Rekenkamer
OOST-NEDERLAND

Informatieveiligheid Overijssel

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 Overijssel

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.

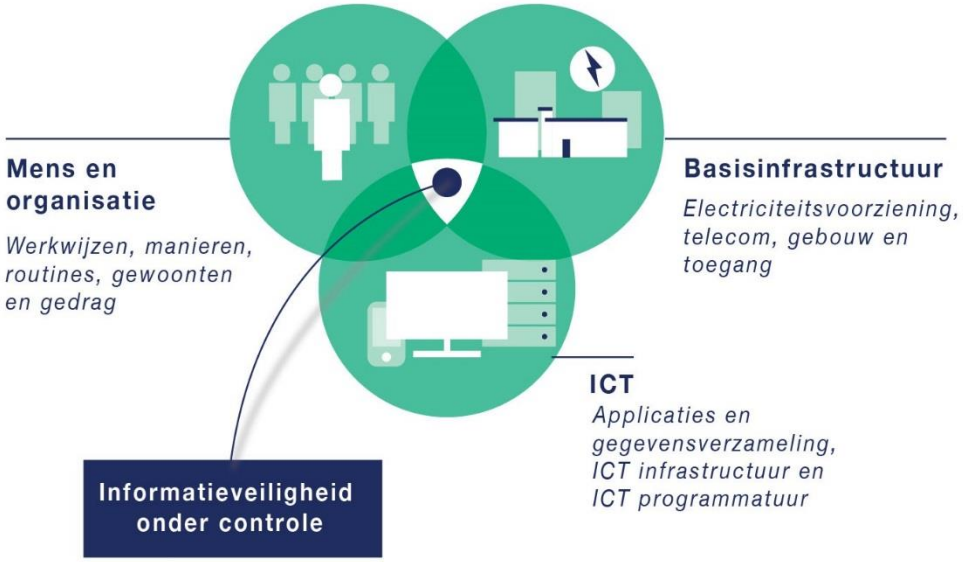
Informatieveiligheid richt zich op bescherming van informatie om de continuïteit van bedrijfsactiviteiten te waarborgen.[4] Als de informatieveiligheid onvoldoende is gewaarborgd, kunnen er risico's ontstaan bij de uitvoering van provinciale taken en het functioneren van de organisatie. De maatregelen 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, wijzigingen of toevoegen van informatie.
- Bij *beschikbaarheid* gaat het er om dat geautoriseerde gebruikers toegang hebben tot de informatie aanverwante en 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 informatieveiligheid, p. 6.*

Figuur 1: *Aandachtsgebieden van informatieveiligheid*



Bron: Interprovinciale Baseline Informatieveiligheid, bewerking Randstedelijke Rekenkamer & 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:

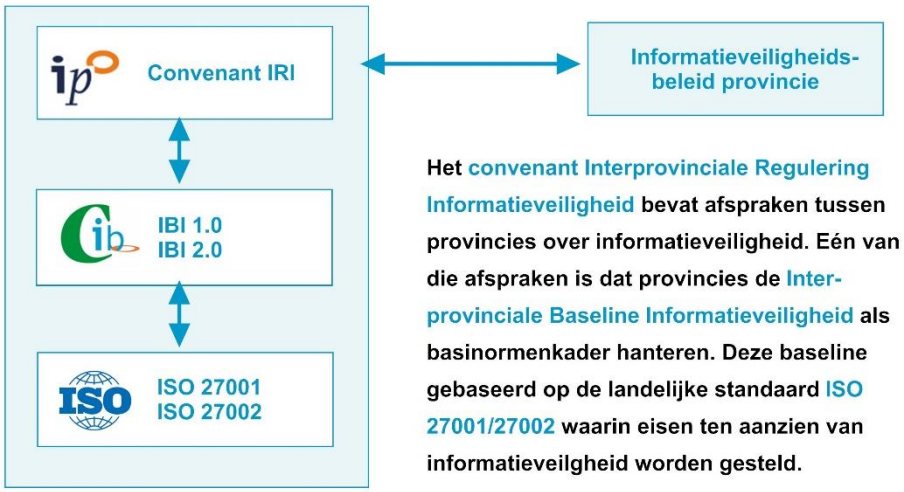
- sturing en verantwoordelijkheid;
- beleid en normenkader;
- verantwoording en toezicht;
- bewustwording, kennis en coördinatie.

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 het IBI. De Interprovinciale Baseline Informatiebeveiliging 2.0 is in 2016 opgesteld. Een baseline die gebaseerd is op ISO27001 en ISO27002. 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. Figuur 3 geeft schematisch weer hoe deze verschillende documenten zich tot elkaar verhouden.

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

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



Bron: Geïnspireerd op een uitsnede van figuur uit rapport 217a-onderzoek beheersing informatiebeveiliging van Concerncontrol Overijssel (maart.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 zijn. 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 het houden van toezicht op en het afleggen van verantwoording over informatieveiligheid is geregeld.

2 Beleid

In dit hoofdstuk staat het informatieveiligheidsbeleid van de provincie Overijssel centraal.

2.1 Informatieveiligheidsbeleid

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 Informatiebeveiliging (IBI).

Bevindingen

- In het strategisch informatieplan (STIP) zijn doelen opgenomen voor informatieveiligheid.
- Aanvullend is informatieveiligheidsbeleid vastgesteld door het concern management (directie en hoofd eenheden). Daarin is uitgewerkt hoe de doelen uit het STIP behaald kunnen worden.
- Het informatieveiligheidsbeleid is vastgesteld in 2016. Een herziening staat gepland in de nieuwe coalitieperiode.
- Het beleid is op een aantal punten niet bijgewerkt of geactualiseerd terwijl daar wel aanleiding toe is. Dit wordt mede veroorzaakt door beperkte personele capaciteit.
- Het huidige informatieveiligheidsbeleid is gebaseerd op de standaard ISO27002 en sluit daarmee grotendeels aan op de IBI.

Informatiebeleid

Informatieveiligheid is onderdeel van het overkoepelende informatiebeleid dat door de directie is vastgesteld in 2014. Het informatiebeleid is vastgelegd in het *strategisch informatieplan (STIP) 2015-2019*, *'informatie voor participatie'*.

In het STIP zijn voor 2019 de volgende zes doelen vastgesteld voor informatieveiligheid:

- een afgesproken beveiligingsniveau te garanderen;
- de meest kritische processen en data te benoemen;
- met de juiste maatregelen de risico's te beheersen;
- adequaat en helder te communiceren over incidenten met partners en klanten;
- adequaat en proactief te reageren op incidenten;
- personeel is bewust bekwaam over het thema informatieveiligheid.

