Rekenkamer
OOST-NEDERLAND

Informatieveiligheid Gelderland

Nota van bevindingen

Colofon

De Rekenkamer Oost-Nederland is een onafhankelijk orgaan dat onderzoek doet naar de doeltreffendheid, doelmatigheid en rechtmatigheid van het gevoerde bestuur van de provincies Gelderland en Overijssel.

De bestuursleden van de Rekenkamer zijn: de heer drs. M.M.S. Mekel (voorzitter), mevrouw B. Vlieger-Ruitenberg MBA (tot 1 januari 2019) en de heer ir. T.J.A. Gies. De secretaris-directeur is mevrouw drs. S.W. Mathijssen RO.

Dit rapport is voorbereid door een onderzoeksteam bestaande uit mevrouw S. Spenkelink, MSc en de heer T. Schaaf, MSc, MA.

Rekenkamer Oost-Nederland
Achter de Muren Zandpoort 6
7411 GE Deventer
Telefoon: 0570 - 66 58 00
info@rekenkameroost.nl
www.rekenkameroost.nl
Twitter: @RekenkamerOost

Rekenkamer
OOST-NEDERLAND

Informatieveiligheid Gelderland

Nota van bevindingen

Deventer, januari 2019

Inhoudsopgave

1 Over dit onderzoek

In dit eerste hoofdstuk van deze nota van bevindingen geven we in het kort weer wat we hebben onderzocht.

1.1 Aanleiding

Provincies zijn voor de uitvoering van hun taken steeds meer afhankelijk van informatiesystemen en informatiestromen. Dit komt onder andere door de toegenomen digitalisering van de provinciale dienstverlening en doordat de samenwerking met andere bedrijven en contacten met burgers en bedrijven vaker digitaal van aard is. Digitale veiligheid neemt dan ook een steeds belangrijkere positie in. Overheden, zoals provincies, hebben hier een maatschappelijke verantwoordelijkheid: burgers, bedrijven en overheidspartners moeten erop kunnen rekenen dat dat de informatie betrouwbaar is en dat er zorgvuldig met gegevens wordt omgegaan. Een betrouwbare informatievoorziening is van essentieel belang voor het functioneren van de processen van de provincie.[1] Daarnaast speelt mee dat er verschillende wetten zijn (gekomen) die eisen stellen aan het verwerken en opslaan van informatie. Hierbij kan gedacht worden aan de Algemene verordening gegevensbescherming (inclusief meldplicht datalekken) en de Archiefwet. Bovendien kunnen inbreuken op de informatieveiligheid leiden tot financiële en/of imagoschade, bijvoorbeeld als onbevoegden toegang krijgen tot gevoelige bedrijfseconomische gegevens of persoonsgegevens van burgers.

De laatste jaren zijn er verschillende incidenten en publicaties geweest die hebben aangetoond dat de digitale veiligheid van overheden een aantal kwetsbaarheden bevatte. Zo werd de Tweede Kamer in maart 2017 getroffen door een aanval van gijzelingssoftware en bleek in oktober 2017 de e-mail van kabinets- en Kamerleden niet goed beveiligd. In 2017 zijn 10.000 datalekken gemeld bij de Autoriteit Persoonsgegevens (AP) waarvan 2.000 afkomstig vanuit het Openbaar Bestuur. Het aantal meldingen is in 2017 met ruim 70% toegenomen ten opzichte van het jaar ervoor[2]. Ook uit onderzoeken van rekenkamers bleek dat de informatieveiligheid bij

[1] *Cibo en IPO (2010). Interprovinciale Baseline Informatiebeveiliging 1.0, p. 4.*
[2] *Nieuwsbericht Autoriteit Persoonsgegevens van 29 maart 2018.*

meerdere gemeenten en provincies nog te wensen overlaat. Dit was voor ons de aanleiding om het thema informatieveiligheid te gaan onderzoeken.

1.2 Achtergrond

Wat is informatieveiligheid?

De begrippen 'informatieveiligheid' en 'informatiebeveiliging' worden vaak door elkaar gebruikt. Er is echter een duidelijk verschil tussen die begrippen: informatiebeveiliging (de maatregelen) wordt gebruikt om informatieveiligheid (het doel) te waarborgen.[3] In deze onderzoeksopzet hanteren wij de term 'informatieveiligheid'. Wij kiezen hiervoor omdat die term meer recht doet aan de breedte van het onderwerp dan de term 'informatiebeveiliging', die vooral met ICT wordt geassocieerd.

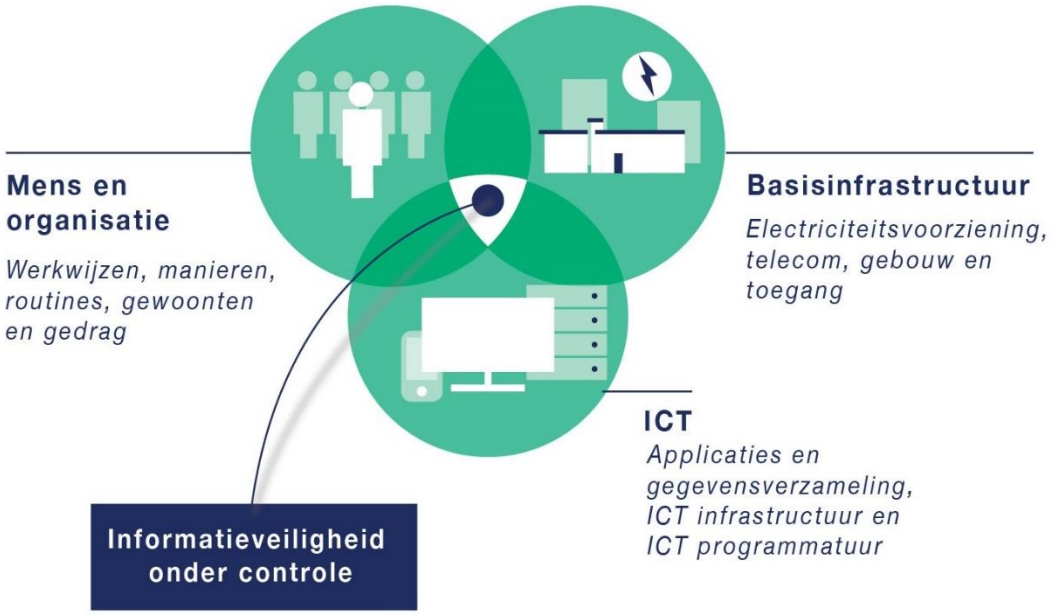
Informatieveiligheid richt zich op bescherming van informatie om de continuïteit van bedrijfsactiviteiten te waarborgen.[4] Als de informatieveiligheid onvoldoende is gewaarborgd, kunnen er risico's ontstaan bij de uitvoering van provinciale taken en het functioneren van de organisatie. De maatregelen die genomen worden, moeten echter in verhouding staan tot de grootte van het risico. 100 procent veiligheid bestaat niet. Het doel van informatieveiligheid is daarom risico's tot een acceptabel niveau terug te brengen. Het gaat daarbij om het behouden van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie.

- Bij *vertrouwelijkheid* gaat het er om dat de informatie alleen toegankelijk is voor degene die hiervoor daadwerkelijk geautoriseerd is (oftewel 'de juiste persoon'). Een voorbeeld van een bedreiging hiervan is de onthulling of het misbruik van informatie door hacking, afluisteren, diefstal of verlies van laptop of mobiel.
- Bij *integriteit* gaat het om de correctheid en volledigheid van informatie en de informatieverwerking (oftewel 'de juiste informatie'). Een voorbeeld van een bedreiging is het onrechtmatig verwijderen, wijzigen of toevoegen van informatie.
- Bij *beschikbaarheid* gaat het er om dat geautoriseerde gebruikers toegang hebben tot de informatie en aanverwante bedrijfsmiddelen op het moment dat het nodig is (oftewel 'het juiste moment'). Een bedreiging hiervan is vertraging of uitval van de infrastructuur doordat deze overbelast of defect is, bijvoorbeeld door een DDoS-aanval respectievelijk een brand. [5]

Om de risico's op schending van of inbreuk op de informatieveiligheid te verkleinen, zijn er verschillende aandachtsgebieden waarop kan worden gestuurd en waar maatregelen kunnen worden genomen. De Interprovinciale Baseline Informatieveiligheid maakt een onderscheid naar drie aandachtsgebieden, zie figuur 1.

[3] *Cibo en IPO (feb. 2016). Interprovinciale baseline informatieveiligheid versie 2.0, p. 4.*
[4] *Cibo en IPO (2010). Interprovinciale Baseline Informatiebeveiliging 1.0.*
[5] *Combinatie van Cibo en IPO (feb. 2016). Interprovinciale baseline informatieveiligheid versie 2.0, p. 4 en Randstedelijke Rekenkamer (2015). Onderzoeksopzet, p. 6.*

Figuur 1: *Aandachtsgebieden van informatieveiligheid*



Bron: Interprovinciale Baseline Informatieveiligheid, bewerking Randstedelijke Rekenkamer en Bureau Twaalf (2016).

Het is belangrijk dat de focus op het geheel van de aandachtsgebieden mens en organisatie, basisinfrastructuur en ICT ligt. Dit is waar de cirkels in bovenstaande figuur elkaar overlappen. Vaak wordt bij informatieveiligheid direct gedacht aan ICT, maar het nemen van technische maatregelen alleen (denk bijvoorbeeld aan het installeren van een antivirusprogramma of autorisatierechten) is niet voldoende. Ook maatregelen op het aandachtsgebied mens en organisatie (bijvoorbeeld het creëren van bewustzijn en het instellen van procedures) en de basisinfrastructuur (bijvoorbeeld de toegangs-beveiliging van gebouwen en ruimtes of de noodstroomvoorziening) zijn belangrijk.[6]

Relevante ontwikkelingen

Er zijn de afgelopen jaren verschillende initiatieven genomen om de informatieveiligheid van overheden te verbeteren. In figuur 2 staan de belangrijkste initiatieven vanuit de provincies.

[6] *Combinatie van Cibo en IPO (2016). Interprovinciale Baseline Informatieveiligheid 2.0, p. 6 en Randstedelijke Rekenkamer (2015). Onderzoeksopzet Informatieveiligheid, p. 7.*

Figuur 2: *Tijdlijn relevante initiatieven verbetering informatieveiligheid provincies*

Bron: Rekenkamer Oost-Nederland o.b.v. tekst Randstedelijke Rekenkamer (2015).

Omdat provincies veel vergelijkbare werkprocessen hebben, streven zij - onder het motto 'generiek waar het kan, specifiek waar het moet' - zo veel mogelijk naar samenwerking op het terrein van informatieveiligheid. Vanuit dit streven is in 2008 het Centraal Informatiebeveiligingsoverleg (Cibo) opgericht. In dit platform, onderdeel van het IPO, wisselen provincies kennis en ervaring uit en wordt de gezamenlijke ontwikkeling van informatieveiligheid vormgegeven.[7] Vanuit elke provincie is een deelnemer vertegenwoordigd die werkzaam is op het gebied van informatieveiligheid. In 2010 stelde het Cibo de eerste Interprovinciale Baseline Informatiebeveiliging (IBI) op. 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. De IBI geeft een standaard werkwijze waarmee per bedrijfsproces of informatiesysteem bepaald wordt welke beveiligingsmaatregelen getroffen moeten worden.

Om de informatieveiligheid van de provincies verder te optimaliseren en te professionaliseren is het Convenant Interprovinciale Regulering Informatieveiligheid in 2014 opgesteld. Dit is ondertekend door alle provincies en op zowel ambtelijk als bestuurlijk niveau vastgesteld. Het convenant is een afsprakenkader rondom vier thema's:

- sturing en verantwoordelijkheid;
- beleid en normenkader;
- verantwoording en toezicht en
- bewustwording, kennis en coördinatie.

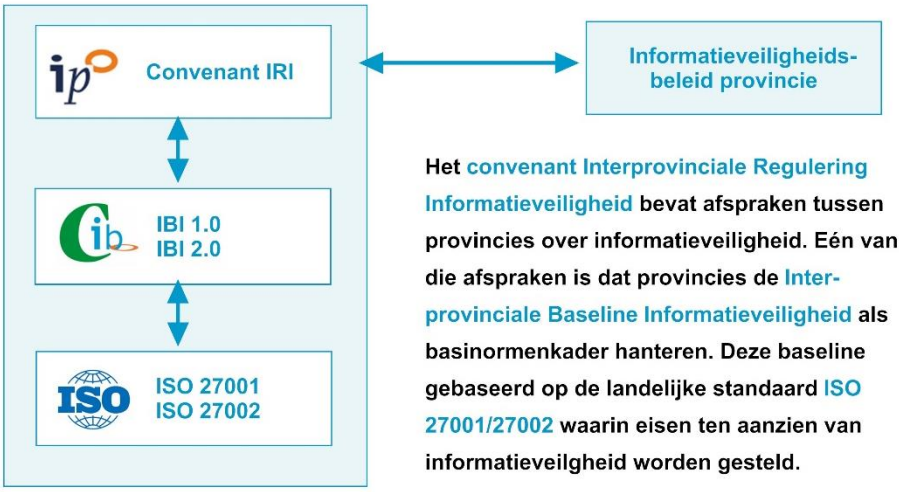
Het is de bedoeling dat de provincies door de gezamenlijke afspraken één standaard ontwikkelen en behouden waardoor informatieveiligheid geen vrijblijvend proces is.

De vaststelling van het bovengenoemde Convenant (waarin onder andere is afgesproken dat het Cibo zorgdraagt voor een actuele baseline die door alle provincies toegepast wordt) was één van de ontwikkelingen die aanleiding gaf tot actualisatie van de IBI. De Interprovinciale Baseline Informatiebeveiliging 2.0 is in 2016 opgesteld. Een baseline die gebaseerd is op ISO 27001 en ISO 27002. Op dit moment wordt gewerkt aan een Baseline Informatiebeveiliging Overheid (BIO) voor zowel het Rijk, gemeenten, provincies als waterschappen. Met de invoering van de BIO wordt de IBI vervangen.

[7] *Cibo (2014). Agenda voor ontwikkeling informatieveiligheid provincies 2014.*

Figuur 3 geeft schematisch weer hoe deze verschillende richtlijnen zich tot elkaar verhouden.

Figuur 3: *Verhouding tussen Convenant IRI, IBI en ISO-standaarden*



Bron: Rekenkameer Oost-Nederland. Geïnspireerd op een uitsnede van figuur uit rapport 217a-onderzoek beheersing informatiebeveiliging van Concerncontrol Overijssel (mrt. 2018), p. 4.

1.3 Wat heeft de rekenkamer onderzocht?

Doel

Het doel van dit onderzoek is om:

> Provinciale Staten van Gelderland en Overijssel te ondersteunen in hun kaderstellende en controlerende rol door inzichtelijk te maken of de informatieveiligheid van de provincie voldoende is geborgd.

Centrale vraag

In dit onderzoek staat de volgende vraag centraal:

> *Hebben de provincies Gelderland en Overijssel de informatieveiligheid voldoende geborgd?*

De uitwerking van de centrale vraag in onderzoeksvragen vindt u in bijlage 1. Ook vindt u daar meer informatie over de aanpak van het onderzoek, zoals het normenkader en de onderzoeksmethodiek. Eén van de onderdelen van de onderzoeksaanpak was dat een externe partij de bescherming van informatie in de praktijk heeft onderzocht door te kijken of zij hier toegang tot kon krijgen.

Focus

In dit onderzoek staat de informatieveiligheid bij de provincies Gelderland en Overijssel centraal. Het onderzoek richt zich op informatieveiligheid in de breedte. Hiermee richten we ons op alle aspecten van informatieveiligheid om zo een totaalbeeld te krijgen. We besteden aandacht aan het beleid, de organisatie en de praktijk van de provinciale informatieveiligheid.

Om het onderzoek in de juiste context te plaatsen zijn de volgende zaken nog van belang.

- Het onderzoeksobject is de provincie. Hiermee wordt bedoeld dat aan de provincie verbonden partijen niet tot de reikwijdte van het onderzoek behoren.
- Het verzamelen van de gegevens waarop dit onderzoek is gebaseerd, heeft in de periode juli 2018 - november 2018 plaatsgevonden. De bevindingen geven derhalve de situatie van dat moment weer, tenzij anders wordt aangegeven.
- Met de inwerkingtreding van de AVG is er in toenemende mate aandacht voor privacy, ook binnen de provincie. Wij realiseren ons dat privacy en informatieveiligheid aan elkaar gerelateerde thema's. De privacy is meegenomen voor zover het direct raakt aan informatieveiligheid en niet als apart thema onderzocht.

1.4 Opbouw

In hoofdstuk 2 staat het informatieveiligheidsbeleid van de provincie centraal. Hoofdstuk 3 gaat over de wijze waarop de sturing op en verantwoordelijkheid voor informatieveiligheid binnen de provincie zijn verankerd. Vervolgens kijken we in hoofdstuk 4 naar de uitvoering van maatregelen voor informatieveiligheid en het resultaat daarvan. Dat resultaat bestaat uit de uitkomst van praktijktesten. Tot slot gaan we in hoofdstuk 5 in op de wijze waarop toezicht en verantwoording over informatieveiligheid is geregeld.

2 Beleid

In dit hoofdstuk staat het informatiebeveiligingsbeleid van de provincie Gelderland centraal. Ook is er aandacht voor de planning van informatieveiligheid, bijvoorbeeld de informatiebeveiligingsjaarplannen.

Normen

- De provincie heeft een beleidskader informatieveiligheid:
  - dat is vastgesteld op minimaal directieniveau;
  - maximaal vier jaar oud is en gewijzigd is bij belangrijke ontwikkelingen en
  - gebaseerd op de Interprovinciale Baseline Informatieveiligheid.

Bevindingen

- Het managementteam van de afdeling Informatievoorziening & Automatisering stelde het informatiebeveiligingsbeleid op 9 februari 2016 vast. Het beleid is gebaseerd op de Interprovinciale Baseline Informatie-veiligheid. Aan de verschillende categorieën van de IBI is een hoofdstuk gewijd met doelen, risico's en beheersmaatregelen. Het beleid is door organisatorische en wettelijke wijzigingen niet actueel meer.
- In het beleid staat dat er een meerjarenplanning en jaarplannen voor informatieveiligheid worden gemaakt. De afgelopen jaren is er in de praktijk niet gewerkt met een meerjarenplanning, op één jaar na waren er wel jaarplannen. Hierin stonden doelen en een activiteitenoverzicht voor betreffend jaar.

2.1 Informatiebeveiligingsbeleid

Visie, doel en uitgangspunten

Het managementteam van de afdeling Informatievoorziening & Automatisering stelde op 9 februari 2016 het informatiebeveiligingsbeleid vast.[8] In dit beleid noemt de provincie als **visie** dat zij de komende jaren inzet op het verhogen van informatieveiligheid en verdere professionalisering van de informatiebeveiligingsfunctie. Een betrouwbare informatievoorziening noemt zij noodzakelijk voor het goed functioneren van de organisatie en de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

Als **doel** geeft de provincie aan dat het informatiebeveiligingsbeleid het kader is voor passende personele, organisatorische en technische maatregelen om informatie te beschermen en te waarborgen, zodat de organisatie voldoet aan relevante wet- en regelgeving. Er wordt naar gestreefd om 'in control' te zijn en daarover op passende wijze verantwoording af te leggen. In control betekent dat de provincie weet welke maatregelen genomen zijn, dat er een SMART-planning is van de maatregelen die nog niet genomen zijn en als laatste dat dit geheel verankerd is in de zogenoemde 'plan, do, check, act (PDCA)-cyclus'.

Het informatiebeveiligingsbeleid kent de volgende **uitgangspunten**:

1. Het informatiebeveiligingsbeleid van de provincie Gelderland is in lijn met het algemene beleid van de provincie en de relevante wet- en regelgeving.
2. Het beleid is gebaseerd op de Interprovinciale Baseline Informatieveiligheid (IBI) die is afgeleid van de Code voor Informatiebeveiliging (NEN/ISO 27002).
3. Voor iedere maatregel uit de IBI geldt: Pas toe of leg uit. De uitleg bevat altijd een risicoafweging.
4. Het informatiebeveiligingsbeleid wordt vastgesteld door de directie. Het beleid wordt minimaal één keer per vier jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld.

Dat het beleid gebaseerd is op het IBI (uitgangspunt 2) blijkt uit het feit dat dat de hoofdstukken van het beleid overeenkomen met de categorieën van het IBI. De provincie noemt voor elk van de categorieën beheersmaatregelen die zij relevant vindt om te nemen, met daarbij de doelen die zij wil bereiken en de risico's die zij wil beheersen. Het volgende kader geeft een voorbeeld van deze opzet.

[8] *Terugkoppeling AMT I&A 9 februari 2016 [excel-bestand].*

Voorbeeld opzet beleid

Hoofdstuk 14: Beveiliging van informatiesystemen

14.1 Risico's
Als beveiliging geen onderdeel uitmaakt van informatiesystemen is de betrouwbaarheid van de informatie niet gewaarborgd.

14.2 Doelstelling
Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.

14.3 Beheersmaatregelen [NB 3 van de 13]
- Projecten met een hoog risicoprofiel worden altijd getoetst op architectuur en informatiebeveiliging.
- (Web)applicaties worden ontwikkeld en tenminste getest op basis van bekende kwetsbaarheden.
- Beveiligingscertificaten worden centraal beheerd binnen de provincie.

Actualiteit en volledigheid

Het in 2016 vastgestelde informatiebeveiligingsbeleid is op een aantal onderdelen niet actueel meer. Dit komt grotendeels door organisatorische en wettelijke wijzigingen. Zo zijn de werkwijze met uitvoering door een externe partij (zie paragraaf 3.2.2) en de AVG nog niet verwerkt. Eerder heeft de accountant ook al geadviseerd om het informatiebeveiligingsbeleid periodiek te actualiseren en daarbij de nieuwe wet- en regelgeving mee te nemen.[9] In een interview is aangegeven dat er plannen zijn om het informatiebeveiligingsbeleid te actualiseren. Dit wordt opgepakt als er overeenstemming is bereikt met de externe dienstverlener over de precieze rol- en taakverdeling. De gesprekken hierover vinden ten tijde van dit onderzoek nog plaats.

Als actie in zowel het informatiebeveiligingsjaarplan voor 2015 als dat voor 2017 was opgenomen om in overleg met andere stakeholders (bijvoorbeeld Facilitaire Dienstverlening) de scope van het informatiebeveiligingsbeleid te verbreden. Aangegeven is dat - er los van wat in het huidige informatiebeveiligingsbeleid staat - nog geen beleid over fysieke veiligheid is. Het voornemen is hier een protocol voor te ontwikkelen. Wat hierin wordt opgenomen is nog niet bekend. De planning is om dit maart 2019 af te ronden.[10]

Informatieveiligheid krijgt een plek in het bredere informatiebeleid. Hier wordt op dit moment aan gewerkt.

