de informatievoorziening is bijvoorbeeld de Wet bescherming persoonsgegevens (Wbp) en de Archiefwet. De afspraken over informatiebeveiliging betreffen NEN/ISO normen 27001 (proces; hoe stuur je), de Nederlandse Overheid Referentie Architectuur (NORA), de Provinciale Enterprise Referentie Architectuur (PETRA), de Interprovinciale Baseline Informatiebeveiliging (IBI) van het Centraal Informatiebeveiligingsoverleg (CIBO) van het Interprovinciaal Overleg (IPO) die de basisset van beveiligingsmaatregelen omvat (NEN/ISO 27002) en richtlijnen van het National Cyber Security Centre (NCSC) voor het ontwikkelen van webapplicaties. Vanuit de ambtelijke organisatie is aangegeven dat er sprake is van een passend beveiligingsniveau, als voldaan wordt aan de IBI.

Ook stelt de kadernota dat informatiebeveiliging een integraal onderdeel moet gaan uitmaken van de bedrijfsvoering. In alle onderdelen van de provincie dient bij het dagelijks handelen, bij elke ontwikkeling en elk project aandacht te zijn voor (nut en noodzaak van) informatiebeveiliging (I-projectenportfolio). Om dat te bereiken wil de provincie de verantwoordelijkheden in de lijn tot op medewerkersniveau uitzetten. Het belang van

[4] In de nota Digitale Duurzaamheid (december 2015) wordt beschikbaar gedefinieerd als: "overheidsinformatie is gegarandeerd op elk moment binnen een acceptabele tijd opvraagbaar voor iedereen die daar recht op heeft. De hiervoor benodigde beschikbaarheid van applicaties en netwerken zijn gegarandeerd". En betrouwbaar als: "de informatie mag na ontvangst of creatie niet beschadigd of ongeautoriseerd gewijzigd zijn, ook moet deze volledig zijn".

bewustwording en bijbehorend gedrag van medewerkers voor informatiebeveiliging wordt onderstreept. Gesteld wordt dat technische maatregelen geen resultaat hebben als het bewustzijn en gedrag van mensen achter blijft; deze zijn noodzakelijk bij het verhogen van de weerbaarheid van de provincie. Omdat 100% veiligheid niet bestaat, wil de provincie zorgdragen voor adequate inrichting van incidentbeheersing (onverwachte gebeurtenissen die de betrouwbaarheid van de informatievoorziening verstoren of in gevaar kunnen brengen). Door de beveiligingsmaatregelen te implementeren, de verantwoordelijkheden uit te zetten in de lijn en te leren van bevindingen uit evaluaties/audits en incidenten ontstaat, zo wordt gesteld een basisbeveiligingsniveau en de mogelijkheid om verbeteringen aan te brengen. Een basisbeveiligingsniveau/baseline heeft als doel om met een vastgestelde set van maatregelen 70-80% van alle informatie binnen de organisatie adequaat te beveiligen.

### Externe ontwikkeling: landelijke taskforce (februari 2013)

Naar aanleiding van een aantal landelijke informatiebeveiligingslekken stelde de Minister van Binnenlandse Zaken en Koninkrijkrelaties (BZK) vervolgens 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).

| Interprovinciaal beleid en landelijke aandacht voor informatieveiligheid |
|---|
| Provincies werken samen in het Centraal Informatiebeveiligingsoverleg (CIBO), een onderdeel van het 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 standaard werkwijze waarmee per bedrijfsproces of informatiesysteem bepaald wordt welke beveiligingsmaatregelen getroffen moeten worden.<br><br>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.<br><br>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. |

### Informatiebeveiligingsbeleid (juni 2013)

Door de hierboven genoemde taskforce en diverse andere ontwikkelingen binnen en buiten de provinciale organisatie is het onderwerp informatiebeveiliging zichtbaar hoger op de agenda gekomen van de provincie Noord-Brabant, zo wordt in de eindevaluatie van het ICT-beleid in 2015 gesteld. In juni 2013 is zo ook het *Informatiebeveiligingsbeleid Provincie Noord-Brabant* vastgesteld en door de algemene directie geaccordeerd. Het betreft een nadere uitwerking van het onderdeel informatiebeveiliging uit de kadernota. In het

document beschrijft de provincie wat informatiebeveiliging is, waarom ze deze beveiliging noodzakelijk acht en wat haar visie en beleid is op dit terrein. Het document is niet aan PS aangeboden, omdat het een verdere (tactische) invulling van de kadernota betreft en dit destijds werd gezien als een ambtelijke verantwoordelijkheid en bevoegdheid.

De provincie zet in op informatiebeveiliging voor de borging van een betrouwbare informatievoorziening welke ze essentieel acht voor het goed functioneren van haar processen en (daarmee) correcte uitvoering van haar taken. Het uitvallen van informatiesystemen of het door onbevoegden kennisnemen, wijzigen en/of verwijderen van informatie kunnen verstrekkende gevolgen hebben voor onder andere het imago en de beleidsuitvoering van de provincie, zo wordt gesteld.

Informatiebeveiliging wordt gedefinieerd als:

| Definitie informatiebeveiliging |
| --- |
| Het kunnen waarborgen dat de juiste informatie op het juiste moment door de juiste personen gebruikt kan worden. |

Informatiebeveiliging is daarmee een kwaliteitsaspect van de provinciale bedrijfsvoering, zo wordt gesteld, en omvat de drie aspecten die reeds in de kadernota waren opgenomen. Ook wordt de noodzaak van informatiebeveiliging onderstreept die voortkomt uit de toenemende digitalisering van de provinciale dienstverlening, de samenwerking met onder andere overheden, wet- en regelgeving die eisen stelt aan informatie, zoals de Wbp[5], en de maatschappelijke verantwoordelijkheid van de provincie waarbij verwacht mag worden dat zij zorgvuldig omgaat met de gegevens die zij beheerd.

In lijn met het doel dat in de kadernota werd gegeven, wordt gesteld dat de provincie met informatiebeveiliging streeft naar beveiliging van haar informatie en alle daaraan gerelateerde aspecten die aansluiten bij het ambitieniveau van haar organisatie met een acceptabele balans tussen kosten en baten, lusten en lasten (visie). De daarbij te hanteren uitgangspunten worden opgesomd. Deze omvatten naast procedurele en technische maatregelen als wetgeving, afspraken en verantwoordelijkheden in de lijn, ook het bewustzijn van medewerkers. Elementen die ook al in de kadernota werden genoemd (insteek op techniek en mens). Veelal als een uitwerking van de kadernota worden onder andere de volgende acties opgesomd:

- Training medewerkers in en monitoring op het naleven van de regels voor toegang tot beveiligde omgevingen (zoals gebruik van wachtwoorden, algemeen geldende gedragscode).
- Afhankelijk van het bedrijfsrisico gebruik van een passend authenticatiesysteem.
- Vaststellen verantwoordelijkheden en procedures voor het beheer en de bediening van alle informatie(voorzieningen).
- De provincie werkt met projectportfoliomanagement. Bij implementatie van nieuwe systemen benodigde beveiligingsmaatregelen vaststellen op basis van een risicoanalyse in de Project Start Architectuur (PSA).
- Centrale registratie informatiebeveiligingsincidenten in een incidentenregister, afhandeling en evaluatie om met name te kijken welke maatregelen genomen kunnen

[5] In het Informatiebeveiligingsbeleid ontbreekt de bijlage met kaders en richtlijnen en daarmee inzicht in de inhoudelijke eisen. Ook wordt de IBI niet vermeld bij de voorbeelden van richtlijnen waaraan de provincie zich committeert.

worden om herhaling in de toekomst te voorkomen.

- Jaarlijkse risicoanalyses om het beveiligingsniveau vast te stellen en om te bepalen welke maatregelen getroffen moeten worden om de risico's tot aanvaardbare proporties terug te dringen. De te treffen maatregelen worden opgenomen in een jaarlijks centraal integraal beveiligingsplan voor de gehele organisatie.
- Regelmatige toets informatiebeveiligingsbeleid op volledigheid en actualiteit.
- Minimaal eenmaal per vier jaar externe audit en indien noodzakelijk herziening beleid.
- Jaarlijkse rapportage concerncontroller of accountant over evaluatie implementatie van het beleid.
- Tweemaal per jaar rapportage aan de Chief Information Officer (CIO) over de betrouwbaarheid van de informatievoorziening: bijvoorbeeld voortgang geplande maatregelen, beveiligingsincidenten, communicatie over en coördinatie van informatiebeveiliging, bewustzijn en gedrag van medewerkers.

Daarnaast wordt in aanvulling op de kadernota de organisatie van informatiebeveiliging beschreven (zie paragraaf 3.9).

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

De Interprovinciale Baseline Informatiebeveiliging (IBI) bevat 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 er door de provincie Noord-Brabant in samenwerking met de provincie Utrecht in 2015 een traject in gang gezet om de IBI 1.0 uit 2010 te herijken op basis van nieuwe risicoanalyses. De uitkomsten hiervan zijn verwerkt en hebben geleid tot de IBI 2.0 die in 2017 is vastgesteld na interprovinciale goedkeuring in het CIBO, en derhalve vigerend is. Verder hebben de provincies in 2017 met elkaar afgesproken dat ze in 2021 allemaal ISO 27001 gecertificeerd moeten zijn 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.

### Externe ontwikkeling: Wbp (2015 en 2018)

Eén 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.
Per 25 mei 2018 zal deze Nederlandse privacywetgeving worden vervangen door de Europese Algemene Verordening Gegevensbescherming (AVG).

### Vigerend informatiebeveiligingsbeleid

Vanuit de ambtelijke organisatie is aangegeven dat het Informatiebeveiligingsbeleid uit 2013 het vigerende beleid is voor *informatiebeveiliging*. Dit beleid werd ten tijde van het rekenkameronderzoek geactualiseerd in verband met de inwerkingtreding van de AVG in 2018. Hoewel in de rapportage IPO-monitor van de provincie van maart 2017 nog werd voorzien dat dataprivacy zou worden geïntegreerd in de actualisatie van het informatiebeveiligingsbeleid, is hier uiteindelijk van afgezien. Daar het twee verschillende onderwerpen betreft, worden de missie en visie op deze terreinen ook in afzonderlijke documenten beschreven, zo is vanuit de ambtelijke organisatie aangegeven. Ze overlappen

slechts op de technische maatregelen ter bescherming van de persoonsgegevens.

De rekenkamer constateert dat uit de documenten niet duidelijk wordt wat de status is van de door de directie vastgestelde Informatievisie uit 2015 en hoe deze zich verhoudt tot de Kadernota en de Visie en hoofdlijnen informatiebeleid uit 2016. Ze betreffen bijvoorbeeld, zo wordt erin aangegeven en/of luidt de titel, allemaal visies op informatie. Daarnaast betreffen de recentere nota's actualisaties op onderdelen, maar blijven de oude kaders ook nog geldig.

# 3. Uitvoering beleid

In dit hoofdstuk geven we inzicht in hoe de provincie Noord-Brabant de informatiebeveiliging in de praktijk heeft ingevuld. Daartoe beschrijven we hoe de beoogde invulling, zoals omschreven in de kadernota en het informatiebeveiligingsbeleid, tot uiting komt in de praktijk.

## 3.1 Evaluatie kadernota

Conform de afspraken is de kadernota geëvalueerd. Op 31 oktober 2014 verscheen het rapport over de intern uitgevoerde tussenevaluatie van de kadernota. Een jaar later, op 10 november 2015 verscheen het rapport van de extern uitgevoerde 'eind'evaluatie. In beide evaluaties stond de vraag centraal of de doelstellingen uit de kadernota op effectieve en efficiënte wijze zijn behaald. Er worden in de evaluaties veelal vergelijkbare conclusies getrokken. De doelstellingen zijn grotendeels bereikt; de meeste doelstellingen zijn gerealiseerd. Zo is de technische basis, conform routekaart, grotendeels op orde gebracht. Maar er wordt niet geredeneerd vanuit informatiestrategie en -behoefte, zo wordt gesteld (zie ook paragraaf 2.1). Daarnaast wordt aandacht gevraagd voor onder andere de projectenportfolio (zie paragraaf 3.2) en bewustwording op het gebied van informatiebeveiliging (zie paragraaf 3.4). De rekenkamer stelt vast dat ook na 2015 nog via een routekaart wordt gewerkt. In de Routekaart ICT 2015-2018 van 15 juni 2015 zijn 40 projecten opgenomen die verspreid over de betreffende periode moeten worden opgepakt, veelal betreft het upgraden, vervanging of uitbreiding.

## 3.2 Informatieveiligheid integraal onderdeel dagelijks handelen

Binnen de provinciale organisatie is in 2006 allereerst vanuit de techniek (operationeel) aandacht ontstaan voor informatiebeveiliging. Zoals eerder opgemerkt is in 2013 beleid geformuleerd voor informatiebeveiliging. Conform de kadernota en het informatiebeveiligingsbeleid zijn de verantwoordelijkheden in de lijn uitgezet. De betreffende projectteams/programmaeigenaren zijn verantwoordelijk voor hun projecten en programma's. Medewerkers zijn verantwoordelijk voor de informatie en de veiligheid daarvan, waarover zij voor de uitvoering van hun taken beschikken. De namen en functies van alle uitvoeringsverantwoordelijken en verantwoordelijken voor de verschillende processen en de daarbij behorende informatie zijn vastgelegd in het risicomanagementinformatiesysteem (RMIS). De processen voor de besturing van informatiebeveiliging zijn ook in dit systeem opgenomen.

De provincie werkt met projectportfoliomanagement voor projecten en een changemanagementproces voor wijzigingen. Bij de integrale aanpak die de provincie hanteert, dient bij alle projecten, ontwikkelingen en handelingen ook informatiebeveiliging aandacht te krijgen; de kaders en richtlijnen dienen te worden geborgd. Van 2015 tot eind 2017 was er een I-board die adviseerde over de strategische inzet van ICT-projecten. Hierin

zaten ook beleidsmensen om de organisatie (gebruikerskant) bij ICT-projecten te betrekken.
Uit de bestudeerde documenten en gevoerde gesprekken blijkt dat het projectportfolio- en changemanagementproces echter niet altijd worden gevolgd:

- Zo gingen niet alle projecten langs het ICT-kernteam (IKT) dat tot medio 2015 het tactisch portfoliomanagement bekeek.
- Is de gebruikerskant niet altijd voldoende georganiseerd.
- Is bij aanvang van projecten regelmatig onvoldoende aandacht voor informatiebeveiliging.
- Worden niet alle projecten meegenomen in het portfolioproces en niet alle wijzigingen in het changemanagementproces.
- Is bijvoorbeeld in 2014, voorafgaand aan de implementatie, het nieuwe documentmanagementsysteem (Corsa), op initiatief van de beleidsmedewerker informatiebeveiliging buiten het betreffende proces om, getest op beveiligingsissues.

Het proces wordt vaak omzeild en/of niet gevolgd, zo wordt in een voor de provincie uitgevoerd onderzoek gesteld. Er is onvoldoende aandacht voor en er wordt niet genoeg gestuurd op de naleving van kaders en richtlijnen. Dit eerste komt, zo wordt gesteld, omdat medewerkers zich onvoldoende bewust zijn dat privacy en informatiebeveiliging betrokken moeten worden bij de uitvoering van werkzaamheden. Maar ze worden ook bewust vergeten, zo wordt in het onderzoek gesteld. In een memo aan de directie uit februari 2017 wordt aangegeven dat de kaders en richtlijnen worden gemeden omdat deze als te lastig en vertragend worden beschouwd en in een gesprek is aangegeven dat er verschillende belangen spelen (beheerbelang versus organisatiebelangen). Hierdoor worden informatiebeveiliging en/of privacy(discipline) vaak niet of te laat betrokken/geraadpleegd. Naar aanleiding van verschillende onderzoeken werd dan ook aandacht gevraagd voor het (naleven van het) projectportfolio- en/of changemanagementproces. Bijvoorbeeld in 2014 bij een mysteryguest/beveiligingsonderzoek, eind 2014 bij de tussenevaluatie van de kadernota en in 2016 en 2017 bij een uitgevoerde privacyscan. Nadat uit een beveiligingsonderzoek van begin 2017 bleek dat er op onder andere voornoemde punten weinig was veranderd ten opzichte van het vorige onderzoek, heeft de CIO onder andere opgedragen dat alles via het portfolioproces moet verlopen en alle projecten langs de CIO moeten; er kwam daarmee meer dwang. Zie voor andere bevindingen over het betrekken van informatiebeveiliging in het dagelijks handelen paragraaf 3.3 en 3.4.

Conform het informatiebeveiligingsbeleid worden informatiebeveiligingsincidenten centraal geregistreerd in een incidentenregister en volgens de daarvoor geldende procedure afgehandeld. De incidenten worden door de medewerkers van het dienstenplein vastgelegd in facilitor. Daarna worden ze doorgezet naar de verantwoordelijke medewerker die de melding behandelt, eventueel acties uitvoert of deze belegt bij de betreffende medewerkers.

Zoals voorgeschreven in het informatiebeveiligingsbeleid maakt de provincie in het kader van toegangsbeveiliging gebruik van authenticatiesystemen. Zo werkt de provincie voor mail, webmail en de (virtuele) werkplek met een authenticatiesysteem. De rekenkamer constateert op basis van haar onderzoek dat in het authenticatiesysteem voor webmail nog verbeteringen zouden kunnen worden doorgevoerd (zie ook paragraaf 4.2 en 4.3).