Informatieveiligheidsbeleid

Aanvullend op het informatiebeleid heeft de provincie Overijssel informatieveiligheidsbeleid. Dit beleid is opgesteld in samenwerking met een externe partij.[8] Het doel is om aanvullend op het STIP een kader met bijbehorende maatregelen te bieden. Het informatieveiligheidsbeleid is begin 2016 door het Concern Managementteam (CMT) vastgesteld[9] voor een periode van 4 jaar. Hiermee wordt aangesloten bij de periode van het STIP en het coalitieakkoord. Het informatieveiligheidsbeleid bestaat uit vier delen.

Deel 1: Visie en strategie

Deel 1 bevat strategische aspecten voor informatieveiligheid. Visie en de principes voor informatieveiligheid van de provincie Overijssel worden geschetst. Daarmee worden kaders gesteld waarbinnen de specifieke maatregelen uit beleid deel 2 worden ingezet. Ook worden stappen beschreven die na het vaststellen van impact van een kwetsbaarheid moeten leiden tot de juiste maatregelen. Daarnaast worden de interne organisatie voor informatieveiligheid en acties voor komende jaren beschreven.

Deel 2: beheersmaatregelen

In deel 2 zijn tactische componenten voor informatieveiligheid in de vorm van concrete maatregelen opgenomen. De ISO27002 norm (zie hoofdstuk 2 achtergrond) is hiervoor de basis. De IBI wordt niet genoemd, maar wordt wel grotendeels gevolgd omdat de IBI gebaseerd is op de IS27002-standaard. Per hoofdstuk uit de ISO27002 wordt de doelstelling gegeven. Ook worden de beheersmaatregel, de beleidslijn en het organisatieonderdeel dat verantwoordelijk is voor de uitvoering beschreven. Afgesloten wordt met een voorbeeld van beheersmaatregelen. Het volgende kader geeft een voorbeeld van deze opzet.

[8] *Interview met ambtelijk medewerker provincie Overijssel.*
[9] *Provincie Overijssel (februari 2016). CMT extract informatiebeveiligingsbeleid.*

Kader met voorbeeld van opzet

6.1 Bedrijfseisen voor toegangsbeveiliging
Doelstelling:
Toegang tot informatie en informatieverwerkende faciliteiten beperken.

6.1.1 Beleid voor toegangsbeveiliging
Beheersmaatregel:
Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.

Beleidslijn:
Om effectieve toegangscontrole tot vertrouwelijke en privacygevoelige informatie te kunnen invoeren en onderhouden is er een provincie Overijssel breed toegangsbeleid dat voor iedere gebruiker is afgestemd op individuele classificatie van toegang tot informatie.

Toegangsbeveiliging is een samenspel van beleid voor bedrijfseisen voor toegangsbeheersing, beheer van toegangsrechten van gebruikers, verantwoordelijkheden van gebruikers en toegangsbeveiliging van systemen en toepassingen.

Verantwoordelijke:	Eenheid Bedrijfsvoering

Het informatieveiligheidsbeleid deel 2 is niet up-to-date. Dit blijkt uit opmerkingen die nog in de tekst staan die bedoeld zijn om nog aanpassingen aan het document te doen. Ook staat bij de verantwoordelijke voor het uitvoeren van beheersmaatregelen nu nog bij 20 maatregelen ‘nader te bepalen’ bij de verantwoordelijke afdeling.

Deel 3: monitor implementatie

Deel 3 gaat over monitoring van de implementatie van beheersmaatregelen. In de praktijk is dit de interprovinciale Cibo-monitor (2014). Er wordt in deel 3 van het beleid beschreven dat jaarlijks zal worden getoetst en gerapporteerd in IPO verband. Na 2015 is dit deel van het beleid niet geactualiseerd.[10]

[10] *Interview met ambtelijk medewerkers provincie Overijssel.*

Deel 4: projectportfolio

In deel 4 van het informatieveiligheidsbeleid staan projecten voor 2015 en 2016. Dit kan gezien worden als een soort jaarplan. De drie projecten zijn: bewustwordingscampagne betrouwbaar omgaan met persoonsgegevens, informatieveiligheid implementeren in de planning en control cyclus (ISMS) en activiteiten in het kader van wet datalekken. Dit document is na februari 2016 niet meer geactualiseerd. Voor de jaren 2017 en 2018 zijn geen jaarplannen voor informatieveiligheid gemaakt. Wel is er voor 2017 en 2018 een planning voor bewustwordingsactiviteiten.[11] In de jaarplannen van de eenheid bedrijfsvoering wordt kort ingegaan op informatieveiligheid.[12]

Actualisatie informatieveiligheidsbeleid

De provincie is voornemens het informatieveiligheidsbeleid te actualiseren. Een reden waarom het beleid in 2018 niet is aangepast, is dat in 2018 een 217a onderzoek, een nulmeting ISO27001 en een rekenkameronderzoek zijn uitgevoerd voor informatieveiligheid. Overijssel heeft daarom gekozen het beleid in dat jaar nog niet aan te passen. Voor het nieuwe beleid wordt de ISO27001-standaard als norm gebruikt in combinatie met de aanstaande Baseline Informatiebeveiliging Overheid (BIO) als normenkader.[13] De Baseline Informatiebeveiliging Overheid 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.

[11] *Provincie Overijssel (2018), awareness campagne 2017/2018*
[12] *Provincie Overijssel (2017), Eenheid bedrijfsvoering, werkplan 2018.*
[13] *Provincie Overijssel (december 2018). Reactie ambtelijk hoor en wederhoor.*

3 Sturing en verantwoordelijkheid

In dit hoofdstuk gaan we na of de provincie Overijssel 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 onderdeel van de portefeuille van de Commissaris van de Koning.
- GS zijn betrokken bij informatieveiligheid bij grote gebeurtenissen zoals bij het opstellen van informatieveiligheidsbeleid of interprovinciaal convenant. Ze worden niet regelmatig geïnformeerd over de stand van zaken van informatieveiligheid.
- De directie heeft het informatieveiligheidsbeleid vastgesteld. In het beleid is omschreven dat de directie jaarlijks een rapportage ontvangt. In de praktijk gebeurt dit niet.

Vervolg bevindingen op de volgende pagina.

Vervolg bevindingen

- In de praktijk zijn het bedrijfsvoeringsoverleg en het hoofd Eenheid Bedrijfsvoering de managementlagen die het meest betrokken zijn. De rol die zij hebben, is beperkt uitgewerkt in het informatieveiligheidsbeleid.
- De provincie Overijssel heeft in haar informatieveiligheidsbeleid aandacht voor de verdeling van verantwoordelijkheden binnen de organisatie, maar niet alle rollen worden beschreven.
- De personele bezetting is beperkt. Dit brengt risico's met zich mee waar Concerncontrol begin 2018 al op heeft gewezen. In november 2018 is de personele capaciteit nog niet aangepast.
- De externe dienstverlener die een groot deel van de IT-taken voor de provincie Overijssel uitvoert, ONS, beschikt over eigen beleid voor informatieveiligheid. Bij uitvoering daarvan wordt ook rekening gehouden met beleid van de provincie.