[9] *PWC (december 2017). Rapportage interim-bevindingen 2017 provincie Gelderland p. 11.*
[10] *Ambtelijk interview.*

2.2 Informatiebeveiligingsjaarplannen

Beleid over planning

De provincie Gelderland noemt informatiebeveiliging in haar beleid een continue verbeterproces en geeft aan dat de 'Plan-Do-Check-Act-methodiek' het managementsysteem voor informatiebeveiliging vormt. Het hierboven beschreven organisatiebrede informatiebeveiligingsbeleid is slecht één van de onderdelen van de PLAN uit de PDCA-cyclus. In het beleid wordt ook gesproken over een meerjarenplanning, jaarplanning en beveiligingsplannen.

Planning in de praktijk

In de praktijk maakt de provincie geen meerjarenplanning voor informatiebeveiliging. Als reden is aangegeven dat een meerjarenplanning geen meerwaarde heeft, vanwege de snelheid van ontwikkelingen op het gebied van informatieveiligheid.

De Information Security Officer heeft jaarplannen informatiebeveiliging gemaakt voor 2015 en 2017. Hierin staan de doelen voor betreffende jaar en een overzicht van de te ondernemen activiteiten. Dergelijke jaarplannen worden besproken in en vastgesteld door het operationele security team (zie paragraaf 3.2.1). Facilitaire Dienstverlening (verantwoordelijk voor de fysieke beveiliging) is niet bij de informatiebeveiligings-plannen betrokken.[11] Een informatiebeveiligingsplan voor 2018 is niet gemaakt, omdat de focus lag op de transitie van de IT-dienstverlening naar een externe partij.[12] Het is de bedoeling voor 2019 weer een plan te maken.[13]

[11] *Ambtelijke interviews.*
[12] *Over 2016 was aangegeven dat dit plan destijds wel gemaakt was, maar momenteel niet meer vindbaar was (telefonisch genoemd bij toelichting op aangeleverde informatie).*
[13] *Schriftelijke antwoorden provincie Gelderland 13 juli 2018.*

3 Sturing en verantwoordelijkheid

In dit hoofdstuk gaan we na of de provincie Gelderland de sturing op en verantwoordelijkheid voor informatieveiligheid goed heeft verankerd. Allereerst gaan we in op de betrokkenheid van GS en management bij informatieveiligheid. Vervolgens is er aandacht voor de verantwoordelijkheidsverdeling rondom informatieveiligheid. Hierbij maken we onderscheid tussen de interne organisatie en de externe dienstverlening.

Normen

- De provincie heeft informatieveiligheid als onderdeel van de portefeuille van een lid van GS belegd.
- Bestuur en management van de provincie zijn zich bewust van de risico's die ze lopen en hun verantwoordelijkheid daarin.
- Er is een duidelijke verantwoordelijkheidsverdeling voor informatieveiligheid en deze is vastgelegd.

Bevindingen

- Informatieveiligheid is belegd bij de gedeputeerde met 'informatie-voorziening & automatisering' in de portefeuille. GS zijn tot nu toe vooral betrokken bij datalekken. Er zijn geen structurele rapportages aan GS over informatieveiligheid.
- De directie heeft de verantwoordelijkheid voor informatieveiligheid gedelegeerd naar de afdelingsmanager I&A. De directie stelt het informatie-beveiligingsbeleid niet vast en ontvangt geen halfjaarlijkse rapportages conform beleid. Afgesproken is dat zij worden geïnformeerd rondom projecten die gaan over / raken aan informatieveiligheid (bv. AVG) en als er iets speelt (bv. incidenten of testen).

Vervolg bevindingen op de volgende pagina.

Vervolg bevindingen

- Het management is vooral betrokken op het niveau van de afdelings-manager. Met name het management van I&A heeft een aantal besluiten genomen, bijvoorbeeld de vaststelling van het informatiebeveiligingsbeleid en een aantal uitwerkingen daarvan. Het afdelingsmanagement wordt geïnformeerd als er iets speelt bijvoorbeeld een datalek of testresultaten. In die gevallen hebben zij ook een taak: namelijk GS informeren respectievelijk opvolging faciliteren.
- De provincie Gelderland heeft in haar informatiebeveiligingsbeleid aandacht voor verdeling van verantwoordelijkheden binnen de organisatie. Deze sluit echter niet op alle punten aan op de huidige praktijk. Zo komt het operationeel security team niet aan de orde en IB-coördinatoren en het vakberaad informatieveiligheid worden wel genoemd, maar die bestaan niet.
- De provincie besteedt sinds kort een groot deel van haar IT-taken uit. Informatieveiligheid is in de aanbesteding meegenomen. De implementatie loopt moeizaam. Het informatiebeveiligingsplan van de externe dienstverlener is december 2018 definitief geworden.

3.1 Betrokkenheid van GS en management

Bij informatieveiligheid gaat het niet alleen om ICT, maar ook om de basisinfrastructuur en mens & organisatie. Informatieveiligheid is daarom een breed en complex onderwerp, dat de hele organisatie raakt. Informatieveiligheid kan een politiek-bestuurlijke impact hebben, wanneer gevoelige informatie bijvoorbeeld in verkeerde handen valt of cyberaanvallen de organisatie raken. Om deze redenen kan informatieveiligheid niet alleen de verantwoordelijkheid van de ambtelijke organisatie zijn, maar is het van belang dat informatieveiligheid bestuurlijk is belegd. Om de veiligheid van informatie te borgen, hebben de provincies in het Convenant Interprovinciale Regulering Informatieveiligheid daarom afgesproken dat zij informatieveiligheid bestuurlijk beleggen binnen de provincie.

Het bestuurlijk beleggen van informatieveiligheid alleen is niet voldoende. Het is ook van belang dat GS en het management in de praktijk invulling geven aan deze verantwoordelijkheid. In het convenant hebben de provincies met elkaar afgesproken dat het bestuur en het management van iedere provincie zich bewust moeten zijn van de risico's die de provincie loopt en hun rol en verantwoordelijkheid daarin. GS en het management moeten daarom regelmatig worden geïnformeerd over de stand van zaken op het gebied van informatieveiligheid. Daarnaast is het van belang dat het management actief om informatie vraagt aan de ambtelijke organisatie en op cruciale onderdelen besluiten neemt ten aanzien van informatieveiligheid.

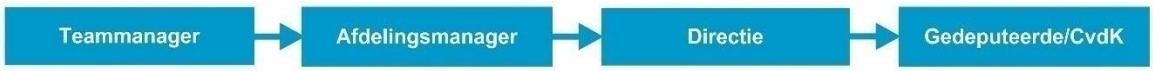
In lijn met bovenstaande kijken we in deze paragraaf naar de betrokkenheid van GS en management. Onder management verstaan we de directie en afdelingsmanagers.

3.1.1 Betrokkenheid van GS

Beleid over de rol van GS

In het informatiebeveiligingsbeleid (hierna: beleid) komt de rol van Gedeputeerde Staten aan de orde bij de 'rapportage en escalatielijn'. Die ziet er als volgt uit:

Figuur 4: *Rapportage- en escalatielijn voor informatieveiligheid*



Bron: Provincie Gelderland (februari 2016). Informatiebeveiligingslijn provincie Gelderland versie 1.1, p. 15.

In figuur 4 staat de Gedeputeerde/CvdK genoemd als laatste in de keten van informatievoorziening. Er is aangegeven dat afhankelijk van de inhoud de keten in de volgorde wordt uitgevoerd, maar ook ingekort kan worden.[14]

Rol van GS in de praktijk

Ambtelijk wordt aangegeven dat GS politiek verantwoordelijk zijn voor informatieveiligheid. Informatieveiligheid is ondergebracht bij de gedeputeerde met 'Informatievoorziening & Automatisering' in de portefeuille. GS zijn op dit moment niet actief betrokken bij informatieveiligheid. Er is het vertrouwen dat het goed gaat. De informatievoorziening aan GS over het thema is niet structureel/minimaal. Zij ontvangen hier geen periodieke rapportages over. Wel worden GS geïnformeerd bij incidenten zoals datalekken (zie kader). Het rapporteren aan GS bij een datalek is daarbij de verantwoordelijkheid van de afdeling waar het datalek heeft plaatsgevonden en gebeurt aan de gedeputeerde die betreffende afdeling in de portefeuille heeft. Tot op dit moment (sept. 2018) zijn er zes datalekken gemeld bij de Autoriteit Persoonsgegevens.[15]

Datalekken

Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegeven bij een organisatie zonder dat dit de bedoeling was. Sinds 1 januari 2016 is in Nederland de meldplicht datalekken van kracht. Dit betekent dat organisaties die persoonsgegevens verwerken in bepaalde gevallen een datalek binnen 72 uur moeten melden aan de Autoriteit Persoonsgegevens (AP) en aan betrokkenen (de personen op wie de gegevens betrekking hebben).[16]

De provincie Gelderland beschikt over een protocol meldplicht datalekken. Een belangrijk onderdeel hierin is het stappenplan met de afwegingen over er sprake is van een datalek, of dit gemeld moet worden aan AP en/of betrokkenen. Het protocol is gebaseerd op een model zoals beschikbaar gesteld door de Autoriteit Persoonsgegevens. In het protocol is aangegeven dat medewerkers verplicht zijn een hulplijn (de Functionaris Gegevens-bescherming) in te schakelen. In het protocol is geen aandacht voor de betrokkenheid van management en bestuur.

[14] *Provincie Gelderland (februari 2016). Informatiebeveiligingsbeleid provincie Gelderland versie 1.1, p. 15.*
[15] *Schriftelijke informatie van de provincie Gelderland.*
[16] *https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken*

3.1.2 Betrokkenheid van management

Beleid over de rol van het management

In het beleid staat informatie over de verantwoordelijkheid van de directie en het management bij informatieveiligheid. Hierin staat:

- De **directie** is verantwoordelijk voor het opstellen, uitvoeren, handhaven, bewaken en uitdragen van het beleid. Zij maakt een inschatting van het belang en de risico's van verschillende delen van de informatievoorziening voor de organisatie en bepaalt welke risico's acceptabel en niet acceptabel zijn. De verantwoordelijkheid van de directie wordt geduid als de beslissende of sturende rol.
- Het **afdelingsmanagement Informatievoorziening & Automatisering** (I&A) is verantwoordelijk voor het opstellen van de kaders voor informatiebeveiliging en (de bewaking van) de implementatie daarvan. Hij/zij geeft namens de directie op dagelijkse basis invulling aan de sturende rol door besluitvorming in de directie voor te bereiden en toe te zien op de uitvoering ervan.
- Het **lijnmanagement** (proceseigenaren) zijn verantwoordelijk voor de sturing op informatieveiligheid en de controle op naleving.[17]

Om verantwoordelijkheid te kunnen nemen, is informatie noodzakelijk. In het beleid staat het volgende over rapportages over informatieveiligheid:

- Over het functioneren van informatiebeveiliging wordt jaarlijks gerapporteerd conform de P&C-cyclus.
- De Information Security Officer rapporteert eens per half jaar over de stand van zaken. Daarbij gaat het om een rapportage aan de directie.
- Bevindingen van externe controles van de informatieveiligheid worden gerapporteerd aan de afdelingsmanager I&A en desgewenst wordt de directie geïnformeerd.
- Alle afdelingen rapporteren aan de directie/ISO. Dit gaat onder andere over bedrijfscontinuïteit.

Rol van het management in de praktijk

Rol van de directie in de praktijk

Ambtelijk wordt aangegeven dat de directie de verantwoordelijkheid voor informatieveiligheid heeft gedelegeerd naar het afdelingsmanagement I&A. Besluiten worden veelal daar genomen. [18] Zo is het informatiebeveiligingsbeleid van de provincie Gelderland niet vastgesteld door de directie zoals in het beleid staat, maar heeft het afdelingsmanagementteam (AMT) van I&A dat gedaan.

[17] *Meer specifiek is over de taken van de afdelingsmanager in het beleid aangegeven dat diegene: op basis van een expliciete risicoafweging betrouwbaarheidseisen voor zijn informatiesystemen vaststelt (classificatie); verantwoordelijk is voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit betrouwbaarheidseisen; stuurt op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn) en rapporteert over wet- en regelgeving en algemeen beleid van de provincie in de managementrapportages. Ook is in het beleid expliciet genoemd dat het toezicht houden op informatiebeveiliging binnen afdelingen (zoals het uitvoeren van risicoanalyses, het bijhouden van autorisatiematrices en het uitvoeren van clean desk) is belegd bij de afdelingsmanagers.*

[18] *Ambtelijk interview en schriftelijke informatie 23 november 2018.*

De directie ontvangt geen structurele rapportages conform het beleid. Na overleg met de directie is besloten dit te laten vervallen. Reden hiervan is de hoeveelheid informatie en overleggen. Zij worden nu geïnformeerd over informatieveiligheid als:

- er incidenten hebben plaats gevonden;
- er uitkomsten van praktijktesten bekend zijn en
- het onder een bepaald project (zoals de ISO 27001-certificering of de AVG) hangt.[19]

Daarnaast zijn zij in de bewustwordingscampagne betrokken. Zo was een phishing mail die dit jaar is verstuurd zogenaamd van de provinciesecretaris afkomstig.

Wat betreft bijeenkomsten gaf een directielid in januari 2018 een toelichting aan PS over een datalek dat had plaatsgevonden (zie meer informatie paragraaf 5.2) en is de directie in juni 2018 op bezoek geweest bij het datacenter van de provincie in Amsterdam.

Afdelingsmanagement I&A

Zoals hierboven genoemd wordt in de praktijk de verantwoordelijkheid voor informatieveiligheid door de directie vooral gelegd bij het afdelingsmanagement Informatievoorziening & Automatisering. Het gaat hier om de verantwoordelijkheid voor de operationele invulling. Dit betreft overigens alleen verantwoordelijk is voor het ICT-deel van informatieveiligheid. Een deel van de verantwoordelijkheid ligt ook bij (het management van de) de afdelingen Facilitaire Zaken en Personeel & Organisatie.

De afdelingsmanager van I&A neemt besluiten over zaken die informatieveiligheid raken. Het gaat bijvoorbeeld om:

- het vaststellen van het informatiebeveiligingsbeleid en uitwerkingen daarvan zoals accountbeleid en patchbeleid[20] (als lid van het afdelingsmanagement van I&A);
- besluiten omtrent budget: informatieveiligheid wordt veelal betaald vanuit het budget van de afdeling I&A en de afdelingsmanager is budgethouder;
- besluiten als deelnemer van het Strategisch Informatie Overleg (SIO). Dit is een landelijk overleg in IPO-verband. Hierin worden ook beslissingen genomen die raken aan informatieveiligheid. Zo besloten zij recentelijk om zich voor te bereiden op ISO-certificering.[21]

De Information Security Officer is formeel ondergebracht bij de afdeling I&A, maar rapporteert rechtstreeks aan de directie. Het afdelingshoofd I&A ontvangt dezelfde informatie. Hierbij gaat het bijvoorbeeld om de uitkomsten van praktijktesten van informatieveiligheid. Het afdelingshoofd heeft geen invloed op deze informatie-voorziening aan de directie anders dan achteraf, zo is aangegeven. Hier is voor gekozen omdat de ISO deels rapporteert over zaken die de afdeling I&A in beheer heeft. Rol van het afdelingsmanagement bij de testresultaten is het faciliteren van opvolging en te controleren of dat gebeurt. Behalve de uitkomsten van testen ontvangt het

[19] *Ambtelijk interview.*
[20] *Patchbeleid en accountbeleid kunnen gezien worden als een nadere uitwerking van het informatiebeveiligingsbeleid. In het patchbeleid ('life cycle management') staan afspraken over het updaten van software. Het accountbeleid heeft als doel om ervoor te zorgen dat gebruikers precies genoeg rechten krijgen om hun werk uit te voeren gedurende de tijd dat ze voor de provincie werken. Meer over patchbeleid en accountbeleid in paragraaf 4.1.3 van dit rapport.*
[21] *Ambtelijk interviews.*

afdelingsmanagement I&A bijvoorbeeld ook de informatiebeveiligingsjaarplannen (zie paragraaf 2.2). Deze worden door het afdelingsmanagement vanaf de zijlijn gevolgd. De ISO en de adviseur veiligheid hebben ook informeel overleg met het afdelings-management I&A respectievelijk het afdelingsmanagement van Facilitaire Dienstverlening. Informatie gaat dus niet alleen via rapportages, maar ook mondeling.[22]

Lijnmanagement

Ambtelijk wordt bevestigd dat er bij informatieveiligheid ook een rol ligt bij de afdelingsmanagers. Zij moeten bevorderen dat medewerkers van hun afdeling zich houden aan de richtlijnen voor informatieveiligheid in het beleid. In de praktijk betekent dat vooral het goede voorbeeld geven. Ook worden zij ingeschakeld om workshops over informatieveiligheid voor hun afdeling te faciliteren. Die workshops worden gegeven door de ISO, meer hierover is te vinden paragraaf 4.1.3. Verder zouden zij als hr-manager informatieveiligheid een keer aan bod moeten laten komen in gesprekken met de medewerkers. Het is niet duidelijk is in hoeverre dit in de praktijk gebeurt, want dit wordt niet gerapporteerd.

Om het management te faciliteren wordt het informatiebeveiligingsbeleid beschikbaar gesteld via Intranet (beleidsportaal I&A) en is de ISO beschikbaar voor advies en vragen. Ook wordt er af en toe in management overleggen aandacht aan besteed. Zo kwam onlangs het thema digitale vaardigheden (waar bewustwording en vaardigheden omtrent informatiebeveiliging onder valt) aan de orde in een vergadering van het 'management team breed'.[23]

3.2 Verantwoording uitvoerende rollen en verantwoordelijkheden

Om informatieveiligheid organisatorisch goed te verankeren, is het van belang dat er een duidelijke verantwoordelijkheidsverdeling is binnen de organisatie. Het niet expliciet beleggen van verantwoordelijkheden (en bijbehorende activiteiten, procedures en instrumenten) belemmert het daadwerkelijk en structureel uitvoeren en borgen van de beheersmaatregelen. Omdat informatieveiligheid betrekking heeft op verschillende aandachtsgebieden (mens & organisatie, basisinfrastructuur, ICT), is het daarbij van belang dat meerdere disciplines betrokken zijn bij informatieveiligheid.

3.2.1 Interne organisatie

Bedrijfsvoeringsafdelingen

In het informatiebeveiligingsbeleid staat genoemd dat bedrijfsvoeringsafdelingen verantwoordelijk zijn voor de uitvoering van het betreffende beleid. Het gaat hier om drie afdelingen:

- Personeel & Organisatie voor de arbeidsvoorwaardelijke zaken;

[22] *Ambtelijke interviews.*
[23] *Ambtelijke interviews.*

- Facilitaire Zaken voor de fysieke toegangsbeveiliging en
- Informatievoorziening & Automatisering voor de technische beveiliging.

Wat betreft I&A is het goed om hier te noemen dat de provincie een belangrijk deel van haar ICT-dienstverlening heeft uitbesteed aan een externe dienstverlener. Het contract hiertoe is mei 2017 getekend. Het ICT-deel van informatiebeveiliging is hier onderdeel van. Deze transitie betekent dat de I&A organisatie wordt omgevormd tot een regieorganisatie. Ambtelijk werd benadrukt dat, ondanks dat de uitvoering deels elders plaatsvindt, de provincie hier verantwoordelijk voor blijft.

In het beleid is een omschrijving van de verantwoordelijkheid van de bedrijfsvoerings-afdelingen opgenomen. Hierin staat dat deze afdelingen verantwoordelijk zijn voor beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen en voor alle beheeraspecten van informatiebeveiliging zoals ICT-, facilitaire en personele zaken. Ook verzorgen zij logging[24], monitoring en rapportage en leveren zij beveiligingsadvies. De beveiligingsmaatregelen waar het concreet om gaat, staan ook in het beleid genoemd. Hierbij is niet per (groep) maatregel(en) aangegeven wie daarvoor verantwoordelijk is.

Niet alle medewerkers van de bedrijfsvoeringsafdelingen houden zich natuurlijk even veel bezig met informatieveiligheid. Bij de afdeling I&A zijn vooral de leden van het operationeel security team en in het bijzonder de Information Security Officer (vanuit een onafhankelijke rol) er mee bezig. Bij de afdeling Facilitaire Dienstverlening is er een adviseur veiligheid. Deze houdt zich bijvoorbeeld bezig met de voorbereiding van en eventuele maatregelen omtrent bijeenkomsten en bezoeken en de dagelijkse veiligheid van het gebouw. Het operationeel security team en de adviseur veiligheid worden in het beleid niet genoemd, de ISO wel. In het beleid worden ook nog IB-coördinatoren[25] genoemd, maar die zijn er niet.

Information Security Officer en operationeel security team

Information Security Officer

In 2014 is er binnen de provincie Gelderland een Information Security Officer (ISO) benoemd. Zijn verantwoordelijkheden en taken zijn volgens het beleid:

- namens de afdelingsmanager I&A (functioneel) verantwoordelijk voor de realisatie van de kaderstelling en sturing;[26]
- de uitvoering van het beleid;
- gevraagd en ongevraagd adviseren over informatieveiligheid en eens per half jaar rapporteren over de stand van zaken;
- bevorderen van de algehele communicatie en bewustwording rondom informatieveiligheid en

[24] Informatiesystemen en ICT-infrastructuur genereren loginformatie voor veel activiteiten, soms als normale statusmelding, soms als resultaat van een activiteit van een gebruiker of beheerder maar ook informatie als resultaat van onvoorziene omstandigheden of fouten. Een log beschrijft wat er gebeurt binnen systemen (Bron: IBD (jan. 2014). Aanwijzing logging, p. 5).

[25] IB is een afkorting voor informatiebeveiliging.

[26] Deze sturing heeft betrekking op: (a) concern risico's (b) de getroffen maatregelen, die overeenstemmen met de betrouwbaarheidseisen en/of deze voldoende bescherming bieden en (c) actualiteit van het informatiebeveiligingsbeleid en stelt deze waar nodig bij.

- namens de directie zorgen voor toezicht op de uitvoering van het beleid.[27]

De halfjaarlijkse rapportages (derde bullet) zijn de laatste jaren niet gemaakt. Aangegeven is dat dit mede komt doordat de transitie van IT-taken naar een externe dienstverlener ook veel tijd heeft gekost van de ISO. Het plan is deze rapportages in de toekomst weer op te pakken.