## 3.3 Jaarlijkse risicoanalyse en beveiligingsplan

### Risicoanalyse

In het beleid (kadernota en informatiebeveiligingsbeleid) is vastgelegd dat jaarlijks een risicoanalyse wordt uitgevoerd om het beveiligingsniveau vast te stellen en om te bepalen welke maatregelen getroffen moeten worden om de risico's tot aanvaardbare proporties terug te dringen. De rekenkamer constateert dat er in de praktijk, in lijn met interprovinciale afspraken, nagenoeg jaarlijks een rapportage/memo is opgesteld waarin verantwoording wordt afgelegd over de voortgang en volwassenheid van informatiebeveiliging. Hierin is bepaald in hoeverre aan de gestelde afspraken/eisen (IBI) wordt voldaan en welke aandachtsgebieden er zijn. Alleen de rapportage over 2015 ontbreekt. In interprovinciaal verband is destijds besloten om geen rapportage over 2015 op te stellen, omdat in dat jaar een update van de IBI heeft plaatsgevonden. De (samenvattende) rapportages worden opgesteld op basis van de IBI-monitor. Dit betreft een spreadsheet/database met, verdeeld over de in de IBI onderscheiden hoofdstukken, zo'n 6.000 maatregelen. Op basis daarvan wordt, via een formele registratie, door de provincie bepaald in hoeverre ze voldoet aan de baseline (IBI) en daaruit volgen de aandachtsgebieden voor de provincie op het gebied van informatieveiligheid. In de rapportage wordt aangegeven hoe de provincie er per IBI-hoofdstuk voor staat en welke aandachtsgebieden er zijn. Naast deze IBI-monitor en de in principe jaarlijkse rapportages daarover zijn er op reguliere basis risicoanalyses uitgevoerd op diverse processen (die een verhoogd risico lopen vanuit het oogpunt van informatieveiligheid), zoals bijvoorbeeld de processen burgemeesterszaken en Bibob (Wet bevordering integriteitsbeoordelingen door het openbaar bestuur). Voor deze processen wordt daarbij het risicoprofiel bepaald met de bijbehorende maatregelenset; welke maatregelen moeten worden geïmplementeerd ter verbetering van de informatieveiligheid.

Wat betreft de rapportages stelt de rekenkamer vast dat in september 2013 de *Quickscan informatiebeveiliging* van de provincie verscheen, die later door de provincie CIBO- en nog later IPO-monitor werd genoemd.[6] Uit de rapportage 2013 bleek dat wat betreft informatievoorziening, bedrijfscontinuïteitsbeheer en beveiliging van personeel (bewustwording) extra aandacht behoefden. Uit de twee daarna verschenen rapportages over respectievelijk 2014 en 2016 bleek dat alleen bedrijfscontinuïteitsbeheer (risico- en continuïteitsmanagement) nog achterbleef. Gesteld werd dat de provincie in 2014 redelijk tot goed inzicht had in de informatiebeveiligingsrisico's. In de *Monitoringtool baseline informatiebeveiliging 2014* van het CIBO, met het interprovinciale beeld, werd gesteld dat de provincie Noord-Brabant bij de hoogst scorende provincies hoort.

### Beveiligingsonderzoeken (penetratietesten en mysteryguestonderzoeken)

Sinds 2014 wordt de implementatie van de maatregelen ook gecontroleerd via tweejaarlijkse beveiligingsonderzoeken (penetratietesten en mysteryguestonderzoeken). Deze worden uitgevoerd door een externe partij gespecialiseerd in informatiebeveiliging. Naar aanleiding van de bevindingen van deze onderzoeken zijn eveneens, waar nodig, maatregelen genomen.
In 2014 voerde het externe bureau in opdracht van de CIO en in lijn met de doelstellingen van de taskforce BID voor het eerst verschillende penetratietesten en een mysteryguestonderzoek uit. Dit om een beeld te krijgen van waar de provincie in 2014 stond

[6] De rekenkamer kiest ervoor om in deze rapportage verder te spreken van rapportage IPO-monitor of CIBO-rapportage.

op het gebied van informatieveiligheid. De onderzoeken waren gericht op het toetsen van het beveiligingsbewustzijn van medewerkers van de provincie en het identificeren van zwakheden in de digitale en fysieke beveiliging (van het provinciehuis). Bij het eerste onderzoek werden behoorlijk wat beveiligingsissues gevonden, zowel technisch als bij houding en gedrag, zo wordt vermeld in een overzicht met afspraken van de directie van 26 mei 2014. Gesteld wordt dat de provincie slechter scoort dan het bedrijfsleven, maar vergelijkbaar met andere overheden. De directie/CIO besluit op alle aanbevelingen actie te ondernemen en in lijn met de kadernota en het informatiebeveiligingsbeleid proportionele (afgewogen) maatregelen te nemen. Naast technische acties, zoals een inhaalslag om belangrijke updates te installeren, het inrichten van een update-managementproces en een hardeningsproces, wil de provincie ook zwaar inzetten op bewustwording van medewerkers.
In juni 2014 volgde een penetratietest op de proefomgeving MyCorsa NxT. Er werden verschillende beveiligingsrisico's achterhaald waardoor aanvallers ongeautoriseerde toegang zouden kunnen verkrijgen tot Corsa als gebruiker of als beheerder. Vóór implementatie van Corsa waren de risico's afgedekt, zo wordt gesteld.
In september 2014 werd er vervolgens een penetratietest uitgevoerd op de website van de provincie. Hierbij kon geen ongeautoriseerde toegang tot systemen of data worden verkregen, maar werd wel een aantal belangrijke verbeterpunten vastgesteld die door de provincie zijn opgepakt.

Begin 2017 werden voor de tweede keer penetratietesten en een mysteryguestonderzoek uitgevoerd, met in 2017 expliciete aandacht voor Bibob, het proces rondom burgemeesterszaken en kabinetszaken. Aanvullend werd een phishingsimulatie[7] uitgevoerd. De provincie had hiertoe najaar 2016 het externe bureau opdracht gegeven. Via een memo van 8 februari 2017 werd de directie geïnformeerd over de bevindingen van het onderzoek. Geconstateerd werd onder andere dat ten opzichte van 2014 zowel de fysieke beveiliging (receptie) alsmede het beveiligingsbewustzijn op het gebied van phishing is toegenomen, maar dat er wel sprake is van minder sociale controle binnen het beveiligde gedeelte van het gebouw.[8] In een door GS op 9 mei 2017 geaccordeerde memo van 25 april 2017 over het onderzoek werd echter gesteld dat het beveiligingsbewustzijn van de medewerkers en de fysieke beveiliging van het provinciehuis onvoldoende zijn: niet vergrendelde en/of onbeheerde werkplekken, toegang 'gegeven' tot (mogelijk) gevoelige informatie van de provincie door het klikken op de link in een phishingmail en onbekenden die in het beveiligde gedeelte van het provinciehuis hun gang kunnen gaan. In de rapportage IPO-monitor van de provincie over 2016 van maart 2017 werd gesteld dat uit verschillende onderzoeken in 2016 is gebleken dat de fysieke beveiliging van het gebouw in opzet goed is geregeld en op orde is. Het gedrag/beveiligingsbewustzijn blijft dus achter.
In de memo van februari 2017 staat verder dat de technische informatiebeveiliging (systemen en beheer) onvoldoende is. Het was tijdens het onderzoek begin 2017 namelijk gelukt om volledige controle te verkrijgen over de technische infrastructuur van de provincie en daarmee toegang tot alle informatie waaronder de financiële administratie, burgemeesterszaken en Bibob. Een aantal (technische) bevindingen was ook al bij de eerste testen in 2014 geconstateerd. Als verklaring voor het aantreffen van vergelijkbare problemen, werd, in lijn met bevindingen uit een privacyscan die de provincie in 2016 liet

[7] Een phishingsimultatie bootst een gerichte cyberaanval na om te kijken in hoeverre medewerkers (bewust of onbewust) bereid zijn om potentieel kwaadaardige software (malware) te laten uitvoeren die bijvoorbeeld per emailbericht wordt aangeboden.
[8] Dit laatste is een gevolg van de nieuwe manier van werken (flex-concept).

uitvoeren met het oog op de toekomstige AVG (zie paragraaf 3.6), in 2017 wederom onder andere gesteld:

- Er is onvoldoende sturing op het integraal werken binnen het cluster I&I. Dat resulteert in een verkokerde aanpak waardoor er onder andere onvoldoende zicht en controle op de naleving van afgesloten contracten met externe partijen is. Ook is er onvoldoende sturing op operationeel beheer binnen I&I waardoor werkzaamheden niet op een juiste manier geprioriteerd worden. Dit resulteert erin dat het op orde houden van de basisinfrastructuur geen prioriteit heeft waardoor onder andere bevindingen uit eerdere onderzoeken nog niet zijn opgepakt.
- Er is onvoldoende aandacht voor kaders en richtlijnen, deze worden gemeden omdat deze als te lastig en vertragend worden beschouwd. Deze cultuur van het omzeilen van procedures heeft eveneens voor problemen gezorgd.

De CIO heeft binnen de organisatie aandacht gevraagd voor deze punten, zo is vanuit de ambtelijke organisatie aangegeven. De CIO richtte in 2017 een taskforce op om de aanbevelingen uit het onderzoek op te pakken (via een plan van aanpak) en de voortgang van de uit te voeren acties te monitoren. Deze betroffen onder andere:

- Borgen dat de operationele taken op het gebied van informatiebeveiliging worden belegd binnen ICT-beheer en ICT-beheer dient zorg te dragen dat het plan van aanpak per direct wordt opgepakt.
- Borgen dat voor elk project het projectportfoliomanagementproces en voor elke wijziging het changemanagementproces wordt gevolgd, zodat kaders en richtlijnen juist worden toegepast.
- Zorgen voor inrichting van monitoring en handhaving voor de naleving van contracten en de handhaving van kaders en richtlijnen in het algemeen en te zorgen dat kaders en richtlijnen ook voldoende geborgd zijn binnen het sourcingtraject.
- Aanpassen van standaardwachtwoorden.
- Netwerksegmentatie in publieke ruimtes.
- Plaatsen van updates van relevante softwarepakketten.
- Oppakken verbeterplan voor rechtenbeheer.
- Starten campagne voor alle medewerkers om de veiligheidsrisico's vanuit bewust handelen te beheersen (beveiligingsbewustzijn verhogen).

In mei 2017 werd de taskforce opgeheven, omdat met de acties de bevindingen zijn opgelost, zo wordt gesteld. Wel wordt expliciet aandacht gevraagd om de oplossingen in de processen te borgen om te voorkomen dat dezelfde bevindingen in een volgend onderzoek weer optreden. De stand van zaken van de oplossingen wordt wekelijks besproken totdat de problemen zijn opgelost, zo is aangegeven. Vanuit de ambtelijke organisatie is verder aangegeven dat in 2017 is voorgesteld om de mysteryguestonderzoeken jaarlijks in plaats van tweejaarlijks te gaan uitvoeren.

### Informatiebeveiligingsplan

De rekenkamer stelt vast dat de beoogde *centrale* informatiebeveiligingsplannen, waarin de maatregelen/acties zouden worden opgenomen die noodzakelijk worden geacht om de aandachtspunten uit onder andere de risicoanalyses, rapportages op basis van de IBI-monitor en beveiligingsonderzoeken op een acceptabel niveau te krijgen, in de praktijk nooit als zodanig zijn opgesteld. In de praktijk zijn de werkzaamheden/acties die voor een lopend jaar werden voorzien, vastgelegd in het persoonlijk werkplan (PWOP) van de

beleidsmedewerker informatiebeveiliging. Daarnaast is er een database ('toolbox') waarin per informatieproces de te nemen (beheers)maatregelen zijn opgenomen en de implementatie ervan wordt gevolgd tot configuratie. Sinds eind 2016 wordt daarin ook het eigenaarschap van elke maatregel vastgelegd. Op basis van deze database wordt ook de rapportage ten behoeve van de 'jaarlijkse' rapportage IPO-monitor en de rapportage over de betrouwbaarheid van de informatievoorziening aan de CIO opgesteld.

## 3.4 Bewustwording

In de kadernota en het informatiebeveiligingsbeleid wordt het belang van bewustwording en bijbehorend gedrag van medewerkers voor informatiebeveiliging onderstreept. In de loop van de jaren is in de meeste onderzoeken aandacht gevraagd voor (het ontwikkelen en vasthouden van) bewustwording op het gebied van informatiebeveiliging (en later ook privacy): quickscan informatiebeveiliging 2013, evaluatie kadernota eind 2014 en eind 2015, mysteryguestonderzoek 2014, privacyscan 2016, rapportage IPO-monitor 2016 en mysteryguestonderzoek 2017.
In de praktijk heeft de provincie verschillende inspanningen verricht om het bewustzijn en de vaardigheden van medewerkers te vergroten. Zo zijn de bevindingen van de eerste penetratietesten/mysteryguestonderzoek uit 2014 gebruikt voor het opzetten van een bewustwordingsplan 'Bewust veilig digitaal werken'. Via Brain en Yammer (intranet) zijn medewerkers geïnformeerd over de bevindingen van het onderzoek en de te nemen maatregelen, is een handreiking gedaan om phishingberichten te herkennen met een instructie over de procedure om verdachte emailberichten te melden en zijn er trainingen en workshops gegeven. Daarnaast zijn verschillende documenten opgesteld en op intranet geplaatst, zoals de algemeen geldende gedragscode die beschreven staat in de Leidraad Integer Handelen, een procedure voor geheime dossiers en een werkinstructie over hoe om te gaan met vertrouwelijke informatie (zoals kabinets- en personeelszaken).
Nadat in maart 2016 bij de privacyscan werd geconcludeerd dat het merendeel van de medewerkers niet voldoende op de hoogte is van de risico's op het gebied van informatiebeveiliging en privacy, en begin 2017 bij het tweede mysteryguestonderzoek werd geconcludeerd dat het beveiligingsbewustzijn van de medewerkers onvoldoende is, is conform de aanbevelingen ook in 2017 weer een campagne gestart en zijn trainingen en e-learnings aangeboden om het beveiligingsbewustzijn te verhogen. Zo is gebruik gemaakt van banners op elke tussenverdieping om aandacht te vragen voor het onderwerp en verscheen op 6 maart 2017 een bericht met filmpje op het intranet van de provincie ('Informatiebeveiliging doen we samen´) waarin aandacht wordt gevraagd voor het belang, de risico's en regels van informatiebeveiliging. In dit bericht wordt gesteld dat de informatiebeveiliging binnen de provincie ondermaats is. De belangrijkste bevindingen uit het mysteryguestonderzoek worden gegeven. Ook worden de regels en risico´s, die ook op een andere plek op het intranet te vinden zijn, gegeven. Regels waaronder:

- Kies sterke wachtwoorden voor je apparaten.
- Berg je vertrouwelijke stukken op (ook tijdens werktijd).
- Laat geen onbekenden binnen in het beveiligde gedeelte.
- Spreek onbekenden in het gebouw aan.

Ook wordt meer in algemene zin op intranet aandacht gevraagd om veilig en zorgvuldig met informatie om te gaan, zodat besluitvorming niet onder druk komt doordat informatie in

verkeerde handen valt. Er wordt een aantal principes opgesomd, waaronder dat documenten van de provincie nooit automatisch openbaar zijn, in Corsa alle documenten zijn in te zien tenzij sprake is van vertrouwelijkheid of geheimhouding, interne vertrouwelijkheid altijd aan de orde is bij onder andere kabinetszaken, Bibob en personeelszaken en dat medewerkers zich bewust moeten zijn van risico's in het digitaal werken en de juiste, veilige instellingen dienen toe te passen op tablet en/of smartphone. Tevens was er in 2017 een week van de integriteit, waarin op maandag 20 maart 2017 een workshop Dataveiligheid werd gegeven met de naam: Hoe bescherm jij je tegen een hack (phishing)?

Desgevraagd is vanuit de ambtelijke organisatie aangegeven dat de bewustwordings-trainingen vrijwillig en informeel waren, maar in februari 2017 heeft de CIO besloten dat de e-learnings verplicht moeten worden gevolgd door de medewerkers. De rekenkamer merkt hierbij op dat reeds bij de bespreking van de kadernota in maart 2013 vanuit PS werd gevraagd om een minder vrijblijvende aanpak van de bewustwordingsacties. Vanuit de ambtelijke organisatie is verder aangegeven dat de verwachting is dat de opsplitsing van de H&O-taken van managers ook een positieve bijdrage zal leveren aan het verhogen van het bewustzijn van informatieveiligheid. Elke H-manager dient er op te sturen dat elke medewerker zo'n training doorloopt en zich bewust is van informatieveiligheid. Zo maken bijvoorbeeld e-learnings nu deel uit van 'het goede gesprek' tussen H-manager en medewerker.

Ook is aangegeven dat het belangrijk is dat ook GS, PS en de directie worden meegenomen in het traject van bewustwording op het gebied van informatiebeveiliging en dataprivacy. Op verschillende manieren is namelijk naar voren gekomen dat ook de bewustwording van GS/PS op het gebied van informatiebeveiliging op een hoger niveau gebracht moet worden, zo wordt in de ambtelijke reactie gesteld. Zo wordt bijvoorbeeld nog steeds door verschillende personen e-mail van het @brabant.nl-account automatisch doorgestuurd naar een gmail-adres. Naar aanleiding van schriftelijke vragen vanuit PS over informatieveiligheid najaar 2017, geven GS wat betreft bewustwording aan dat indien gewenst de beleidsmedewerker informatiebeveiliging een toelichting kan geven specifiek gericht op PS-leden.

Het ontwikkelen en vasthouden van bewustwording en vaardigheden op het terrein van informatiebeveiliging zijn een continu proces en vormen een blijvend aandachtspunt, zo stelt de provincie. Het is een lastig traject omdat het gedrag en cultuur betreft en dat is moeilijker te veranderen.

## 3.5 Audit implementatie informatiebeveiligingsbeleid

In het informatiebeveiligingsbeleid staat het voornemen dat de implementatie van het beleid jaarlijks wordt geëvalueerd door de concerncontroller of de accountant. In de kadernota staat dat het ICT-beleid jaarlijks wordt meegenomen in de accountantscontrole. In de praktijk is de audit van het informatiebeveiligingsbeleid ook bij de accountant neergelegd. Desgevraagd is vanuit de ambtelijke organisatie aangegeven dat informatieveiligheid geen

onderdeel uitmaakt van het takenpakket van de eenheid Concerncontrol & Auditing.[9]
De accountant beoordeelt jaarlijks de IT-omgeving en daarmee de informatiebeveiliging van de provincie. Dit gebeurt sinds 2012 naar aanleiding van een aanbeveling in het rekenkameronderzoek *Strategisch Informatiebeleid provincie Noord-Brabant* om de accountant stelselmatig zijn bevindingen te laten rapporteren over de stand van zaken rondom informatiebeveiliging. In de boardletter rapporteert de accountant jaarlijks zijn bevindingen. De accountant richt de controles daarvoor voornamelijk op SAP omdat deze van materieel belang is voor de jaarrekeningcontrole (heeft een financiële component) en de provinciale processen voor een belangrijk deel worden ondersteund door SAP.
Wat betreft informatiebeveiliging kijkt de accountant naar de governance, zo is vanuit de ambtelijke organisatie aangegeven. In de boardletter 2014 en 2016 wordt het meest uitgebreid ingegaan op informatiebeveiliging. Zo wordt daarin de uitvoering van informatiebeveiliging beschreven. In de boardletter 2014 merkt de accountant op dat de provincie in 2013 en 2014, naar aanleiding van het rekenkameronderzoek naar het strategisch informatiebeleid, diverse acties in gang heeft gezet voor het structureren en daarmee verscherpen van de informatiebeveiliging. In de boardletter 2016 stelt de accountant dat de aandacht van de provincie rondom informatiebeveiliging gepast en de procedures in opzet toereikend zijn.