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.

3.1.1 Betrokkenheid van GS

Beleid over rol GS bij informatieveiligheid
GS zijn politiek verantwoordelijk voor informatieveiligheid. In het informatieveiligheidsbeleid wordt beschreven dat deze portefeuille op dit moment toebehoort aan de Commissaris van de Koning. In het beleid staat niet beschreven wanneer GS betrokken worden.[14]

Rol GS bij informatieveiligheid in de praktijk
Informatieveiligheid behoort toe aan de portefeuille kwaliteit openbaar bestuur van de Commissaris van de Koning. Op het niveau van GS staat informatieveiligheid niet vaak op de agenda. Besluiten over informatieveiligheid, komen niet op het niveau van GS. De directie is het hoogste niveau dat hierover besluiten neemt. GS worden in de praktijk betrokken bij incidenten of bijzondere gebeurtenissen die informatieveiligheid raken. Deze hebben afgelopen jaren nauwelijks plaatsgevonden. Op een aantal momenten zijn GS wel betrokken. Het convenant IRI is in 2014 bijvoorbeeld besproken in een portefeuilleoverleg met de Commissaris van de Koning.[15] Toen het informatieveiligheidsbeleid in 2015 is opgesteld is dit ook ter sprake gekomen in GS. Er is geen GS-nota gestuurd. In het voorjaar van 2018 hebben GS wel de uitkomsten van een 217a-onderzoek van Concerncontrol over informatieveiligheid vastgesteld. Ondanks dat GS inhoudelijk weinig met informatieveiligheid te maken krijgen, wordt ambtelijk evenwel betrokkenheid bij dit thema ervaren.[16] Van een regelmatige informatievoorziening over de stand van zaken is evenwel geen sprake.

3.1.2 Management

Beleid over de rol van het management
Ambtelijk is de directie van de provincie eindverantwoordelijk voor het functioneren van de organisatie en het realiseren van de provinciale doelen. De directie is dus ook eindverantwoordelijk voor informatieveiligheid. De directie en de hoofdeenheden vormen samen het Concern Managementteam (CMT). In het CMT vindt strategische sturing en besluitvorming plaats. De verschillende rollen van het management zijn beschreven in het algemene beleid van de provincie en behalve de rol van de directie niet specifiek voor informatieveiligheid.[17]

In het informatieveiligheidsbeleid staat dat er minimaal eenmaal per jaar kort en bondig gerapporteerd wordt aan de directie. Bij beveiligingsincidenten wordt de directie door procesverantwoordelijken geïnformeerd. Dit kan gaan over inbreuken op en verstoring in: informatietechnologie, datacommunicatie of andere infrastructurele voorzieningen

[14] *Provincie Overijssel (2016). Informatiebeveiligingsbeleid.*
[15] *Provincie Overijssel (oktober 2014). Notitie portefeuilleoverleg*
[16] *Interview met ambtelijk medewerkers provincie Overijssel.*
[17] *Provincie Overijssel (2016). Informatiebeveiligingsbeleid. Provincie Overijssel (2016). Besturings- en managementconcept.*

die gevolgen kunnen hebben voor de continuïteit en integriteit van bedrijfsprocessen. [18] Een incident dat bijvoorbeeld aan de directie gerapporteerd moet worden, is een datalek.[19] Ook is het beleid aan de directie te rapporteren als gesignaleerd wordt dat informatieveiligheidsbeleid niet wordt nageleefd.

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.
- In Overijssel is er een proces voor het melden van datalekken ingericht. Hierin is beschreven welke stappen er bij een mogelijk datalek doorlopen worden en wie hierbij betrokken zijn.

Rol van management in de praktijk

De teamleider, hoofd eenheid, bedrijfsvoeringsoverleg, het concern managementteam (CMT) en directie hebben beslissingsbevoegdheid. Per besluit wordt afgewogen op welk niveau in de organisatie behandeling plaats moet vinden.

Het informatieveiligheidsbeleid is vastgesteld in het CMT.[20] Jaarlijkse werkplannen van de eenheid bedrijfsvoering, waarin informatieveiligheid ook een plek heeft, worden besproken met de directie.[21] Ook zijn enkele besluiten die het bedrijfsvoeringsoverleg (BO) nam over informatieveiligheid ter kennisname aan het CMT gestuurd, bijvoorbeeld het proces voor het melden van datalekken.[22] Op dit moment vindt geen jaarlijkse structurele rapportage plaats aan het CMT of de directie (zoals in het beleid wordt beschreven). De intentie was om de jaarlijkse Cibo-monitor hiervoor te gebruiken. In 2015 en 2016 is deze monitor in Overijssel niet uitgevoerd (hierover meer in paragraaf 5.1). In 2017 is de monitor wel uitgevoerd, maar de rapportage is niet gedeeld met het CMT. De rapportage van 2014 is ook niet in de directie besproken maar in het bedrijfsvoeringsoverleg. In de monitor worden specifieke en technische maatregelen beschreven. De directie wil op dat detailniveau geen informatie.[23]

De meeste besluiten worden genomen in het bedrijfsvoeringsoverleg, waarin de adjunct hoofden eenheden vertegenwoordigd zijn. Naast het nemen van beslissingen worden hier uitkomsten van testen en relevante ontwikkelingen besproken. In het bedrijfsvoeringsoverleg zijn diverse onderdelen van informatieveiligheid besproken en vastgesteld. Voorbeelden zijn de bewustwordingscampagne, risicovolle processen en het proces voor datalekken. [24] Ook als er acties zijn voor meerdere eenheden worden deze besproken in het bedrijfsvoeringsoverleg. In de praktijk is van het management het bedrijfsvoeringsoverleg daarom het meest nauw betrokken bij informatieveiligheid.