De ISO werkt voltijd aan informatieveiligheid. In de praktijk is er de laatste jaren veel tijd gegaan naar de uitbesteding van de IT-dienstverlening (omdat informatieveiligheid hier een belangrijk onderdeel van is) en naar bewustwordingsactiviteiten.[28]

In het beleid wordt genoemd dat de ISO een onafhankelijke positie heeft. Aangegeven wordt dat die onafhankelijke positieve een objectieve toetsing van genomen besluiten en onderzoeksresultaten waarborgt. In interviews wordt hierbij vooral benadrukt dat de ISO rechtstreeks rapporteert aan de directie en niet aan het afdelingsmanagement (zie eerdere toelichting in paragraaf 3.1.2). Ook wordt bij de onafhankelijk van de ISO een voorbeeld omtrent kosten gegeven. De ISO heeft een eigen budget, over het algemeen bedoeld voor relatief kleine onderzoeken. Dit betekent dat grotere projecten en acties van het budget van de afdeling I&A gaan, bijvoorbeeld uit het 'potje' voor applicatiebeheer. Wanneer het afdelingshoofd I&A (als budgethouder) en de ISO het niet eens zouden kunnen worden, dan kan de ISO naar de directie gaan. Overigens is dit in de praktijk nog niet voorgevallen.[29]

In het informatiebeveiligingsbeleid staat als uitgangspunt dat de provincie benodigde mensen en middelen beschikbaar stelt om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in het beleid. Hierover bestonden verschillende beelden. Enerzijds werd aangegeven dat beschikbare financiële middelen voldoende waren en dat de provincie in vergelijking met andere soortgelijke organisaties goed zit qua beschikbare personele capaciteit. Anderzijds werd aangegeven dat er geen oordeel over de beschikbare financiën gegeven kon worden en dat er over gedebatteerd kon worden of de beschikbare capaciteit afdoende was. Hierbij werd aangegeven dat er soms zaken rondom IT en informatiebeveiliging nog niet in documenten beschreven zijn doordat er geen tijd voor was (andere taken en prioriteiten).[30]

Operationeel security team

Er zijn een aantal personen bij I&A aangewezen voor specifieke taken rondom informatiebeveiliging. Deze personen vormen samen het operationeel security team. In het informatiebeveiligingsbeleid komt dit team niet aan de orde. Het operationeel security team is zo'n vier jaar geleden van start gegaan. Het team kent drie leden: de ISO, een technisch architect en een adviseur infrastructuur. De laatste twee houden zich een deel van hun tijd met informatieveiligheid bezig. De ISO staat aan het hoofd van het team. Als de ISO niet beschikbaar is, nemen de leden van het security team waar ('achtervang'). Het team houdt zich - zoals de naam al zegt - bezig met allerlei

[27] *Meer specifiek staat bijvoorbeeld genoemd dat de ISO de classificaties van bedrijfskritische systemen centraal vastlegt en de algehele communicatie en bewustwording rondom informatieveiligheid bevordert.*
[28] *Ambtelijk interview.*
[29] *Ambtelijk interview.*
[30] *Ambtelijke interviews.*

operationele zaken rondom informatieveiligheid. Het gaat daarbij specifiek om de ict/techniek. Concreet worden bijvoorbeeld informatiebeveiligingsjaarplannen en testresultaten in het team besproken.

Overleg en samenwerking

Het is vooral de ISO die de contacten met de andere afdelingen onderhoudt. Hiervoor is geen structureel overleggremium ingesteld, maar overleg vindt informeel plaats indien dit nodig wordt geacht. Zo heeft de ISO een á twee keer per week contact met de adviseur veiligheid.[31]

In het beleid worden twee interne teams / overleggen genoemd.

- Voor interne crisisbeheersing is er een **kernteam IB**, bestaande uit de ISO, een jurist en een communicatiemedewerker. In een interview werd aangegeven dat de Functionaris Gegevensbescherming ook deel is van het team. Het kernteam IB wordt samengesteld op basis van beschikbaarheid op het moment van het optreden van een ernstig beveiligingsincident.[32] De betrokkenheid van een communicatie-medewerker is afhankelijk van de mate waarin het incident media-aandacht genereerd.[33] Bij incidenten gaat het veelal om datalekken. Tot nu toe zijn er zes gemeld bij de Autoriteit Persoonsgegevens. De procedure voor datalekken met het kernteam is nu drie keer toegepast. Of dit gebeurt is afhankelijk van de grootte en de ernst van het datalek.
- In het beleid staat dat de ISO minimaal eenmaal per jaar een **vakberaad informatiebeveiliging** organiseert. Er is aangegeven dat dit overleg binnen de provincie een adviesfunctie heeft richting de directie en zich met name richt op beleid en adviseert over strategische en/of tactische informatiebeveiligings-kwesties. Er staat niet bij wie de (beoogde) deelnemers aan het vakberaad zijn. Navraag leert dat het vakberaad in de praktijk niet gehouden wordt.

Organisatie overig

Tot slot zijn er binnen de organisatie ook nog andere functies die niet specifiek gaan over informatieveiligheid, maar er wel aan raken. Hierbij kan gedacht worden aan de Functionaris Gegevensbescherming.[34] Ook zijn er meerdere personen (bv. informatieadviseurs van de afdeling I&A) die zich bezig houden met digitalisering en digitale vaardigheden.[35] Hier valt informatieveiligheid ook onder.

[31] *Ambtelijk interviews.*
[32] *Provincie Gelderland (juli 2016). Huidige situatie informatiebeveiliging [intern document], p. 4.*
[33] *Ambtelijk interview.*
[34] *Deze functionaris informeert en adviseert de organisatie bij onderwerpen die betrekking hebben op de AVG. Daarnaast is deze functionaris verantwoordelijk voor het contact met de Autoriteit Persoonsgegevens. De FG'er is ondergebracht bij Control (Bron: https://www.gelderland.nl/Privacybeleid en ambtelijk interview).*
[35] *Er is een Digitale Innovatie Tafel (DIT). Doel daarvan is het vormgeven van de digitale ambitie van de provincie en het ondersteunen van de organisatie bij digitale opgaven en het verbeteren en vernieuwen van hun proces door digitalisering. Het DIT komt maandelijks samen en er zit een vertegenwoordiger in vanuit ieder beraad en een vertegenwoordiger vanuit het Digitaal Innovatie Platform. De belangrijkste rollen van dit Platform zijn: de organisatie steunen bij innovatie door digitalisering en helpen bij (verplichte) digitale opgaven en portofoliomanagement. De kern van het platform zijn de informatieadviseurs van de beraden. Sinds 1 oktober is er een manager digitale transformatie (Bron: Intranet provincie Gelderland).*

3.2.2 Externe dienstverlening

In voorgaande paragraaf werd duidelijk dat de provincie Gelderland een groot deel van haar IT (waaronder informatieveiligheid) heeft uitbesteed externe dienstverleners. De belangrijkste externe dienstverlener is sinds kort OGD ict-diensten. Daarnaast zijn er andere externe leveranciers die applicaties voor de provincie leveren. Aangezien de provincie de afgelopen tijd vooral met de uitbesteding naar OGD bezig is geweest, gaan we hier kort op in.

Het traject begon in 2015 met het besluit van de provincie dat zij een belangrijk deel van haar IT-taken wilde uitbesteden. Als reden hiervoor gaven GS aan dat de snelheid van ICT-ontwikkelingen noopte om keuzes te maken waar de provinciale organisatie zich wel en niet in wilde specialiseren. Hierbij is in het 'in het belang van de continuïteit voor de toekomst van de dienstverlening' besloten:

- strategisch adviseurs en informatiearchitecten in dienst van de provincie te houden (zodat de provincie in staat is zelf de juiste keuzes te maken over welke hard- en software binnen welke architectuur nodig zijn om het werk goed te kunnen doen) en
- de uitvoerende kant van I&A, het beheer en onderhoud van hardware en het technisch beheer van software en applicaties te gaan outsourcen aan daarin gespecialiseerde bedrijven.[36]

In september 2016 heeft de provincie haar (aangepaste) aanbesteding uitgezet. Informatieveiligheid kwam in deze aanbesteding duidelijk aan de orde: als een apart subgunningscriterium wat 15% van het in totaal te behalen punten vormde[37] en in het Programma van Eisen hadden 44 van de 121 gestelde eisen betrekking op het onderdeel informatieveiligheid.[38] Binnen het subgunningscriterium informatieveiligheid kwamen de volgende thema's terug: security incidenten, security bedreigingen en kwetsbaarheden, privacy, compliance en beveiligingsbewustzijn.[39]

In mei 2017 ondertekenden de directeuren van de provincie en OGD ict-diensten het contract voor de levering aan IT-diensten aan de provincie Gelderland. Het gaat hierbij om een contract van minimaal vier jaar[40], waarbij OGD de diensten rondom infrastructuur, hosting, werkplekken en servicedesk van de provincie overneemt en uitvoert. In het contract staan bepalingen die betrekking hebben op informatieveiligheid.[41] Op 17 juli 2017 heeft OGD de genoemde diensten officieel overgenomen.[42]

[36] *Provincie Gelderland (april 2016). PS2016-217 Antwoord van GS Gelderland op schriftelijke Statenvragen van SP over personeelsbeleid en bedrijfsvoering.*
[37] *Ambtelijk interview.*
[38] *Provincie Gelderland (september 2016). Bijlage B-008 Programma van Eisen - Infrastructuur, hosting, werkplek en servicedesk.*
[39] *Provincie Gelderland (september 2016). Bijlage C-007 Antwoordtemplate Informatiebeveiliging - Infrastructuur, hosting, werkplek en servicedesk.*
[40] *De provincie Gelderland is gerechtigd de overeenkomst twee keer met een periode van maximaal twee jaar te verlengen onder zelfde voorwaarde (Bron: Provincie Gelderland (juni 2016). Pocket-editie contract OGD).*
[41] *Provincie Gelderland (juni 2016). Pocket-editie contract OGD [Intern document].*
[42] *https://www.gelderland.nl/Griffienieuws/Provincie-heeft-een-nieuwe-IT-leverancier.html*

Implementatie en informatiebeveiligingsplan

De provincie geeft aan dat de implementatie moeizaam verloopt. Naar haar mening was er een duidelijke uitvraag in de aanbesteding gedaan en waren de afspraken in het contract duidelijk. Daar bleken toch verschillende beelden over te zijn, waardoor er discussie is over de sturingswijze. Er is het afgelopen jaar gewerkt aan een informatiebeveiligingsplan. Dit is een plan van OGD voor haar ICT-dienstverlening aan de provincie Gelderland, met betrekking tot infrastructuur, hosting, werkplek en servicedesk. OGD en de provincie hebben meer dan een jaar gesproken over het plan voordat overeenstemming is bereikt. Het plan is 14 december 2018 definitief gemaakt.[43] Het plan is belangrijk voor de borging van informatieveiligheid naar de toekomst. Dat het informatiebeveiligingsplan lange tijd niet definitief was, wilde niet zeggen dat de uitvoering rondom informatieveiligheid nog niet liep. Dat gebeurde al wel op basis van het contract.

In paragraaf 5.1 gaan we nader in op hoe de provincie zicht houdt op de dienstverlening door OGD.

[43] *Ambtelijke interviews en schriftelijke informatie van de provincie Gelderland.*

4 Uitvoering en resultaat

Dit hoofdstuk richt zich ten eerste op de uitvoering van het beleid en de benodigde informatieveiligheidsmaatregelen. Ten tweede wordt er ingegaan op de vraag of de genomen maatregelen voldoende waarborgen bieden tegen oneigenlijke toegang tot systemen en bestanden. Dit betreft de resultaten van testen die toetsen of de informatieveiligheid in de praktijk ook daadwerkelijk op orde is.

4.1 Bepalen en uitvoeren van maatregelen

4.1.1 Bepalen maatregelen

Norm

- De provincie heeft op basis van risicoanalyses bepaald welke aanvullende maatregelen zij moet nemen.
  - Er is inzichtelijk wat de belangrijkste kroonjuwelen zijn en wat het effect van een cyberaanval op deze kroonjuwelen kan zijn.

Bevindingen

- In het beleid staan maatregelen die standaard geïmplementeerd moeten worden. Verder wordt in het beleid uitgegaan van een risicogerichte aanpak. Er is een procesomschrijving voor risicoanalyses opgesteld.
- De provincie houdt zich deels aan haar procesomschrijving voor risico-analyses. Zij heeft Business Impact Analyses uitgevoerd om tot classificatie van informatie te komen, in 2016 op hoofdprocessen en in 2017 en 2018 voor een aantal grotere applicaties. Afhankelijk van de uitkomst van de BIA worden aanvullende maatregelen bepaald. Dit gebeurt naar eigen inzicht en niet via de stap van een kwetsbaarheden- en bedreigingenanalyse zoals de procesomschrijving stelt.

Vervolg bevindingen op de volgende pagina.

Vervolg bevindingen

- Er wordt binnenkort gestart met een tool om op meer systematische wijze te bepalen welke beveiligingseisen in contracten opgenomen moeten worden.
- Binnen de provincie lijkt er overeenstemming over wat essentiële en qua informatieveiligheid gevoelige systemen/applicaties en ruimten zijn. In 2016 bij de BIA's op de hoofdprocessen is de beschikbaarheid van deze essentiële systemen betrokken. De applicaties en bijbehorende classificatie zijn vastgelegd in een database.

In het Convenant Interprovinciale Regulering Informatieveiligheid (2014) spraken de provincies af passende (beheers)maatregelen te implementeren, gebaseerd op risicoanalyse en -afweging. In september 2018 hebben de Nederlandse Beroepsvereniging van Accountants (NBA) en de Cyber Security Raad (CSR) de Cybersecurity Health Check gepubliceerd. Deze health check is bedoeld als een goede start om de belangrijkste cyberrisico's in beeld te brengen en te mitigeren. De health check begint met de fase van 'identificatie'. Hierbij wordt aangegeven dat het van belang is om inzichtelijk te maken wat de belangrijkste 'kroonjuwelen'[44] zijn en wat het effect van een cyberaanval op deze 'kroonjuwelen' kan zijn. In deze paragraaf gaan we in op hoe de provincie Gelderland identificeert welke maatregelen er genomen moeten worden en of kroonjuwelen in beeld gebracht zijn.

Beleid over bepalen maatregelen

In het beleid staat dat de aanpak van informatiebeveiliging van de provincie Gelderland 'risk based' is. Dit betekent dat beveiligingsmaatregelen worden getroffen op basis van een toets tegen de Interprovinciale Baseline Informatiebeveiliging (zie paragraaf 1.2). Als een systeem meer maatregelen nodig heeft (hoe dit wordt bepaald, wordt in het beleid niet genoemd), wordt een risicoanalyse uitgevoerd. De proceseigenaar inventariseert daarvoor de kwetsbaarheid van het werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident. Aangegeven wordt dat hierbij rekening wordt gehouden met de beschermingseisen van de informatie. Het risico is de kans op beveiligingsincidenten en de impact daarvan op het werkproces. Dit risico wordt bepaald door de proceseigenaar. De risicoanalyse kan aanleiding geven tot het nemen van aanvullende beveiligingsmaatregelen.

De provincie heeft het beleid rondom risicoanalyses nader uitgewerkt in een proces-omschrijving.[45] Hierin staat dat informatieveiligheid bij elk initiatief (project/wijziging) meegenomen moet worden in de vorm van een risicoanalyse. Doel is om na te gaan welke aanvullende maatregelen genomen moeten worden bovenop datgene wat standaard moet worden geïmplementeerd door het volgen van het informatieveiligheidsbeleid. Gaat het om gegevens zonder veel risico's dan zijn aanvullende maatregelen waarschijnlijk niet nodig. Om daar achter te komen moet de

[44] *De term kroonjuwelen wordt in het kader van informatieveiligheid vaak gebruikt als term om de belangrijkste processen van een organisatie te beschrijven.*
[45] *Zie: https://organsiatie.prvgld.nl/kennis/architectuurportaal/samenwerkdeel/Paginas/Beveiliging.aspx*

eerste fase van een risicoanalyse, de business impact analyse (BIA), altijd worden uitgevoerd. In figuur 5 geven we de drie fasen uit de procesomschrijving weer.

Figuur 5: *Risicoanalyse informatieveiligheid provincie Gelderland*

Bron: Afbeelding Rekenkamer Oost-Nederland op basis van informatie intranet provincie Gelderland.

De eerste stap is de Business Impact Analyse (BIA). Het doel is om tot een classificatie van de gegevens en/of processen te komen. Daarvoor wordt nagegaan hoe groot de schade is die geleden zou worden als de integriteit, vertrouwelijkheid of beschikbaarheid van betreffend proces en gegevens geschonden zou worden. Dit wordt de gevolgschade genoemd. Het uitvoeren van een BIA is verplicht voor elk project. Afhankelijk van de uitkomst hiervan worden de volgende fasen doorlopen. De tweede fase is een kwetsbaarheden- en bedreigingenanalyse. Hierbij wordt gekeken wat de concrete bedreigingen voor de betreffende gegevens / processen zijn en welke kwetsbaarheden het systeem bevat. De bedreiging in combinatie met de kwetsbaarheid vormt de kans. Samen met het resultaat van de BIA (gevolgschade) wordt nu het risico ingeschat (risico = kans x gevolg). Het kan zijn dat op basis van de BIA en de kwetsbaarheden- en bedreigingenanalyse wordt geconcludeerd dat er geen aanvullende beveiligingsmaatregelen nodig zijn. De laatste fase kan dan worden overgeslagen. Die fase is namelijk het kiezen van aanvullende maatregelen. Met die maatregelen kunnen kwetsbaarheden en daarmee ook het uiteindelijke risico worden aangepakt. Bij het bepalen van de maatregelen moeten risico's, kosten en gebruiksgemak worden afgewogen.

Bepalen van maatregelen in de praktijk

Uitvoering business impact analyses

Ambtelijk wordt aangegeven dat in de praktijk van de drie fasen uit de proces-omschrijving (zie figuur 5) alleen de eerste fase, de Business Impact Analyse, wordt uitgevoerd. Dit is ook de enige fase die verplicht is. Na deze eerste fase worden soms naar eigen inzicht (maatwerk) aanvullende maatregelen bepaald. Hiermee worden de stap van een kwetsbaarheden- en bedreigingenanalyse uit de procesomschrijving overgeslagen. Er is geen specifieke reden genoemd waarom de procesomschrijving niet gevolgd wordt.

In 2016 is gestart met de BIA's. Deze zijn uitgevoerd op de hoofdprocessen/afdelingen van de provincie. Aan de hand van de risicoprofielen die er per hoofdproces uitkwamen, zijn classificeringen toegekend aan applicaties die tot een hoofdproces behoren. Deze

classificering wordt bijgehouden in de ‘service management tool’ van de provincie (Topdesk).

In 2017 en 2018 zijn BIA’s uitgevoerd op de grote applicaties. Hierbij wordt voor de BIA niet sec gekeken naar het product (applicatie) zelf, maar naar het grotere proces waarbinnen dit ingezet (een abstractieniveau hoger dus). In 2017 zijn er vijf BIA’s gehouden en in 2018 zijn tot nu toe twee BIA’s gedaan. De intentie is om in de toekomst meer BIA’s uit te voeren, maar momenteel gaat veel tijd en energie naar de transitie van IT-taken naar OGD.[46]

Eisen informatiebeveiliging bij inkoop en aanbesteding

Binnenkort start de provincie met de tool ‘security proof inkopen’ (wordt nu getest). Hiermee kunnen beveiligingseisen bepaald wordt voor producten, bijvoorbeeld applicaties, die de provincie wil inkopen.[47] De tool is ontwikkeld door een werkgroep van het Centrum voor Informatiebeveiliging en Privacy (CIP) op basis van model van Rijkswaterstaat. In de tool wordt een koppeling gemaakt tussen eisen, beheersdoelen en contractteksten.[48] Door het invullen van een vragenlijst in de tool, wordt bepaald aan welke beheersdoelen voldaan moet worden binnen de aanbesteding en wordt vervolgens een pakket aan eisen gegenereerd die relevant zijn. Die eisen kunnen vervolgens in de aanbesteding / het contract opgenomen worden. Door de tool worden meer systematisch aanvullende maatregelen bepaald, waar tot nu toe per geval naar eigen inzicht werd bedacht wat er extra gevraagd moest worden.[49]

Kroonjuwelen

De provincie Gelderland spreekt niet van kroonjuwelen in haar beleid en andere documenten over informatieveiligheid. In een interview werd gesproken over zogenoemde ‘mission critical systems’: systemen waar de organisatie echt niet zonder kan. Voor de provincie gaat het om systemen die nodig zijn om informatie te verwerken, te communiceren, te besluiten of te betalen (zoals Office, Exchange, DMS en Oracle financials).[50] Verder werd een aantal kleinere specifieke processen en bijbehorende informatie vertrouwelijk genoemd. Het gaat hierbij bijvoorbeeld om de wet bibob (Wet bevordering integriteitsbeoordelingen door het openbaar bestuur), de SBA (Screening en Bewakingsaanpak) en burgemeestersbenoemingen.[51]

Applicaties zoals bovenstaande met bijbehorende classificatie zijn opgenomen in een database. In de BIA’s op hoofdprocessen die eerder in deze paragraaf werden genoemd, is onder meer gekeken naar de beschikbaarheid van deze essentiele systemen. De kwetsbaarheden van deze systemen wordt bijvoorbeeld beperkt doordat deze (uitgezonderd Exchange voor e-mail) niet via internet benaderd kunnen worden. Daarmee zijn ze minder gevoelig voor cyberaanvallen. Er wordt binnen de organisatie soms wel gevraagd of deze openbaar toegankelijk gemaakt kunnen worden vanuit het

[46] *Alinea’s gebaseerd op ambtelijke interviews. De Rekenkamer heeft twee uitgevoerde BIA’s ingezien.*
[47] *Ambtelijk interview.*
[48] *https://www.cip-overheid.nl/wp-content/uploads/2018/04/20180415-Security-Proof-Inkopen-2pager-1.pdf*
[49] *Ambtelijk interview.*
[50] *Ambtelijk interview.*
[51] *Startgesprek en ambtelijk interview.*

oogpunt van gebruiksgemak, maar vanuit het oogpunt van informatieveiligheid is dit niet gebeurd.[52]

Bij informatieveiligheid zijn niet alleen systemen belangrijk, er kunnen ook fysiek plekken zijn waarvan het belangrijk is deze extra te beschermen vanuit het oogpunt van informatieveiligheid. In gesprekken werden onder meer de kamers van de Commissaris van de Koning en GS, de mer-ruimte[53] en de ruimte van SBA genoemd. Voor deze ruimten is er onder meer voor gekozen om extra autorisatie in te zetten. Concreet betekent dit dat een persoon aanvullende rechten nodig heeft op zijn of haar toegangspas.