## 3.6 Regelmatige toets informatiebeveiligingsbeleid

In het informatiebeveiligingsbeleid is vastgelegd dat het informatiebeveiligingsbeleid regelmatig getoetst dient te worden op volledigheid en actualiteit, minimaal eenmaal per vier jaar een externe audit dient plaats te vinden en indien noodzakelijk het beleid herzien moet worden.[10] Sinds vaststelling van het beleid in 2013 zijn er verschillende ontwikkelingen geweest die het beleid raken. Voorbeelden daarvan zijn de actualisatie van de IBI in 2015 en 2017, de uitbreiding van de Wbp in 2015 met datalekken en de CIO-rol die sinds 2016 niet meer bij de directeur Bedrijfsvoering ligt. In 2015 hebben de beleidsmedewerker informatiebeveiliging en de CIO verkennend gesproken over de impact van de uitbreiding van de Wbp. Door een personele wisseling van de CIO liep het oppakken van dit onderwerp echter vertraging op en is het pas najaar 2016 met de benodigde prioriteit en samen met de toekomstige AVG opgepakt door de nieuwe CIO, zo is vanuit de ambtelijke organisatie aangegeven.

In maart 2016 verschenen de bevindingen van een door een externe partij uitgevoerde privacyscan. Daarbij werd gesteld dat om op 25 mei 2018 te (kunnen) voldoen aan de eisen van de Wbp en de toekomstige AVG er nog behoorlijk wat werk moet worden verzet. Ook al wordt er een significant gat geconstateerd tussen de volwassenheid van informatiebeveiliging en de bescherming van persoonsgegevens, moet er ook op informatiebeveiliging nog werk worden verzet. Zo dient, naast de reeds genoemde aandachtspunten in voorgaande paragrafen, onder andere:

- een informatiebeveiligings- en privacymanagement en bestuursmodel te worden ingericht (inclusief wettelijk verplichte functionaris gegevensbescherming (FG)),

[9] Met ingang van 1 januari 2018 is de clusterstructuur vervallen. In deze rapportage zal daarom soms nog gesproken worden van cluster en soms van eenheid.
[10] In de op 23 juni 2017 verschenen actualisatie van de IBI staat: het is de verantwoordelijkheid van de eigenaar van het beveiligingsbeleid om dit minstens eenmaal per jaar te herzien.

waarmee met daadkracht/slagkracht daadwerkelijk veranderingen en naleving worden geborgd;
- het inkoopbeleid/contractmanagement te worden herzien en nageleefd, waarin privacy en informatiebeveiliging worden geïntegreerd. Zo dienen er ook bewerkersovereenkomsten te worden afgesloten waarin verantwoordelijkheden omtrent datalekken of privacy- en informatiebeveiliging zijn opgenomen;
- een eenduidig proces te worden ingericht dat waarborgt dat medewerkers alleen toegang hebben tot systemen en dergelijke waartoe ze daadwerkelijk toegang nodig hebben.

Via een memo van 20 april 2017 werd de directie geïnformeerd over de uitkomsten van het privacy(compliance)onderzoek. Aan de directie werd geadviseerd:
- een taskforce in te richten om de bevindingen in de lijn te beleggen en hierop te sturen;
- te borgen dat er in de lijn voldoende capaciteit en middelen worden vrijgemaakt om de aanbevelingen op te kunnen pakken en te zorgen dat medewerkers het komende jaar worden “opgeleid” om op een juiste manier met persoonsgegevens om te gaan;
- te zorgen voor formatie en functieprofiel voor een FG.

In de rapportage IPO-monitor 2016 van maart 2017 worden eveneens benodigde aanpassingen in het kader van dataprivacy opgesomd, zoals: herziening informatiebeveiligingsbeleid en dataprivacy daarin integreren, herziening uitvoeringsregelingen, procedures, contracten en dergelijke.

Vanuit de ambtelijke organisatie is aangegeven dat het in 2013 vastgestelde informatiebeveiligingsbeleid momenteel wordt geactualiseerd in verband met de inwerkingtreding van de AVG in 2018. De rekenkamer constateert dat het beleid na vier jaar wordt geactualiseerd, op basis van de in de afgelopen jaren uitgevoerde jaarlijkse audits van de accountant, jaarlijkse DigiD-audits van het Rijk en verschillende onderzoeken/scans door externe partijen.

## 3.7 Rapportage informatiebeveiliging aan CIO

In het informatiebeveiligingsbeleid staat dat de CIO twee keer per jaar een rapportage ontvangt over informatiebeveiliging en de betrouwbaarheid van de informatievoorziening. In de praktijk verloopt de informatievoorziening aan de CIO langs verschillende kanalen, zoals via de I-board of via een directe lijn bij casuïstiek.
De beleidsmedewerker informatiebeveiliging heeft veelvuldig contact met de CIO, onder andere naar aanleiding van onderzoeken. Afhankelijk van het onderwerp sluiten ook andere medewerkers aan. Ook de clustermanager I&I rapporteert aan de CIO, maar daar was, vooral voor 2016, een behoorlijke afstand, zo is gesteld. In een gesprek is door een bij informatieveiligheid betrokken ambtenaar aangegeven dat er geen specifieke rapportages informatiebeveiliging aan de CIO zijn geweest. Wel heeft de CIO in 2013, 2015 en 2017 de CIBO-rapportages ontvangen. Ook de uitkomsten van de mysteryguestonderzoeken inclusief ‘hoe daarop te sturen’ zijn door de beleidsmedewerker informatiebeveiliging in 2014 en 2017 aan de CIO gestuurd, evenals de bevindingen van de overige penetratietesten (minimaal 16). Daarnaast waren er diverse losse rapportages waarin in meer of mindere mate ook wordt ingegaan op het onderwerp informatiebeveiliging: de

resultaten van de evaluaties van de kadernota in 2014 en 2015, de bevindingen van de privacyscan in 2016 en de jaarlijkse boardletters van de accountant. Vanuit de ambtelijke organisatie is aangegeven dat naar aanleiding van de bevindingen van het mysteryguestonderzoek in 2017 een nieuwe kwartaalrapportage is toegevoegd waarin de CIO wordt geïnformeerd door de clustermanager I&I, de programmamanager/ opdrachtgever ICT-beheer & projecten en de beleidsmedewerker informatiebeveiliging.

## 3.8 Middelen

### Financiële middelen

Desgevraagd is vanuit de ambtelijke organisatie aangegeven dat er tot op heden geen specifieke budgetten beschikbaar of benoemd zijn voor informatieveiligheid. Dit is, zo wordt gesteld, zeer zeker een punt van aandacht. De kosten voor informatiebeveiliging worden primair bekostigd uit het ICT-projectenbudget en bij onvoldoende dekking wordt geput uit het reguliere budget Basisinfrastructuur.

In de kadernota wordt gesteld dat de nota binnen de reguliere financiële budgetten tot en met 2015 bereikt moet worden. Daarbij wordt aangegeven dat het ICT-projectenbudget in de periode 2012 tot en met 2015 jaarlijks afgerond € 1.500.000 zal bedragen en met ingang van 2016 terug zal lopen naar € 700.000 per jaar wat niet voldoende wordt geacht, zo wordt in de nota gesteld. Verder wordt in de kadernota aangegeven dat het budget Basisinfrastructuur voor 2012 € 5,3 miljoen en voor 2013 tot en 2015 jaarlijks ongeveer € 4 miljoen zal bedragen. In de tussenevaluatie van de kadernota wordt voor het totale ICT-budget opgemerkt dat in 2013 en 2014 moest worden ingezet op reserves omdat realisatie hoger was dan begroot ondanks kostenreducties. PS honoreren met de voorjaarsnota 2014 een verzoek om extra budget.

Voor het ICT-beleid in totaliteit was in de begroting 2012 tot en met 2016 respectievelijk voor 2012 € 9 miljoen, voor 2013 € 8 miljoen, voor 2014 € 7,7 miljoen, voor 2015 € 7.839.000 en voor 2016 € 7.874.000 begroot.[11] Vanaf 2016 werkt de provincie met één organisatiekostenbudget (OKB).

Sinds 2016 is van belang dat de AP bij een datalek een boete kan opleggen aan de provincie. De Wbp/AVG kan dus (onverwachte) financiële gevolgen hebben voor de provincie.

### Personeel

In de kadernota wordt niet afzonderlijk ingegaan op de personele inzet op informatiebeveiliging. Voor ICT wordt gesteld dat de personele inzet in de periode 2013-2015 zal worden gekenmerkt door enerzijds de personele krimpopgave (formatie I-domein van iets minder dan 160 in 2005 naar ongeveer 90 in 2015) en anderzijds de inzet van eigen personeel op cruciale expertise, inhuur zal steeds meer worden beperkt tot niet-cruciale expertise. Zo wordt bijvoorbeeld sinds mei 2014 de functie van clustermanager niet meer door een externe medewerker ingevuld. In de tussenevaluatie wordt opgemerkt dat na een tijdelijke toename vooralsnog nog geen daling van uitgaven voor inhuur wordt

[11] De ICT-budgetten voor 2015 en 2016 zijn inclusief de kosten voor telecommunicatie en mobiele toestellen. Ook omvatten ze de ruimte voor inhuur welke in 2017 van deze budgetten is afgeraamd.

geregistreerd. In 2013 en 2014 waren de uitgaven voor inhuur respectievelijk 31 en 41% van de totale personeelskosten van het cluster I&I. In de tussenevaluatie van de kadernota uit 2014 werd opgemerkt dat een sourcingstrategie van het cluster I&I naar verwachting najaar 2015 ontwikkeld zou worden. Vanuit de ambtelijke organisatie is aangegeven dat de provincie, mede ingegeven door een krimp-opdracht, momenteel aan het bekijken is welke taken door anderen/externen kunnen worden gedaan en wat de provincie nodig heeft om daarover goed de regie te kunnen houden. Daartoe wordt eerst een visie en strategie voor sourcingbeleid uitgewerkt. Hiervoor is in beeld gebracht wat de provincie zelf zou moeten doen en wat geoutsourcet kan worden; welke expertise in huis benodigd is en welke kan worden ingehuurd. Vanuit de ambtelijke organisatie is aangegeven dat de provincie zal moeten accepteren dat ze op IT-gebied afhankelijker wordt van andere partijen. Er zijn te veel ontwikkelingen en deze gaan te snel voor het beperkte aantal mensen dat daarvoor bij de provincie beschikbaar is, zo wordt gesteld. Door de operationele IT-omgeving te outsourcen, wordt dit opgelost. Opgemerkt wordt dat strategie, dataprivacy en beleid voor informatieveiligheid niet kan worden geoutsourcet.
Het sourcingtraject zal in drie stappen gaan omdat het teveel is om in één keer te doen en de provincie daarnaast als organisatie ook de mogelijkheid wil hebben om te kunnen ontwikkelen/leren: (1) basisinfrastructuur/generieke ICT, (2) applicatiebeheer, (3) applicatieontwikkeling/testen, geo-diensten en datawarehouses. In de ambtelijke reactie is aangegeven dat stap 1 nu (april 2018) wordt geoutsourcet. Over stap 2 en 3 wordt nog besloten. De nieuwe CIO speelt hier een belangrijke rol bij, zo wordt gesteld.
De veiligheid van informatie is bij deze stappen essentieel; de veiligheid van de infrastructuur/applicaties dient daarvoor geregeld te zijn. De externe partij is daarvoor verantwoordelijk, maar de provincie geeft daarvoor kaders en richtlijnen mee. Vanuit de ambtelijke organisatie is in januari 2018 aangegeven dat de sourcingstrategie voor I&I inmiddels is opgesteld, maar nog moet worden bepaald op welk niveau een en ander vastgesteld dient te worden.

De strategische sleutelposities voor het informatiebeleid (inclusief beveiliging) zijn de CIO en de (strategisch) beleidsmedewerker informatiebeveiliging. De CIO was tot en met 2017 een rol die moest worden uitgevoerd naast vele andere taken die de directeur had en sneeuwde daardoor soms onder, zo is vanuit de ambtelijke organisatie aangegeven. Najaar 2017 hebben PS het OKB opgehoogd met 1 fte voor de aanstelling van een nieuwe CIO. Deze zal al zijn aandacht volledig op de I-taken kunnen richten, omdat het geen rol meer is maar een (fulltime) functie. De nieuwe CIO treedt per 1 juni 2018 in dienst.
De beleidsmedewerker informatiebeveiliging betreft 1 fte en deze vervulde naast de taken voor informatieveiligheid op alle vlakken (operationeel, tactisch en strategisch), tot begin 2018 ook de taak van FG. De functie startte op tactisch-operationeel niveau, maar kreeg ook strategische elementen. Vanuit de ambtelijke organisatie is aangegeven dat al geruime tijd werd gevraagd om ondersteuning/capaciteit op tactisch-operationeel niveau. De discussie om de functie beleidsmedewerker informatiebeveiliging op te splitsen in twee functies (één op strategisch en één op tactisch-operationeel niveau) loopt sinds 2013. Maar de organisatie moest bij dit nieuwe onderwerp groeien; informatieveiligheid is een lastig onderwerp, zo wordt gesteld, want als er ‘niets’ gebeurt dan wordt ervan uitgegaan dat er wel voldoende capaciteit beschikbaar is. Met het oog op de toenemende uitbreiding en verzwaring van de werkzaamheden op het gebied van informatieveiligheid, gecombineerd

met het 24/7 bereikbaar zijn, heeft de provincie er in 2017 echter toch voor gekozen om de functie van beleidsmedewerker informatiebeveiliging op te splitsen in twee nieuwe functies. Het betreft op strategisch niveau de Chief Information Security Officer (CISO-functie en op operationeel/tactisch niveau de ISO. Voor de CISO-functie is de organisatie voornemens de huidige beleidsmedewerker informatiebeveiliging op deze functie te plaatsen.
Per 1 maart 2018 is de ISO in dienst getreden. Daarnaast wordt de provincie verplicht met ingang van de AVG tot het instellen van een Functionaris Gegevensbescherming (FG). In de boardletter 2016 werd vermeld dat het aanstellen van een FG voor eind 2016 op de planning stond. De rekenkamer constateert dat dat er echter niet van is gekomen.
Najaar 2017 werden PS gevraagd het OKB op te hogen met 1 fte voor de aanstelling van een FG. PS gingen daarmee akkoord en er is een functieprofiel opgesteld voor de FG.
De werving van de FG is voorjaar 2018 gestart. De nieuwe CIO zal deelnemen in de sollicitatieprocedure voor de FG-functie, zo is aangegeven.

Naast deze functies voeren ook andere medewerkers werkzaamheden uit voor informatieveiligheid, bijvoorbeeld ICT-beheer die onder andere verantwoordelijk zijn voor het draaien van updates (patches), het dienstenplein die onder andere de beveiligingsincidenten registreert en alle andere medewerkers omdat bij het integrale werken ook informatiebeveiliging mee dient te worden genomen. Het is onbekend om hoeveel fte dit gaat, omdat het slechts een klein onderdeel is van de werkzaamheden van deze medewerkers.

## 3.9 Organisatie

### Eigenaren informatie(voorzieningen)

De primaire verantwoordelijkheid voor de informatiebeveiliging en classificatie (extern openbaar, intern openbaar, vertrouwelijk) ligt bij de eigenaar van de informatie. Proces- en programma-eigenaren zijn, geassisteerd door I-discipline medeverantwoordelijk om informatievoorzieningen binnen de kaders, waaronder die voor beveiliging in te richten.
Uit de bestudeerde documenten en gesprekken blijkt dat het doortrekken van de verantwoordelijkheden in de lijn/tot op medewerkersniveau, in de praktijk nog aandacht behoeft (zie onder andere paragraaf 3.2).

### Portefeuillehouder

Gedeputeerde Van der Maat is portefeuillehouder informatie(beveiliging).

### Gedeputeerde Staten

GS zijn verantwoordelijk voor het informatiebeleid en dienen daartoe de visie op informatiebeleid vast te stellen. De rekenkamer constateert dat GS hieraan invulling hebben gegeven met de kadernota, de *nota Digitale Duurzaamheid* en daarmee ook indirect de *Visie en hoofdlijnen informatiebeleid.* De ambtelijke organisatie geeft invulling aan de uitvoering.

### Directieraad

In het informatiebeveiligingsbeleid staat dat de directieraad/algemene directie zorgdraagt voor het uitdragen van het informatiebeveiligingsbeleid naar alle medewerkers en

bestuurders. Uit de bestudeerde documenten en gesprekken blijkt dat hieraan invulling is gegeven, maar dat dit 'continu' en blijvend aandacht verdient (bewustwording). In de kadernota staat dat de directieraad eindverantwoordelijk is voor handhaving van de kaders.

### Chief Information Officer (CIO)

In de kadernota is vastgelegd dat ook de CIO verantwoordelijk is voor het informatie(beveiligings)beleid en de uitvoering daarvan. Daarin is ook gekozen om de CIO-rol bij de directeur Bedrijfsvoering en Financiën te beleggen. Bij de bespreking van de kadernota in maart 2013 geven GS naar aanleiding van vragen vanuit PS (waaronder dat het een zware functie is voor een parttime CIO) aan dat er bewust voor is gekozen om van de CIO géén aparte functie te maken in het licht van de organisatieontwikkeling en de daarmee gepaard gaande verkleining van de directie(raad) en het feit dat het op directieniveau geen fulltime uit te voeren taken vraagt. Verder wordt opgemerkt dat deze rol expliciet in de functieomschrijving van de directeur Bedrijfsvoering wordt opgenomen, omdat de CIO-rol wel specifieke kennis en competenties vraagt.