[18] *Provincie Overijssel (2016). Informatiebeveveiligingsbeleid.*
[19] *Provincie Overijssel (2016). Procesplaat meldplicht datalekken.*
[20] *Beleid en CMT extract*
[21] *Provincie Overijssel (2017) Werkplan eenheid bedrijfsvoering 2018.*
[22] *Provincie Overijssel (2016). Bedrijfsvoeringsoverleg notitie proces datalekken.*
[23] *Interview met ambtelijk medewerkers provincie Overijssel.*
[24] *Provincie Overijssel, notities bedrijfsvoeringsoverleg en Interview met ambtelijk medewerkers provincie Overijssel.*

In een interview wordt aangegeven dat de managementteams van alle eenheden (dit zijn er bij de provincie Overijssel acht) belangrijk zijn voor informatieveiligheid. Dit geldt vooral voor bewustwording van medewerkers. De meeste onderdelen uit het informatieveiligheidsbeleid worden echter afgedekt door de eenheid Bedrijfsvoering. Het hoofd Bedrijfsvoering neemt besluiten op dit niveau en is budgethouder. De teamleider van team Informatie beslist over uitvoeringszaken en is budgetbeheerder. Daarmee ligt de verantwoordelijkheid voor de directe uitvoering vooral bij de teamleider.[25]

3.2 Verdeling 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

Organisatie informatieveiligheid

De regievoering, coördinatie en advisering over informatieveiligheid aan de portefeuillehouder en management berust bij de eenheid Bedrijfsvoering. Informatieveiligheid is, zoals eerder aangegeven, een samenspel van organisatie, menselijke en technische factoren. De provincie Overijssel geeft in haar beleid aan dat uitvoering van de verschillende beheersmaatregelen en de advisering daarom berust bij verschillende eenheden in de organisatie.[26] Hoofd Bedrijfsvoering is verantwoordelijk voor vaststellen van beschikbare capaciteit.[27]

In het informatiebeleid zijn voor de uitvoering van beheersmaatregelen per thema -aansluitend op de ISO-norm- de verantwoordelijke eenheden beschreven. De meeste taken voor informatieveiligheid zijn ondergebracht bij de eenheid Bedrijfsvoering. Alleen waar het gaat om communicatiebeleid of de administratieve organisatie zijn ook andere eenheden aan zet. In de eenheid Bedrijfsvoering zijn namelijk onder andere de teams Facilitaire Zaken (loket, gebouwindeling, brandbeveiliging etc.), HRM (bewustwording, toetsing, aanvragen examens, vog-reglement etc.) en Informatie (beleid, functioneel beheer etc.) ondergebracht. Collega's zijn zelf verantwoordelijk voor rapportage van relevante ontwikkelingen, zoals beveiligingsincidenten, aan hun teamleider.[28]

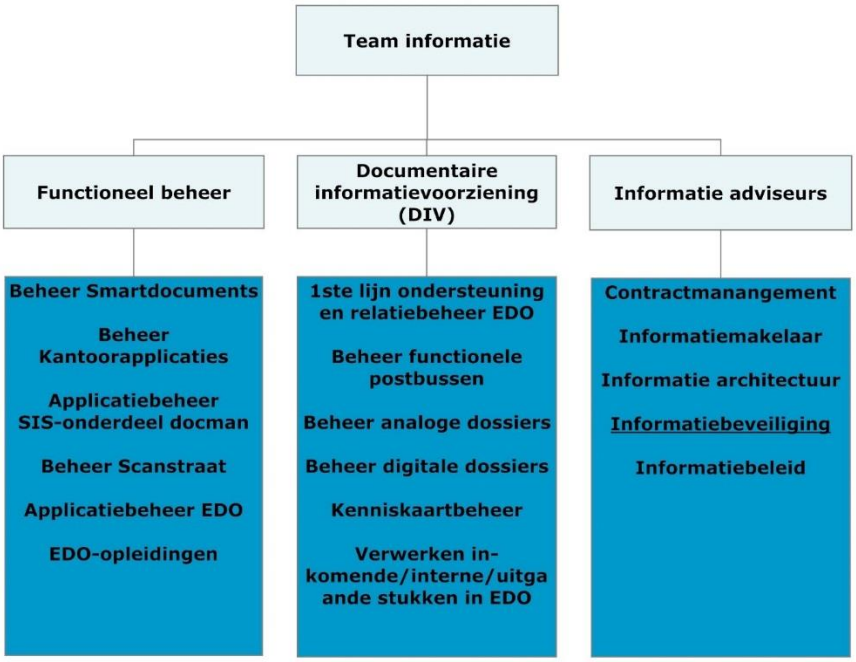
[25] *Interview met ambtelijk medewerkers provincie Overijssel en Provincie Overijssel (2019). Reactie ambtelijk hoor en wederhoor.*
[26] *Provincie Overijssel (2016). Informatiebeveiligingsbeleid.*
[27] *Provincie Overijssel (2019). Reactie ambtelijk hoor en wederhoor.*
[28] *Interview met ambtelijk medewerkers provincie Overijssel.*

Naast de verantwoordelijkheidsverdeling, zijn voor de thema's specifieke maatregelen uitgewerkt. Per maatregel is een organisatieonderdeel (dat kan een team of eenheid zijn) benoemd dat primair verantwoordelijk is. Voor back-ups zijn bijvoorbeeld het team Informatie (eenheid Bedrijfsvoering) en de externe dienstverlener het Shared Service Centrum verantwoordelijk.[29]

Team Informatie

In de vorige paragraaf werd duidelijk dat meerdere teams verantwoordelijkheden hebben als het gaat om informatieveiligheid. De regievoering voor thema informatieveiligheid is in de organisatie wel bij één team ondergebracht, team Informatie (zie figuur 4).

Figuur 4: *Team informatie*



Bron: Intranet Provincie Overijssel (laatst geraadpleegd 1 oktober 2018)

Team Informatie moet ervoor zorgen dat de provincie grip krijgt en houdt op de grote hoeveelheid informatie. Informatieveiligheid is hier onderdeel van.[30] De financiële middelen voor informatieveiligheid zijn onderdeel van het budget van team Informatie. Er is geen afzonderlijk budget voor informatieveiligheid. In interviews is aangegeven dat het budget voor informatieveiligheid altijd voldoende is geweest. De uitgaven aan informatieveiligheid zijn de afgelopen jaren toegenomen.

In de vorige paragraaf werd duidelijk dat de teamleider van team Informatie verantwoordelijk is voor de uitvoering van informatieveiligheid. Daarbij wordt ze inhoudelijk in belangrijke mate ondersteund door een adviseur informatie. Eén van de

[29] *Provincie Overijssel (2016). Informatiebeveiligingsbeleid.*
[30] *Provincie Overijssel, intranet (laatst geraadpleegd 1 oktober 2018) en interviews met ambtelijk medewerkers van de provincie Overijssel.*

vijf informatieadviseurs houdt zich bezig met informatieveiligheid. Deze adviseur informatiebeveiliging is verantwoordelijk voor het opstellen en actualiseren van informatieveiligheidsbeleid, coördinatie van de uitvoering, organiseren van bewustwordingsacties en monitoring en bewaken van het informatieveiligheidsbeleid. Ook begeleidt hij externe gespecialiseerde partijen die worden ingehuurd bijvoorbeeld bij het opstellen van het informatieveiligheidsbeleid. Daarmee is hij binnen de organisatie de belangrijkste schakel voor informatieveiligheid. De adviseur informatiebeveiliging heeft alleen een adviserende bevoegdheid, geen beslissingsbevoegdheid. De rol van de adviseur informatiebeveiliging wordt in het beleid niet beschreven. De provincie kent in haar organisatie geen (chief) information security officer.