In de praktijktest die wij door een extern bureau hebben laten uitvoeren, hebben we hen expliciet meegegeven om te kijken of ze bij gevoelige informatie en ruimten konden. De uitkomsten van deze praktijktest zijn te vinden in paragraaf 4.2.

4.1.2 Uitvoering maatregelen

Normen

- De provincie heeft de 'basis' maatregelen genomen en monitort de uitvoering daarvan.
- De provincie controleert de uitvoering van de aanvullende maatregelen die uit de risicoanalyses komen.

Bevindingen

- De provincie heeft in 2016 voor het laatst een zelfevaluatie gedaan om te zien in hoeverre zij de Interprovinciale baseline informatieveiligheid heeft geïmplementeerd. Gelderland scoorde (behalve op het onderdeel beleid) lager dan de provincies gemiddeld. Zij haalde - net als de andere provincies - het gestelde ambitieniveau niet.
- De naleving van de Business Impact Analyses (op basis waarvan aanvullende maatregelen worden bepaald) wordt nog niet gecheckt. Soms wordt bij aanbestedingen getoetst of aan de beveiligingseisen wordt voldaan, maar dat gebeurt in de minderheid van de gevallen.

De provincies spraken in het Convenant Interprovinciale Regulering Informatieveiligheid af dat zij de 'basis' maatregelen van de Interprovinciale Baseline Informatieveiligheid en de aanvullende maatregelen op basis van risico's zouden implementeren. Om een beeld te krijgen of dit gebeurt, kijken we in deze paragraaf naar de wijze en uitkomsten van monitoring en controle van informatieveiligheidsmaatregelen door de provincie Gelderland.

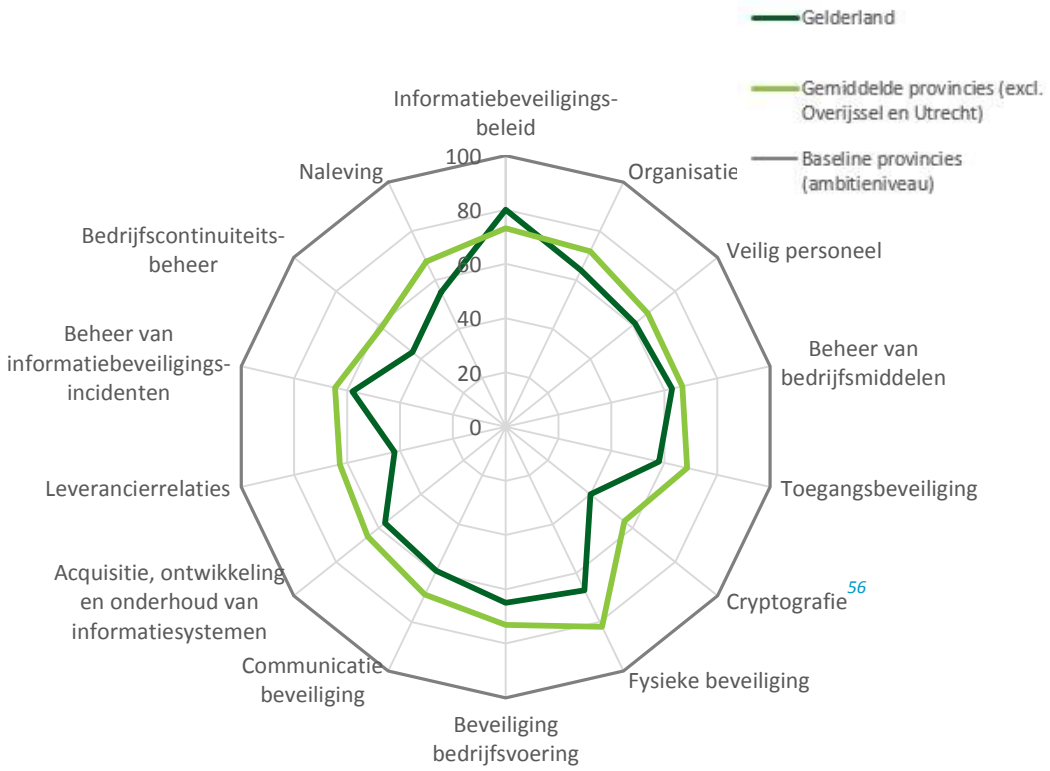
[52] *Ambtelijk interview.*
[53] *MER staat voor Main Equipment Room. Dit is de serverruimte.*

Basis maatregelen

De provincie beschikt niet over één informatiesysteem waarin alle maatregelen uit het beleid en de uitvoering daarvan wordt bijgehouden. Wel heeft zij een managementsysteem (Topdesk geheten) waarin bijvoorbeeld meldingen en wijzigingsverzoeken bijvoorbeeld met betrekking tot informatieveiligheid kunnen worden gedaan. Dit systeem is echter niet geschikt voor een overzicht van alle maatregelen en bijbehorende acties. Dit bijhouden gebeurt nu deels in losse documenten en deels via overleggen.[54]

Wel werd de stand van zaken van de uitvoering voorheen bijgehouden in de interprovinciale monitoringstool van het Cibo.[55] In paragraaf 4.1 lichten we de tool verder toe. De provincie Gelderland heeft de Cibo-monitor voor het laatst ingevuld in 2016. Dit betreft een eigen inschatting en geen controle of de maatregelen daadwerkelijk zijn uitgevoerd. In 2016 kwam er het volgende beeld uit voor de provincie Gelderland:

Figuur 6: *(inter)provinciaal beeld implementatie baseline informatieveiligheid eind 2016*



Bron: Notitie Cibo-monitor juli 2017.

[54] *Ambtelijk interview.*

[55] *In dit platform, onderdeel van het IPO, wisselen provincies kennis en ervaring uit en wordt de gezamenlijke ontwikkeling van informatieveiligheid vormgegeven. Vanuit elke provincie is een deelnemer vertegenwoordigd die werkzaam is op het gebied van informatieveiligheid. Zij hebben in 2010 het IBI opgesteld en in 2016 geactualiseerd.*

[56] *Encryptie is een techniek om informatie te beschermen. Voor toegangsbeveiliging is het belangrijk dat authenticatiegeheimen zoals wachtwoorden worden beschermd tijdens de verwerking, het transport en de opslag. Een solide encryptiebeleid is daarbij een randvoorwaarde. Met encryptiebeleid geeft de organisatie aan hoe zij omgaat met voorzieningen, procedures en certificaten t.b.v. versleuteling van gegevens (Bron: https://www.noraonline.nl/wiki/ISOR:Cryptografie_bij_authenticatie).*

Figuur 6 laat zien dat de provincie Gelderland zichzelf eind 2016 op alle onderdelen van het IBI, uitgezonderd beleid, lager beoordeelde dan het gemiddelde van de provincies. De buitenste grijze ring (100%) is de baseline oftewel het ambitieniveau van de provincies. Aan die ambitie voldoet Gelderland - net als de andere provincies - niet. De provincie Gelderland gaf destijds aan een uitdaging voor zichzelf te zien op het gebied van continuïteits- en leveranciersmanagement. Zij verwachtte gedurende 2017 (wanneer de operationele ICT in beheer zou worden genomen van een externe leverancier) ook op het vlak van informatiebeveiliging een forse kwaliteitsverbetering te realiseren. In 2017 zou de focus liggen op het maken van afspraken met de leverancier, het meetbaar maken van naleving en de werking van maatregelen en de sturing daarop.[57] In 2018 is de provincie hier nog mee bezig.

De interprovinciale monitor biedt voor elke maatregel ruimte voor opmerkingen of een toelichting op het gegeven oordeel. De provincie Gelderland had dit in 2016 bij geen van de maatregelen ingevuld. Daardoor was het voor ons niet goed navolgbaar waar het oordeel op was gebaseerd. Daarnaast is er ruimte voor een toelichting op de te nemen acties naar aanleiding van het oordeel. De provincie Gelderland had deze acties bij geen van de maatregelen ingevuld. Hierdoor was het voor ons niet inzichtelijk welke acties de provincie op basis van het oordeel zou nemen om de scores te verbeteren. De provincie geeft aan dat de monitor kan leiden tot het stellen van prioriteiten die bijvoorbeeld landen in het informatiebeveiligingsplan (zie paragraaf 2.2). Wanneer we kijken naar de drie onderdelen waar de provincie Gelderland in de Cibo-monitor 2016 het laagst op scoorde (cryptografie, leveranciersrelaties en bedrijfscontinuïteitsbeheer) dan zien we alleen de tweede daarvan terugkomen in het informatiebeveiligingsplan 2017 van de provincie.

De provincie geeft aan dat de Information Security Officer op dit moment bezig is met een totaalbeeld van de stand van zaken van de ISO 270002 maatregelen in kaart te brengen.

Aanvullende maatregelen

In de procesbeschrijving van de risicoanalyses (zie toelichting bij figuur 5) is geen processtap opgenomen over de controle of de aanvullende maatregelen daadwerkelijk zijn uitgevoerd. Die aanvullende maatregelen kunnen bijvoorbeeld als eis opgenomen worden bij een aanbesteding / als bepaling in een contract.

Ambtelijk werd aangegeven dat de naleving van de BIA's nog niet wordt gecheckt. Aangegeven werd dat bij aanbestedingen soms wordt getoetst of deze aan de eisen voldoet, maar dat gebeurt in de minderheid van de gevallen. De uitvraag in het kader van de aanbesteding van de IT-dienstverlening wordt als voorbeeld genoemd waar wel scherp is bekeken of er voldaan werd aan de eisen in de kader van informatieveiligheid. Dit was een belangrijk punt in de beoordeling (zie paragraaf 3.2.2).

[57] *Notitie Cibo-monitor juli 2017, p. 8.*

4.1.3 Verdieping uitvoering per aandachtsgebied

Om een goed beeld te geven van de maatregelen brengen we in deze paragraaf op de drie aandachtsgebieden van informatieveiligheid een verdieping aan. Het gaat om de aandachtsgebieden: mens & organisatie, ICT en basisinfrastructuur.

Normen

- *Aandachtsgebied mens en organisatie*: De provincie voert periodiek een bewustwordingsprogramma rondom informatieveiligheid uit.
- *Aandachtsgebied ICT*:
  De provincie heeft de vijf informatieveiligheidsstandaarden geïmplementeerd bij haar website en e-mails.
  De provincie heeft de basis IT-hygiënemaatregelen (patch management, toegangsbeheer en back ups) op orde.
- *Aandachtsgebied basisinfrastructuur*: De provincie neemt afdoende maatregelen voor de fysieke beveiliging van informatie.

Bevindingen

Aandachtsgebied mens en organisatie (bewustwording)

- De provincie heeft in haar beleid aandacht voor bewustwording.
- Er zijn diverse activiteiten uitgevoerd om de bewustwording van medewerkers te vergroten. Bijvoorbeeld: workshops, berichten op intranet en het neerleggen van kaartjes wanneer een pc's niet zijn afgesloten.
- De provincie heeft medewerkers via een aantal documenten bekend gemaakt met hun verantwoordelijkheden bij informatieveiligheid.

Aandachtsgebied ICT (IT-hygiëne en informatiebeveiligingsstandaarden)

- De provincie Gelderland had in januari 2018 drie van de vijf verplichte informatieveiligheidsstandaarden voor haar website en e-mail geïmplementeerd.
- In het beleid staan beheersmaatregelen over patching, toegangsbeheer en back ups. Uitwerkingen hiervan zijn deels vastgesteld (accountbeleid en patchbeleid wel, back up beleid nog niet formeel).
- Patching, toegangsbeheer en back ups zijn onderdeel van de uitbesteding van de IT-diensten en daarmee momenteel op sommige punten nog in ontwikkeling.
- Uit de praktijktest kwamen een aantal voorbeelden waaruit bleek dat niet alle beheersmaatregelen voor patching en toegangsbeheer waren opgevolgd (back ups waren geen onderdeel van de praktijktest).

Vervolg bevindingen op de volgende pagina.

Vervolg bevindingen

Aandachtsgebied basisinfrastructuur

- Fysieke beveiliging is onderdeel van het informatiebeveiligingsbeleid. De provincie heeft het voornemen dit verder uit te werken in een protocol.
- De provincie neemt maatregelen voor de fysieke beveiliging. Tegelijkertijd zijn er voor de uitwerking in de praktijk nog verbeterpunten, zo blijkt uit de Cibo-monitor en de praktijktest. Die liggen voor een belangrijk deel bij de bewustwording van medewerkers.

Verdieping aandachtsgebied mens en organisatie

Bevorderen bewustwording

Eén van de aandachtsgebieden van informatieveiligheid is mens & organisatie. Het gedrag van mensen is van cruciaal belang voor het borgen van informatieveiligheid. Met ICT-maatregelen (bijvoorbeeld firewalls, wachtwoordbeleid) en fysieke maatregelen (bijvoorbeeld toegangspasjes en -poorten) kan de informatieveiligheid binnen een organisatie worden bevorderd. Maar ICT en fysieke maatregelen alleen zijn niet voldoende. Zo is een strikt wachtwoordbeleid zinloos als wachtwoorden regelmatig gedeeld worden of op een zichtbare plek zijn opgeschreven.

Het gedrag van mensen in een organisatie is dus eveneens zeer belangrijk. Iedereen dient zich ervan bewust te zijn dat men met zijn of haar gedrag de mate van informatieveiligheid kan beïnvloeden. De Rekenkamer heeft onderzocht wat de provincie heeft gedaan om het bewustzijn van informatieveiligheid bij de provincie te vergroten.

Beleid over bewustwording

In het informatiebeveiligingsbeleid is expliciet genoemd dat medewerkers via persoonlijk leiderschap zelf verantwoordelijk zijn voor de eigen informatiebeveiliging. Er worden taken omschreven voor het sturen op/bevorderen van bewustwording voor de ISO en het afdelingsmanagement:

- de ISO bevordert de algehele communicatie en bewustwording rondom informatieveiligheid;
- de afdelingsmanager stuur op beveiligings-/risicobewustzijn en op naleving.

Concreet is onder meer aangegeven dat:

- alle medewerkers (en voor zover van toepassing externe gebruikers van de provinciale systemen) training moeten krijgen in procedures die binnen de provincie of de afdeling gelden voor informatiebeveiliging. Deze training dient regelmatig herhaald te worden om het beveiligingsbewustzijn op peil te houden. De doelgroep en timing wordt in het beleid als volgt gespecificeerd: Alle nieuwe personen, dus ook externen en stagiaires, volgen bij binnenkomst een bewustwordingstraining informatieveiligheid;

- in werkoverleggen periodiek aandacht wordt geschonken aan informatieveiligheid. Voor zover relevant worden hierover afspraken vastgelegd in planningsgesprekken.

In het meest recente informatiebeveiligingsjaarplan (voor 2017) was het uitvoeren van acties voor het verbeteren van informatiebeveiligingsbewustzijn bij medewerkers opgenomen als één van de activiteiten.

Bewustwording in de praktijk

Bewustwording onder medewerkers

De provincie geeft aan dat de bewustwording onder medewerkers een aandachtspunt blijft. Zo wordt gezien dat medewerkers:

- hun laptops en telefoons open en onbeheerd achter laten in vergaderzalen en werklandschappen;
- in phishing mail 'trappen' en
- onbekenden in het provinciehuis niet aanspreken of niet vragen wie er (zonder pasje) met hen mee door de deur loopt.

Hierbij worden verschillen tussen de afdelingen waargenomen. Bij afdelingen die te maken hebben met subsidies en financiën is er meer aandacht voor informatie-veiligheid, omdat het belang daarvan groter is en er daar periodiek audits worden uitgevoerd. Bij andere afdelingen leeft het minder.[58]

Wij namen zelf een aantal gevallen waar waarbij documenten op een zodanige plek op Intranet waren opgeslagen dat informatie ingezien kon worden door alle medewerkers. Het ging hier bijvoorbeeld om een verslag van een werkoverleg met informatie over ziekte van een medewerker, interviewverslagen van een onderzoeksbureau en reflectieverslagen van stagiairs.

Bewustwordingsactiviteiten

De provincie heeft geen separaat bewustwordingsprogramma waarin staat beschreven wat er wordt gedaan om de bewustwording te bevorderen. Uit interviews en documenten blijkt wel dat er verschillende bewustwordingsactiviteiten zijn ondernomen.

- *Workshops en introductieprogramma*
  De ISO stelt de afgelopen 1,5 jaar ongeveer zestig workshops over informatie-veiligheid te hebben gegeven. De doelgroep (soort afdeling/team) en de omvang daarvan verschilt sterk. Er wordt geprobeerd concrete voorbeelden van risico's te gebruiken die afgestemd zijn op de doelgroep. Ook komen praktische richtlijnen aan bod zoals het afgesloten achterlaten van de computer en het niet 'inpluggen' van onbekende usb-sticks. Informatieveiligheid is tegenwoordig ook onderdeel van het introductieprogramma voor nieuwe medewerkers. Tot nu toe werd de fysieke kant van informatieveiligheid hier nog bij betrokken. Recent is afgesproken dat te gaan veranderen.[59]

[58] *Alinea gebaseerd op meerdere ambtelijke interviews.*
[59] *Ambtelijk interviews.*

- *Bijeenkomsten en berichten intranet*
  Er zijn het laatste jaar op intranet verschillende artikelen/informatieve berichten gezet over (mogelijke) dreigingen en het daarbij gewenste informatieveiligheid handelen.[60] Ook het informatiebeveiligingsbeleid en de uitwerking daarvan (bv. patch- en accountbeleid) is op Intranet te vinden.[61] Er zijn verschillende bijeenkomsten geweest waar medewerkers heen konden die gingen over of raakten aan informatieveiligheid. Voorbeelden hiervan zijn een lezing van Maria Genova in juni 2017[62], de Einsteinweek in september 2017[63] en de privacy-driedaagse in mei 2018. Een deel van de informatie op Intranet en de bijeenkomsten komt voort uit de aandacht die de provincie heeft voor digitalisering. Meer hierover in onderstaand kader.

Digitale vaardigheden
Binnen de provincie Gelderland loopt een programma Digitale Vaardigheden. Recent onderzoek van de Hogeschool Arnhem Nijmegen concludeerde dat ruimt 40% van de grootste groep medewerkers binnen de provincie (de beleidsmedewerkers) zichzelf onvoldoende tot gemiddeld digitaal vaardig noemt. De provincie wil hier meer op inzetten. In het eerdergenoemde strategische informatiebeleid (paragraaf 2.1) wordt het versterken van de i-functie waaronder het vergroten van de i-vaardigheid van medewerkers één van de bouwstenen. Er wordt bijvoorbeeld nagedacht over een digitaal paspoort met bijbehorende cursussen/opleiding.

- *Kaartjes afsluiten computers*
  Afgelopen zomer zijn door de provincie de zogenoemde ‘oeps-kaartjes’ ontwikkeld[64] (zie figuur 7). In totaal zijn er drie oplages gemaakt van 500 stuks per keer. Die zijn uitgedeeld aan een groep mensen die veel van werkplek wisselen.[65] Zij leggen de kaartjes op de computers van medewerkers die hun computer niet hebben afgesloten. Het achterliggende idee is dat deze medewerkers de kaartjes vervolgens kunnen plaatsen bij andere collega’s wanneer die ook vergeten zijn om hun computer af te sluiten (die het kaartje weer kunnen ‘doorgeven’ aan anderen). Zo blijft de distributie gaande. [66]

[60] Voorbeelden hiervan zijn: ‘Nieuws over grote datalekken’ (10 januari 2018), ‘Nieuwe vorm van nepmails’ (maart 2018), ‘Wachtwoord zoekmachine: loop ik risico? (6 april 2018) ‘Datalekken: Onze collega’s zijn het grootste risico (23 mei 2018), ‘Is je smart phone wel goed beveiligd? (21 september 2018), ‘Veilig omgaan met provinciale spullen’ (24 oktober 2018).
[61] Een deel van de informatie staat op de afdelingssite van I&A (het beleidsportaal) en een deel op de kennissite Snel & Slim: Digitaal Gelderland. Er is een aparte kennissite over privacy. Soms staat er een bericht op het Serviceplein. Dit gaat bijvoorbeeld om een waarschuwing voor een phishing mail (bericht 1 november 2018 ‘Waarschuwing: Phishingmail “Uw factuur” van Vodafone’).
[62] Schrijfster van het boek ‘Komt een vrouw bij de hacker’.
[63] De Gelderse Einsteinweek is een evenement georganiseerd door de gemeente Arnhem, de gemeente Nijmegen en de provincie Gelderland waarin experts en wetenschappers mensen een week lang meenemen in de wereld van innovatie en technologie. Een onderdeel was een interne workshop ‘Beveilig je pc’ voor ambtenaren. Bron: http://gelderseeinstein.nl/organisatie/ en https://gelderseeinstein.nl/featured_item/cursus-beveilig-je-pc/
[64] Intranet provincie Gelderland. Bericht ‘Veilig omgaan met provinciale spullen’ van 24 oktober 2018.
[65] Schriftelijke informatie van de provincie Gelderland.
[66] Ambtelijk interview en schriftelijke informatie.

Figuur 7: *Kaartjes bewustwording afsluiten computer (voor- en achterkant)*

Bron: Ontvangen van de provincie Gelderland.

- *Phishingactie*
  In april 2018 heeft de provincie Gelderland een 'phishing awareness - actie' laten uitvoeren. In paragraaf 4.2 van dit rapport gaan we nader in op deze actie.

Documenten en richtlijnen verantwoordelijkheid provinciale medewerkers

Naast bovengenoemde bewustwordingsactiviteiten, heeft de provincie medewerkers in een aantal documenten gewezen op hun verantwoordelijkheid bij informatieveiligheid. We geven deze in tabel 1 weer.