Per 1 september 2013 trad een nieuwe directeur Bedrijfsvoering en Financiën in dienst die, conform het GS-besluit uit november 2012/kadernota, ook de rol van CIO ging vervullen en dit tot 1 december 2015 heeft gedaan. Vanuit de ambtelijke organisatie is aangegeven dat in eerste aanleg bij de CIO om aandacht moest worden gevraagd voor informatiebeveiliging, omdat het een nieuw vakgebied betrof. Sinds het op de agenda van de CIO is geland, heeft de beleidsmedewerker informatiebeveiliging veel contact gehad met de CIO, zo wordt gesteld. De strategische kant sneeuwde bij de 1e CIO onder, door de vele andere taken van de directeur.
Na het vertrek van deze CIO in december 2015 zijn de taken voor korte periode overgenomen. Doordat deze vervanging slechts een relatief korte periode betrof, heeft het oppakken van onderwerpen als dataprivacy, enige vertraging opgelopen.

Eind september 2016 heeft de algemeen directeur de CIO-rol op zich genomen en heeft deze tot december 2017 ingevuld. De algemeen directeur wilde dat de CIO-rol op directieniveau belegd bleef om strategisch te kunnen adviseren over I. Omdat de directie op dat moment maar uit één persoon bestond, heeft de algemeen directeur deze taak opgepakt. De CIO was lid van de directie en het centraal managementteam. Hiermee, zo wordt gesteld, was sturing op informatievoorziening op deze niveaus geborgd, zoals door de rekenkamer aanbevolen bij het onderzoek naar strategisch informatiebeleid. De strategische kant kreeg bij deze 2e CIO meer aandacht dan bij de 1e CIO, maar het bleef lastig door de vele andere taken van de algemeen directeur. In 2017 had de CIO het voornemen om monitoring en handhaving op te pakken.

In juni 2018 treedt de nieuwe CIO in dienst. Tot die tijd is de CIO-taak belegd bij de nieuwe algemeen directeur die in december 2017 in dienst trad, en worden de stukken aan de directie voorgelegd. Uit het functieprofiel van de nieuwe CIO blijkt onder andere dat deze integraal verantwoordelijk is voor het strategische informatiebeleid en het strategische informatiemanagement, sturing dient te geven aan de operationalisatie en implementatie van de visie en strategie, zorg dient te dragen voor kaderstelling en richtlijnen, de onderlinge samenhang dient te bewaken en dient toe te zien op naleving, zodat

concernbreed op uniforme en professionele wijze samengewerkt kan worden. De nieuwe CIO is een puur adviserende functie die onafhankelijk zal worden uitgevoerd onder de algemeen directeur. De CIO zal gevraagd en ongevraagd de algemeen directeur mogen adviseren; contact met GS dient via de algemeen directeur te verlopen. De nieuwe CIO zal zijn aandacht volledig op I-taken kunnen richten, omdat het nu een eigenstandige (fulltime) functie betreft. Het is de bedoeling dat de CIO echte doorzettingskracht/macht zal hebben (monitoring en handhaving), maar dit moet na indiensttreding van de nieuwe CIO nog worden vormgegeven. Door de nieuwe CIO anders te positioneren, waarbij een eigenstandig mandaat is voorzien en zelfstandig takenpakket, kunnen structuren sneller worden opgezet en besluiten sneller worden genomen, zo wordt verondersteld. De CIO zal eveneens agendalid worden/blijven van de directie.
In een statenmededeling van 25 september 2017 wordt gesteld dat een van de eerste taken van de nieuwe CIO is, de hoofdlijnen van het Informatiebeleid en de ICT-strategie in het licht van nieuwe ontwikkelingen te herijken, waaronder de provinciale inzet rondom informatieveiligheid, privacy, gegevensbescherming en e-dienstverlening.

Desgevraagd heeft de toenmalige CIO in november 2017 tegenover de rekenkamer aangegeven dat ze de nieuwe CIO wil meegeven dat het goed zou zijn om de I-visie nog eens tegen het licht te houden (te actualiseren), weer eens met een fris timmermansoog naar het projectenportfolio te kijken en als organisatie meer ontvankelijk te zijn voor externe ontwikkelingen (voelhoorns zijn te weinig op buiten gericht) en daarvoor weerbaarheid te ontwikkelen.

### ICT-kernteam (IKT)

In 2010 is het ICT-kernteam (IKT)geformeerd dat tot medio 2015 goedkeuring moest geven voor de start van iedere fase van een project en kende budget toe voor de uitvoering van de fase; het toetste en besloot over voortgang en afstemming met andere projecten. Het IKT keek vooral naar het tactisch portfoliomanagement en bestond uit een dwarsdoorsnede van de I-kolom (vertegenwoordigers van het architectuurteam, I-control, projectenbureau en ICT-beheer en demandmanagement, de voorzitter was namens de directie gemandateerd om besluiten te nemen).
Het IKT is als zodanig niet meer actief, de taken zijn anders belegd: via een portfolio- en projectteam. In het portfolioteam zit architectuur, informatiebeveiliging, I-control, dataprivacy, een adviseur concernteam en demandmanagement. Vooralsnog is besloten dat beleidsafdelingen die om I&I-oplossingen/projecten vragen, samen met een informatieadviseur hun behoeften vastleggen in een opdrachtformulier genaamd i-OG/ON-formulier. Dit formulier wordt voorzien van een advies van het portfolioteam en, op verzoek van de directie, ook van concerncontrol en het concernteam. Na instemming van de CIO met het i-OG/ON-formulier wordt een businesscase opgesteld, welke na beoordeling en goedkeuring projectmatig in uitvoering wordt genomen en niet meer terugkomt in het portfolioteam.

### I-board

In januari 2014 werd het centraal managementteam gevraagd om in te stemmen met het opstellen van een IT-Governance Board. Desgevraagd is vanuit de ambtelijke organisatie aangegeven dat dit is uitgesteld door verschillende managementwisselingen. Pas na een

vergelijkbare vraag uit december 2014 werd ingestemd en is in januari 2015 een I-board ingevoerd die naast het IKT werd geplaatst. In maart 2015 is deze in gebruik genomen met een brede afvaardiging vanuit/dwarsdoorsnede van de organisatie (vanuit de beleidskant twee directeuren, twee lijnmanagers en een programmamanager, de CIO, concerncontroller, IT-controller en afvaardiging MT-I). De board werd voorgezeten door de clustermanager I&I. Doel was om op deze wijze de organisatie te betrekken bij strategische afwegingen en de I-board had daarmee een bredere rol dan het IKT. De I-board kwam ongeveer een keer per maand bij elkaar.
In december 2017, met het vertrek van de 2e CIO, werd de I-board ontbonden. De I-board had enkel een adviesfunctie, de CIO nam de besluiten. De board adviseerde de CIO over de strategische inzet van ICT (I-projectportfoliomanagement/poortwachter), onder andere door te beoordelen of projecten aansluiten bij de provinciale doelstellingen en projecten te prioriteren (herinvoering vroegere projectenportfolio waarmee werd gewerkt voor invoering van de routekaart uit de kadernota). Ontwikkelingen op het gebied van ICT en beveiliging en het projectenportfolio werden kritisch gevolgd. De I-board en daarmee de CIO zijn verantwoordelijk voor het I-projectportfoliomanagement. In de evaluatie van de kadernota werden kanttekeningen geplaatst bij de beperkte ICT-achtergrond van de CIO en I-board. Uitvoering van een opleidingsplan moest zorgen dat ze voldoende kundig werden en bleven voor hun taak. De impact van de I-board zakte ook enige tijd weg na het vertrek van de 1e CIO, toen er een tijdje geen CIO om tafel zat.

### Managers I&I

Inhoudelijk wordt de CIO ondersteund door de programmamanager informatiebeleid van de eenheid I&I waar per juli 2013 de I-activiteiten zijn ondergebracht.
Deze programmamanager is in 2017 gedelegeerd opdrachtgever geweest voor fase 1 van het dataprivacy-traject, omdat de 2e CIO door de vele andere taken, niet overal opdrachtgever voor kon zijn.
De clustermanager I&I heeft een direct hiërarchische lijn met de algemeen directeur die ook de rol van CIO uitvoert en ze hebben frequent overleg (tweewekelijks).

### Beleidsmedewerker informatiebeveiliging

Op het gebied van informatiebeveiliging wordt de CIO geadviseerd door de beleidsmedewerker informatiebeveiliging.
In het informatiebeveiligingsbeleid staat dat de directeur Bedrijfsvoering verantwoordelijk is voor de revisie van het beleid. De rekenkamer constateert dat het informatiebeveiligingsbeleid in elk geval op dit punt aanpassing behoeft, omdat de CIO-functie ondertussen niet meer belegd is bij de directeur Bedrijfsvoering. In de onderhanden zijnde actualisatie van het informatiebeveiligingsbeleid zou voor een meer tijdsonafhankelijkere term kunnen worden gekozen: CIO.
In het informatiebeveiligingsbeleid staat eveneens, dat het onderhoud/de actualisatie van het beleid door de directieraad is belegd bij de beleidsmedewerker informatiebeveiliging. Deze coördineert de revisie en is penvoerder. Ook stelt hij de informatiebeveiligingsplannen op en betrekt daarbij alle directies die bij de uitvoering van de plannen een rol spelen. Tevens is hij verantwoordelijk voor het (laten) registreren van beveiligingsincidenten in de incidentenregistratie bij het dienstenplein. Bij nieuwe niet eerder opgetreden incidenten coördineert hij de afhandeling van het incident en daarbij het beperken van de schade en

verzorgt hij de evaluatie. Bij ernstige incidenten rapporteert hij rechtstreeks aan de CIO en indien nodig aan het Nationaal Cyber Security Centrum (NCSC). Ook stelt hij tweemaal per jaar de rapportage informatiebeveiliging voor de CIO op. De CIO bepaalt (op basis van deze rapportage) of de gedelegeerde verantwoordelijkheid voor informatiebeveiliging naar behoren wordt ingevuld.
Uit de bestudeerde documenten en gesprekken blijkt dat de beleidsmedewerker informatiebeveiliging aan de meeste taken, zoals omschreven in het beleid, invulling geeft. Een uitzondering daarop zijn informatiebeveiligingsplannen en de halfjaarlijkse rapportage informatieveiligheid, die niet als dusdanig maar op een andere wijze worden ingevuld.
Ten tijde van het rekenkameronderzoek werd het informatiebeveiligingsbeleid geactualiseerd. Vanuit de ambtelijke organisatie is aangegeven dat direct na indiensttreding van de nieuwe CIO, deze een conceptversie zal ontvangen van het geactualiseerd informatiebeveiligingsbeleid en het opgestelde privacybeleid.
De beleidsmedewerker informatiebeveiliging vervulde naast de taken voor informatieveiligheid, tot begin 2018 ook de taak van FG. De functie was lang kwetsbaar doordat veel taken bij één persoon waren belegd, zonder goede achtervang. Zoals eerder gemeld, is er in 2017 voor gekozen om de functie op te splitsen in twee nieuwe functies. De organisatie is voornemens de strategische CISO-functie te laten invullen door de huidige beleidsmedewerker informatiebeveiliging en per 1 maart 2018 is de ISO in dienst getreden. De nieuwe CIO zal na indiensttreding de sollicitatieprocedure voor de FG-functie moeten oppakken, zo is aangegeven.
De ISO is onder andere verantwoordelijk voor het opstellen van uitvoeringsbepalingen, procedures en instructies die in beleid zijn benoemd, het uitvoeren van risicoanalyses en het coördineren van awarenesscampagnes en hij controleert, registreert, adviseert en geeft voorlichting. De ISO rapporteert aan de CISO. De CISO rapporteert aan de directie/CIO en valt onder de CIO welke onder de algemeen directeur valt, is opdrachtnemer van de strategische opdracht informatieveiligheid, verantwoordelijk voor onder andere het strategische informatiebeveiligingsbeleid, zorgt daarbij voor kaderstelling en richtlijnen en ziet toe op implementatie en naleving ervan en voor het functioneel richting geven aan de ISO.
De FG rapporteert evenals de CISO aan de directie/CIO. Doel is hetzelfde als bij de CISO maar betreft dan het dataprivacybeleid in plaats van het informatiebeveiligingsbeleid. Naast het opstellen van het beleid is de FG ook verantwoordelijk voor onder andere afhandelen van klachten over gebruik persoonsgegevens, inventariseren gegevensbewerkingen en dergelijke. De FG fungeert namens de directie als een onafhankelijk toezichthouder vanuit de Wbp en de AP (vooruitgeschoven post van de AP).

De provincie gaat nu een nieuwe fase in met een nieuwe algemeen directeur, een nieuwe CIO en de functie van CISO, ISO en FG. Alles wordt daarmee vernieuwd en de nieuwe algemeen directeur en CIO zullen moeten besluiten hoe het wordt ingericht.

### Control

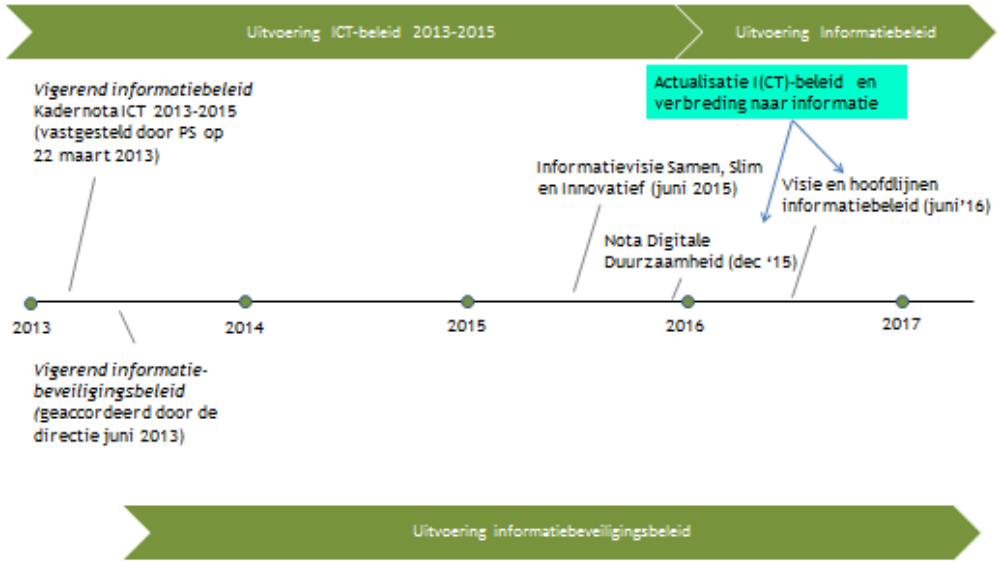
In het informatiebeveiligingsbeleid staat dat de accountant of de concerncontroller jaarlijks de implementatie van het beleid evalueert. Het is de accountant die jaarlijks de IT-omgeving en daarmee de informatiebeveiliging beoordeelt (zie paragraaf 3.5).

De eenheid Concerncontrol & Auditing is in 2014 gecentraliseerd om een onafhankelijkere positie te verkrijgen en valt sindsdien onder de algemeen directeur. De concerncontroller is onafhankelijk en mag rechtstreeks contact opnemen met GS, als het nodig wordt geacht om de algemeen directeur te passeren. Informatieveiligheid maakt geen onderdeel uit van het takenpakket van de eenheid. Wel wordt het meegenomen in de integrale en risicogerichte aanpak die de controllers hanteren bij het geven van advies over besluitvormingsdocumenten richting GS en in audits. De inzet is vooral gericht op het interpreteren van aandachtspunten, risico's en behoeften. De concerncontroller zat in de I-board. De verantwoordelijkheid voor het in kaart brengen van risico's en het eventueel treffen van beheersmaatregelen is belegd in de programma's. De risicomanager binnen concerncontrol vervult de rol van aanjager richting de organisatie in het vergroten van het risicobewustzijn.

De IT-controller is organisatorisch geplaatst binnen de I-kolom vanwege het belang om goed zicht te houden op IT-activiteiten en uitvoering daarvan. Hij zou een onafhankelijke positie moeten hebben, maar die is er nu niet. De IT-controller richtte het projectportfoliomanagement (PPM) in, waarmee aan de voorkant de kaders, waaronder die van informatiebeveiliging, dienen te worden geborgd.
Hij maakte deel uit van de I-board en is voor risicomanagement aangesloten bij concerncontrol. De IT-controller is bezig met dataprivacy, I-governance (onder andere in relatie tot de nieuwe topstructuur) en ondersteuning/advies CIO, strategisch risicomanagement, I-benchmarks en op dit moment ook met het sourcingtraject.

### Provinciale Staten

Conform de kadernota zijn PS in het kader van hun controlerende rol via de reguliere planning & controlcyclus op hoofdlijnen geïnformeerd over het informatiebeleid (dat beveiliging omvat, 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 Noord-Brabant in de praktijk. 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 engineering-aanvallen;
- inzicht te krijgen in de risico’s en kwetsbaarheden met betrekking tot de onderzochte systemen, panden (het provinciehuis) 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 provinciehuis 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 @brabant.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 provinciehuis en welke informatie ze daarbij kunnen vinden. De mysteryguest heeft zonder voorkennis en toestemming op twee dagen het beveiligde deel van het provinciehuis proberen binnen te komen en daarbij enkele met malware geprepareerde USB-sticks achtergelaten. Voor de inlooptest is een vrijwaring van de provincie ontvangen.

De penetratietest heeft plaatsgevonden in de periode van 6 juni tot en met 10 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 6 juni tot en met 21 juli.
Tijdens deze test is naar aanleiding van een kritieke bevinding ook de beleidsmedewerker informatiebeveiliging 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 beleidsmedewerker informatiebeveiliging 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 4 tot en met 8 september. Tijdens deze testen is er nauw contact geweest met de beleidsmedewerker informatiebeveiliging. Op 26 en 28 september hebben de inlooptesten plaatsgevonden, op 9 oktober volgde het phishingonderzoek en op 9 en 10 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 28 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.[12] 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 dan wel nog niet aanwezig waren.

[12] *Rapportage Penetratietest Provincie Brabant* van Hoffmann Cybersecurity.

## 4.2 Bevindingen/Resultaten technisch onderzoek

### 4.2.1 De systemen

**Externe toegankelijkheid vanaf het internet**

Het aantal kwetsbaarheden dat is aangetroffen tijdens het externe beveiligingsonderzoek vanaf het internet is laag. Van de 11 bevindingen heeft het gespecialiseerde bureau er echter wel twee als kritiek geclassificeerd. Van de overige bevindingen hebben er drie een hoog risico, twee een gemiddeld risico en vier een laag risico.