De adviseur informatiebeveiliging besteedt gemiddeld ongeveer één dag per week tijd aan informatieveiligheid. Daarmee is hij de enige specialist binnen de provinciale organisatie. In 2016 en 2017 is de informatieadviseur anderhalf jaar afwezig geweest. Zijn taken zijn tijdelijk door een externe adviseur waargenomen. Zijn opdracht was vooral zorgen voor voortgang van lopende zaken. Doorontwikkeling van het beleid is blijven liggen.

Capaciteit

Over de beschikbare capaciteit zijn in het 217a onderzoek van de provincie (maart 2018) kritische opmerkingen gemaakt (zie kader voor de conclusies). In november 2018 is de capaciteit nog hetzelfde.

Concerncontrol:

‘De conclusie is dat de huidige beschikbare capaciteit en kwaliteit voor 2018 niet meer voldoende is om de minimale structurele taken uit te kunnen voeren, laat staan als er nog meer gevraagd gaat worden met ISO certificering en de invoering van de AVG. In het geval van ISO moeten extra activiteiten op het vlak van monitoring en controle uitgevoerd gaan worden, ook naar derde partijen waar het gaat om naleving van de eisen die vanuit IB en privacy gesteld worden. Wij lopen hier een compliance risico dat voor ISO27001 kan betekenen dat het ISO certificaat (ambitie) niet behaald wordt. Vanuit de AVG kan het leiden tot significante boetes als de provincie nalatig is bij implementatie en naleving van beveiligingsmaatregelen. Als er problemen ontstaan dan zorgt dit met zekerheid voor ongewenste media aandacht.’

‘Omdat wij verwachten dat al dit jaar extra druk gaat ontstaan vanuit de nieuwe privacyregelgeving en dat de aanloop naar ISO certificering ook meer inspanning gaat vragen, adviseren wij om een heroverweging te maken ten aanzien van de huidige omvang van de IB organisatie en de benodigde competenties.’

Provincie Overijssel, Concerncontrol (maart 2018). Art. 217a onderzoek beheersing informatiebeveiliging.

In interviews wordt aangegeven dat dit beeld herkend wordt. Er wordt toegelicht dat de provincie ambitieus is en de werkzaamheden op het gebied van informatieveiligheid steeds specialistischer worden. Deze ambities en ontwikkelingen knellen met de beschikbare capaciteit. Uitbesteden is niet altijd een optie omdat daar ook intern specifieke kennis voor nodig is en het begeleiden van uitbesteedde projecten ook tijd kost. In hoofdstukken 2, 4 en 5 komt daarnaast aan de orde dat onderdelen van het informatieveiligheidsbeleid de afgelopen jaren niet altijd uitgevoerd zijn. Hier is beperkte personele capaciteit mede oorzaak van.[31]

Coördinatieoverleg informatiebeveiliging

Verschillende onderdelen van bedrijfsvoering die zich bezighouden met informatieveiligheid zitten samen in het coördinatieoverleg informatiebeveiliging (CIB). Dit overleg is ingesteld door de directie. Het CIB heeft geen functioneel zelfstandige positie naast de lijn richting het BO en de directie, maar vervult in de uitvoering een brugfunctie tussen de verschillende onderdelen van de organisatie.[32] De informatieadviseur is voorzitter van het CIB. Daarnaast zijn het afdelingen facilitair, personeelszaken, de functionaris gegevensbeheer en namens het Shared Service Centrum een de Technisch Information Security Officer vertegenwoordigd. Het CIB voert maandelijks overleg. In het overleg wordt besproken wat er speelt. Dat kan gaan om incidenten, tussenstanden van bewustwordingsacties, resultaten van testen en onderzoeken. Zo wordt geborgd dat verschillende teams integraal samen kunnen werken aan overlappende thema's zoals fysieke en IT-maatregelen.[33]

Het CIB heeft de volgende taken en verantwoordelijkheden:

- opstellen van informatieveiligheidsbeleid en informatiebeveiligingsactieplan;
- bewaken van de voortgang van de uitvoering van het informatieveiligheidsbeleid en -plan;
- bewaken van het niveau van informatieveiligheid;
- evalueren van beveiligingsincidenten;
- toetsen op het feit dat informatieveiligheid een onderdeel uitmaakt van het informatieplannings-, systeemontwikkelings- en onderhoudsproces;
- bevorderen van het beveiligingsbewustzijn in de organisatie;
- het te hanteren coördinatiemechanisme voor overleg en rapportage met betrekking tot informatieveiligheid.[34]

3.2.2 Externe dienstverlening

De provincie Overijssel heeft uitvoering van de ICT (waaronder de uitvoering van informatiebeveiliging) uitbesteed aan externe dienstverleners. De belangrijkste externe dienstverlener is ONS. Zij beheren de ICT-infrastructuur voor de provincie. Daarnaast zijn er nog andere externe leveranciers die applicaties voor de provincie leveren. Omdat

[31] *Interview met ambtelijk medewerkers provincie Overijssel.*
[32] *Provincie Overijssel (2016). Informatiebeveiligingsbeleid.*
[33] *Interview met ambtelijk medewerkers provincie Overijssel.*
[34] *Provincie Overijssel (2016). Informatiebeveiligingsbeleid.*

ONS een belangrijk onderdeel voor informatieveiligheid van de provincie is, gaan we hier in deze paragraaf iets dieper op in.

Organisatie ONS

De provincie heeft de (beveiliging van) ICT sinds 2013[35] ondergebracht bij een Shared Service Centrum (SSC) onder de naam Overheid en Service (ONS). ONS werkt ook voor de gemeenten Zwolle en Kampen. ONS is een gemeenschappelijke regeling van de provincie met de gemeenten Zwolle en Kampen. De regeling is per 1 januari 2018 omgezet van een centrumregeling naar een bedrijfsvoeringsorganisatie.

Afspraken met ONS zijn vastgelegd in diverse stukken[36], waaronder een Service Level Agreement (SLA). Afstemming met ONS gebeurt via een aantal overleggen.

- De provincie en beide gemeenten voeren maandelijks een zogenaamd breed tactisch overleg (BTO) met ONS waarin lopende zaken over informatieveiligheid worden besproken en besluiten worden genomen.
- Er is bilateraal overleg tussen de servicemanager van ONS en de contracthouder bij de provincie.[37]
- Eens per maand is er een strategisch partner overleg (SPO) op managementniveau. Dit overleg gaat niet alleen over informatieveiligheid. In dit overleg worden strategische besluiten genomen, nadat deze zijn afgestemd in het BTO.
- Architectuuroverleg tussen specialisten van ONS en de drie partners.
- Bedrijfsvoeringsberaad met als deelnemers de hoofden bedrijfsvoering en de directeur van ONS.
- Bestuursoverleg met als deelnemers de bestuurders (portefeuillehouders) van de partners en directeur ONS.