Tabel 1: *Overzicht documenten m.b.t. verantwoordelijkheden medewerkers o.g.v. informatieveiligheid*

Document	Toelichting	Doelgroep
Gedragscode integriteit provinciale ambtenaren	Een van de kernbegrippen die aan bod komt, is betrouwbaarheid. Hierbij is aangegeven dat de ambtenaar kennis en informatie waarover hij uit hoofde van zijn functie beschikt, aanwendt voor het doel waarvoor die zijn gegeven. In de gedragscode is verder niet expliciet een gedragsregel opgenomen over (omgang met) informatie.	De code richt zich primair op werknemers in provinciale dienst.[67] Ook is deze van toepassing op stagiairs.[68]
Eed / belofte	Hierin zweert / verklaart en belooft de ambtenaar onder andere om zorgvuldig om te gaan met informatie.	Werknemers die in provinciale dienst komen.
Algemene inkoop-voorwaarden (2015 en nieuwe in 2018)	Een van de artikelen in de algemene inkoopvoorwaarden heeft betrekking op geheimhouding en bekendmaking. Dit gaat onder andere over de omgang met vertrouwelijke informatie en gegevens. In 2018 is de vertrouwelijke behandeling eveneens van toepassing verklaard op (persoons)gegevens. Dit vanwege de inwerkingtreding van de AVG.[69]	Opdrachtnemers[70]
Gebruiksvoorwaar-den mobiele devices		Gebruikers van mobiele devices

[67] *Provincie Gelderland (januari 2018). Gedragscode integriteit provinciale ambtenaren (derde alinea van de inleiding).*
[68] *Provincie Gelderland (januari 2018). Regeling rechtspositie stagiairs provincie Gelderland, artikel 6.2.*
[69] *Provincie Gelderland. PS2018-604. Statenbrief algemene inkoopvoorwaarden.*
[70] *Iedere (rechts)persoon alsmede diens vertegenwoordiger(s), gemachtigde(n) en rechtsverkrijgende(n), die met de provincie een overeenkomst sluit tot het verrichten van leveringen en/of diensten, waarop deze algemene inkoopvoorwaarden toepasselijk zijn, alsmede zijn werknemers en door hem bij de uitvoering van de overeenkomst ingeschakelde derden (artikel 1.5).*

Verdieping aandachtsgebied ICT

Informatieveiligheidstandaarden en basis IT-hygiënemaatregelen

Informatieveiligheidstandaarden

Er is niet één bepaalde standaard die alle beveiligingsrisico's afdekt. Het gaat om een samenspel van meerdere standaarden.[71] In paragraaf 4.1.2 zijn we al in gegaan op Interprovinciale Baseline Informatieveiligheid (gebaseerd op de landelijke standaard ISO 27002), maar er zijn meer standaarden die belangrijk zijn bij informatiebeveiliging en veilige gegevensuitwisseling. Het gebruik van zogenoemde 'open (ICT-)standaarden' is al meer dan tien jaar beleid vanuit de Nederlandse overheid. Overheden zijn verplicht om de standaarden van de 'pas toe of leg uit'-lijst van het Forum Standaardisatie te gebruiken.[72] Daarnaast zijn er overheidsbreed afspraken gemaakt over de implementatie van onder meer informatieveiligheidsstandaarden.[73] Het Forum Standaardisatie toetst over overheden de informatieveiligheidsstandaarden geïmplementeerd hebben. Hun monitor liet begin 2018 het volgende beeld zien:

Tabel 2: *Toepassing informatieveiligheidsstandaarden door provincie Gelderland (jan. 2018)*

Onderdeel	Implementatie Gelderland	Toelichting
Web - gelderland.nl	• DNSSEC: Ja • TLS: Ja	**DNSSEC** (domeinnaambeveiliging) voorkomt dat cybercriminelen het internetverkeer van een organisatie kunnen omleiden naar valse websites of e-mail postbussen. **TLS** (beveiligde verbinding) zorgt ervoor dat hackers de internetverbinding met een website of e-mail server niet kunnen afluisteren en zo gevoelige informatie kunnen onderscheppen.
Mail - @gelderland.nl	• SPF: Ja • DKIM: Nee • DMARC: Nee	De combinatie van **SPF, DKIM en DMARC** (anti-phishing, rapportages) bestrijdt e-mailfraude waaronder phishing en de verspreiding van gijzelsoftware.[74]

Bron: Halfjaarlijkse meting Informatieveiligheidstandaarden Forum Standaardisatie begin 2018, p. 15 en https://magazine.forumstandaardisatie.nl/nl_NL/6322/90028/uitleg.html

[71] *Forum Standaardisatie (november 2014). Verkennend onderzoek ISO 27001 en ISO 27002, p. 6.*

[72] *Dit Forum heeft als doel op interoperabiliteit* en leveranciersonafhankelijk te bevorderen via het gebruik van open standaarden voor digitale gegevensuitwisseling in de publieke sector. De leden van het Forum worden benoemd door het ministerie van BZK en hebben zitting op persoonlijke titel. Er zit ook iemand van het IPO in het Forum Standaardisatie.*

** Interoperabiliteit is het vermogen van (informatie)systemen om digitale gegeven en informatie te kunnen uitwisselen binnen en tussen organisaties.*

[73] *Dit worden zogenoemde 'streefbeeldafspraken' genoemd. Voor standaarden waarop deze afspraken betrekking hebben geldt dat niet het tempo van 'pas toe of leg uit' wordt opgevolgd (oftewel wachten op een volgend investeringsmoment en dan de standaarden implementeren) maar dat actief wordt ingezet op implementatie van de standaarden op de korte termijn. Een overzicht van de gemaakte afspraken is te vinden op: https://www.forumstandaardisatie.nl/thema/iv-meting-en-afspraken*

[74] *Bron: https://magazine.forumstandaardisatie.nl/nl_NL/6322/90028/uitleg.html (onderdeel: welke informatieveiligheidsstandaarden)*

Uit tabel 2 komt naar voren dat de provincie Gelderland DKIM en DMARC in januari 2018 nog niet hadden geïmplementeerd. Dit werd bevestigd in een interview. Aangegeven werd dat dit komt doordat er een transitie naar een nieuw e-mailsysteem plaatsvindt en DKIM en DMARC dan geïmplementeerd worden.[75]

Basis IT-hygiënemaatregelen

In de eerdergenoemde Cybersecurity Health Check van de NBA en de CSR wordt gesproken over het belang van het op orde hebben van de 'basis IT-hygiënemaatregelen'. Hierbij gaat het om patch management[76], toegangsbeheer en back ups. Hieronder gaan we na wat hierover in het Gelderse informatiebeveiligings-beleid staat en hoe dit in de praktijk geregeld is. Voor de praktijk is het goed te realiseren dat al deze drie de onderdelen in de uitvraag voor de uitbesteding van IT-diensten zaten. Met de transitie van de IT-diensten naar OGD zijn ook deze drie onderdelen dus momenteel nog in ontwikkeling.[77]

Patchmanagement

In het beleid (februari 2016) staat dat patches en updates zo spoedig mogelijk en na positief te zijn getest, worden doorgevoerd. In de aanbesteding van de IT-diensten (september 2016) was er aandacht voor patching. Zo stond in het programma van eisen dat de opdrachtnemer geaccordeerd beleid met betrekking tot het actief uitvoeren van security patches en updates op de omgeving[78] moest hebben.

De provincie heeft het beleid op het gebied van patches uitgewerkt. De zestien afspraken hierin zijn afgestemd met de gecontracteerde externe dienstverlener (OGD) en in 2017 vastgesteld door het AMT van I&A. Een belangrijke afspraak is dat updates, patches en servicepack binnen 1 maand na release moeten worden geïnstalleerd. Om dit te bereiken is er een ijkpunt (tweede dinsdag van de maand) gesteld. Relevante vraag is hier natuurlijk of patches en updates daadwerkelijk binnen een maand worden geïnstalleerd.

In het accountantsverslag 2017 had één van de belangrijkste bevindingen over de algemene IT-controls betrekking op het bijwerken van updates voor informatie-beveiliging. Dit ging erover dat de aanbevolen updates destijds niet geïnstalleerd voor het financieel systeem Oracle.[79]

De Rekenkamer heeft in augustus 2018 een extern bureau laten testen of informatie bij de provincie Gelderland in de praktijk voldoende wordt beschermd tegen toegang door onbevoegden. Er werden een aantal kwetsbaarheden gevonden die een risico vormden voor de informatieveiligheid (zie paragraaf 4.2 voor meer informatie). Het ging in één geval om een kritisch risico: er kon toegang verkregen worden tot informatie doordat een beveiligingsupdate niet was toegepast. Dus er is in ieder geval één voorbeeld

[75] *Ambtelijk interview.*
[76] *Hierbij gaat het om het bijwerken, testen en installeren van software (bron: NBA en SCR. Cyber security health check). Een patch is een stukje software dat gebruikt wordt om fouten in software op te lossen of updates uit te voeren.*
[77] *Ambtelijk interview.*
[78] *Het gaat hier om hardware, besturingssystemen, middleware, applicatie en infrastructuur.*
[79] *PWC Accountantsverslag 2017 provincie Gelderland, p. 4 en 9.*

waarbij het beleid niet is gevolgd. Vanzelfsprekend zegt dit niet automatisch dat dit bij andere patches en updates ook zo is. De provincie gaf aan dat betreffende beveiligingsupdate kort nadat de rapportage van de praktijktest was ontvangen alsnog is toegepast.[80]

Ambtelijk is aangegeven dat is uitgevraagd bij de externe dienstverlener dat patches en updates zo veel mogelijk geautomatiseerd gebeuren en dat periodiek aan de provincie gerapporteerd wordt of deze zijn uitgevoerd. Dat is belangrijk omdat de provincie zo kan controleren of de systemen voldoen aan het informatiebeveiligingsbeleid. Aan deze rapportering wordt gewerkt. De provincie verwachtte in oktober 2018 dat deze er ongeveer twee maanden later zou moeten zijn.[81]

Toegangsbeheer

In het beleid is een hoofdstuk over toegangsbeveiliging opgenomen. Hier staan verschillende beheersmaatregelen in, bijvoorbeeld rondom authenticatie en autorisatie. De provincie heeft onderdelen van het beleid met betrekking tot toegangsbeveiliging nader uitgewerkt. Zo is in 2017 nieuw wachtwoordenbeleid ingericht[82] en in 2018 accountbeleid vastgesteld.[83] Dit accountbeleid heeft als doel ervoor te zorgen dat gebruikers precies genoeg rechten krijgen om hun werk uit te voeren gedurende de tijd dat ze voor de provincie werken.[84] Het beleid is zodanig opgezet dat er mechanismes zijn wanneer het reguliere proces faalt. Stel er wordt vergeten door te geven dat iemand zijn account moet stoppen, dan wordt volgens het beleid het account 90 dagen na de laatste succesvolle inlogpoging automatisch gedeactiveerd (en weer 90 dagen later automatisch verwijderd). De procedure voor toegangsbeheer is verwerkt in een medewerker mutatieformulier. Wanneer dit wordt ingediend, worden verschillende vervolgstappen in het proces, bijvoorbeeld rondom autorisaties, genomen.[85]

In het accountantsverslag 2017 was één van de belangrijkste bevindingen over de algemene IT-controls gericht op het autorisatiebeleid. Dit ging over het financieel systeem Oracle. Hierbij beschikten meer mensen dan nodig over beheerrechten, ontbrak een actuele autorisatiematrix en was er sprake van beperkte wachtwoordrestricties.[86] De provincie geeft aan dat deze punten voor 2018 zijn opgelost.[87]

Uit de eerdergenoemde praktijktest kwam een drietal concrete gevallen naar voren waar het beleid danwel het programma van eisen omtrent toegangsbeheer niet was gevolgd.

- In het beleid staat dat het fysieke (bekabelde) netwerk niet toegankelijk is voor onbeheerde apparatuur. Bij de praktijktest bleek het netwerk wel toegankelijk voor

[80] *Ambtelijk interview.*
[81] *Ambtelijk interview.*
[82] *PWC Accountantsverslag 2017 provincie Gelderland, p. 16.*
[83] *Ambtelijk interview.*
[84] *Accountbeleid provincie Gelderland.*
[85] *Ambtelijk interview.*
[86] *PWC Accountantsverslag 2017 provincie Gelderland, p. 4 en 9.*
[87] *Schriftelijke informatie.*

onbekende apparatuur, maar door de aanwezige restricties kon weinig benaderd worden.[88] Deze restricties konden wel omzeild worden. Meer uitleg hierover in paragraaf 4.2.

- In het beleid staat dat wachtwoorden aan eisen dienen te voldoen en dat deze worden afgedwongen door het systeem. In het wachtwoordenbeleid staan deze eisen. In de praktijktest werden standaardwachtwoorden aangetroffen waardoor tot enkele systemen beperkte ongeautoriseerde toegang kon worden verkregen. Hoewel betreffend standaardwachtwoord wel aan de eisen voldoet, is de aanbeveling geen voorspelbare wachtwoorden te gebruiken.
- In het programma van eisen stond dat de opdrachtnemer toegang tot data van de provincie Gelderland vanaf het internet uitsluitend met twee factor authenticatie[89] borgt. Bij de praktijktest bleek dit bij de web-mail niet het geval. Ook bleek het mogelijk om onopgemerkt veelvuldige geautomatiseerde inlogpogingen op meerdere accounts te doen.

Back ups

In het beleid zijn een aantal beheersmaatregelen opgenomen die betrekking hebben op back ups. Bijvoorbeeld dat back ups zijn gescheiden in twee locaties of datacenters en dat de back up- en herstelprocedures regelmatig (tenminste 1x per jaar) worden getest. In de aanbesteding van IT-diensten was er aandacht voor back ups. Zo is in het programma van eisen opgenomen dat de opdrachtnemer borgt dat de back ups van data fysiek op een andere locatie dan datacenter worden bewaard en dat de opdrachtnemer borgt dat back ups in overeenstemming met het back up beleid worden gemaakt.

De gekozen externe dienstverlener heeft twee gescheiden datacenters. Het primaire datacenter is in Amsterdam en het secundaire datacenter is in Zwolle. Hiermee wordt dus voldaan aan de eis uit de aanbesteding dat back ups op verschillende locaties moeten worden bewaard. Bij uitval start binnen vier uur het secundaire datacenter op basis van een back up.[90] De provincie geeft aan dat een uitwijktest is uitgevoerd. Dit bleek goed te gaan. Het testen van de back up is een eis van de provincie aan de externe dienstverlener. De externe dienstverlener moet deze test uitvoeren en hierover aan de provincie rapporteren. De provincie geeft aan dat zij in het verleden zelf geen grote periodieke testen van de back ups deed.[91] Als reden werd genoemd dat in de dagelijkse praktijk al regelmatig bepaalde gegevens en bestanden teruggezet moesten worden uit de back up.[92]

[88] *Netwerksegmentatie is in dit geval extra belangrijk. Netwerksegmentatie betekent dat het netwerk ingedeeld is in verschillende zones. Wanneer er sprake is van netwerksegmentatie dan heeft een hacker of malware wanneer het toch is gelukt binnen te komen niet gelijk vrij spel binnen het hele netwerk. In het Gelderse informatiebeveiligingsbeleid staat dat het netwerk waar nodig is gesegmenteerd. Uit de praktijktest bleek inderdaad dat de provincie netwerksegmentatie had toegepast.*

[89] *Twee factoren authenticatie is een methode waarmee de identiteit van de gebruiker vast wordt gesteld door middel van twee verschillende componenten. Hierbij kan bijvoorbeeld gedacht worden aan een wachtwoord en een pincode of goedkeuring via de mobiel. Het is in feite een extra beveiligingslaag.*

[90] *Pocket versie contract OGD.*

[91] *Ambtelijk interview. Zie ook: Provincie Gelderland (2016). Huidige situatie informatiebeveiliging versie 1.0 [intern document], p. 11.*

[92] *Ambtelijk interview.*

Ambtelijk wordt aangegeven dat het back up-beleid onderdeel wordt van het informatiebeveiligingsjaarplan waar momenteel aan gewerkt wordt (zie paragraaf 3.2.2). Het is niet bekend wanneer dit definitief wordt.[93]

Verdieping aandachtsgebied basisinfrastructuur

Fysieke beveiliging

Fysieke beveiliging in het beleid

In het informatieveiligheidsbeleid is naast organisatie en ICT ook aandacht voor de fysieke beveiliging en beveiliging van de omgeving. Hier is een hoofdstuk aan gewijd. De doelstelling van de provincie voor de fysieke veiligheid is:

- ICT-voorzieningen, die kritieke of gevoelige bedrijfsactiviteiten ondersteunen, behoren fysiek te worden ondergebracht in beveiligde ruimten, beschermd door afgegrensde beveiligde gebieden, in een gecontroleerde omgeving, beveiligd met geschikte beveiligingsbarrières en toegangsbeveiliging. Ze behoren fysiek te worden beschermd tegen toegang door onbevoegden, schade en storingen;
- het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie, bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten;
- het voorkomen van verlies, schade of diefstal van apparatuur en bescherming tegen fysieke bedreigingen en gevaren van buitenaf.

Om deze doelen te bereiken zijn in het beleid twaalf beheersmaatregelen opgenomen. Dit gaat bijvoorbeeld over autorisatie en de uitgave van toegangsmiddelen, beveiliging in en rond het gebouw (bv. receptie, cameratoezicht) en verwijdering en hergebruik van ICT-apparatuur.

Zoals eerder aangegeven in het fysieke beleid nog niet verder uitgewerkt en is het voornemen hier een protocol voor te ontwikkelen. Dit moet maart 2019 klaar zijn. Het is nog niet bekend hoe dat ingevuld zal worden. Er zijn wel protocollen voor cameratoezicht.

Fysieke beveiliging in de praktijk

In de Cibo-monitor uit 2016 scoort de provincie Gelderland op het onderdeel fysieke beveiliging 67% (zelfinschatting). De provincie scoorde met name laag op beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein. Verder werd de praktijk van onder meer de plaatsing en bescherming van apparatuur, beveiliging van bekabeling en onbeheerde bedrijfsapparatuur laag beoordeeld. Het (veilig) verwijderen van bedrijfsmiddelen en apparatuur werd juist hoog beoordeeld door de provincie. De Cibo-monitor is in 2017 en 2018 niet ingevuld door de provincie. Zodoende zijn er geen scores van recentere jaren bekend. Dit had anders kunnen uitvallen dan in 2016, bijvoorbeeld omdat er zaken zijn veranderd met de verbouwing van het provinciehuis.

Eén van de onderdelen van de praktijktest die we in 2018 hebben laten uitvoeren, was een inlooptest met een mystery guest. Hierbij is waargenomen dat de toegangsdeur tussen het openbare gedeelte en het kantoorgedeelte was beveiligd met een

[93] *Ambtelijk interview.*

controlesysteem (paslezer). Dit is in lijn met het doel voor fysieke beveiliging in het beleid. De mystery guest heeft uiteindelijk wel toegang gekregen tot niet publieke ruimten zoals werkplekken. Dit lukte door achter iemand aan te lopen die wel een pas had. Het aandachtspunt ligt hier dus ook meer op het vlak van de bewustwording waar we het eerder in deze paragraaf al aandacht voor hadden. Het is de mystery guest niet gelukt de serverruimte te betreden. Ook die was - in lijn met beleid - afgesloten met een controlesysteem.

Aandachtspunten die de provincie zelf aangaf rondom fysieke veiligheid waren ook gerelateerd aan het gedrag/bewustwording van medewerkers. Het ging bijvoorbeeld om medewerkers die de parkeergarage soms als looproute gebruiken en onbekende personen die achter hen aan lopen door de deur niet aanspraken. Dit levert potentiële beveiligingslekken op, zo stelt de provincie.

4.2 Resultaat praktijktesten

Normen

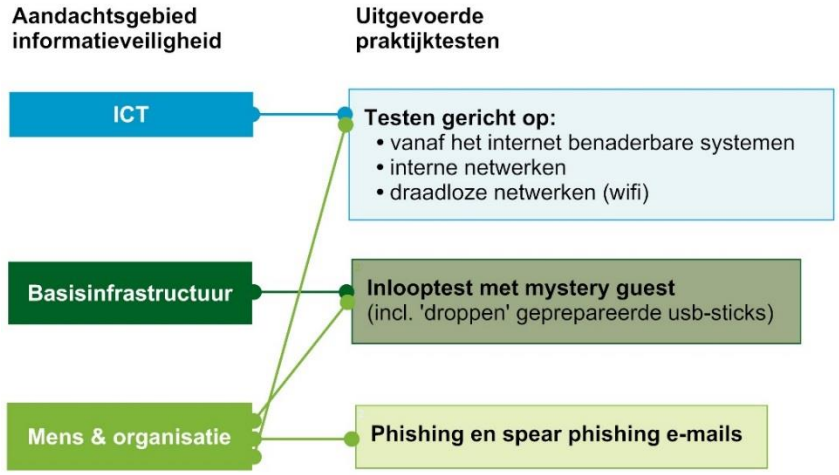
- De provincie doorstaat de specifieke test.
- Uit de test komen geen kwetsbaarheden die al bekend zijn bij de provincie en al opgelost hadden kunnen zijn.

Bevindingen

- In opdracht van de Rekenkamer zijn in de zomer 2018 praktijktesten uitgevoerd. Hierin kwamen alle aandachtsgebieden van informatieveiligheid (ICT, basisinfrastructuur en mens & organisatie) terug. De provincie heeft in mei 2018 zelf een phishing-campagne laten uitvoeren.
- Uit de testen van de systemen en netwerken blijkt dat de provincie meerdere effectieve beschermingsmaatregelen heeft genomen om weerbaar te zijn tegen cyberaanvallen. Er zijn ook een aantal kwetsbaarheden gevonden die een risico vormen voor de informatieveiligheid. Het ging in één geval om een kritisch risico: er kon toegang verkregen worden tot informatie doordat een beveiligingsupdate niet was toegepast. De provincie bleek op dit punt haar eigen beleid niet te hebben gevolgd.
- Het doel van de provincie is dat medewerkers zich bewust zijn van informatieveiligheid. Uit de inlooptest en (spear) phishing testen bleek dat dit nog niet het geval is. Bij de inlooptest is ongeautoriseerd toegang tot niet-publieke ruimtes en beperkte toegang tot dossiers en gegevens verkregen. Het versturen van spear phishing e-mails leidde tot het verkrijgen van toegang tot accounts en bestanden en tot het verkrijgen van inloggegevens. Twee van de achtergelaten geprepareerde usb-sticks werden gevonden en adequaat afgehandeld. Bij de phishing-actie in opdracht van de provincie klikte iets minder dan de helft van de ontvangers op de link.

In deze paragraaf gaan we in op het resultaat van het informatieveiligheidsbeleid en de uitvoering daarvan. Wordt informatie bij de provincie Gelderland door de genomen maatregelen voldoende beschermd tegen toegang door onbevoegden? Om deze vraag te kunnen beantwoorden, maken we gebruik van praktijktesten uit medio 2018. Die testen zijn - op een phishing mail na - in opdracht van de Rekenkamer uitgevoerd. In figuur 8 hebben we schematisch weergegeven welke praktijktesten in 2018 zijn uitgevoerd. Na de figuur volgen de uitkomsten.

Figuur 8: *Uitgevoerde praktijktesten 2018 naar aandachtsgebied*



Uitkomsten testen

Hieronder gaan we in op de uitkomsten van de uitgevoerde praktijktesten. Voordat we hierop ingaan, zijn twee zaken belangrijk voor de interpretatie van de uitkomsten:

- de mogelijkheid bestaat dat het externe bureau niet iedere kwetsbaarheid heeft gevonden, omdat hun onderzoek gebonden was aan een budget- en tijdslimiet;
- de bevindingen zijn een momentopname. Er kunnen na de uitvoering van de test veranderingen plaatsvinden (bijvoorbeeld in hard- of software, beschikbare technologie, indeling van het gebouw) die nieuwe kwetsbaarheden met zich meebrengen.