De meest opvallende kritieke bevinding was de aanwezigheid van een webshell op één van de servers van de provincie. Een webshell is een “achterdeurtje” waarmee de hacker via een browser communiceert met, in dit geval, de server en deze bestuurt. De webshell werd aangetroffen nadat een andere kwetsbaarheid (met een hoog risico)[13] op het systeem was aangetroffen waardoor er in beperkte mate toegang kon worden verkregen tot dit systeem. Er is geconstateerd dat de aangetroffen webshell sinds eind januari 2016 aanwezig was op het desbetreffende systeem en draaide met dermate hoge privileges dat dit een kritiek risico vormde. Deze bevinding is na ontdekking dan ook direct gemeld aan de provincie. De provincie heeft vervolgens meteen een gespecialiseerde partij ingeschakeld om een onafhankelijk forensisch onderzoek naar deze bevinding te laten uitvoeren. In overleg met deze partij heeft de provincie ook direct het betreffende systeem uitgeschakeld (‘uit de lucht gehaald’). Uit het forensisch onderzoek en na interne controle, zo heeft de provincie aangegeven, is gebleken dat de aanwezigheid van deze webshell tot gevolg had dat onbevoegden gebruik konden maken van de rekencapaciteit van de betreffende server (de webshell is gebruikt om een bitcoinminer te installeren) en de informatie konden inzien die op de server stond. Er is, zo stelt de provincie en de door haar ingeschakelde partij, geen onbevoegde toegang geweest tot vertrouwelijke informatie van de provincie, daar het betreffende systeem alleen openbare informatie bevatte.

De andere kritieke bevinding behelst dat het tijdens het externe onderzoek is gelukt om toegang te krijgen tot alle (provinciale) gegevens waartoe een betreffende medewerker toegang had. Hiertoe zijn eerst uit openbare documenten die via de website van de provincie (www.brabant.nl) in te zien en te downloaden zijn, e-mailadressen van provinciale medewerkers achterhaald (laag risico). Het is vervolgens gelukt om, in een beperkt aantal pogingen, van één van deze e-mailadressen het wachtwoord te achterhalen. Hiervoor is een aantal eenvoudige/voorspelbare wachtwoorden geprobeerd, waarvan er één geldig bleek (eenvoudig/voorspelbaar wachtwoord, hoog risico). Met de betreffende gegevens (e-mailadres en wachtwoord) was het mogelijk om in te loggen op de webmailomgeving van de desbetreffende medewerker (geen two-factor authenticatie op webmail; hoog risico). In de mailbox werden voor deze medewerker ook de SMS-toegangscodes voor de two-factor inlogprocedure voor de thuiswerkplek (Citrix) afgeleverd (in combinatie met voorgaande bevindingen: kritiek risico). Zodoende kon met de inloggegevens van de medewerker op de remote werkplek worden ingelogd en was het mogelijk om gegevens in te zien waartoe deze medewerker toegang had.

[13] De website bleek kwetsbaar voor zogenaamde ‘XXE-injectie’ waardoor interne systemen konden worden bevraagd en ook bestanden op het systeem konden worden gelezen.

### Interne test/toegankelijkheid

De interne beveiligingstest is uitgevoerd vanaf een kantoor met twee werkplekken in het medewerkersgedeelte van het provinciehuis. Deze was door de provincie voor het onderzoek ter beschikking gesteld. Het kantoor gaf toegang tot het netwerk en de aanwezige thinclients. Het eerste deel van de interne test is uitgevoerd 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 20 bevindingen gedaan, Hiervan heeft het gespecialiseerde bureau er drie als kritiek geclassificeerd. Van de overige bevindingen hebben er zes een hoog, vier een gemiddeld en vier een laag risico en zijn er drie informatieve bevindingen.

Tijdens het eerste deel van de interne test is het door middel van het achterhalen van de gegevens van een domeinaccount op een van de thinclients uiteindelijk gelukt om beheerdersrechten te verkrijgen. Daarnaast is een wachtwoord van een ander beheerdersaccount gekraakt uit een hash[14]. Hoewel de serviceaccounts in het algemeen zeer sterke wachtwoorden bleken te hebben, was dit wachtwoord te zwak. De lengte van het wachtwoord was met negen karakters kort en gebaseerd op een woordenboekwoord, welke het wachtwoord voorspelbaar en relatief eenvoudig te kraken maken. Met de verkregen beheerdersrechten (privileges) was er toegang tot vrijwel alle gegevens en bestanden van de provincie. Zo was het mogelijk om vertrouwelijke informatie in te zien van onder andere de griffie, de directie en de Zuidelijke Rekenkamer. Tijdens dit eerste deel van de interne test is verder bijvoorbeeld ook een groot aantal systemen en applicaties aangetroffen die niet meer ondersteund worden door de leverancier en/of die verouderd waren (beschikbare beveiligingsupdates (patches) 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.
Tijdens het tweede deel van de interne test is gebruik gemaakt van het testaccount. Bij deze test zijn diverse accountgegegevens (gebruikersnamen en wachtwoorden) in scripts aangetroffen, waaronder van accounts met hoge (beheerders)privileges. Een (kwaadwillende) gebruiker op het netwerk kan hierdoor, indien in het bezit van voldoende kennis, relatief eenvoudig zijn of haar privileges verhogen of gegevens inzien waar hij of zij normaal gesproken geen autorisatie toe heeft. De combinatie met de bevindingen uit de externe test, waarbij met een geraden wachtwoord toegang werd verkregen tot een virtuele desktop, maakt dat dit een nog groter risico is. Immers, een kwaadwillende die op eenzelfde wijze, vanaf het internet, toegang verkrijgt, kan vervolgens ook bij de scripts met logingegevens/wachtwoorden komen.

Met de diverse achterhaalde accounts en het testaccount was er toegang tot gedeelde mappen waarin zich onder andere ook logingegevens bevonden voor de Corsa-database, het documentregistratie(- en archief)systeem van de provincie. Met deze gegevens kon toegang verkregen worden tot deze database, buiten de reguliere Corsa-webinterface om.

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

Desgevraagd heeft de provincie aangegeven dat door middel van deze toegang ook daadwerkelijk alle niet-vertrouwelijk gekwalificeerde gegevens in Corsa konden worden ingezien; het Corsa-systeem is op dit moment ingericht volgens het uitgangspunt van de organisatie dat alle informatie voor medewerkers toegankelijk is tenzij (uitgezonderd informatie zoals Bibob en personeelsgegevens welke extra afgeschermd zijn).
Het aantal kwetsbare systemen dat is aangetroffen, was laag ten opzichte van het totaal aantal systemen en de systemen waarover controle is verkregen via kwetsbare software waren dermate gehardened[15] dat dit niet direct geleid heeft tot hogere privileges. De accounts waaronder de kwetsbare diensten draaien hadden gelimiteerde privileges waardoor de directe impact beperkt bleef. Ook had tenminste één van deze accounts een dermate sterk wachtwoord, dat het vrijwel uitgesloten is dat dit vanuit een hash gekraakt had kunnen worden. Dit wachtwoord is echter op een andere wijze achterhaald.

Tijdens de interne test is het ook mogelijk gebleken om op de begane grond van het provinciehuis een laptop te verbinden met een netwerkpoortje waarop een presentatiescherm (hippo) was aangesloten. De ruimte was vrij toegankelijk voor publiek. Op deze wijze kon dezelfde netwerktoegang worden verkregen als binnen de, voor het onderzoek ter beschikking gestelde, kantoorruimte. Een kwaadwillende zou deze ingang kunnen gebruiken om kwetsbare systemen proberen aan te vallen. Tevens zou een kwaadwillende, die logingegevens heeft verkregen via bijvoorbeeld phishing, de two-factor authenticatie voor de virtuele werkplek kunnen omzeilen door zich via deze weg op het netwerk aan te melden. Vanuit de provincie is aangegeven dat de provincie op de hoogte is van de potentiële netwerktoegang vanuit de publieke ruimte, dat er reeds een traject was gestart om deze situatie te verbeteren en het op dit moment niet langer mogelijk is om via de betreffende poorten toegang te verkrijgen tot het interne netwerk.

#### 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. Van het wifi-netwerk voor medewerkers, het zakelijke wifi, is een zogenaamde ‘WPA handshake’ onderschept die gebruikt kan worden om het wifi-wachtwoord te achterhalen. Een aanval op deze handshake heeft tijdens de test echter geen succes gehad. Deze bevinding is dan ook als informatief geclassificeerd.

### 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 @brabant.nl. Dit waren 1.791 emailadressen. De aanval heeft er toe geleid dat 36 ontvangers van de e-mail hun gebruikersnaam en wachtwoord invulden op een, voor dit onderzoek geprepareerde website. De aanval is door de provincie gedetecteerd, 19 minuten nadat een technisch beheerder de mail had ontvangen is door hem een waarschuwingsmail verstuurd naar de medewerkers van de provincie en is de besmette link in het e-mailbericht geblokkeerd.

[15] Hardening: het weerbaar maken; het toepassen van maatregelen op de configuratie van een systeem zodat de impact van aanvallen, als die in eerste instantie slagen, beperkt blijft.

Ook zijn er twee spear phishingaanvallen uitgevoerd, waarbij geselecteerde emailadressen een met malware geïnfecteerde bijlage kregen toegestuurd. De eerste spear phishingaanval via e-mail is niet geslaagd, omdat documenten correct werden geblokkeerd. De aanval met een zogenaamd “Wob-verzoek” via een vragenformulier op de website van de provincie is geslaagd. Hierdoor is op een tweetal systemen toegang tot het account van een medewerker verkregen en gevoelige informatie toegankelijk geworden.

Tenslotte heeft op twee dagen een inlooptest plaatsgevonden. Op beide dagen heeft de mysteryguest ongeautoriseerd toegang tot werkplekken, systemen en vertrouwelijke gegevens verkregen, onder andere op de kamer van de medewerkers van burgemeestersbenoemingen (kamer met de naam “Burgemeesterszaken”) die zich bevindt in het bestuurdersgedeelte van het provinciehuis. Over de met malware geprepareerde USB-sticks die door de mysteryguest zijn achtergelaten, is niets vernomen. Desgevraagd is vanuit de provinciale organisatie aangegeven dat de gedropte USB-sticks niet bruikbaar zijn binnen de provincie, omdat dat met maatregelen is afgevangen: alleen ‘provinciale USB-sticks’ werken/zijn te gebruiken.

## 4.3 Getroffen maatregelen

Zoals 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. Deze zijn vervolgens, zo is vanuit de ambtelijke organisatie aangegeven, binnen I&I besproken met de betreffende verantwoordelijken: de beleidsmedewerker informatiebeveiliging, de opdrachtgever ICT-beheer & projecten, de opdrachtnemer ICT-beheer en de betreffende beheerders. Tevens is het rapport besproken met de algemeen directeur/CIO. De bevindingen zijn daarna uitgezet onder de verantwoordelijken en zij hebben deze opgepakt. De aangetroffen kwetsbaarheden zijn door de provincie daar waar mogelijk direct opgelost en eind januari 2018 was 80-90% opgelost, zo wordt gesteld. Daarbij wordt door de provincie aangegeven dat sommige lastiger zijn op te lossen dan anderen en nog tijd vergen. Voor wat betreft two-factor authenticatie voor webmail wordt aangegeven dat naar aanleiding van het beveiligingsonderzoek uit 2014 is overwogen om dit in te voeren. Omdat dit volgens de organisatie een te grote impact had op de gebruiksvriendelijkheid voor de werknemers, is destijds door de CIO besloten om af te zien van invoering. Dit is gebeurd op basis van een zogenoemde risicoacceptatie. Omdat de rekenkamer dit risico nu wederom constateerde, heeft de CIO het advies van de beleidsmedewerker informatiebeveiliging overgenomen om de two-factor authenticatie in te voeren voor webmail.brabant.nl.

De provincie constateert, de bevindingen van de verschillende beveiligingsonderzoeken vergelijkend, dat er een inhaalslag is gemaakt op het gebied van technische informatiebeveiliging. Zoals reeds eerder vermeld, had de provincie begin 2017 zelf ook de toegankelijkheid van haar systemen laten testen door een externe partij en bleken veel bevindingen hetzelfde te zijn als in de twee jaar daarvoor uitgevoerde test. Begin 2017 is een taskforce opgericht om de bevindingen op te lossen, waaronder het versterken van wachtwoorden en het draaien van beveiligingsupdates. De rekenkamer constateert dat een half jaar later in haar onderzoek op een aantal punten weer vergelijkbare bevindingen zijn

gedaan, zoals beveiligingsupdates (patches) die niet waren gedraaid. Gevraagd naar redenen voor het aantreffen van vergelijkbare 'problemen'/bevindingen, is vanuit de ambtelijke organisatie aangegeven dat de updates niet gedraaid zijn door achterstallig onderhoud bij ICT-beheer. De follow-up van de bevindingen uit januari 2017 worden, zo is aangegeven, wekelijks besproken door de verantwoordelijken en de patches zouden eigenlijk één keer per maand moeten worden doorlopen, zoals begin 2017 is afgesproken om te borgen dat de geconstateerde problemen voortaan worden voorkomen. De rekenkamer constateert dat dit laatste niet is gelukt. Het uitvoeren van de betreffende updates en het toezicht daarop valt onder de verantwoordelijkheid van de opdrachtnemer ICT-beheer. De beleidsmedewerker informatiebeveiliging controleert periodiek door middel van externe audits of dit ook daadwerkelijk gebeurt. Op basis van de uitkomsten vindt dan bijsturing plaats.
Begin 2017 werd de provincie geattendeerd op wachtwoorden die niet aan de (inter)provinciale eisen van een wachtwoord voldeden, zoals 'welkom01'. Deze zijn, zo wordt gesteld, vervangen door complexe wachtwoorden. Ook is het nu zo dat, als een wachtwoord niet voldoet aan de eisen, het wachtwoord bij het wijzigen/instellen niet wordt geaccepteerd door het systeem en een ander wachtwoord moet worden gekozen dat voldoet aan de eisen. Sinds 28 juni 2016 zijn de eisen waarmee de provincie het gebruik van sterke wachtwoorden borgt, de volgende: regels qua complexiteit (minimaal 9 en maximaal 14 karakters, niet een deel van je (inlog)naam, 3 van de volgende eisen: 'minimaal 1 hoofdletter, minimaal 1 letter, minimaal 1 numeriek, minimaal 1 speciaal karakter'), geen hergebruik van wachtwoorden en wachtwoord is 70 dagen geldig. Daarmee is, zo is desgevraagd aangegeven, de verversingsdatum verkort. De door de rekenkamer aangetroffen wachtwoorden als 'Zomer2017!' voldoen wel aan de provinciale eisen, maar zijn voorspelbaar en relatief eenvoudig te kraken. De rekenkamer constateert dat, ondanks de aandacht die in 2017 onder andere in e-learnings is gevraagd voor het belang van sterke wachtwoorden, er wachtwoorden worden gebruikt die voorspelbaar en relatief eenvoudig zijn te kraken.

Wat betreft de phishingmail constateert de rekenkamer dat 36 ontvangers hun logingegevens 'weggaven', ondanks de maatregelen die op technisch gebied zijn genomen en de acties op het gebied van bewustwording die de provincie ongeveer een half jaar voor de aanval uitvoerde na een andere phishingsimulatie. De intentie is om zoveel mogelijk kwaadwillende mails op voorhand te blokkeren. Dagelijks worden zo'n 2.000 tot 3.000 phishingmails uit het mailverkeer gevist, zo wordt aangegeven. Indien er toch kwaadwillende mail in mailboxen wordt afgeleverd, zal deze na een melding via het dienstenplein en beoordeling door ICT-beheer alsnog worden verwijderd. De mailserver wordt dan opdracht gegeven om de betreffende mail te verwijderen uit de mailboxen. Dit verloopt op systeemniveau zonder tussenkomst van menselijk handelen. De rekenkamer constateert dat conform deze procedure is gehandeld. Nadat de phishingmails waren verwijderd, verscheen er ook nog een prikkelende waarschuwingsboodschap van ICT-beheer op het interne sociale netwerk van de provincie (Yammer). Overigens is de ervaring dat in de loop van de tijd minder mensen op dit soort mails reageert, zo is vanuit de ambtelijke organisatie aangegeven. In het eerste onderzoek waren het er 656, in het tweede 83, in het derde 47 en nu 36. Het kan, zo wordt gesteld, iedereen overkomen om op een link in zo'n mail te klikken, maar het wordt als kwalijk ervaren dat er toch nog zoveel mensen hun inlognaam en wachtwoord invulden.

# 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 de periode september 2012 tot en met eind 2017/begin 2018.

## 5.1 Rollen PS

Provinciale Staten hebben (in 2013) kaders vastgesteld voor informatiebeveiliging als onderdeel van het ICT-beleid (kaderstellende rol). Verder hebben ze (in de begrotingen) middelen toegekend voor de uitvoering van dit ICT-beleid (budgetrecht). Daarnaast is het de taak van PS om het door GS gevoerde bestuur te controleren en eventueel bij te sturen met behulp van de kaders. In het ICT-beleid (de kadernota) is vastgelegd dat PS toezicht houden op de realisatie van het ICT-beleid.

In de Nota Digitale Duurzaamheid (2015) stellen GS dat PS voor de duurzame toegankelijkheid van informatie een toezichthoudende rol hebben. In de Visie en hoofdlijnen provinciaal informatiebeleid (2016) stellen GS dat zij verantwoordelijk zijn voor het informatiebeleid, daartoe een visie op informatiebeleid vaststellen en dat PS daarvan en over de uitvoering kennis nemen op basis van hun controlerende rol.

Systemen van PS en fractiemedewerkers zijn gescheiden van de provinciale systemen. De griffie is bijvoorbeeld verantwoordelijk voor iBabs en de beveiliging daarvan. De eigenaar van de onderliggende software is verantwoordelijk voor het systeem.