In paragraaf 4.1 gaan we nader in op hoe de provincie zicht houdt op de dienstverlening door externe dienstverlening.

Beleid ONS

Uitvoerende partij ONS heeft een eigen informatieveiligheidsbeleid. In 2018 heeft ONS stappen gezet haar Plan Do Check Act cyclus in te richten. Er is in 2018 nieuw informatieveiligheidsbeleid vastgesteld. In het beleid van ONS is aandacht voor de organisatie en verdeling van rollen en taken, strategisch beleid en inrichting van een Information Security Management System (ISMS). Daarnaast zijn voor informatieveiligheid risico's, doelen en beheersmaatregelen benoemd. Het beleid is gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).[38] In interviews is aangegeven dat de BIG in het verlengde ligt van de provinciale baseline. Op een aantal punten stelt de provincie strengere eisen. In deze gevallen neemt ONS de strengere maatregelen van de provincie over.[39] Naast meerjarenbeleid heeft ONS een jaarlijkse security planning.

[35] *Provincie Overijssel (PS/2013/450), besluit gemeenschappelijke regeling shared service centrum bedrijfsvoering.*
[36] *ONS (2018). Service Level Agreement generiek. Provincie Overijssel (2017). Beweerkersovereenkomst ONS. ONS (2017). Dossier Afspraken & Procedures. ONS (2016). Servicecatalogus ONS-ICT.*
[37] *ONS (2017). Dossier Afspraken & Procedures.*
[38] *ONS beleidsplan informatiebeveiliging (2017), Shared Service Centrum ONS Zwolle 2016-2021.*
[39] *Interviews met ONS en ambtelijk medewerkers.*

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 waarborg 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. Bepalen en uitvoeren van maatregelen

4.1 Uitvoering en resultaat

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.
- De provincie controleert de uitvoering van de aanvullende maatregelen die uit de risicoanalyses komen.

Bevindingen

- De provincie bepaalt met een Business Impact Analyses welke risico's er voor processen en applicaties zijn voor de onderdelen beschikbaarheid, integriteit en vertrouwelijkheid. Op basis van de uitkomsten wordt een maatregelenpakket vastgesteld en worden waar nodig aanvullende opgesteld.

Vervolg bevindingen op de volgende pagina.

Vervolg bevindingen

- Het proces om de maatregelen te bepalen, komt niet overeen met de vijf stappen die in het beleid zijn beschreven.
- Via een risicoanalyse zijn in 2015 acht 'kroonjuwelen' vastgesteld.
- De provincie controleert niet op de uitvoering van aanvullende maatregelen,

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'[40] zijn en wat het effect van een cyberaanval op deze 'kroonjuwelen' kan zijn. In deze paragraaf gaan we in op hoe de provincie Overijssel identificeert welke maatregelen er genomen moeten worden en of kroonjuwelen in beeld gebracht zijn.

[40] *De term kroonjuwelen wordt in het kader van informatieveiligheid vaak gebruikt als term om de belangrijkste processen van een organisatie te beschrijven.*

Beleid over bepalen maatregelen

In het informatieveiligheidsbeleid is beschreven dat de provincie een aantal stappen wil doorlopen om tot een set van passende maatregelen te komen (zie tabel 1). Hierbij wordt een afweging gemaakt tussen: risico, betrouwbaarheid, dreiging en beschikbare middelen.

Tabel 1: *Stapsgewijze aanpak van impact naar maatregelen*

Stap	Doel
1. Impactanalyse	De impactanalyse geeft inzicht in de gevolgen van aantasting van de vertrouwelijkheid, de integriteit en de beschikbaarheid. De impactanalyse wordt uitgevoerd op basis van een interprovinciaal model.
2. Kwetsbaar-heidanalyse	Inzicht geven in de vatbaarheid van de organisatie voor verstoringen via: • Toetsing tegen specifieke referentiekaders (bijv. ISO27001, ISO27002). • Ethical hacking en social engineering. • On-site beoordeling (fysieke beoordeling van de beveiliging van het gebouw).
3. Beheersmaat-regelen	De basismaatregelenset schept het minimale niveau van beveiliging voor de hele organisatie. Het basisniveau biedt minimale zekerheid voor beschikbaarheid, integriteit en vertrouwelijkheid van het proces. De basisset beschrijft maatregelen voor de fysieke omgeving, ICT, medewerkers en organisatie.
4. Risicoanalyse	Wanneer uit de impactanalyse blijkt dat er aanvullende beheersmaatregelen nodig zijn naast de basismaatregelen, dan wordt er een risicoanalyse uitgevoerd. Een risicoanalyse bestaat uit een tweetal componenten; de kans dat een dreiging ontstaat en de verwachte impact van de dreiging (risico = kans x impact).
5. Risicobeheer-singsstrategie	Bepalen hoe de provincie Overijssel om wil gaan met de beheersing van risico's die voortkomen uit de risicoanalyse. De provincie kiest per risico één van de mogelijkheden: • Mijden. Bijvoorbeeld risicovolle actie niet uitvoeren. • Mitigeren. Risico terugbrengen met juiste set maatregelen. • Overdragen. Door verzekering afsluiten of risico neerleggen bij leverancier. • Accepteren. De mogelijke impact accepteren.

Bron: Provincie Overijssel, informatieveiligheidsbeleid.

Bepalen van maatregelen in de praktijk

In de praktijk worden de stappen om te komen tot maatregelen niet doorlopen zoals in het beleid beschreven is. Tabel 2 geeft een overzicht hoe er invulling wordt gegeven aan de stappen.

Tabel 2: *Van impact naar maatregelen in de praktijk*

Stap	Uitgevoerd?
1. Impactanalyse	Wordt structureel uitgevoerd in de vorm van een business impact analyse. Hiervan is een uitgebreide procedure beschreven. Dit is de belangrijkste methode om te komen tot passende maatregelen.
2. Kwetsbaar-heidsanalyse	Zit gedeeltelijk in de impactanalyse. Kwetsbaarhedenanalyses zoals ethical hacking of toetsing hebben incidenteel wel plaatsgevonden, maar worden niet structureel gebruikt om te komen tot maatregelen.
3. Beheersmaat-regelen	Er is een basismaatregelenset opgesteld. Via de impactanalyse wordt bepaald of aanvullende maatregelen nodig zijn.
4. Risicoanalyse	Is eenmalig uitgevoerd in 2015 op de belangrijkste processen. Wordt nu niet meer uitgevoerd. Reden daarvan is dat het inschatten van de risico's weinig toevoegt ten opzichte van de impactanalyse, omdat de risico's moeilijk in te schatten blijken. Het is te specialistisch voor provinciemedewerkers.
5. Risicobeheer-singsstrategie	Is niet als zodanig uitgewerkt. Als een opdrachtgever niet akkoord gaat met maatregelen komt dit terug in de impactanalyse. Dit komt in de praktijk weinig voor.