Uitkomsten penetratietest (voornamelijk aandachtsgebied ICT)

Uit de test kwam dat de provincie Gelderland meerdere effectieve beschermings-maatregelen heeft getroffen om weerbaar te zijn tegen cyberaanvallen. Maatregelen die gericht zijn op het tijdig signaleren of het voorkomen / beperken van de schade van een hack. Zo bleek de provincie:

- het aanvalsoppervlak te hebben beperkt door netwerksegmentatie en filtering;[94]
- kwetsbaarhedenscans[95] uit te voeren en
- detectie en monitoring te hebben ingericht.

[94] *Filtering betekent dat de 'verkeersstromen' tussen de verschillende segmenten van het netwerk wordt beperkt.*
[95] *Een kwetsbaarhedenscan betekent dat systemen en applicaties automatisch worden gescand op de aanwezigheid van bekende kwetsbaarheden en configuratiefouten.*

Het lukte de onderzoekers niet om binnen de beschikbare tijdsperiode toegang te krijgen tot de zogenoemde kroonjuwelen of om de rechten van de systeembeheerder[96] te verwerven. Bij de kroonjuwelen kan gedacht worden aan het account van de Commissaris van de Koning of gevoelige informatie rondom burgemeesters-benoemingen.

Het is wel gelukt om vanaf het internet toegang te krijgen tot systemen en gegevens van enkele gebruikers. Hiervoor zijn kwetsbaarheden in de zogenoemde authenticatievoorzieningen[97] gebruikt. De onderzoekers konden ook bij documenten die vertrouwelijk waren, bijvoorbeeld kopieën van 116 paspoorten. Verder zijn best practices en 'hardening'[98] niet overal consistent toegepast. Hierbij kan bijvoorbeeld gedacht worden aan het onbereikbaar maken van beheerpagina's of het toepassen van beveiligingsinstellingen. Het gevolg is dat de systemen van de provincie niet optimaal beschermd waren. Er werd bijvoorbeeld ook gezien dat er niet op alle websites gebruik werd gemaakt van HSTS.[99] Dit is een voorbeeld van een bevinding die al bekend had kunnen zijn bij de provincie, omdat dit ook uit een geautomatiseerde scan van externe websites uit november 2017 kwam.[100] Overigens is dit een kwetsbaarheid met een gemiddeld risico, omdat het lastig is er misbruik van te maken.

Op het interne netwerk is het gelukt om restricties te omzeilen en in beperkte mate toegang te krijgen tot gegevens. De provincie heeft hiervoor een account beschikbaar gesteld, maar dit had ook gekund met de accounts waar de inloggegevens van zijn achterhaald. Verder zijn er inlogcombinaties achterhaald via mobiele apparaten. Hiermee kon toegang verkregen worden tot e-mails en bestanden van de gebruikers van die apparaten.

Uitkomsten inlooptest (aandachtsgebied basisinfrastructuur en mens & organisatie)

In juli 2018 is twee keer een inlooptest uitgevoerd bij het provinciehuis. De mystery guest kon ongeautoriseerde toegang krijgen tot niet-publieke ruimten en in beperkte mate tot dossiers en gegevens. Tijdens zijn bezoeken is hij niet opgemerkt of aangesproken. Er bleken - behalve printers - geen (computer)systemen toegankelijk te zijn. Ook is het niet gelukt om de serverruimte binnen te komen. Twee van de achtergelaten USB-sticks[101] zijn ingeleverd waarna de vondst op correcte wijze als

[96] Een belangrijk doelwit van hackers is het domain administrator account. Dit wordt vaak beheerd door de systeembeheerder. Hiermee heeft hij / zij toegang tot alle systemen en applicaties. Zodra een hacker controle heeft over dit account kan die overal bij en dus grote schade aanrichten.

[97] Authenticatie betekent dat wordt nagegaan of een gebruiker, computer of applicatie daadwerkelijk is wie hij/zij beweert te zijn. Een voorziening waarmee dit gedaan kan worden is bijvoorbeeld het werken met wachtwoorden.

[98] Hardening is het proces waarmee:
(a) overbodige functies in besturingssystemen uitgeschakeld worden en/of van het systeem verwijderd worden en
(b) zodanige waarden worden toegekend aan beveiligingsinstellingen dat de mogelijkheden om een systeem te compromitteren worden verlaagd en een maximale veiligheid ontstaat.
Met systemen wordt in dit verband bedoeld: servers, actieve netwerkcomponenten zoals Firewalls en switches, desktops, laptops, mobiele devices. Kortom: alles met een besturingssysteem. (Bron: InformatieBeveiligingsDienst (oktober 2013). Hardening beleid voor gemeenten versie 1.0, p. 6).

[99] Met behulp van HSTS worden gebruikers beschermd tegen zogenoemde man-in-the-middle aanvallen door af te dwingen dat een versleutelde verbinding werd gebruikt. Een 'man-in-the-middle aanval' is een aanval waarbij informatie tussen twee communicerende partijen onderschept wordt, zonder dat beide partijen daar weet van hebben.

[100] Audit report. Site report for externe websites full-scan. Reported on 30 november, 2017.

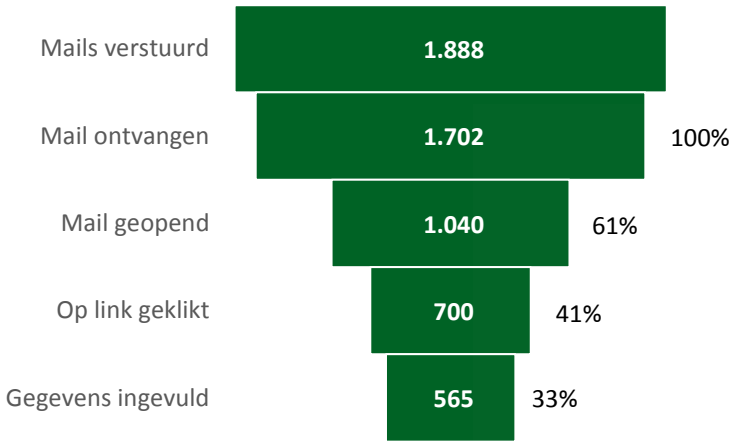
[101] De mystery guest heeft meerdere usb-sticks achter gelaten met daarop geprepareerde bestanden. Die bestanden nemen contact op met een systeem op internet zodat gezien kan worden of de bestanden geopend worden.

beveiligingsincident is afgehandeld. De overige USB-sticks zijn binnen de onderzochte periode niet gebruikt.

Uitkomsten (spear)phishing (aandachtsgebied mens & organisatie)

In figuur 9 zijn de resultaten van de phising-campagne uit mei 2018 weergegeven. Het doel van deze test was om vast te stellen hoe bestendig de provincie Gelderland is tegen phishing-aanvalsscenario's en het aandragen van mogelijke verbeteringen.[102]

Figuur 9: *'Ruwe' phishing-resultaten provincie Gelderland (april 2018)*



Bron: Afbeelding Rekenkamer Oost-Nederland op basis van Secura (mei 2018). Rapport social engineering.

Figuur 9 laat zien dat de campagne is uitgevoerd bij 1.888 medewerkers waarvan 1.702 de mail ontvangen hebben.[103] Daarvan hebben in een tijdsbestek van ongeveer 48 uur: 1.040 personen de mail geopend, 861 personen op de link in de mail geklikt en 565 personen hebben hun gegevens ingevuld. Er zijn bij de ISO, de Service Desk en de persoon die de e-mail zou hebben verzonden een grote hoeveelheid e-mails en telefoongesprekken binnen gekomen, zo stelt het rapport. Het precieze aantal wordt daarbij niet genoemd. In verband met het onderzoek is hier bewust neutraal op gereageerd en afgezien van het starten van de gebruikelijke procedure bij een dergelijke phishing-aanval. Zo werd het bewustzijn van de medewerkers getest, in plaats van de procedures. [104] Een aandachtspunt dat de provincie in het rapport mee kreeg, was dat er zonder dat de provincie daarover geïnformeerd werd een nl.domeinnaam geregistreerd kon worden die sterk lijkt op de provincie Gelderland of de afkorting daarvan.[105] Later heeft de provincie een bericht op intranet geplaatst dat een phishing-mail in het kader van een test was verstuurd. In dit bericht werden ook tips gegeven hoe herkend had kunnen worden dat de mail nep was hoe je moet handelen als je denkt een nep-mail ontvangen te hebben.

[102] *Secura (mei 2018). Rapport social engineering: Phishing awareness in opdracht van de provincie Gelderland, p. 4.*
[103] *Er werden 171 out-of-office- en/of vakantiemeldingen ontvangen en 15 mails konden niet bezorgd worden.*
[104] *Secura (mei 2018). Rapport social engineering: Phishing awareness in opdracht van de provincie Gelderland, p. 2 en informatie van de provincie Gelderland.*
[105] *Secura (mei 2018). Rapport social engineering: Phishing awareness in opdracht van de provincie Gelderland, p. 15.*

In augustus 2018 zijn er in opdracht van de Rekenkamer “gerichte” spear phishing e-mails gestuurd. Ten eerste zijn er twee spear phishing e-mails verstuurd met een kwaadaardige link naar een website die malware[106] bevatte. Dit leidde in beide gevallen tot volledige toegang tot de accounts en gegevens (waaronder verslagen van voortgangsgesprekken) van de medewerkers die de link hadden geopend. Hierdoor bleek dat de provincie een kritieke beveiligingsupdate die besmetting had kunnen voorkomen niet had toegepast. Zo kon eenvoudig toegang verkregen worden tot alle bestanden van gebruikers die de link openden. In het informatiebeveiligingsbeleid van de provincie Gelderland staat als beheersmaatregel dat beveiligingsupdates en beveiligingspatches zo spoedig mogelijk en na positief te zijn getest, worden doorgevoerd. In dit geval was dit niet gebeurd.[107] De bijbehorende aanbeveling was dan ook om kritieke beveiligingsupdates zo snel mogelijk toe te passen. In een ambtelijk interview werd genoemd dat dit kort na de ontvangst van de rapportage is gebeurd.

Ten tweede zijn er spear phishing e-mails verstuurd met als doel geldige inloggegevens te verzamelen. Bij dit type aanval wordt geprobeerd om inloggegevens van medewerkers met een specifieke functie te krijgen, omdat zij toegang kunnen geven tot specifieke informatie. Vervolgens kan het mogelijk zijn om die informatie te misbruiken om rechten te vergroten om toegang tot informatie uit te breiden. Dergelijke e-mails worden meestal niet verstuurd naar alle gebruikers omdat de kans groter is dat de aanval dan opgemerkt en/of afgeslagen wordt. Uiteindelijk zijn in totaal 41 e-mails[108] gestuurd. Er zijn vier geldige inlogcombinaties verkregen. Met deze inloggegevens konden de externe onderzoekers toegang krijgen tot de e-mail en bestanden van deze gebruikers, evenals specifieke informatie waar betreffende gebruikers toegang toe hadden gezien hun functie. Voor zover bekend is deze aanval niet opgemerkt.

Getroffen maatregelen

Op 28 augustus 2018 ontving de provincie Gelderland het rapport van de praktijktest dat is uitgevoerd in opdracht van de Rekenkamer. Dit rapport bevatte een omschrijving van de gevonden kwetsbaarheden en per kwetsbaarheid een aanbeveling hoe daarmee om kan worden gegaan. Het rapport is gedeeld met betrokken afdelingsmanagers en directie. De provincie geeft aan dat de kwetsbaarheid als ‘wijzigingsverzoeken’ in het managementsysteem te hebben opgenomen. Een deel van deze wijzigingen wordt door de externe dienstverlener opgepakt en een deel door de provincie. De externe dienstverlener heeft een plan van aanpak opgesteld voor de voorgestelde wijzigingen. Ten tijde van het schrijven van deze nota (begin november) was een deel van deze wijzigingen met betrekking tot ICT, waaronder de update met betrekking tot de enige kritische kwetsbaarheid, reeds opgepakt. De inlooptest had nog niet geleid tot aanpassingen in de praktijk.[109]

[106] *Malware staat voor ‘malicious software’. Het is een verzamelnaam voor allerlei soorten ongewenste en schadelijke programma’s.*
[107] *Betreffende beveiligingsupdate was mei 2018 uitgekomen en was op het moment van de test (augustus 2018) dus drie maanden beschikbaar.*
[108] *De externe onderzoekers hebben willekeurige e-mail adressen van medewerkers met verschillende functies geselecteerd op basis van LinkedIn profielen.*
[109] *Ambtelijke interviews.*

In mei 2018 ontving de provincie Gelderland het rapport met de uitkomsten van de phishing actie die in haar opdracht was uitgevoerd. Dit rapport is gedeeld met afdelingsmanagement en directie. In het rapport stonden drie aanbevelingen. Die ziet u in tabel 3.

Tabel 3: *Aanbevelingen phishing-campagne april 2018*

Niveau	Aanbevelingen
Strategisch niveau	1. Stel een security-awareness-programma op, waarin alle medewerkers deelnemen en waarin men wordt getraind om phishing e-mails en social-engineering-aanvallen te herkennen en hierop te anticiperen. 2. Stel reguliere phishing-onderzoeken (2/3 maal per jaar) in om herkenning van phishing-emails te verbeteren.
Tactisch niveau	3. Overweeg andere/extra periodieke audits waarbij wordt gekeken of de genomen maatregelen een positief effect hebben op de security-awareness van de organisatie.

Bron: Secura (mei 2018). Rapport social engineering: Phishing awareness in opdracht van de provincie Gelderland.

De test liet zien dat bewustwording een punt van aandacht is. Hier zal in de toekomst dan ook op ingezet blijven worden, zo werd in verschillende interviews naar voren gebracht. De provincie kon nog niet aangeven hoe bovenstaande aanbevelingen precies opgepakt gaan worden.

5 Toezicht en verantwoording

In dit hoofdstuk gaan we in op de wijze waarop de provincie Gelderland het houden van toezicht op en het afleggen van verantwoording over informatieveiligheid heeft geregeld.

5.1 Toezicht

Normen

- De provincie laat periodiek een onafhankelijke toets uitvoeren op het beveiligingsniveau en de implementatiestatus van het informatieveiligheids-beleid.
- De provincie voert zelfevaluaties uit.

Bevindingen

- Onafhankelijke toetsen vinden periodiek plaats in de vorm van een jaarlijks onderzoek van de accountant.
- De provincie heeft in 2016 voor het laatste een zelfevaluatie gedaan. Dit ging over de implementatie van de Interprovinciale Baseline Informatieveiligheid.
- De provincie heeft in de periode tussen 2013 en 2018 geen praktijktesten zoals inloop-, phishing en pentesten laten uitvoeren. De uitbesteding van IT-taken (langer geduurd dan gepland) en de verbouwing van het provinciehuis werden als redenen genoemd.
- In 2018 heeft een nulmeting plaatsgevonden bij provincies op de implementatie van de ISO 27001 (over het managementsysteem voor informatiebeveiliging). Op een groot aantal punten - uitgezonderd communicatie en documentatie - voldoet de provincie Gelderland nog niet.

Bij het borgen van informatieveiligheid van provincies staat het principe van verplichtende zelfregulering centraal. Dit houdt onder andere in dat de provincie

onafhankelijke onderzoeken laat toetsen of de informatieveiligheid op orde is. In het convenant Interprovinciale Regulering Informatieveiligheid staat daarover dat onafhankelijk onderzoek bijdraagt aan het creëren van grotere transparantie over informatieveiligheid. Hierdoor is zonder extra regeldruk elke provincie aanspreekbaar op haar beveiligingsniveau.

In deze paragraaf gaan we eerst in op wat in het beleid staat over toezicht. Daarna bekijken we hoe het toezicht er in de praktijk uitziet. Hiervoor hebben we uitgezocht in hoeverre de provincie Gelderland onafhankelijke onderzoeken heeft laten uitvoeren naar het beveiligingsniveau en de implementatiestatus van het informatieveiligheids-beleid. Daarnaast hebben we gekeken in hoeverre de provincie Gelderland zelf onderzoek doet naar het informatieveiligheid. De provincies hebben in het convenant afgesproken de interprovinciale monitor informatieveiligheid (Cibo-monitor) als instrument voor deze zelfevaluatie te gebruiken. Tot slot gaan we in op het toezicht op externe leveranciers.

Beleid over toezicht en testen

In het informatieveiligheidsbeleid van de provincie Gelderland uit februari 2016 staat het volgende over controles en testen.

- Het toezicht op de uitvoering ligt bij de afdeling Control en auditinstanties (accountant en auditdienst).
- De Information Security Officer zorgt namens de directie voor het toezicht op de uitvoering van het informatiebeveiligingsbeleid.
- Control is onderdeel van het werkproces met als doel het waarborgen van de kwaliteit van informatie en ICT, en naleving van wet- en regelgeving.
- Er is externe controle. Dit betreft controle buiten het primaire proces door de accountant en ethical hackers. Dit heeft het karakter van een steekproef. Jaarlijks worden meerdere van dergelijke onderzoeken uitgevoerd.
- Voor de CHECK uit de PDCA-cyclus wordt genoemd: self assesments, TPM[110], interne controle, management rapportages, vulnerability scanning[111], pentesten, social engineering testen, evaluatie en rapportage.
- De kwaliteit van de informatieveiligheid wordt in opdracht van de directie periodiek onderzocht door de accountant en onafhankelijke externen (bijvoorbeeld door middel van penetratietesten).
- Er wordt een beveiligingsdocumentatiedossier aangelegd en onderhouden. Hier staat alle relevante verplichte en niet-verplichte documenten waaruit blijkt / kan worden aangetoond dat aan de beveiligingseisen is voldaan.

[110] *Third Party Memorandum of Derdenverklaring. Dit is een verklaring die wordt afgegeven door een onafhankelijke audit partij over de kwaliteit van een ICT-dienstverlening en -beheersing van een organisatie. Dit wordt een TMP / Derdenverklaring genoemd omdat de eerste partij de product/leverancier is, de tweede partij de klant/afnemer en de derde partij is de onafhankelijke derde.*

[111] *Dit is een computerprogramma waarmee gekeken wordt of computers, netwerken of applicaties bekende kwetsbaarheden bevatten.*

Toezicht en testen in de praktijk

In tabel 4 noemen we welke controles en testen op het gebied van de informatieveiligheid door de provincie of in opdracht van de provincie zijn uitgevoerd.

Tabel 4: *Uitgevoerde controles en testen door/in opdracht van provincie Gelderland*

Uitvoerder	Scope en frequentie

Extern (onafhankelijke toetsing)	• Periodiek:
	  o Aandacht van accountant voor thema in boardletters en jaarverslagen, in het bijzonder in 2017.
	• Incidenteel:
	  o test van specifieke applicatie (Besluiten 2.0) in 2017;
	  o test bewustwording medewerkers via phishing e-mail in 2018 (daarvoor penetratie- en inlooptest in 2013);
	  o nulmeting ISO 27001 in 2018.[112]

Provincie (zelfevaluatie)	• Cibo-monitor over de implementatie van de IBI (2014 en eerder, 2016).

Bron: Rekenkamer Oost-Nederland op basis van informatie ontvangen van de provincie.

Periodieke externe toetsing

De accountant heeft de afgelopen jaren aandacht besteed aan (aspecten van) informatieveiligheid. Zie bijlage 2 voor een overzicht. Aspecten van informatieveiligheid (bijvoorbeeld autorisaties) kwamen veelal aan bod bij de algemene IT-controles rondom het financieel systeem. De accountant had in 2017 extra aandacht voor IT en privacy. Dit op verzoek van PS.

Incidentele externe toetsing

Uit tabel 4 blijkt dat er ook testen zijn die incidenteel zijn uitgevoerd.

Ten eerste is in 2017 het programma Besluiten 2.0 getest door een extern bureau. Dit is het digitale besluitvormingsproces van de provincie. Het idee is om in de toekomst meer applicaties door een onafhankelijke partij te laten testen. Bijvoorbeeld als een nieuwe versie van het financiële systeem Oracle geïmplementeerd wordt.[113]

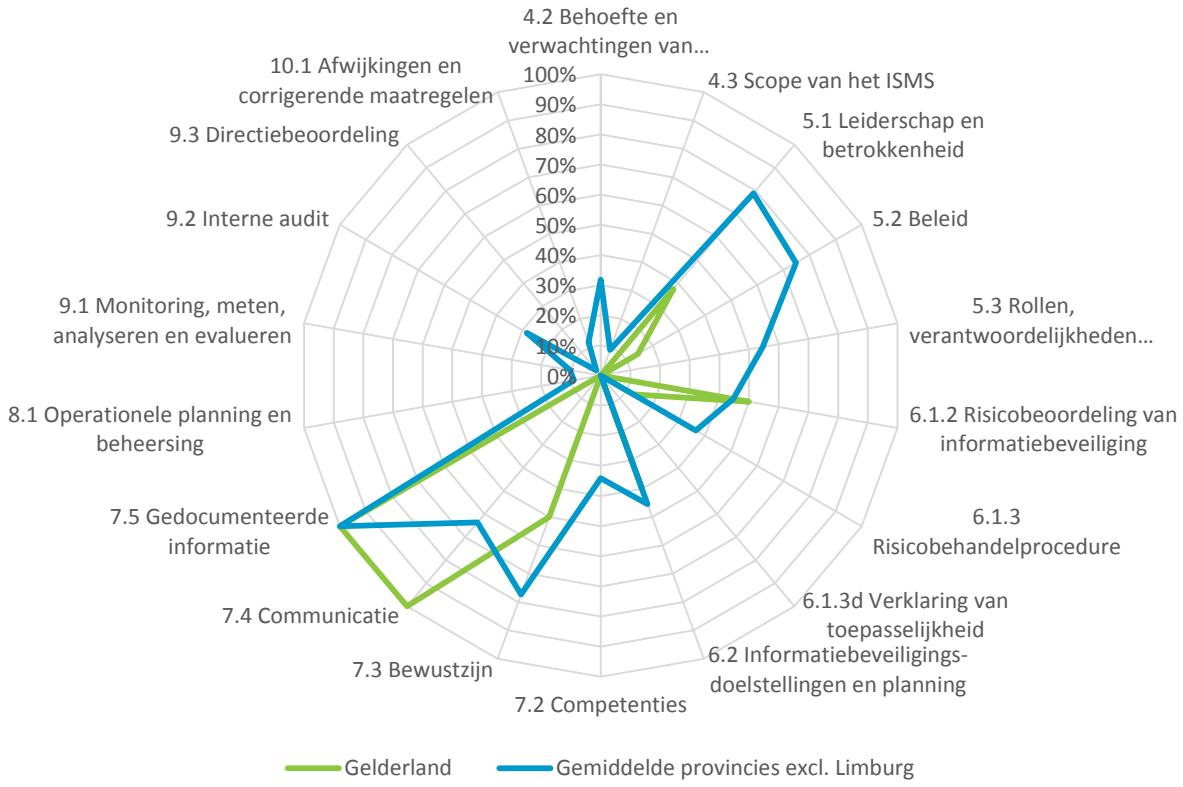
Ten tweede is in 2018 de bewustwording van medewerkers getoetst (zie ook paragraaf 3.3). Tussen 2013 en 2018 zijn geen praktijktesten van informatiebeveiliging (zoals penetratietesten, inlooptesten of phishing-testen) uitgevoerd. Hiermee is het beleid, wat spreekt over jaarlijkse externe onderzoeken, niet gevolgd. De accountant maakte hier ook een punt van. Zij adviseerde in 2017 om *"[…] periodiek vast te stellen dat de grootste risico's binnen de IT-omgeving zijn afgedekt, bijvoorbeeld door het laten uitvoeren van technische penetratietesten op de IT-infrastructuur"*.[114] De provincie geeft zelf twee verklaringen voor het niet uitvoeren van deze testen. Ten eerste de transitie van de IT-taken naar een externe dienstverlener. Die duurde langer dan verwacht. Een

[112] *Formele opdrachtgever is Bij12. Bij12 is de uitvoeringsorganisatie voor de samenwerkende provincies.*
[113] *Ambtelijk interview.*
[114] *PWC (december 2017). Rapportage interim-bevindingen 2017 provincie Gelderland p. 11.*

test uitvoeren op een omgeving die verandert is niet handig, want wat test je dan? Ten tweede werd het gebouw verbouwd en is dit relatief kort geleden in gebruik genomen. Mensen hebben tijd nodig om aan een gebouw te wennen.[115]

Tot slot is in 2018 onderzocht of de provincie voldoet aan de ISO 27001. De ISO 27001 bevat eisen waar het managementsysteem voor informatieveiligheid aan moet voldoen. De focus is gericht op het aantoonbaar managen en beheersen van informatieveiligheid. De ISO 27001 is de standaard waarvoor organisaties zich kunnen certificeren. De provincies hebben afgesproken dat zij eind 2023 het ISO 27001-certificaat gehaald willen hebben. Daar zijn ze zich momenteel op het voorbereiden. Onderdeel van die voorbereiding was een nulmeting bij elke provincie om te kijken hoe het er nu voor staat. Deze nulmeting liet het volgende beeld zien:

Figuur 10: *Uitkomst nulmeting 27001 provincie Gelderland*



Bron: Presentatie Digitrust Nulmeting ISO27001 BIJ12 + 12 provincies.