## 5.2 Informatie aangeboden aan PS

De rekenkamer constateert dat PS via de kadernota zeer op hoofdlijnen zijn geïnformeerd over de kaders, uitgangspunten en governance voor informatiebeveiliging. Zo wordt wel gesteld dat de provincie wetgeving en afspraken wil naleven, maar er wordt geen inzicht gegeven in de inhoud daarvan.
De rekenkamer constateert dat PS daarnaast, zoals vastgelegd in de kadernota, met ingang van 2013 via de reguliere planning & controlcyclus zijn geïnformeerd over de doelstellingen en de uitvoering van het ICT-beleid. In de paragraaf Bedrijfsvoering van de begrotingen en jaarstukken wordt in het algemeen op een hoog aggregatieniveau ingegaan op met name (de mate van realisatie van) de ICT-ambitie en speerpunten uit de kadernota: basis op orde (houden) en daarna actief volger van ICT-ontwikkelingen, digitaal werken en bij de basis op orde de governance/CIO. Vaak betreft het procesachtige informatie: er wordt bijvoorbeeld melding gemaakt dat er beleid is, de CIO-functie is ingevuld, de governance verder is geprofessionaliseerd met oprichting van de I-board en dat het beleid grotendeels is gerealiseerd, maar er wordt in het algemeen niet aangegeven wat er nog niet is gerealiseerd en wat nog (extra) aandacht vereist.

Ook is de informatie vaak alleen voor mensen met parate kennis van de beleidsvoornemens echt iets zeggend/begrijpelijk en wordt er specifiekere informatie gegeven in de jaarstukken dan in de begroting zodat de aansluiting lastig is te maken (wat is wel/niet gerealiseerd van wat werd beoogd).
Er wordt veelal niet specifiek ingegaan op informatieveiligheid en de kosten daarvan. Alleen in de jaarstukken 2013 wordt opgemerkt dat concrete acties zijn uitgewerkt in het kader van informatieveiligheid en wordt daarbij een voorbeeld genoemd, in de jaarstukken 2015 dat door bepaalde ontwikkelingen informatieveiligheid meer aandacht vraagt en in de jaarstukken 2016 dat informatieveiligheid meer aandacht heeft gekregen mede door nieuwe wetgeving en daarvoor ook een privacy impactanalyse is uitgevoerd om te kunnen bepalen in hoeverre wordt voldoen aan nieuwe wetgeving en welke verbeteracties nog nodig zijn.
In de kadernota wordt gesteld dat in de jaarstukken aandacht zal worden besteed aan de mate waarin de provincie beschikt over een ICT-beleid dat in de pas loopt met recente ontwikkelingen op dit gebied, de interne sturing en beheersing van de ICT-voorziening, het (externe) toezicht op de ICT-voorziening en de (vermindering van) externe inhuur. De rekenkamer stelt vast dat in de praktijk in de jaarstukken niet wordt ingegaan op het in de pas lopen van het beleid met recente ontwikkelingen, het (externe) toezicht en de vermindering van externe inhuur. In de jaarstukken tot en met 2016 wordt wel inzicht gegeven in de omvang van de inhuur van externe arbeidscapaciteit[16], maar dat betreft alle inhuur en niet specifiek de inhuur van externe arbeidscapaciteit voor ICT.

De accountant heeft, in opdracht van PS en zoals vastgelegd in de kadernota, jaarlijks aan PS gerapporteerd over zijn bevindingen op het gebied van informatieveiligheid.[17]
In de kadernota is eveneens vastgelegd dat PS in 2014 ook buiten de P&C-cyclus zullen worden geïnformeerd over de voortgang, dan een geactualiseerde versie ontvangen en dat er een eindevaluatie als afsluiting van de beleidscyclus zal worden uitgevoerd. De rekenkamer constateert dat PS eind 2014, eind 2015 en in juni 2016 via een statenmededeling en de onderliggende documenten zijn geïnformeerd over respectievelijk de resultaten en aanbevelingen van de tussenevaluatie en de eindevaluatie van het ICT-beleid en de notitie Visie en hoofdlijnen provinciaal informatiebeleid. De rekenkamer constateert verder dat PS via de evaluatierapportages van eind 2014 en eind 2015 en de boardletters 2014 en 2016 van de accountant inhoudelijk zijn geïnformeerd over de uitvoering van informatiebeveiliging binnen het ICT-beleid, maar niet over de kosten daarvan. De informatie in deze documenten is informatief en begrijpelijk. In 2014 hebben PS geen geactualiseerde versie van de kadernota ontvangen, zoals gemeld in de kadernota. De tussenevaluatie gaf daartoe geen aanleiding.
Vanuit de ambtelijke organisatie is aangegeven dat PS via de bevindingen van de jaarlijkse controle door de accountant worden geïnformeerd over de stand van zaken van informatieveiligheid en dat dat wat GS betreft voor nu voldoende informatie is. De bevindingen van de accountant zouden eventueel aanleiding moeten geven voor vervolgvragen: ‘piepsysteem’. Daarnaast worden PS niet geïnformeerd over informatieveiligheid, maar uiteraard wordt er wel op eventuele vragen van PS gereageerd zo wordt aangegeven.

PS hebben bij de bespreking van de kadernota in 2013 en de jaarstukken in 2015 vragen gesteld over het ICT-beleid, in 2013 ook aandacht gevraagd voor beveiliging en ICT-

[16] Zie ook het rekenkameronderzoek uit 2016 *Externe inhuur provincie Noord-Brabant*.
[17] Conform een aanbeveling van de rekenkamer uit 2012 (*Strategisch Informatiebeleid provincie Noord-Brabant*).

beveiliging als speerpunt aangewezen voor de accountantscontrole 2013. In 2014 werd naar aanleiding van recente hacks van overheidsites gevraagd naar de stand van zaken van de informatiebeveiliging. In 2017 zijn vanuit PS op verschillende momenten naar aanleiding van gebeurtenissen vragen gesteld die betrekking hadden op informatie-veiligheid. Zo werd ook toen bijvoorbeeld weer gevraagd naar de status van de informatieveiligheid.

Onderstaand wordt ingegaan op de documenten waarin PS geïnformeerd zijn over informatieveiligheid of beleid dat informatieveiligheid omvat dan wel raakt. De documenten zijn zoveel als mogelijk chronologisch weergegeven. In verband met de leesbaarheid wordt daarvan in een enkel geval afgeweken.

### Begroting 2012 (november 2011)

In de paragraaf Bedrijfsvoering van de begroting 2012 wordt aangegeven dat de technische basis van de ICT-voorziening wordt gemoderniseerd en het bestaande pakket van applicaties wordt gesaneerd. Gesteld wordt dat een beknopte I-visie met daarin de manier waarop de provincie wil inspelen op de digitalisering van de overheid voor het eind van 2011 ter kennis van PS zal worden gebracht. Digitalisering/informatiestrategie[18] is een van de speerpunten van GS uit het Uitvoeringsprogramma Tien voor Brabant 2011-2015.
In 2012 is € 9 miljoen beschikbaar voor informatisering en automatisering. Er is een reserve ICT-basisinfrastructuur en duurzame productiemiddelen. Conform eerdere besluitvorming is de (geraamde) inzet van middelen uit deze reserve:

| | Rekening | Begroting | | | | |
|---|---|---|---|---|---|---|
| | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 |
| Middelen uit de reserve ICT x € 1.000 | 3.920 | 5.000 | 5.530 | 4.125 | 3.993 | 3.963 |

De rekenkamer constateert dat er in deze begroting en de bespreking ervan in PS niet (expliciet) wordt ingegaan op informatieveiligheid en de geraamde kosten daarvan.

### Startnotitie Strategisch IT-beleid (2012)

In september 2012 besprak de commissie Economische Zaken en Bestuur (EZB) de *Startnotitie Strategisch IT-beleid*, werd gekozen voor de ICT-ambitie ‘eerst de basis op orde en daarna actief volger van ICT-ontwikkelingen mits onderbouwd door een goede businesscase’, en werd aan GS gevraagd in lijn daarmee een kadernota op te stellen.

### Boardletter 2012 (november 2012)

PS ontvingen najaar 2012 de *Rapportage interim-bevindingen controle 2012 Grip op financiële positie*. De accountant stelt dat naar aanleiding van een conclusie van de rekenkamer dat de governance van IT onvoldoende is geborgd, GS een startnotitie strategisch IT-beleid hebben opgesteld die wordt uitgewerkt in een kadernota en eerste stappen zijn gezet om de CIO-functie vorm te geven. Verder wordt aangegeven dat aansluitend bij een aanbeveling van de rekenkamer de IT-omgeving is beoordeeld. Deze wordt van voldoende niveau geacht om (de continuïteit) van de geautomatiseerde gegevensverwerking te waarborgen.
PS zijn via deze boardletter geïnformeerd over genomen stappen in het informatiebeleid.

[18] Tot de begroting 2013 wordt gesproken van informatietechnologie in plaats van informatiestrategie.

### Begroting 2013 (november 2012)

In de paragraaf Bedrijfsvoering van de begroting 2013 wordt aangegeven dat voor het speerpunt Informatiestrategie wordt ingezet op een versnelling in 2013. Daaraan wordt inhoudelijk invulling gegeven in de kadernota die begin 2013 aan PS zal worden voorgelegd, zo wordt gesteld. Als beleidsprestatie voor ICT wordt genoemd: basis op orde. Met als bijbehorende indicatoren: kadernota opgesteld in 2013, daarna uitvoering conform nota (2013-2015) en evaluatie in 2015. Voor 2013 is € 8 miljoen begroot.
De rekenkamer constateert dat ook in deze begroting en de bespreking ervan in PS niet (expliciet) wordt ingegaan op informatieveiligheid en de geraamde kosten daarvan.

### Kadernota ICT-beleid 2013-2015 (2013; vastgesteld door PS)

Op 1 maart 2013 werd de kadernota in de commissie EZB besproken. Een deel van de vragen die door PS werden gesteld, beantwoordden GS in een Memorie van Antwoord van 11 maart 2013. Deze betroffen onder andere de verantwoordelijkheden en positionering van de CIO (zware taak voor parttime CIO). Op 22 maart 2013 stelden PS de *Kadernota ICT-beleid 2013-2015* vast. De kadernota omvat ook de uitgangspunten voor informatiebeveiliging. Er wordt geen inzicht gegeven in de benodigde middelen voor informatiebeveiliging. De geraamde budgetten en fte's betreffen het ICT-beleid in totaliteit. Bij de bespreking werd vanuit PS onder andere aandacht gevraagd voor het belang van beveiliging van informatie en systemen en om een minder vrijblijvende aanpak van de bewustwordingsacties. Naast de kadernota ontvingen PS ter kennisname de *Uitwerking kadernota en speerpunten ICT-beleid 2013-2015*. GS stellen daarin dat omdat deze uitwerking de belangrijkste voornemens voor de uitvoering bevat, er geen noodzaak is om uitvoeringsprogramma's op te stellen voor PS.
De rekenkamer constateert dat PS via de kadernota zijn geïnformeerd over de kaders/uitgangspunten van informatiebeveiliging en dat er vanuit PS aandacht is gevraagd voor onder andere het belang van beveiliging, de verantwoordelijkheden en positionering van de CIO en de vrijblijvendheid van bewustwordingsacties.

### Jaarstukken 2012 (mei 2013)

In de inleiding en de paragraaf Bedrijfsvoering van de jaarstukken 2012 wordt gesteld dat het ICT-beleid in 2012 onder de loep is genomen en is aangescherpt, dat de startnotitie strategisch IT-beleid en de kadernota ICT-beleid in de commissie EZB zijn besproken en in dit beleid 'digitaal werken' en 'technische basis op orde' de twee speerpunten zijn. Ten aanzien van de kosten wordt aangegeven dat er sprake is van een zeer minimale overschrijding van de ICT-budgetten (0,8% = € 65.000).
De rekenkamer constateert dat er in dit jaarverslag en de bespreking ervan in PS niet (expliciet) wordt ingegaan op informatieveiligheid en de gerealiseerde kosten daarvan.

### Rapportage jaarrekeningcontrole 2012 (april 2013)

PS ontvingen in april 2013 het *Accountantsverslag 2012 Grip op financiële positie*. De accountant benadrukt daarin het belang van informatiebeveiliging (veranker ICT in beleid en governance, regel ICT-projectmanagement, informatiebeveiliging prominent op bestuurlijke agenda, zorg voor goede afstemming ICT-functie en gebruikers). Voor bevindingen over IT wordt verwezen naar de boardletter 2012.

### Informatiebeveiligingsbeleid (2013; niet PS)

Het *Informatiebeveiligingsbeleid* uit september 2013 dat een nadere uitwerking is van de

kadernota op het gebied van informatiebeveiliging is niet aan PS aangeboden, omdat het een verdere (tactische) invulling van de kadernota betreft en dit destijds werd gezien als een ambtelijke verantwoordelijkheid en bevoegdheid.

### Boardletter tussentijdse controle 2013 (oktober 2013)

PS ontvingen najaar 2013 de *Boardletter tussentijdse controle 2013 provincie Noord-Brabant*. De accountant stelt daarin onder andere dat de rol van ICT steeds duidelijker wordt gedefinieerd, de kadernota wordt gezien als een positieve ontwikkeling in de professionalisering van ICT en de rol van CIO belegd is. Voor de controle 2013 hebben PS ICT-beveiliging als speerpunt aangewezen. Gesteld wordt dat de eerste indruk is dat de beheerprocessen deels voldoen aan de daaraan gestelde eisen, zo is voor informatiebeveiliging beleid vastgesteld. Bij de punten ter verbetering van deze processen wordt onder andere opgemerkt dat gewerkt wordt aan een uitvoeringsplan dat aansluit op het informatiebeveiligingsplan en dat in het kader van informatiebeveiliging bij voorkeur gebruik wordt gemaakt van algemeen geaccepteerde standaarden. Aanbevolen wordt om de generieke IT-beheersmaatregelen zoals versiebeheer, logische toegangscontrole en back-up en recoveryprocedures te laten toetsen door interne audits.
PS zijn via deze boardletter geïnformeerd over het bestaan van het informatiebeveiligingsbeleid.

### Begroting 2014 (november 2013)

In de paragraaf Bedrijfsvoering van de begroting 2014 wordt aangegeven dat voor het speerpunt Informatiestrategie PS in 2013 de kadernota hebben vastgesteld, inclusief de uitvoeringsplannen voor onder andere ‘basis op orde’. In 2014 willen GS het technische gedeelte van ‘basis op orde’ afronden en invulling hebben gegeven aan de CIO-functie. Evenals in de begroting 2013 is de beleidsprestatie ICT: basis op orde. Met als bijbehorende indicatoren: kadernota opgesteld in 2013, daarna uitvoering conform nota (2013-2015), evaluatie in 2015, herziening kadernota in 2016 en uitvoering daarvan in 2017. Voor 2014 is € 7,7 miljoen begroot.
De rekenkamer constateert dat ook in deze begroting en de bespreking ervan in PS niet (expliciet) wordt ingegaan op informatieveiligheid en de geraamde kosten daarvan.

### Jaarstukken 2013 (mei 2014)

In de paragraaf Bedrijfsvoering van de jaarstukken 2013 wordt aangegeven dat PS in maart 2013 de kadernota ICT-beleid hebben vastgesteld en dat mede op basis van deze nota in 2013 met kracht is gewerkt aan de drie afgesproken speerpunten: het op orde brengen van de technische basis, bevorderen van het digitaal werken in de organisatie en het duurzaam digitaliseren van het archief. Ook wordt gesteld dat de verbetering van de technische ICT-basis op schema ligt. Over het Informatie/ICT-veiligheidsbeleid wordt opgemerkt dat er concrete acties zijn uitgewerkt, zoals het consequent laten testen van SAAS-oplossingen (software in de Cloud) op alle voor de provincie relevante veiligheidsaspecten. Dit heeft, zo wordt gesteld, zowel voor de provincie als de betrokken leveranciers toegevoegde waarde. Ten aanzien van de kosten ICT wordt aangegeven dat er sprake is van een overschrijding door het versneld uitvoeren van het programma Basis op orde. De hogere kosten worden afgedekt via de reserve Basisinfrastructuur en duurzame productiemiddelen (€ 1.226.000).

De rekenkamer constateert dat er in dit jaarverslag voor het eerst (expliciet) wordt ingegaan op (een specifiek onderdeeltje van) het informatiebeveiligingsbeleid, maar niet op de gerealiseerde kosten daarvan. In de bespreking in PS van de jaarstukken 2013 wordt niet ingegaan op informatieveiligheid.

### Rapportage jaarrekeningcontrole 2013 (april 2014)

PS ontvingen in april 2014 het document *Uitkomsten controle en overige informatie 2013*. De accountant heeft opzet, bestaan en werking onderzocht van IT-beheersmaatregelen en zich daarbij gericht op de applicatie SAP omdat deze van materieel belang is voor de jaarrekeningcontrole (provinciale processen worden voor een belangrijk deel ondersteund door SAP). Voor bevindingen over IT wordt verwezen naar de boardletter 2013. Benadrukt wordt dat geen integraal onderzoek is uitgevoerd naar het door PS meegegeven speerpunt ICT-beveiliging, maar dat dat zich heeft toegespitst op SAP. Aanbevelingen richten zich op gebruikersbeheer (toegangsbeveiliging: accounts en toegekende rechten en vastleggen van passwordparameters) en wijzigingsbeheer.

### Voorjaarsnota 2014 (juli 2014)

Naar aanleiding van onder andere de constatering dat begin 2014 veel overheidswebsites zijn gehackt, wordt bij de bespreking van de voorjaarsnota op 3 en 4 juli 2014 een motie ingediend. PS verzoeken GS te onderzoeken in hoeverre de informatiebeveiliging op orde is en PS daarover te informeren. De portefeuillehouder zegt toe te komen met een notitie over informatieveiligheid. De motie wordt ingetrokken.

### Boardletter tussentijdse controle 2014 (oktober 2014)

PS ontvingen najaar 2014 de *Boardletter tussentijdse controle 2014 provincie Noord-Brabant*. Evenals in 2013 zijn in 2014 de IT-beheerprocessen, het wijzigingsbeheer, de toegangsbeveiliging en de continuïteit van de gegevensverwerking van de applicatie SAP onderzocht. Ook nu wordt als aandachtspunt genoemd de toegangsbeveiliging van SAP. Verder wordt gesteld dat, mede naar aanleiding van rekenkameronderzoeken, diverse acties in gang zijn gezet voor het structureren van de aanpak en het verscherpen van de informatiebeveiliging binnen de organisatie. Genoemd worden: het afsluiten van een raamovereenkomst met een externe beveiligingsorganisatie die audits uitvoert en die de provincie scherp houdt op trends en ontwikkelingen die van invloed kunnen zijn op de beveiliging binnen de provincie, het vergroten van het beveiligingsbewustzijn bij medewerkers aan de hand van trainingen, het uitvoeren van audits en zogeheten mysteryguestbezoeken, het verplicht opnemen van informatiebeveiliging bij alle (IT gerelateerde) projecten, de betrokkenheid van de CIO bij informatiebeveiliging en het uitvoeren van een risico- en kwetsbaarheidsanalyse op de primaire bedrijfsprocessen, zoals subsidieverlening en inkopen, om na te gaan of de ingerichte beveiligingsmaatregelen en -procedures voldoende toereikend zijn. Er is een werkplan opgesteld dat, in lijn met een aanbeveling uit 2013 voorziet in de beoordeling van de generieke IT-beheersmaatregelen. PS zijn via deze boardletter geïnformeerd over (uitgevoerde) acties op het gebied van informatiebeveiliging.