Bron: Provincie Overijssel, interview met ambtelijk medewerker.

In de praktijk worden vooral de impactanalyse (stap 1) en de eenmalige risicoanalyse (stap 4) gebruikt om de set beheersmaatregelen te bepalen. Daarom gaan we hieronder verder in op deze onderdelen.

Risicoanalyse (stap 4)

Allereerst is de risicoanalyse in 2015 uitgevoerd. Deze is gebruikt om de doelstelling van het Strategisch Informatieplan 'een afdoende beveiligingsniveau' te realiseren.
De zestien meest risicovolle processen en systemen zijn onderzocht.[41] Uit deze analyse zijn acht 'kroonjuwelen' naar voren gekomen. Dit zijn:

- Ondersteuning directie, GS/stukkenstroom, GS Notubox;
- Burgemeestersbenoemingen;
- Financieel Toezicht;
- Concessies OV;
- Beheer en Onderhoud;
- Verstrekken GIS bestanden bronhouderschap;
- Personeelsinformatie;
- Centrale digitale archivering en procesvoortgang besluitvorming (nu via EDO).

[41] *Provincie Overijssel (maart 2016). Memo risicoanalyse 2015.*

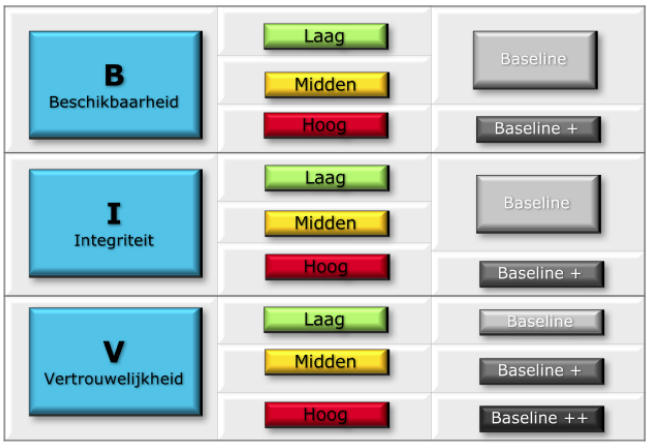
Deze acht processen scoren een hoog risico beschikbaarheid, integriteit en betrouwbaarheid. Voor deze processen geldt dat er altijd de maximale veiligheidsmaatregelen genomen worden. Daarom hoeven hiervoor in de toekomst geen impactanalyses meer uitgevoerd te worden.[42]

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 konden. De uitkomsten van deze praktijktest zijn te vinden in paragraaf 4.2.

Impactanalyse (stap 1)

Voor processen en applicaties die niet als 'kroonjuweel' aangemerkt worden, wordt een Business Impact Analyse (BIA) uitgevoerd. In 2018 zijn tot november ongeveer 15 BIA's uitgevoerd.[43] Het doel van de BIA is het eenduidig classificeren van de informatie die gebruikt wordt binnen een proces of applicatie. De procedure voor een BIA is door de provincie vastgelegd. Zowel in de adviesfase als voor de realisatiefase (voor de uitvraag) wordt een vragenlijst ingevuld door een informatieadviseur, projectleider en stakeholders.[44] Zo wordt vastgesteld wat de mogelijke impact van een applicatie of proces is voor beschikbaarheid, integriteit en vertrouwelijkheid. Per onderdeel wordt een impactscore toegekend: laag, midden of hoog. Aan de hand van deze scores wordt een beveiligingsniveau en bijbehorende maatregelen vastgesteld. Figuur 5 geeft een overzicht. Aan de hand van de uitkomst van de BIA selecteert de adviseur informatiebeveiliging de maatregelpakketten en waar nodig vindt extra overleg met ONS plaats.

Figuur 5: *Impactscores en bijbehorende maatregelensets*



Bron: Provincie Overijssel (november 2017). Business Impact Analyse, procedure en handleiding.

[42] *Provincie Overijssel (november 2017). Business Impact Analyse, procedure en handleiding.*
[43] *Interview met ambtelijk medewerkers provincie Overijssel.*
[44] *Wanneer de gegevensverwerking een hoog privacyrisico oplevert voor de betrokkenen wordt er ook een privacy impact analyse uitgevoerd.*

De provincie heeft een minimaal beveiligingsniveau vastgesteld, dit wordt de baseline genoemd. Het baseline niveau bestaat uit een set maatregelen die in elke situatie voor elk bedrijfsonderdeel van toepassing is en een standaard risiconiveau afdekt tegen geïdentificeerde dreigingen. In de figuur valt af te lezen dat er voor het minimale beveiligingsniveau wordt gekozen als er op *beschikbaarheid* of *integriteit* laag of midden gescoord wordt en op *vertrouwelijkheid* laag.

Als de impact hoger wordt ingeschat moeten er extra maatregelen genomen worden. Hiervoor zijn aanvullende maatregelpakketten opgesteld. In de figuur valt af te lezen dat bij een impactscore 'hoog' voor *beschikbaarheid* of *integriteit* of 'midden' voor *vertrouwelijkheid* extra maatregelen nodig zijn, namelijk een baseline+ pakket. Als uit de BIA blijkt dat de impact voor *vertrouwelijkheid* als hoog wordt ingeschat worden nog weer extra maatregelen genomen. Dit wordt een baseline++ pakket genoemd.[45]

Uitvoering extra maatregelen
In de procedure voor de business impact analyse wordt beschreven dat er een controlefase is. In het kader van de BIA moet steekproefsgewijs door de IB-adviseur nagegaan of de gestelde (aanvullende) maatregelen zijn geïmplementeerd. Na deze check moet een bevindingenrapport opgesteld worden. In de praktijk vinden deze controles niet plaats.[46]

4.1.2 Uitvoering maatregelen

Normen
- De provincie heeft de 'basis' maatregelen genomen en monitort de uitvoering daarvan.