Uit figuur 10 blijkt dat de provincie Gelderland op verschillende onderdelen - uitgezonderd communicatie en documentatie - laag scoort in de nulmeting. De provincie geeft aan dat dit komt omdat veel zaken nog niet op papier staan. Het staat op de planning om komend jaar, als de transitie is afgerond, het beleid te actualiseren en nader uit te werken.[116] In zijn algemeenheid voldeed geen van de provincies aan alle hoofdstukken van de ISO 27001. Er waren negen provincies die gemiddeld onder de 50%

[115] *Ambtelijke interviews.*
[116] *Ambtelijk interviews.*

scoorden. De provincie Gelderland scoorde gemiddelde 22%. Daarmee was zij één van de laagst scorende provincies.

Toetsing door de provincie

Uit tabel 4 blijkt dat de provincie Gelderland voor 2014 en in 2016 een zelfaudit heeft uitgevoerd. De provincies hadden afgesproken de interprovinciale Cibo-monitor jaarlijks in te vullen. Dit hebben zij tot en met 2014 gedaan. Omdat de provincies werkten aan een nieuwe Interprovinciale Baseline Informatieveiligheid, is besloten om in 2015 de monitor op basis van de oude IBI niet meer te gebruiken. De provincies konden er wel zelf voor kiezen om deze monitor in te vullen.[117] De provincie Gelderland heeft er dus niet voor gekozen om dit alsnog zelf te doen. Eind 2016 hebben de provincies, zo ook Gelderland, de Cibo-monitor op basis van de nieuwe IBI ingevuld. In 2017 is dit niet gezamenlijk gedaan. Als reden werd ambtelijk aangegeven dat de provincies hier geen prioriteit aan hebben gegeven.

Overig: doorlopende monitoring en dossiervorming door de provincie

In voorgaande hoofdstukken zijn al een aantal zaken rondom monitoring aan de orde gekomen. Onder andere dat informatie over maatregelen en de uitvoering daarvan zijn verspreid/niet in één systeem zijn opgenomen en dat de naleving van de (aanvullende maatregelen die voortkomen uit de) Business Impact Analyses niet wordt gecheckt.

In het beleid staat dat de provincie een beveiligingsdocumentatiedossier aanlegt en onderhoudt met relevante documenten gelegd waaruit blijkt / kan worden aangetoond dat aan de beveiligingseisen is voldaan. Navraag leert dat dit in de praktijk niet wordt gedaan.[118]

Toezicht en testen externe partijen

Beleid externe partijen

In het informatiebeveiligingsbeleid van de provincie Gelderland staat dat dit beleid, landelijke normen en wet- en regelgeving ook gelden voor externe partijen (leveranciers, ketenpartners) waarmee de provincie samenwerking en informatie mee uitwisselt. Voor externe hosting van data en/of services gelden naast dit generieke informatiebeveiligingsbeleid de richtlijnen voor cloud computing. De provincie blijft hierbij eindverantwoordelijk voor de betrouwbaarheid van uitbestede diensten. Dit is gebonden aan regels[119] en vereist goede (contractuele) afspraken en controle hierop, zo stelt het beleid. Aangegeven wordt dat externe hosting providers verantwoording aan hun opdrachtgevers afleggen over de naleving van het informatiebeveiligingsbeleid. Bij uitbestede (beheer)processen kan een verklaring bij leveranciers worden opgevraagd.[120]

---

[117] *Randstedelijke Rekenkamer (juli 2015). Eindrapporten informatieveiligheid Flevoland, Noord-Holland, Utrecht en Zuid-Holland. Paragraaf 5.3 Uitvoering van een zelfevaluatie (specifieke bron: Provincie Zuid-Holland (2016), e-mail 8 februari 2016 van een Cibo-lid vanuit Zuid-Holland).*

[118] *Ambtelijk interview.*

[119] *Regels die in het beleid worden aangegeven zijn dat externe hosting van data en/of services is goedgekeurd voor verantwoordelijk manager als systeemeigenaar, voorzien is van een advies van de ISO wat betreft informatiebeveiligingsbeleid en voorzien is van een advies van een I&A adviseur wat betreft (technische) beheeraspecten.*

[120] *Het gaat bijvoorbeeld om een TPM- of ISAE3402-verklaring.*

Verder staat bijvoorbeeld in het beleid dat de provincie:

- diensten, rapporten en registraties, die door de derde partij worden geleverd, controleert en beoordeelt en er periodiek audits worden uitgevoerd en
- wijzigingen in de dienstverlening door derden beheert (bijvoorbeeld in bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging).

Monitoring en controle op taken OGD

De belangrijkste externe dienstverlener is OGD. De provincie heeft hier IT-diensten bij ondergebracht.

Bij de aanbesteding is er aandacht geweest voor het testen van informatieveiligheid door de externe dienstverlener. Zo stond in het programma van eisen dat:

- de opdrachtnemer op overeengekomen basis (en bijlage alle releases van webservers, die toegankelijk zijn vanaf het internet) securitytesten (bijvoorbeeld penetratietesten) moet uitvoeren op de IT-omgeving;
- de opdrachtnemer jaarlijks een IT-continuïteitstest moet uitvoeren en
- de opdrachtnemer periodiek security testen moet uitvoeren op de OWASP top 10[121] en de SANS top 20[122] risico's.[123]

Ook stonden hierin eisen in over de verantwoording van de opdrachtnemer richting de provincie. Zo moet de opdrachtnemer op overeengekomen basis aan de provincie rapporteren over security incidenten en zwakke plekken in de beveiliging en een audit proces inregelen waarin (onder andere) periodieke rapportages over auditresultaten zijn geborgd.[124]

De provincie benadrukt dat hoewel OGD de uitvoerende partij is, zij als provincie nog steeds verantwoordelijk is voor de uitvoering. Om die verantwoordelijkheid goed in te kunnen vullen, wil de provincie alle informatie hebben. Op dit moment verloopt dit proces moeizaam. Er is meer dan een jaar met OGD gesproken over het informatiebeveiligingsplan (met daarin nadere afspraken met de provincie over andere testen en verantwoording). Dat is 14 december definitief geworden. De provincie heeft de beschikking over een aantal dashboards, maar die bevatte nog niet alle benodigde informatie.[125] Eens in de twee weken vindt er operationeel overleg plaats tussen de provincie en OGD. Hierin worden lopende security zaken besproken. De resultaten van de praktijktest in opdracht van de Rekenkamer zijn hier bijvoorbeeld in besproken. [126]

[121] *Het Open Web Application Security Project is een open source-project rond computerbeveiliging. Zij publiceren een top 10 van de grootste en meest voorkomende risico's binnen webapplicaties.*
[122] *De SANS 2o 20 is de voormalige naam van een lijst van 20 Critical Security Controls van het Center for Internet Security (CIS).Op de lijst staan de 20 belangrijkste maatregelen om te implementeren om controle te krijgen over cybersecurity.*
[123] *Provincie Gelderland (september 2016). Bijlage B-008 Programma van Eisen Infrastructuur, hosting, helpdesk en servicedesk (E84, E53 en E81).*
[124] *Provincie Gelderland (september 2016). Bijlage B-008 Programma van Eisen Infrastructuur, hosting, helpdesk en servicedesk (E85 en E86).*
[125] *Ambtelijk interview.*
[126] *Ambtelijke interviews.*

Monitoring en controle op andere externe partijen

De provincie houdt er geen strak zicht op dat externe leveranciers audits aanleveren. Wel wordt er geëist dat leveranciers ISO 27001 gecertificeerd zijn. De provincie geeft aan dat dit voldoende informatie geeft. Vaak wordt er ook een wens opgenomen voor een zogenoemde 'ISAE 34XX-certificering'.[127] Dit is een internationale standaard bij outsourcing.[128] Het ISO 27001-certficaat dat een leverancier verstrekt, wordt door de provincie ook getoetst op de 'scope'[129].

5.2 Verantwoording

Norm

- De provincie heeft informatieveiligheid verankerd in de reguliere P&C-cyclus en geeft in het jaarverslag inzicht in de status van informatieveiligheid.

Bevindingen

- Er zijn de laatste jaren geen structurele rapportages over informatieveiligheid aan directie en management gestuurd. Zij zijn wel geïnformeerd als er iets speelt, bijvoorbeeld bij testresultaten of een datalek.
- Informatieveiligheid maakt nog geen deel uit van de bestuurlijke P&C-cyclus. Er wordt niet over gerapporteerd in de begroting en de jaarstukken. Wel is daarin aandacht voor de (risico's omtrent) datalekken en - sinds 2017 - voor de AVG. PS hebben een aantal keer een brief/notitie danwel een uitnodiging voor een bijeenkomst ontvangen die ging over of raakte aan informatieveiligheid.

Het principe van verplichtende zelfregulering bij de borging van informatieveiligheid door provincie, betekent ook dat er geen sprake is van een vrijblijvend proces. Dat maakt het van belang dat bestuur en management van de provincie goed zicht hebben op de stand van zaken bij informatieveiligheid. Daarom is in het convenant Interprovinciale Regulering Informatieveiligheid afgesproken dat over informatie-veiligheid wordt gerapporteerd in de planning & control cyclus. Onder P&C-cyclus verstaan we de rapportagesystematiek aan management, GS en PS. We kijken dus ook naar de verantwoording over informatieveiligheid in de jaarstukken.

Verantwoording aan GS, directie en management

In paragraaf 2.1 hebben we al aandacht besteed voor wat in beleid staat over de verantwoording aan GS en management en hoe dit in de praktijk gaat:

> GS zijn tot nu toe vooral betrokken bij datalekken. Er zijn geen structurele rapportages aan GS over informatieveiligheid. De directie ontvangt geen halfjaarlijkse rapportages conform beleid. Dit is een bewuste keuze. Zij worden - zoals met hen is

[127] *Ambtelijk interview.*
[128] *Bron: www.isae3402.nl*
[129] *De ISO 27001 scope geeft aan waarvoor een organisatie het ISO-certificaat precies heeft behaald. Alles wat buiten de scope valt, wordt niet in de certificering meegenomen. Deze scope staat op het certificaat.*

afgesproken - geïnformeerd over projecten die gaan over / raken aan informatieveiligheid (bv. rondom AVG) en als er iets speelt (bv. incidenten of testen). Ook het afdelingsmanagement wordt in die gevallen geïnformeerd. Bij hen vindt informatievoorziening ook meer via overleg en gesprek plaats.

De provincie geeft aan dat volgend jaar de verantwoordingsmethodiek wordt herzien en dat het idee is om dan de structurele rapportages ook weer op te pakken.

Verantwoording aan PS

In het beleid staat dat over het functioneren van informatiebeveiliging jaarlijks wordt gerapporteerd conform de Planning & Controlcyclus. In het beleid en andere documenten zijn geen afspraken met PS opgenomen over de informatievoorziening specifiek rondom informatiebeveiliging.

De schriftelijke informatie die PS de afgelopen jaren ontvingen via brieven en notities had met name betrekking op privacy en datalekken (zie tabel 5). Dit als gevolg van de wet Meldplicht datalekken en de AVG.

Tabel 5: *Brieven en notities aan PS die gaan over / raken aan informatieveiligheid*

Brief/notitie	Toelichting
April 2016: Mededelingen-brief GS aan PS (PS2016-333)	• *Onderwerp*: Wet meldplicht datalekken. • *Aanleiding*: Vraag in Procedurecommissie over betekenis wet. • *Inhoud*: Wat is een datalek, wanneer moet hier melding van gemaakt worden bij de Autoriteit Persoonsgegevens en wat kan het gevolg zijn van niet melden. Ook is aangegeven dat binnen de provinciale organisatie kritische werkprocessen worden doorgelicht op mogelijke datalekken (en waar nodig beheersmaatregelen getroffen) en dat de accountant aandacht besteedt aan de implementatie van de wetgeving.
Mei 2017: Notitie Griffie aan Procedurecommissie (PS2017-299)	• *Onderwerp*: Gevolgen van de gewijzigde privacywetgeving voor het openbaar (actief) publiceren van (ingekomen) stukken op het StatenInformatieSysteem. • *Aanleiding*: Wijziging in procedure van ingekomen stukken naar aanleiding van datalek in februari 2017 in het oude SIS. • *Inhoud*: Uitleg van de gewijzigde procedure rondom ingekomen stukken. Concreet gaat het om verdergaandere anonimisering.
Mei 2018: Extra mede-delingenbrief GS aan PS (PS2018-351)	• *Onderwerp / aanleiding*: Datalek. • *Inhoud*: informatie over een datalek plaatsgevonden bij een uitgaande mail waarbij per ongeluk 1171 externe e-mailadressen waren geopenbaard.

Tabel 5 laat zien dat PS in mei dit jaar zijn geïnformeerd over een datalek van ruim 1.100 e-mailmailadressen. Dit was het grootste datalek dat tot nu toe (september 2018) bij de provincie Gelderland heeft plaatsgevonden. Het kleinste bestond uit gegevens van twee personen. Tot nu toe (sept. 2018) zijn er zes datalekken gemeld bij de Autoriteit

Persoonsgegevens. Per keer wordt de afweging gemaakt om PS wel of niet te informeren over het datalek. De proceseigenaar (veelal afdelingsmanagement) informeert de verantwoordelijk Gedeputeerde. Zij maken die afweging. Hierbij is onder andere de omvang van het datalek onderdeel van die afweging. [130]

Jaarverslagen

In de jaarverslagen van de provincie Gelderland is er met name aandacht voor (het risico van) datalekken en - sinds 2017 - voor de implementatie van de AVG. De jaarverslagen bieden geen zicht op de status van de informatieveiligheid.

In de accountantsverslagen en met name de boardletters die ook naar PS gaan, was wel aandacht voor (aspecten van) informatiebeveiliging. Zie hiervoor de toelichting in de vorige paragraaf. Zoals we daar al noemden, had de rekeningcommissie de accountant in 2017 het onderwerp IT en privacy als speerpunt meegegeven. Het onderwerp kwam duidelijk in de boardletter 2017 terug en bij de bespreking daarvan. De Rekeningcommissie wees in die bespreking expliciet op fysieke toegang als security-aspect.[131]

In de vergaderingen van PS van de afgelopen jaren was weinig aandacht voor informatieveiligheid. Er zijn geen schriftelijke vragen ingediend die gaan over het thema danwel daaraan raken. Wel is in vergaderingen een enkele keer een mondelinge vraag gesteld of opmerking hierover gemaakt.[132]

Bijeenkomsten

PS ontvangen niet alleen schriftelijk verantwoording, maar worden ook via bijeenkomsten geïnformeerd. PS zijn de afgelopen jaren voor een aantal bijeenkomsten uitgenodigd die gingen over of raakten aan informatieveiligheid. In tabel 6 noemen we er een aantal. Ook hebben PS een workshop informatiebeveiliging aangeboden gekregen, waar gebruik van is gemaakt.

Tabel 6: *Bijeenkomsten PS die gaan over / raken aan informatieveiligheid*

Datum	Toelichting
17 juni 2015	Introductie nieuwe Statenleden: Bijeenkomst over papierloos vergaderen met de Notubox en informatiebeveiliging.
23 t/m 29 sept. 2017	Gelderse Einsteinweek: Masterclasses en workshops over andere privacy, cyber security etc.
31 jan. 2018	Eén van de directieleden heeft in de vergadering van de procedure-commissie een toelichting gegeven over een datalek dat had plaatsgevonden. Het ging hier om spam die Statenleden hadden ontvangen via de mailman waarbij (doordat ruim veertig personen naar iedereen reageerden) e-mailadressen bekend zijn geworden.[133]

[130] *Ambtelijk interviews.*
[131] *Provincie Gelderland. PS2018-38. Ontwerpverslag Rekeningcommissie 17 januari 2018. Agendapunt 2.*
[132] *Zie bijvoorbeeld PS2015-395 (verslag PS-vergadering 3 juni 2015, p.3) en PS2017-415 (verslag PS-vergadering 27 en 28 juni 2017, p. 15-16).*
[133] *Provincie Gelderland. PS2018-80. Verslag vergadering Procedurecommissie 31 januari 2018.*

Bijlagen

Bijlage 1: Onderzoeksopzet

Doel en vraagstelling

Doel

Het doel van dit onderzoek is om:

> Provinciale Staten van Gelderland en Overijssel te ondersteunen in hun kaderstellende en controlerende rol door inzichtelijk te maken of de informatieveiligheid van de provincie voldoende is geborgd.

Centrale vraag

In dit onderzoek staat de volgende vraag centraal:

> *Hebben de provincies Gelderland en Overijssel de informatieveiligheid voldoende geborgd?*

Onderzoeksvragen

De centrale vraag hebben we uitgewerkt in een aantal onderzoeksvragen. Deze vragen zijn gebaseerd op de vier thema's uit het Convenant Interprovinciale Regulering Informatieveiligheid (zie paragraaf 1.2.2).

1. Hebben de provincies Gelderland en Overijssel de sturing op en de verantwoordelijkheid voor informatieveiligheid goed verankerd?
2. Is het informatieveiligheidsbeleid van de provincies Gelderland en Overijssel adequaat in opzet, uitvoering en resultaat?
   a. Hebben de provincies Gelderland en Overijssel informatieveiligheidsbeleid opgesteld dat voldoet aan de gestelde eisen?
   b. Voeren de provincies Gelderland en Overijssel de benodigde informatieveiligheidsmaatregelen uit?
   c. Is informatie bij de provincies Gelderland en Overijssel in de praktijk voldoende beschermd tegen toegang door onbevoegden?
3. Hebben de provincies Gelderland en Overijssel voldoende aandacht voor bewustwording op het gebied van informatieveiligheid?

4. Hebben de provincies Gelderland en Overijssel het afleggen van verantwoording over en het houden van toezicht op informatieveiligheid goed geregeld?

Normenkader

Voor dit onderzoek naar de informatieveiligheid van de provincie Gelderland hebben we het volgende normenkader opgesteld:

Tabel 7: *Normen onderzoek informatieveiligheid*

Thema	Norm	Bron

Beleid	• De provincie heeft een beleidskader informatieveiligheid:
	  ○ dat is vastgesteld op minimaal directieniveau,
	  ○ maximaal vier jaar oud is en gewijzigd is bij belangrijke ontwikkelingen en
	  ○ gebaseerd op de Interprovinciale Baseline Informatieveiligheid.
		○ IBI (hfst. 5.1.1 - B1)
		○ IBI (2010, A5.1.2)
		○ Convenant (B)

Sturing en verantwoordelijkheid	• De provincie heeft informatieveiligheid als onderdeel van de portefeuille van een lid van GS belegd. • Bestuur en management van de provincie zijn zich bewust van de risico's die ze lopen en hun verantwoordelijkheid daarin. • Er is een duidelijke verantwoordelijkheidsverdeling voor informatieveiligheid en deze is vastgelegd.	• Convenant IRI (A) • Convenant IRI (A) • IBI (hfst. 6.1)

Uitvoering	• De provincie heeft op basis van risicoanalyses bepaald welke aanvullende maatregelen zij moet nemen.
	  ○ Er is inzichtelijk wat de belangrijkste kroonjuwelen zijn en wat het effect van een cyberaanval op deze kroonjuwelen kan zijn.
	• De provincie heeft de 'basis' maatregelen genomen en monitort de uitvoering daarvan.
	• De provincie controleert de uitvoering van de aanvullende maatregelen die uit de risicoanalyses komen.
		• Convenant IRI (A), IBI B1, p. 1
		  ○ Cyber security health check
		• IBI, p. 7-8

Verdieping uitvoering	• De provincie voert periodiek een bewustwordings-programma rondom informatieveiligheid uit. • De provincie heeft de vijf informatieveiligheidstandaarden geïmplementeerd bij haar website en e-mails. • De provincie heeft de basis IT-hygiënemaatregelen (patch management, toegangsbeheer en back ups) op orde. • De provincie neemt afdoende maatregelen voor de fysieke beveiliging van informatie.	• Convenant IRI (D) • Streefbeeld-afspraken NBDO • Cyber security health check
Resultaat (praktijktest)	• De provincie doorstaat de specifieke test. • Uit de test komen geen kwetsbaarheden die al bekend zijn bij de provincie en al opgelost hadden kunnen zijn.	