### Begroting 2015 (november 2014)

In de paragraaf Bedrijfsvoering van de begroting 2015 wordt aangegeven dat voor het speerpunt Informatiestrategie PS in 2015 op basis van ‘basis op orde’ de focus op het

verder professionaliseren van de IT-governance ligt en daarnaast de ICT-ontwikkelingen actief worden gevolgd. Ook zal in 2015 de eindevaluatie van de kadernota worden uitgevoerd. De PS-leden die de ICT-ambitie nog voor ogen hebben, kunnen hieruit afleiden dat de provincie in 2015 toe is aan de tweede stap van deze ambitie (als basis op orde is, actief volger van ICT-ontwikkelingen). Voor 2015 is € 7.839.000 begroot, voor 2016 € 8.506.000, voor 2017 € 8.567.000 en voor 2018 € 8.630.000.[19]
De rekenkamer constateert dat ook in deze begroting en de bespreking ervan in PS niet (expliciet) wordt ingegaan op informatieveiligheid en de geraamde kosten daarvan.

### Tussentijdse evaluatie kadernota (2014)

Via een statenmededeling van 1 september 2014 zijn PS geïnformeerd over de opzet van de tussentijdse evaluatie van de (uitvoering van de) kadernota. Ze ontvingen daarbij eveneens het onderzoeksplan van deze tussenevaluatie die intern is uitgevoerd. Conform afspraak zijn PS vervolgens via een statenmededeling van 2 december 2014 geïnformeerd over de resultaten en aanbevelingen van de tussenevaluatie. Als bijlage was de rapportage van de evaluatie bijgevoegd. Gesteld wordt dat de doelstellingen van de kadernota grotendeels zijn bereikt, dat het op orde brengen van de technische basis binnen afzienbare tijd wordt afgerond en de organisatiestructuur conform kadernota is vormgegeven (nieuwe directeur Bedrijfsvoering en Financiën per 1 september 2013 die CIO-rol vervult, nieuwe clustermanager per 1 mei 2014), doortrekken sturings- en verantwoordingslijn tot op medewerkersniveau behoeft nog wel de nodige aandacht. Aanbevolen wordt nieuwe projectenportfolio-afweging te organiseren (I-board). Gesteld wordt dat informatiebeveiliging de afgelopen periode een belangrijk onderdeel was: er is een informatiebeveiligingsbeleid en jaarlijks informatiebeveiligingsplan opgesteld, er wordt voldaan aan NEN ISO normen en IPO kaders. Om te bepalen in hoeverre aan de gestelde normen wordt voldaan, wordt jaarlijks een quickscan uitgevoerd en een actieplan opgesteld én in uitvoer genomen, zo wordt gesteld. Verder wordt aangegeven dat de provincie deelneemt aan een pilot met IBD-gemeenten (Informatiebeveiligingsdienst-gemeenten). Ook, zo wordt gesteld, is een mysteryguestonderzoek uitgevoerd en worden naar aanleiding daarvan de nodige maatregelen genomen. Dit in lijn met de doelstellingen op nationaal (taskforce BID) en lokaal niveau om het bewustwordingsniveau op het gebied van informatiebeveiliging te verhogen. Concluderend wordt (onder consequenties) gesteld dat deze tussenevaluatie geen aanleiding geeft om het beleid bij te stellen. De kadernota heeft benoemd dat ‘de basis op orde brengen’ niet het einddoel zal zijn: daarin werd aangegeven dat aansluitend ‘de basis op orde houden’ centraal komt te staan om een actieve volger van IT-ontwikkelingen te kunnen zijn. Aan die koers zal de provincie in 2015 en verder onverminderd vasthouden, zo wordt gesteld.
De statenmededeling is gepubliceerd op de lijst van ingekomen stukken van 9 februari 2015, waarbij als behandeladvies vanuit de commissie EZB is opgenomen: overlaten aan individuele Statenleden. De rekenkamer constateert dat de resultaten van de tussenevaluatie niet in PS zijn geagendeerd/besproken. Wel zijn PS via de statenmededeling geïnformeerd over de stand van zaken van de uitvoering van de kadernota, waarbij ook expliciet en inhoudelijk werd ingegaan op informatiebeveiliging. Om de gegeven informatie te kunnen plaatsen, dienen PS echter wel de inhoud van de kadernota paraat te hebben, dan wel het gehele evaluatierapport te lezen.

[19] De ICT-budgetten zijn inclusief de kosten voor telecommunicatie en mobiele toestellen. Ook omvatten ze de ruimte voor inhuur welke in 2017 van deze budgetten is afgeraamd.

### Jaarstukken 2014 (mei 2015)

In de paragraaf Bedrijfsvoering van de jaarstukken 2014 wordt aangegeven dat in 2014 vervolg is gegeven aan de realisatie van het ICT-beleid en dat de geplande resultaten uit de kadernota in 2014 grotendeels zijn gerealiseerd. Een aantal projecten voor de basis op orde wordt echter in 2015 afgerond. Zoals voorgenomen in de begroting 2014 is de invulling van de CIO-functie gerealiseerd. Ook wordt aangegeven dat in de tweede helft van 2014 een tussenevaluatie van de kadernota is uitgevoerd en PS via een statenmededeling zijn geïnformeerd over de bevindingen daarvan. Verder wordt eerst gesteld dat er een start is gemaakt met het implementeren van het risicomanagement op basis van de vastgestelde beleidsnota, maar later in de tekst dat het risicomanagement verder is uitgewerkt.
Ten aanzien van de kosten informatisering en automatisering wordt aangegeven dat er sprake is van een overschrijding (€ 558.000) door onder andere de ambities van basis op orde-projecten. Gesteld wordt dat het merendeel van de hogere kosten wordt afgedekt via de reserve Basisinfrastructuur en duurzame productiemiddelen. Tijdens de bespreking van deze jaarstukken is vanuit PS gevraagd naar de onttrekking van bijna een half miljoen euro aan de reserve ICT-infrastructuur. GS geven in reactie daarop aan dat het eenmalige extra kosten ICT en infrastructuur betreft door de verbouwing van het provinciehuis.
De rekenkamer constateert dat er in dit jaarverslag en in de bespreking daarvan in PS niet (expliciet) wordt ingegaan op het informatiebeveiligingsbeleid en ook niet op de gerealiseerde kosten daarvan.

### Rapportage jaarrekeningcontrole 2014 (april 2015)

PS ontvingen in april 2015 het document *Uitkomsten controle en overige informatie 2014*. Voor bevindingen over IT wordt verwezen naar de boardletter 2014.

### Informatievisie Samen, Slim en innovatief (2015, niet PS)

De *Informatievisie Samen, Slim en Innovatief* die in juni 2015 door de CIO werd vastgesteld, is niet aan PS aangeboden. In 2016 zijn er verschillende documenten aan PS aangeboden, waarin melding wordt gemaakt dat in 2015 een informatievisie is opgesteld (nota Digitale Duurzaamheid, jaarstukken 2015 en Visie en hoofdlijnen informatiebeleid). In de Visie en hoofdlijnen wordt daarnaast de informatievisie samenvattend beschreven.

### Boardletter tussentijdse controle 2015 (oktober 2015)

PS ontvingen najaar 2015 de *Boardletter tussentijdse controle 2015 provincie Noord-Brabant*. Daaruit blijkt dat de accountant zich evenals in 2013 en 2014 wat betreft IT-beheersmaatregelen heeft gericht op SAP. Aangegeven wordt dat ze van mening zijn dat de beheersing van het SAP-systeem voldoet aan de door hen gestelde eisen en hun bevindingen uit 2014 van adequate opvolging zijn voorzien.

### Begroting 2016 (november 2015)

In de paragraaf Bedrijfsvoering van de begroting 2016 wordt aangegeven dat de provincie de ambitie heeft om vanuit een heldere ICT-strategie te werken. In 2016 ligt onder nadere de focus op het verder professionaliseren van de IT-omgeving en de samenwerking met ketenpartners. Als vigerend beleid wordt, evenals in voorgaande begrotingen, de startnotitie ICT-beleid uit 2012 genoemd, gesteld wordt dat het volgende afweegmoment in 2016 zal plaatsvinden.

De rekenkamer merkt op dat niet de startnotitie maar de kadernota het vigerende beleid is.
De rekenkamer constateert dat in deze begroting PS niet op de hoogte zijn gebracht van de in juni 2015 opgestelde informatievisie (lange termijnvisie en strategie). Ook wordt er, in tegenstelling tot voorgaande begrotingen en jaarstukken en in lijn met de genoemde consequentie van de tussenevaluatie, niet gesproken over de elementen van de ICT-ambitie (basis op orde houden en actief volger van ICT-ontwikkelingen).
Voor ICT worden de lasten voor 2016 begroot op € 7.874.000, voor 2017 op € 7.881.000, voor 2018 op € 7.872.000 en voor 2019 op € 7.872.000.[20]
De rekenkamer constateert dat ook in deze begroting en de bespreking ervan in PS niet (expliciet) wordt ingegaan op informatieveiligheid en de geraamde kosten daarvan.

### Eindevaluatie kadernota (2015)

Via een statenmededeling van 8 december 2015 zijn PS geïnformeerd over de resultaten en aanbevelingen van de extern uitgevoerde eindevaluatie van de (uitvoering van de) kadernota. Als bijlage was de rapportage van de evaluatie bijgevoegd. In de statenmededeling wordt onder andere aangegeven dat de meeste doelstellingen van de kadernota zijn gerealiseerd, dat de technische basis grotendeels op orde is gebracht en de CIO-rol in 2015 bij de algemeen directeur is belegd. Als aandachtspunten worden genoemd: ontbreken sourcingstrategie, opleidingsplan zodat CIO en I-board voldoende kundig zijn en blijven uitgerust, behoefte aan extra kaders met een meer informatiestrategische insteek/visie, bewustzijn medewerkers informatiebeveiliging waarbij gesteld wordt dat blijvend inspanningen zullen moeten worden verricht om deze te vergroten. Gesteld wordt dat informatiebeveiliging in de kadernota relatief onderbelicht bleef, maar de provincie sinds 2013 een systematische werkwijze heeft ingevoerd die aansluit bij (inter)nationale normen en standaarden (met regelmatige toets door een externe partij). Ook wordt opgemerkt dat het beleid zich komende jaren richt op het op orde houden van de informatievoorziening, zoals ook voorzien in de kadernota en dat de verwachting is dat de te nemen maatregelen beperkt zullen blijven en binnen reguliere budgetten kunnen worden opgevangen.
In de Procedurevergadering van PS van 15 februari 2016 wordt geadviseerd om de resultaten voor kennisgeving aan te nemen (behandeladvies). De rekenkamer constateert dat in lijn daarmee de resultaten van de eindevaluatie verder niet in PS zijn geagendeerd/ besproken. Evenals bij de tussenevaluatie zijn PS wel via de statenmededeling geïnformeerd over de stand van zaken van de uitvoering van de kadernota, waarbij ook expliciet en inhoudelijk werd ingegaan op informatiebeveiliging. Om de gegeven informatie te kunnen plaatsen, dienen PS echter ook nu weer de inhoud van de kadernota paraat te hebben, dan wel het gehele evaluatierapport te lezen.

### Nota Digitale Duurzaamheid (2016)

Eén van de aandachtpunten uit de *Informatievisie Samen, Slim en Innovatief* is verdiept in de *Nota Digitale Duurzaamheid* van 11 december 2015. PS zijn via een statenmededeling van 12 januari 2016 geïnformeerd over de nota. Als bijlage was de nota bijgevoegd.
Gesteld wordt dat de nota is opgesteld mede naar aanleiding van rekenkameronderzoek uit 2014 waarin werd aanbevolen om een visie op informatiebeleid en -beheer op te stellen. De nota bevat kaders en maatregelen om digitale informatie toegankelijk en bruikbaar te houden (beheer). De rekenkamer constateert dat de nota de pijler ‘beschikbaarheid van

[20] De ICT-budgetten zijn inclusief de kosten voor telecommunicatie en mobiele toestellen. Ook omvatten ze de ruimte voor inhuur welke in 2017 van deze budgetten is afgeraamd.

informatie' uit het informatiebeleid treft, maar niet direct beveiliging.
De rekenkamer constateert dat in lijn met het behandeladvies (voor kennisgeving aannemen) de statenmededeling verder niet in PS is geagendeerd/besproken.

### Jaarstukken 2015 (april/mei 2016)

In de paragraaf Bedrijfsvoering van de jaarstukken 2015 wordt onder het kopje Informatiestrategie ingegaan op het ICT-beleid. Er wordt gesteld dat in 2015 de realisatie van het ICT-beleid uit de kadernota 2013-2015 is afgerond. De rekenkamer constateert dat voor het speerpunt basis op orde van het ICT-beleid daarentegen ook wordt aangegeven dat de technische basis *grotendeels* op orde is naar de maatstaven van nu en bij de eindevaluatie is gesteld dat het einddoel van de kadernota is de basis op orde houden. Verder wordt gesteld dat de focus in 2015 lag op het professionaliseren van de IT-governance en dit is gerealiseerd met de oprichting van de strategische I-board die onder leiding van de CIO opereert en informatievraagstukken beoordeelt en prioriteert (nauwgezetter informatiseringsontwikkelingen[21] monitoren). Tevens wordt aangegeven dat de ontwikkeling van het plaats- en tijdonafhankelijk werken verder doorzet en dat daarbij informatieveiligheid meer aandacht vraagt. Ook wordt aangegeven dat in 2015 een strategische informatievisie is opgesteld, een nieuw toetsingskader strategisch projectportfoliomanagement[22] in gebruik is genomen en in de tweede helft de eindevaluatie van de kadernota is uitgevoerd en PS via een statenmededeling zijn geïnformeerd over de bevindingen daarvan.
De rekenkamer constateert dat er in dit jaarverslag en in de bespreking daarvan in PS niet (expliciet) wordt ingegaan op het informatiebeveiligingsbeleid en ook niet op de gerealiseerde kosten daarvan. Wel wordt in het jaarverslag gesteld dat informatieveiligheid meer aandacht vraagt bij de ontwikkeling van het plaats- en tijdonafhankelijk kunnen werken van provinciale medewerkers. De rekenkamer constateert verder dat de informatie in het jaarverslag in het algemeen in lijn is met de informatie uit de statenmededeling over de eindevaluatie, maar dat de geplaatste kanttekeningen/maatregelen die de provincie naar aanleiding van deze evaluatie plaats/neemt, niet in het jaarverslag worden gemeld.

### Rapportage jaarrekeningcontrole 2015 (april 2016)

PS ontvingen in april 2016 het document *Uitkomsten controle en overige informatie 2015*. Voor bevindingen over IT wordt verwezen naar de boardletter 2015.

### Visie en hoofdlijnen provinciaal informatiebeleid (2016)

PS zijn via een statenmededeling van 28 juni 2016 geïnformeerd over de *Visie en hoofdlijnen van het provinciaal informatiebeleid* en de uitvoering daarvan. Gesteld wordt dat de aanbeveling uit de eindevaluatie om het ICT-beleid te verbreden naar informatiebeleid en de aanbeveling uit het rekenkameronderzoek uit 2014 over het opstellen van een strategische I-visie aanleiding waren en gebundeld zijn in voorliggende visie. In de visie wordt ook aandacht gevraagd voor informatiebeveiliging en wordt gesteld dat de kaderstelling uit de kadernota ICT-beleid ook na 2015 geldig blijft.
Op de Statendag van 21 oktober 2016 is de statenmededeling geagendeerd in PS-thema Bestuur en Financiën. Voor de rekenkamer valt niet te achterhalen wat er besproken is, omdat, conform de werkwijze van PS van dat moment, er geen (audio)verslagen werden

[21] Uit de ambtelijke reactie blijkt dat in de jaarstukken per abuis wordt gesproken van ICT.
[22] In de jaarstukken wordt gesproken van portfoliomanagement.

gemaakt van informatiebijeenkomsten. In de statenmededeling wordt gesteld dat een statenvoorstel/vaststelling door PS niet nodig wordt geacht omdat de visie geen beleidswijzigingen bevat (betreft voorzetting van de kadernota) en er geen aanvullende financiën worden gevraagd. In een statenmededeling van 25 september 2017 wordt gesteld dat deze visie valt onder door PS vastgesteld beleid en daarvoor geldende kaders.

### Bestuursrapportage 2016 (oktober 2016)

PS bespraken op 21 oktober 2016 de *Bestuursrapportage 2016*. Onder de paragraaf Bedrijfsvoering wordt opgemerkt dat de aangekondigde IT-visie, zoals toegezegd, zal worden betrokken bij het toewerken naar een meer opgavegestuurde netwerkorganisatie. De rekenkamer merkt op dat niet bekend is wanneer deze IT-visie is aangekondigd en hoe deze zich verhoudt tot de Informatievisie uit 2015 en de Visie en hoofdlijnen van het informatiebeleid uit juni 2016.

### Begroting 2017 (november 2016)

In de paragraaf Bedrijfsvoering van de begroting 2017 wordt onder het kopje ICT-ontwikkeling aangegeven dat in 2017 de focus ligt op het versterken van het strategisch projectportfoliomanagement en risicomanagement wat moet resulteren in een ICT-projectenportfolio die optimaal bijdraagt aan het realiseren van de opgaven van Brabant binnen de gestelde kaders. Verder wordt gesteld dat daarnaast het accent ligt op het professionaliseren van de regie en uitvoering op afstand voor geselecteerde onderdelen van ICT-beheer en dat de ICT-ontwikkelingen in 2017 nauwgezet zullen worden gevolgd. Vanaf 2016 werkt de provincie met één organisatiekostenbudget (OKB). In de begroting 2017 is voor de gehele paragraaf Bedrijfsvoering tezamen het geraamde budget opgenomen, waarmee, zo is in de ambtelijke reactie aangegeven, het zicht op IT-gerelateerde budgetten wegvalt.
De rekenkamer constateert dat ook in deze begroting en de bespreking ervan in PS niet (expliciet) wordt ingegaan op informatieveiligheid en de geraamde kosten daarvan.

### Boardletter tussentijdse controle 2016 (november 2016)

PS ontvingen in november 2016 de *Boardletter tussentijdse controle 2016 provincie Noord-Brabant*. De accountant staat daarin ook stil bij informatiebeveiliging die cruciaal wordt geacht door verschillende ontwikkelingen waarmee de provincie te maken heeft. Het vigerende beleid wordt genoemd en de maatregelen die de provincie op dit terrein neemt (jaarlijkse GAP-analyse informatiebeveiligingsbeleid, periodiek attack- en penetratietesten, privacyonderzoek om te bepalen in hoeverre beheersmaatregelen zijn getroffen op het gebied van datalekken en privacy, voornemen privacyofficer aan te stellen). De accountant acht de aandacht van de provincie rondom informatiebeveiliging gepast en constateert dat de procedures in opzet toereikend zijn. De accountant doet aanbevelingen met betrekking tot de beheersmaatregelen (vastlegging, beleggen eigenaarschap, overlap in kaart brengen). GS geven aan dat de aanbevelingen van de accountant reeds worden ondervangen door het gebruik van een nieuwe toolbox. Wat betreft logische toegangsbeveiliging en wijzigingenbeheer SAP stelt de accountant dat daarin verbeteringen zijn doorgevoerd en de procedures daarvoor nu in opzet toereikend zijn ingericht.
De boardletter was geagendeerd in het Platform Planning & Control van PS van 18 november 2016. Voor de rekenkamer valt niet te achterhalen wat er besproken is, omdat, conform de werkwijze van PS van dat moment, er geen (audio)verslagen werden

gemaakt van platformbijeenkomsten.  PS zijn via deze boardletter wel geïnformeerd over het informatiebeleid en uitvoering daarvan in de praktijk.

### Jaarstukken 2016 (april 2017)

In de paragraaf Bedrijfsvoering van de jaarstukken 2016 wordt gesteld dat in 2016 het ICT-beleid is geactualiseerd. De evaluatie van de kadernota in 2015 en het in 2014 gepubliceerde rekenkameronderzoek *Digitalisering en duurzame toegankelijkheid van informatie* lagen daaraan ten grondslag. Aangegeven wordt dat in 2016 eerst de nota Digitale Duurzaamheid en daarna de Visie en hoofdlijnen informatiebeleid aan PS is aangeboden.
Verder wordt gesteld dat informatiebeveiliging, mede door de nieuwe Wet Meldplicht Datalekken, extra aandacht heeft gekregen. Ook heeft een privacy impactanalyse plaatsgevonden om te kunnen bepalen in hoeverre wordt voldoen aan de Wet Bescherming Persoonsgegevens[23] en welke verbeteracties nog nodig zijn.
Daarnaast wordt aangegeven dat de voorgenomen professionalisering van de IT-omgeving gedeeltelijk is gerealiseerd. De IT-omgeving is veilig en betrouwbaar en kende in 2016 geen uitval, er is regelmatig kennisuitwisseling met IT-ketenpartners, maar een gezamenlijke agendering voor realisatie op basis van vrijwilligheid vraagt bestuurlijke steun, zo wordt gesteld.
De rekenkamer constateert dat er in dit jaarverslag (expliciet) wordt ingegaan op informatiebeveiliging, zij het niet inhoudelijk (extra aandacht voor informatiebeveiliging en privacy impactanalyse uitgevoerd in verband met nieuwe wetgeving), en ook worden de gerealiseerde kosten van informatiebeveiliging niet gegeven. De rekenkamer heeft geen verslag aangetroffen van de vergadering van PS waarin de jaarstukken 2016 werden besproken, zodat onbekend is of PS zijn ingegaan op informatiebeveiliging en zo ja, wat er is besproken.

### Rapportage jaarrekeningcontrole 2016 (april 2017)

PS ontvingen in april 2017 het document *Uitkomsten controle en overige informatie 2016*. Voor bevindingen over IT wordt verwezen naar de boardletter 2016.

### Perspectiefnota 2017/Bestuursopdracht Digitalisering (2017)

In de hun vergadering van 21 april 2017 bespraken PS de *Perspectiefnota 2017*. PS vroegen een strategische verkenning Digitalisering uit te voeren. In het licht van deze bestuursopdracht, informatieveiligheid en een door de Rotterdamse Rekenkamer gepubliceerd onderzoek naar dit onderwerp, werd vanuit PS gevraagd of GS PS kunnen informeren over de status van de informatieveiligheid en of daarnaar ook verder onderzoek is gedaan.

In juli 2017 verzocht de portefeuillehouder de Procedurevergadering een informerende themabijeenkomst Digitalisering te organiseren om PS te betrekken bij de visieontwikkeling. Via een statenmededeling van 25 september 2017 worden PS geïnformeerd over de stand van zaken van de bestuursopdracht. Om deze te kunnen realiseren stellen GS voor om het OKB te verhogen in verband met nieuwe taken, waaronder de aanstelling van een CIO en een medewerker gegevensbescherming (intensivering).

[23] In de jaarstukken wordt per abuis gesproken van Wet Bescherming van Privacy & Persoonsgegevens.

Conform het behandeladvies uit de Procedurevergadering van 9 oktober 2017 wordt de statenmededeling besproken in de informerende bijeenkomst Digitalisering (thema Economie en Internationalisering) op 13 oktober. Er is een audioverslag van deze bijeenkomst.

### Boardletter tussentijdse controle 2017 (oktober 2017)

PS ontvingen najaar 2017 de *Boardletter tussentijdse controle 2017 provincie Noord-Brabant*. Daaruit blijkt dat de accountant zich evenals in voorgaande jaren wat betreft IT-beheersmaatregelen heeft gericht op SAP. Echter nu wordt gesteld dat door de geconstateerde tekortkomingen op het gebied van logische toegangsbeveiliging en wijzigingenbeheer voor de jaarrekeningcontrole niet zonder meer kan worden gesteund op de betrouwbare werking van controlemaatregelen binnen SAP. Voor autorisatiebeheer (van gebruikersaccounts) zijn procedures opgesteld, maar niet breed beschikbaar en/of bekend wat risico's met zich meebrengt, zo wordt gesteld. Wijzigingen (inclusief softwarematige updates) worden niet altijd adequaat getest en de testwerkzaamheden worden niet altijd structureel vastgelegd. Aanbevolen wordt stringenter toe te zien op naleving van de procedures op deze gebieden. Daar het beheer van databases is uitbesteed wordt aanbevolen om een procedure op te stellen en in te richten die het outsourcingsproces ondersteunt en waarborgt dat uitbestede processen op de juiste wijze worden uitgevoerd. Gesteld wordt dat de provincie in het kader van de AVG de processen, waarbij persoonsgegevens van belang zijn, in kaart heeft gebracht. Aanbevolen wordt om zo snel mogelijk gepast beleid en procedures in te richten om aan de AVG te voldoen.
De boardletter was geagendeerd in het Platform Planning & Control van PS van 15 december 2017. Voor de rekenkamer valt niet te achterhalen wat er besproken is, omdat, conform de werkwijze van PS van dat moment, er geen (audio)verslagen werden gemaakt van platformbijeenkomsten. PS zijn via deze boardletter wel geïnformeerd over zaken die informatieveiligheid raken.

### Bestuursrapportage 2017/Toelichting 3e wijziging begroting 2017

PS zijn in een statenmededeling van 27 oktober 2017 geïnformeerd over de *Bestuursrapportage 2017*. In de paragraaf Bedrijfsvoering wordt opgemerkt dat vanaf 25 mei 2018 nieuwe Europese wetgeving op het gebied van privacy van toepassing zal zijn (AVG) en dat die invloed heeft op het verwerken van persoonsgegevens binnen de provincie. Gesteld wordt dat om te borgen dat de provincie op tijd compliant is, er verschillende acties in gang zijn gezet, zoals een inventarisatie van verbeterpunten en het opstellen van een functie voor de verplichte functionaris gegevensbescherming.
De rekenkamer constateert dat in deze bestuursrapportage aandacht is voor acties die de informatieveiligheid raken.

### Begroting 2018 (november 2017)

In de paragraaf Bedrijfsvoering van de begroting 2018 wordt aangegeven dat de provincie in 2018 voldoet aan de nieuwe Europese privacywetgeving voor gegevensbescherming en er onder andere een regie-organisatie ICT wordt gerealiseerd. In de begroting 2018 is voor de gehele paragraaf Bedrijfsvoering tezamen het geraamde budget opgenomen.
In de PS-vergadering van 10 november 2017 wordt de begroting 2018 besproken. PS stellen daarbij ook de eerste begrotingswijziging vast welke de voorgestelde ophoging van

het OKB betreft voor nieuwe taken (CIO en FG, zie hiervoor onder het kopje Bestuursopdracht Digitalisering (2017)). Bij de bespreking van de begroting wordt een motie aangenomen waarin GS worden verzocht om Brabant Advies een verkennend onderzoek te laten uitvoeren naar de te verwachten maatschappelijke risico's van de voortgaande digitalisering en PS hierover te informeren. Dit mede omdat met cybercriminaliteit hele netwerken platgelegd kunnen worden.
De rekenkamer constateert dat in deze begroting indirect wordt ingegaan op een element van informatieveiligheid, maar niet op de geraamde kosten van informatieveiligheid. Bij de bespreking van de begroting 2018 in PS wordt, in verband met cybercriminaliteit (welke de informatieveiligheid in gevaar kan brengen), een motie aangenomen om GS te verzoeken een risico-onderzoek te laten uitvoeren.

### Schriftelijke vragen PS-veiligheid ICT-systemen en vertrouwelijkheid mailboxen (oktober/november 2017)

Op 25 oktober en 3 november 2017 is er vanuit PS een aantal schriftelijke vragen aan GS gesteld. Respectievelijk over de veiligheid van ICT-systemen van de provincie naar aanleiding van problemen bij de Tweede Kamer door spoofen en de vertrouwelijkheid van mailboxen naar aanleiding van het verwijderen van een phishingmail uit mailboxen. GS antwoordden dat ze via een tweesporen aanpak zorgen voor een veilige ICT-omgeving en het risico op datalekken willen minimaliseren: technische maatregelen en werken aan bewustwording van medewerkers. Wat betreft bewustwording geven GS aan dat indien gewenst de medewerker informatiebeveiliging een toelichting kan geven specifiek gericht op PS-leden. Verder geven ze aan dat de servers beveiligd zijn tegen spoofing, en phishingmails door de mailserver op systeemniveau worden verwijderd nadat deze daar opdracht toe heeft verkregen. GS beschrijven verder de werkwijze die wordt gehanteerd bij phishingmails en gaan kort in op de acties die tot nu toe zijn uitgevoerd voor de nieuwe Europese verordening (AVG): impact ervan is onderzocht, er is een plan van aanpak zodat in mei 2018 aan de eisen wordt voldaan en er wordt op verschillende manieren aandacht gevraagd voor de menselijke component (bijvoorbeeld gebruik pincodes op mobiele apparatuur, clean desk, melden van veiligheidsincidenten), zo wordt gesteld.

### Nieuwe inrichting i-Governance (2018)

Op 8 september 2017 vroegen PS bij motie om informatie over de stand van zaken ten aanzien van archivering/verslaglegging in de organisatie. Per brief van 5 februari 2018 beantwoordden GS de vragen uit de motie *Archivering op orde*. Eén daarvan betreft de wijze waarop GS de verbeteringen in de archivering duurzaam willen borgen in de organisatie. GS geven aan dat met de voorgenomen aanstelling van een CIO het raamwerk van besluitvorming en verantwoordelijkheden ten aanzien van de informatiehuishouding (de i-Governance) opnieuw ingericht zal gaan worden en daarmee systematisch aandacht krijgen om te komen tot een duurzame borging. Daarbij wordt gesteld dat het belangrijk is dat hierbij alle betrokkenen (GS, directie, CIO, programmamanagers, opdrachtnemers, zaaktypeneigenaren, behandelend ambtenaren, beheerorganisatie en ondersteuning) met hun verantwoordelijkheden in positie worden gebracht en beschikken over de benodigde faciliteiten.

## 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, zijn er geen documenten over informatiebeveiliging/veiligheid aangetroffen op de provinciale website.

# Bijlage 1 Geraadpleegde documenten

Provincie Noord-Brabant (juli 2012), *Startnotitie Strategisch IT-beleid provincie Noord-Brabant* (aan commissie voor Economische Zaken en Bestuur)

Provincie Noord-Brabant (februari 2013), *Kadernota ICT-beleid 2013-2015* en *Uitwerking kadernota en speerpunten ICT-beleid 2013-2015*

Provincie Noord-Brabant (maart 2013), *Statenvoorstel 15/13 Kadernota ICT-beleid 2013-2015*

Provincie Noord-Brabant (september 2013), *Informatiebeveiligingsbeleid Provincie Noord-Brabant*

Provincie Noord-Brabant (september 2013), Memo aan clustermanager, *Quickscan informatiebeveiliging*

Provincie Noord-Brabant (januari 2014), Memo aan CMT: *IT Governance Board en dienstverleningsconcept*

Provincie Noord-Brabant (mei 2014), *Agenda en Afspraken directie 26 mei 2014*

Fox-IT BV (juni 2014), *Rapportage Penetratietest MyCorsa NxT*

BCT (juni 2014), *Highlight Report Juni 2014, Implementatie MyCorsa NxT provincie Noord-Brabant*

Provincie Noord-Brabant (augustus 2014), *Onderzoeksplan Tussentijdse evaluatie ICT-beleid 2013-2015 ex art. 217a Provinciewet*

Provincie Noord-Brabant (september 2014), *Statenmededeling Tussentijdse evaluatie ICT-beleid 2013-2015 ex art. 217a Provinciewet* (onderzoeksplan)

Provincie Noord-Brabant (oktober 2014), *Tussentijdse beleidsevaluatie Kadernota ICT-beleid 2013-2015*

Provincie Noord-Brabant (december 2014), *Statenmededeling Tussentijdse evaluatie ICT-beleid 2013-2015* (resultaten en aanbevelingen)

Provincie Noord-Brabant (december 2014), Memo aan directie en kandidaatleden I-board: *Opstarten I-board*

Provincie Noord-Brabant (februari 2015), *CIBO Monitor 2015* (over 2014)

CIBO (maart 2015[24]), *Monitoringtool baseline informatiebeveiliging 2014, Rapportage interprovinciale beeld implementatie baseline informatiebeveiliging eind 2014*

Provincie Noord-Brabant (juni 2015), *Informatievisie Samen, Slim en Innovatief*

Provincie Noord-Brabant (juni 2015), *Routekaart ICT 2015-2018*

Provincie Noord-Brabant (juli 2015), *Scorelijst Projecten 2015*

Provincie Noord-Brabant (september 2015), *Statenmededeling Evaluatie ICT-beleid 2013-2015 ex art. 217a Provinciewet* (onderzoeksopzet)

Dialogic (november 2015), *Evaluatie van de Kadernota ICT-beleid 2013-2015, eindrapport*

Provincie Noord-Brabant (december 2015), *Statenmededeling Evaluatie ICT-beleid 2013-2015* (resultaten en aanbevelingen)

Provincie Noord-Brabant (december 2015), *Nota Digitale Duurzaamheid, Duurzaam toegankelijke overheidsinformatie*

Provincie Noord-Brabant (januari 2016), *Statenmededeling Nota Digitale Duurzaamheid*

EY (maart 2016), *Wet Meldplicht data lekken, Huidige situatie en plan van aanpak provincie Noord-Brabant*

Provincie Noord-Brabant (mei 2016), *Presentatie Project portfoliomanagement*

Provincie Noord-Brabant (juni 2016), *Statenmededeling Visie en hoofdlijnen informatiebeleid*

Fox-IT BV (september 2016), *Voorstel Security Assesments provincie Noord-Brabant*

Provincie Noord-Brabant (oktober 2016), *Bestuursrapportage 2016*

Fox-IT BV (februari 2017), *Mystery Guest Onderzoek Rapportage*

Provincie Noord-Brabant (februari 2017), Memo aan directie, *Achtergrondinformatie Mystery Guest Onderzoek*

Provincie Noord-Brabant (maart 2017), *Stand van zaken informatiebeveiliging provincie Noord-Brabant, Monitor 2016 en resultaten*

Provincie Noord-Brabant (april 2017), Memo aan directie: *Privacy compliance onderzoek*

Provincie Noord-Brabant (april 2017), Memo Secretaris: *Mystery Guest onderzoek I&I* (vastgesteld/akkoord in GS 9 mei 2017) en stukkenloop van de memo

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

IPO (juni 2017), *Interprovinciale Baseline Informatiebeveiliging, Bijlage B1 De baseline overzicht implementatierichtlijnen basisniveau*

Provincie Noord-Brabant (2017), *Functieprofielen Chief Information Officer, Functionaris Gegevensbescherming, Chief Information Security Officer, Information Security Officer*

Provincie Noord-Brabant (november 2017), *Vragen ex. Art. 30 Reglement van Orde m.b.t. Vertrouwelijkheid mailboxen volksvertegenwoordigers (vragen 3 november 2017 en antwoorden 14 november 2017)*

Provincie Noord-Brabant (november 2017), *Vragen ex. Art. 30 Reglement van Orde m.b.t. Veiligheid ICT-systemen provincie (vragen 25 oktober 2017 en antwoorden 14 november 2017)*

Provincie Noord-Brabant (februari 2018), *Statenmededeling Beantwoording vragen Motie M4: Achivering op orde*

Provincie Noord-Brabant, *Begrotingen* 2013, 2014, 2015, 2016, 2017, 2018 en *Jaarstukken* 2012, 2013, 2014, 2015, 2016

Ernst & Young Accountants (onderzoeksperiode), *Boardletters tussentijdse controle* en *accountantsverslagen* provincie Noord-Brabant

Provincie Noord-Brabant (2012-2018), *Vastgestelde notulen en/of audioverslagen bijeenkomsten PS en Presidium*

Diverse mailwisselingen tussen provincie en derden naar aanleiding van onderzoeken

Relevante documenten via corsa, intranet van de provincie en www.brabant.nl (geraadpleegd juli en december 2017)