Toezicht en verantwoording	• De provincie laat periodiek een onafhankelijke toets uitvoeren op het beveiligingsniveau en de implementatiestatus van het informatieveiligheidsbeleid. • De provincie voert zelfevaluaties uit. • De provincie heeft informatieveiligheid verankerd in de reguliere P&C-cyclus en geeft in het jaarverslag inzicht in de status van informatieveiligheid.	• Convenant IRI (C) • Convenant IRI (C) • Convenant IRI (C)

Onderzoeksmethodiek

In tabel 8 beschrijven we de aanpak voor de beantwoording van de vier onderzoeksvragen.

Tabel 8: *Werkwijze onderzoek informatieveiligheid per onderzoeksvraag*

Vraag	Werkwijze
1.	We zijn onder andere nagegaan of en in welke documenten verantwoordelijkheden, taken en bevoegdheden met betrekking tot informatieveiligheid zijn toegekend aan de verschillende functies binnen de provinciale organisatie.
2.	We hebben het beleidskader informatieveiligheid (vraag 2a) geanalyseerd en zijn nagegaan hoe er in de praktijk invulling wordt gegeven aan dit beleid (2b). Voor het beantwoorden van vraag 2c zijn de waarborgen voor het beschermen van informatie voor toegang door onbevoegden door een externe partij onderzocht.
3.	We hebben (de uitvoering van) het bewustwordingsprogramma en andere activiteiten die mogelijk worden ondernomen om bewustwording van informatieveiligheid te bevorderen, geanalyseerd. Ook dit heeft de externe partij in de praktijk onderzocht.
4.	We zijn nagegaan of informatieveiligheid een plek heeft in de P&C-documenten en of een onafhankelijke toets en zelfevaluatie is uitgevoerd.

Door de provincies is ook onderzoek gedaan naar informatieveiligheid. Deze onderzoeken hebben we - voor zover mogelijk - meegenomen in ons onderzoek om dubbelwerk te voorkomen.

Praktijktest

Een extern bureau heeft in opdracht van de Rekenkamer onderzocht of informatie bij de provincie Gelderland in de praktijk voldoende wordt beschermd tegen toegang door onbevoegden. Dit praktijkonderzoek vond in juli - augustus 2018 plaats. De praktijktest bestond uit een aantal onderdelen:

- externe penetratietest: het testen van de beveiliging van buitenaf (vanaf het internet) tot de infrastructuur van de provincie.
- interne penetratietest: het testen van de beveiliging van binnenuit (het lokale netwerk) tot de infrastructuur van de provincie.
- wifi test: het testen van de draadloze netwerken van de provincie.
- social engineering test: het testen van de bewustwording van medewerkers van de provincie door middel van een inlooptest (inclusief het achterlaten van geprepareerde usb-sticks) en spear phishing.

Bijlage 2: Informatieveiligheid in accountantsverslagen

Tabel 9: *Samenvatting boardletters en jaarverslagen accountant 2015-2017 op onderdeel informatieveiligheid*

Document	Samenvatting
Accountants-verslag 2017	• *Nieuwe AVG heeft aandacht*: De afgelopen maanden voerden het projectteam privacy, in samenwerking met de proceseigenaren en een externe partij diverse acties uit, zoals de ontwikkeling van een nieuw extern privacybeleid, het inventariseren van dataverwerkingen en het in kaart brengen van de bewerkersovereenkomsten. Daarbij zijn de acties om per 25 mei 2018 te voldoen aan de AVG in kaart gebracht en uitgezet. Deze acties zijn bijvoorbeeld: het vaststellen van intern privacybeleid, het verder vergroten van het privacybewustzijn onder medewerkers en het uitvoeren van privacy impact analyses rondom kritische processen (bv. proces burgemeesterbenoemingen). De provincie werkt hiermee zeer actief aan het voldoen aan de regelgeving. • *De kwaliteit van de IT-beheersing is in 2017 toegenomen*: De belangrijkste in 2017 doorgevoerde verbeteringen zijn: het documenteren en accorderen van wijzigingen voor de implementatie in de Oracle-productieomgeving. Ook is monitoring op de naleving van de wijzigingsbeheerprocedure geïmplementeerd. In oktober 2017 is een nieuw wachtwoordenbeleid ingericht; in het voorjaar 2018 wordt de inrichting beoordeeld. De belangrijkste bevindingen richten zich op het autorisatiebeleid en het bijwerken van updates voor de informatiebeveiliging binnen Oracle. • *Uitbesteding IT-diensten is onderhanden*: […] Er is vernomen dat het proces onderhanden is om servicelevelafspraken te maken met de leverancier rondom periodieke rapportering over KPI's op het gebied van de kwaliteit van de dienstverlening. De projectorganisatie monitort intern of de dienstverlening voldoet aan de eisen die zijn gesteld in het aanbestedingsproces. Het belang van deze afspraken wordt onderschreven en er wordt geadviseerd actief te monitoren dat de dienstverlening in lijn is met de afspraken. Er is vernomen dat leveranciers via assuranceverklaringen en certificering aantoonbaar kunnen maken dat ze in control zijn. Er wordt geadviseerd deze verklaringen op te vragen en te beoordelen of de afgenomen dienstverlening

	wordt afgedekt in de reikwijdte van de verklaring(en), dit als onderdeel van de totaalsturing op de uitbestede taken.
Boardletter 2017	• *Provincie erkent risico's cybercrime en treft beheersmaatregelen, implementatie AVG loopt conform planning:* Cyberrisico's blijven toenemen en nieuwe privacywetgeving vraagt om tijd en aandacht. Binnen de organisatie is het risico onderkend en zijn beheersmaatregelen ingericht. De provincie beschikt over een informatiebeveiligingsbeleid en heeft diverse maatregelen genomen om te voorkomen dat cybercriminelen zich te gemakkelijk toegang kunnen verschaffen. Ook is de provincie bezig te onderzoeken hoe de aantoonbaarheid van getroffen maatregelen kan worden verbeterd en welke processen en werkwijzen conform het IBI verder moeten worden geformaliseerd. Gedurende 2017 hebben er geen technische penetratietesten op de IT-infrastructuur plaatsgevonden. Er wordt geadviseerd om actief aandacht te blijven geven aan informatiebeveiliging en periodiek vast te stellen dat de grootste risico's binnen de IT-omgeving zijn afgedekt, bijvoorbeeld door het laten uitvoeren van technische penetratietesten op de IT-infrastructuur. Ook wordt geadviseerd het informatiebeveiligingsbeleid periodiek te actualiseren en hierbij nieuwe wet- en regelgeving mee te nemen. • *Kwaliteit algemene IT-beheersmaatregelen is toegenomen*: De kwaliteit van de IT-beheersing is in 2017 toegenomen. De belangrijkste verbeteringen die in 2017 zijn doorgevoerd, betreffen het documenteren en accorderen van wijzigingen voor de implementatie in de Oracle-productieomgeving. Ook is monitoring op de naleving van de wijzigingsbeheerprocedure geïmplementeerd. In oktober 2017 is een nieuw wachtwoordenbeleid ingericht; in het voorjaar 2018 zullen wij de inrichting beoordelen. De belangrijkste bevindingen richten zich op het autorisatiebeleid en het bijwerken van updates voor de informatiebeveiliging binnen Oracle. • *Uitbesteding IT-diensten vraagt om andere sturing:* Uitbesteding IT-diensten vraagt om andere sturing en invulling van het opdrachtgeverschap. De komende jaren worden in fases een belangrijk deel van de IT-diensten uitbesteed aan leveranciers. De huidige I&A-organisatie wordt hiermee omgevormd tot een regieorganisatie. Begin 2017 zijn de eerste onderdelen van de IT-infrastructuur uitbesteed. De provincie is nog in gesprek met de leverancier over de rapportering van KPI's, waarbij de leverancier aantoont in control te zijn. Het belang van deze afspraken wordt onderschreven en er wordt geadviseerd actief te monitoren dat de dienstverlening in lijn is met gemaakte afspraken.
Accountants-verslag 2016	Gedurende 2016 zijn verbeteracties gerealiseerd in de algemene IT-beheersmaatregelen, maar dit zijn niet het hele jaar effectief geweest. Er is geconstateerd dat in 2016 en begin 2017 een aantal onderbrekingen zijn geweest in de IT-omgeving. Hierdoor hebben diverse systemen af en toe niet gewerkt of waren niet beschikbaar. Er werden een aantal attentiepunten meegegeven, waaronder: - het consequent inrichten en gebruiken van de autorisatiematrix die in het derde kwartaal 2016 is ingevoerd om te bepalen welke autorisaties een gebruiker mag krijgen; - binnen het financieel systeem Oracle zijn beperkte wachtwoordrestricties van kracht en

	- het uitvoeren van een risicoanalyse en op basis hiervan beoordelen in hoeverre het noodzakelijk is om logging van kritische handelingen mogelijk te maken.
Boardletter 2016	• *Uitbesteding IT-diensten vraagt om andere sturing*: De provincie gaat IT-diensten deels uitbesteden aan leveranciers en de huidige I&A organisatie omvormen tot een regie-organisatie. Om te komen tot een regie-organisatie is het belangrijk goede en meetbare afspraken te maken met de toekomstige uitvoeringsorganisatie. Handvaten zijn hiervoor het afsluiten van Service Level Agreements en periodieke rapportering over KPI's. • *Nieuwe privacy wetgeving is vastgesteld*: De provincie beschikte op het moment van de uitvoering van de tussentijdse controle nog niet over een functionaris gegevensbescherming. De provincie heeft een Information Security Officer die zowel verantwoordelijk is voor beveiligings- als privacy-aspecten. Er wordt geadviseerd de beveiligingsorganisatie te versterken. De provincie is eind 2015 een project gestart om te voldoen aan de Wet meldplicht datalekken. Het project heeft ook als doelstelling zorg te dragen voor de vereisten van de AVG. In dit kader heeft de provincie een privacy nulmeting laten uitvoeren en heeft de Security Officer workshop gehouden om het bewustzijn van medewerkers op security en privacy vlak te vergroten. Daarnaast is een inventarisatie uitgevoerd van de verwerkingen van persoonsgegevens. Het belang van het privacy traject wordt onderschreven en er wordt geadviseerd om aanvullend te kijken naar de afhankelijkheid van andere partijen, zoals ketenpartners en leveranciers. Ook wordt het zaak genoemd om via continue monitoring het te implementeren privacy raamwerk en de daarbij behorende procedures en beheersmaatregelen te verbeteren en versterken.
Accountants-verslag 2015	Drie attentiepunten voor de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking: - wijzigingen in applicaties die niet altijd werden gedocumenteerd, - de in- en uitdienstprocedures (incl. wijzigen rechten in applicaties) aanscherpen en - er werd aandacht gevraagd voor de toekenning van rechten in applicaties (soms veel medewerkers met beheersrechten).
Boardletter 2015	Aantal attentiepunten uit beoordeling van de IT-omgeving, onder andere: - beheersing autorisaties bij uitdiensttreding - het vastleggen van testen bij wijzigingen van systemen en - controle inrichting autorisaties applicaties.

Bijlage 3: Afkortingen en begrippen

Tabel 10: *Gebruikte afkortingen*

Afkorting	Uitleg
AP	Autoriteit Persoonsgegevens
AMT	Afdelingsmanagementteam
BIA	Business Impact Analyse
BIO	Baseline Informatiebeveiliging Overheid
Cibo	Centraal Informatiebeveiligingsoverleg
CSR	Cyber Security Raad
FD	Facilitaire Dienstverlening
GS	Gedeputeerde Staten
I&A	Informatisering & Automatisering
IBI	Interprovinciale Baseline Informatieveiligheid
ICT	Informatie- en Communicatietechnologie
IPO	Interprovinciaal Overleg
IRI	Interprovinciale Regulering Informatieveiligheid
ISO	Information Security Officer
ISO	International Organization for Standardisation
ISMS	Information Security Management System
IT	Informatietechnologie
FG	Functionaris voor de Gegevensbescherming
NBA	Nederlandse Beroepsorganisatie van Accountants
NBDO	Nationaal Beraad Digitale Overheid
P&C	Planning & Control
PDCA	Plan, Do, Check, Act
PS	Provinciale Staten
SIO	Strategisch Informatie Overleg
TPM	Third Party Memorandum (Derdenverklaring).

Tabel 11: Begrippen

Begrip	Uitleg
Basisinfrastructuur	Basisinfrastructuur is één van de drie aandachtsgebieden van informatieveiligheid (zie ook: ICT en mens & organisatie). Hierbij gaat het onder andere om elektriciteitsvoorziening, telecommunicatie-voorzieningen en gebouwen en toegang.
Beschikbaarheid	Beschikbaarheid is één van de drie aspecten of eigenschappen van informatieveiligheid (zie ook: integriteit en vertrouwelijkheid). Bij beschikbaarheid gaat het er om dat geautoriseerde gebruikers toegang hebben tot de informatie en aanverwante bedrijfsmiddelen op het moment dat het nodig is.
BIA	De Business Impact Analyse (BIA) is een hulpmiddel om vast te stellen wat de impact op een bedrijfsproces is indien de informatieveiligheid van de informatie niet gewaarborgd of zelfs geschaad is. Op basis hiervan kunnen de risico's in kaart gebracht worden en kunnen maatregelen genomen worden ter vermindering of opheffing van deze risico's.
BIO	De Baseline Informatiebeveiliging Overheid (BIO) wordt de opvolger van de Interprovinciale Baseline Informatiebeveiliging (IBI). Het wordt een formeel basisnormenkader voor alle overheden en bevat richtlijnen op het gebied van informatieveiligheid. Op dit moment (november 2018) wordt nog aan de BIO gewerkt.
Cibo	Het Cibo is onderdeel van het IPO. Het is een platform waarin provincies kennis en ervaring uitwisselen en de gezamenlijke ontwikkeling van informatieveiligheid vormgeven.
Convenant IRI	Het convenant Interprovinciale Regulering Informatieveiligheid (IRI) is een afsprakenkader waarmee provincies informatieveiligheid verder willen optimaliseren en professionaliseren. Het convenant is in 2014 opgesteld en ondertekend door alle provincies. Het is de bedoeling dat de provincies door de gezamenlijke afspraken één standaard ontwikkelen en behouden waardoor informatieveiligheid geen vrijblijvend proces is.
IBI	De Interprovinciale Baseline Informatiebeveiliging (IBI) vormt het formele basisnormenkader voor provincies en bevat richtlijnen op het gebied van informatieveiligheid. De IBI geeft een standaard werkwijze waarmee per bedrijfsproces of informatiesysteem wordt bepaald welke beveiligings-maatregelen getroffen moeten worden. De IBI is gebaseerd op de ISO standaarden.
ICT	ICT is één van de drie aandachtsgebieden van informatieveiligheid (zie ook: basisinfrastructuur en mens & organisatie). Hierbij gaat het onder andere om applicaties en gegevensverzameling, ICT infrastructuur (computers, netwerkapparatuur en randapparatuur) en ICT programmatuur (besturingsprogramma's).
Integriteit	Integriteit is een van één van de drie aspecten of eigenschappen van informatieveiligheid (zie ook: beschikbaarheid en vertrouwelijkheid). Bij integriteit gaat het om de correctheid en volledigheid van informatie en de informatieverwerking.

ISO 27001/27002	De Interprovinciale Baseline Informatiebeveiliging (IBI) is gebaseerd op de landelijke standaarden ISO 27001/27002. Hier staan eisen ten aanzien van informatieveiligheid.
Mens & organisatie	Mens & organisatie is één van de drie aandachtsgebieden van informatieveiligheid (zie ook: basisinfrastructuur en ICT). Hierbij gaat het onder andere om werkwijzen, manieren, routines, gewoonten en gedrag.
Penetratietest	Een penetratietest is een geautoriseerde poging om een beveiligingssysteem te omzeilen of te doorbreken, waarbij een beveiligingsspecialist probeert om zonder de vereiste toegangsgegevens informatie te verkrijgen uit het systeem. Het doel is om inzicht te krijgen in de risico's en kwetsbaarheden van het onderzochte systeem.
Phishing	Phishing is de verzamelnaam voor activiteiten waarmee criminelen vertrouwelijke informatie proberen te bemachtigen. Meestal gebeurt dit via e-mails waarin mensen worden verleid op een kwaadaardige link te klikken of inloggegevens achter te laten. Zo verschaffen criminelen zich toegang tot de systemen en gegevens van de ontvanger van de e-mail.
Social engineering	Social engineering bestaat uit verschillende technieken die kwaadwillenden gebruiken om mensen te misleiden om toegang te krijgen tot informatie. De 'aanval' is dus gericht op een persoon en niet op een systeem. Dit kan bijvoorbeeld door de helpdesk te bellen, door een medewerker om zijn wachtwoord te vragen of door de portier om te praten om het gebouw binnen te komen.
Spear phishing	Spear-phishing is een phishing-variant die gericht is op (een) specifieke (groep) personen.
Verplichtende zelfregulering	In de periode 2013-2015 functioneerde (in opdracht van het ministerie van BZK) de Taskforce Bestuur en Informatieveiligheid Dienstverlening. Deze Taskforce zette in op 'verplichtende zelfregulering' waarbij de verschillende overheidslagen zelf de verantwoordelijkheid nemen voor het maken van niet-vrijblijvende afspraken over informatieveiligheid. De provincies hebben deze afspraken in 2014 vastgelegd in het Convenant IRI.
Vertrouwelijkheid	Vertrouwelijkheid is een van één van de drie aspecten of eigenschappen van informatieveiligheid (zie ook: beschikbaarheid en integriteit). Bij vertrouwelijkheid gaat het om gaat het er om dat de informatie alleen toegankelijk is voor degene die hiervoor daadwerkelijk geautoriseerd is.

Bron: Onder andere Convenant Interprovinciale Regulering Informatieveiligheid (2014), Interprovinciale Baseline Informatieveiligheid (2016) en Randstedelijke Rekenkamer (2016).

Bijlage 4: Bronnenlijst

Geraadpleegde personen

- Information Security Officer provincie Gelderland.
- Systeemarchitect provincie Gelderland.
- Coördinator huisvesting / adviseur (fysieke) veiligheid.
- Afdelingsmanager I&A.

Geraadpleegde documenten

Algemeen

- Cibo en IPO (2010). Interprovinciale Baseline Informatiebeveiliging 1.0.
- Cibo en IPO (2014). Convenant Interprovinciale Regulering Informatieveiligheid.
- Cibo en IPO (2016). Interprovinciale Baseline Informatieveiligheid 2.0.
- Cibo (2017). Memo Rapportage interprovinciale beeld implementatie baseline informatiebeveiliging eind 2016.
- Digitrust (2018). Presentatie Nulmeting ISO27001 BIJ12 + 12 provincies.
- Forum Standaardisatie (2014). Verkennend onderzoek ISO 27001 en ISO 27002.
- Forum Standaardisatie. Halfjaarlijkse meting Informatieveiligheidstandaarden begin 2018.
- Hoffmann B.V. (2018). Managementsamenvatting van Onderzoek naar informatieveiligheid bij de provincie Gelderland i.o.v. Rekenkamer Oost-Nederland,
- IBD (2014). Aanwijzing logging.
- NBA en CSR (2018). Cyber security health check.
- Randstedelijke Rekenkamer (juli 2016). Rapporten informatieveiligheid Flevoland, Noord-Holland, Utrecht en Zuid-Holland.
- Secura (2018). Rapport social engineering: Phishing awareness i.o.v. provincie Gelderland.
- Zuidelijke Rekenkamer (juli 2018). Bestuurlijke nota en nota van bevindingen informatieveiligheid Limburg.

Provincie Gelderland

- Provincie Gelderland. Accountantsverslagen 2015 t/m 2017.
- Provincie Gelderland. Accountbeleid [Intranet].
- Provincie Gelderland (2018). Bericht ‘Datalekken: Onze collega’s zijn het grootste risico’ [Intranet].

- Provincie Gelderland (2018). Bericht ‘Is je smart phone wel goed beveiligd?’ [Intranet].
- Provincie Gelderland (2018). Bericht ‘Nieuws over grote datalekken’ [Intranet].
- Provincie Gelderland (2018). Bericht ‘Nieuwe vorm van nepmails’ [Intranet].
- Provincie Gelderland (2018). Bericht ‘Veilig omgaan met provinciale spullen’ [Intranet].
- Provincie Gelderland (2018). Bericht ‘Waarschuwing: Phishingmail ”Uw factuur” van Vodafone’ [Intranet].
- Provincie Gelderland (2018). Bericht ‘Wachtwoord zoekmachine: loop ik risico? [Intranet].
- Provincie Gelderland. Boardletters 2015 t/m 2017.
- Provincie Gelderland (2016). Bijlage B-008. Programma van Eisen - Infrastructuur, hosting, werkplek en servicedesk.
- Provincie Gelderland (2016). Bijlage C-007. Antwoordplate Informatiebeveiliging - Infrastructuur, hosting, werkplek en servicedesk.
- Provincie Gelderland. Cibo-monitor 2016.
- Provincie Gelderland (2016). Huidige situatie informatiebeveiliging versie 1.0 [intern document].
- Provincie Gelderland (2018). Gedragscode integriteit provinciale ambtenaren.
- Provincie Gelderland (2016). Informatiebeveiligingsbeleid provincie Gelderland versie 1.1.
- Provincie Gelderland. Informatiebeveiligingsjaarplan 2015.
- Provincie Gelderland. Informatiebeveiligingsjaarplan 2017.
- Provincie Gelderland. Life cycle management (patchbeleid) [Intranet].
- Provincie Gelderland (2017). Pocket-editie contract OGD [intern document].
- Provincie Gelderland (2016). PS2016-217 Antwoorden van GS Gelderland op schriftelijke Statenvragen van SP over personeelsbeleid en bedrijfsvoering.
- Provincie Gelderland (2016). PS2016-33 Mededelingenbrief van GS aan PS (punt 2 Wet meldplicht datalekken).
- Provincie Gelderland (2017). PS2017-299 Notitie Griffie aan Procedurecommissie over Gevolgen gewijzigde privacy wetgeving voor openbare (actieve) publicatie van (ingekomen) stukken op het SIS.
- Provincie Gelderland (2017). PS2017-579. Mededelingenbrief GS aan PS van 20 september 2017.
- Provincie Gelderland (2018). PS2018-80. Verslag vergadering Procedurecommissie 31 januari 2018.
- Provincie Gelderland (2018). PS2018-351 Extra mededelingenbrief GS aan PS over datalek.
- Provincie Gelderland (2018). PS2018-604 Statenbrief algemene inkoopvoorwaarden.
- Provincie Gelderland (2018). Regeling rechtspositie stagiairs provincie Gelderland.

Websites

- www.autoriteitpersoonsgegevens.nl/
- www.cip-overheid.nl
- www.forumstandaardisatie.nl