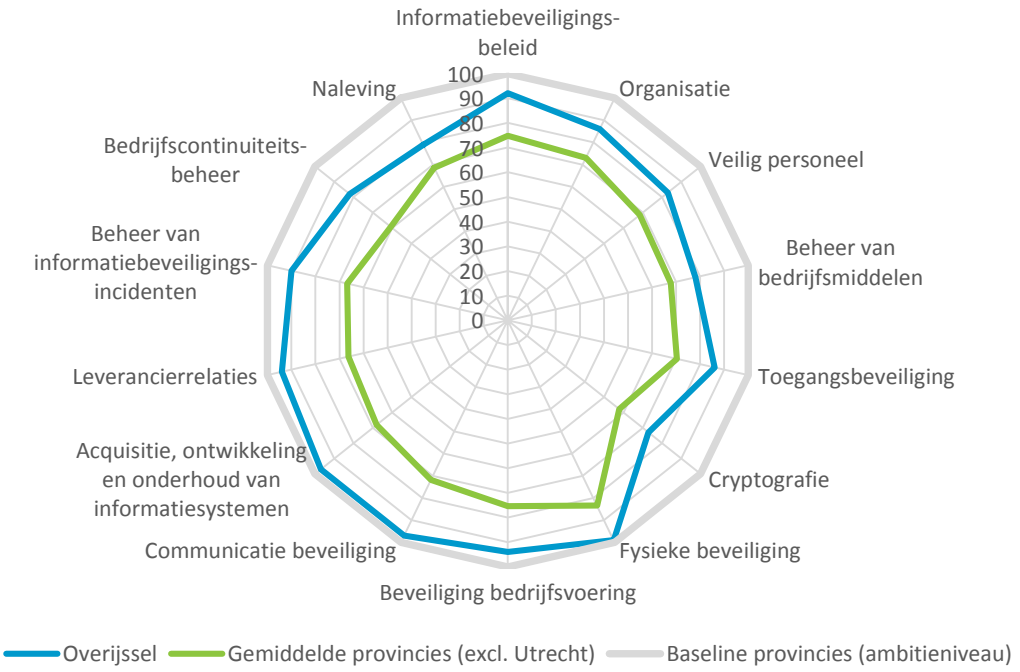
Bevindingen
- De provincie heeft in 2017 voor het laatst een zelfevaluatie gedaan om te zien in hoeverre zij de Interprovinciale Baseline Informatieveiligheid heeft geïmplementeerd. Overijssel scoort niet op alle punten in overeenstemming met haar ambitieniveau. Tegenover het gemiddelde van alle provincies scoort Overijssel relatief hoog.

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. In de vorige paragraaf bleek dat niet gemonitord wordt of aanvullende maatregelen geïmplementeerd worden. In deze paragraaf beschrijven we hoe de basismaatregelen gemonitord en uitgevoerd worden.

[45] *Provincie Overijssel (2017). Business Impact Analyse, procedure en handleiding.*
[46] *Interview met ambtelijk medewerkers provincie Overijssel.*

De provincie monitort of basismaatregelen uit de Interprovinciale Baseline Informatiebeveiliging (IBI) geïmplementeerd zijn. Hiervoor wordt gebruik gemaakt van de interprovinciale monitoringstool van het Cibo.[47] Er wordt organisatiebreed gekeken naar implementatie van technische en procedurele maatregelen zoals deze in het IBI vastgelegd zijn. De IBI is vooral tactisch en operationeel van aard. In 2017 is de uitvoering van de beheersmaatregelen getoetst in een collegiaal self-assessment in 2017. Dit houdt in dat de audit is uitgevoerd door een collega-provincie en dat de vragenlijsten samen met medewerkers van de provincie zijn ingevuld. Figuur 6 geeft een overzicht van de resultaten van de provincie Overijssel. Daarnaast is het gemiddelde van de overige provincies in de figuur opgenomen voor het jaar 2016. De Cibo-monitor is in 2017 niet door de andere provincies ingevuld.

Figuur 6: *(Inter)provinciaal beeld implementatie baseline informatieveiligheid*



Bron: Notitie Cibo-monitor juli 2017 en provincie Friesland en de provincie Overijssel (2017), interprovinciale informatiebeveiligingsaudit conform IBI 2.0.

Conclusie van het collegiale self-assessment 2017 is dat de provincie op de meeste onderdelen goed scoort. In de collegiale self-assessment worden ook afwijkingen tegenover de IBI geconstateerd. Aan de ambitie van 100% wordt niet voldaan. Uit figuur 6 blijkt dat de provincie hoger scoort dan het gemiddelde van andere provincies, die de zelfaudit in 2016 invulden. Een hoge score wil ook niet zeggen dat er in de praktijk geen verbeteringen meer mogelijk zijn, gezien de diverse aanbevelingen die in de audit

[47] *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.*

gedaan worden. Aan sommige aanbevelingen blijkt inmiddels opvolging gegeven te zijn, aan andere nog niet.[48] Bij de vergelijking met andere provincies dient opgemerkt te worden dat het niet alleen om andere jaren gaat, maar ook dat het voor alle provincies een zelfbeoordeling betreft.

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

- De provincie voert periodiek een bewustwordingsprogramma rondom informatieveiligheid uit.
- De provincie heeft de vijf informatieveiligheidsstandaarden geïmplementeerd in haar websites en e-mails.
- De provincie heeft de basis IT-hygiënemaatregelen (patchmanagement, toegangsbeheer en back ups) op orde.
- De provincie neemt afdoende maatregelen voor fysieke beveiliging.

Bevindingen

- De provincie heeft in haar beleid aandacht voor bewustwording met als doel bewustwording onder medewerkers te vergroten.
- Hiervoor zijn diverse bewustwordingsactiviteiten uitgevoerd, zoals phishingtesten, een quiz en een lezing.
- De provincie heeft medewerkers via een aantal documenten bekend gemaakt met hun verantwoordelijkheden bij informatieveiligheid.
- De provincie Overijssel had in januari 2018 alle vijf verplichte informatiebeveiligingsstandaarden geïmplementeerd.
- De IT-hygiënemaatregelen zijn gedeeltelijk op orde, maar kunnen op onderdelen verbeterd worden. Zo heeft de provincie wel beleid voor toegangsbeheer en back-ups en niet voor patching. ONS heeft beleid voor patchmanagement en voert patching en de back-ups uit. Back-ups worden in de praktijk niet getest. Ook toegangsrechten worden in de praktijk niet periodiek door de provincie getoetst, in tegenstelling tot wat in het beleid staat. Een aantal van deze verbeterpunten waren bij de provincie reeds bekend.
- De maatregelen voor fysieke beveiliging zijn grotendeels op orde. Desondanks blijkt dat uitwerking daarvan in de praktijk nog verbeterd kan worden.

[48] *Interview met ambtelijk medewerkers provincie Overijssel.*

Aandachtsgebied mens en organisatie

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 van het feit bewust te zijn dat 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

De medewerker is de eerste en de belangrijkste schakel bij informatieveiligheid.[49] Vanuit hem/haar vindt de creatie, bewerking, opslag en het delen van informatie plaats. In het informatieveiligheidsbeleid dat in 2015 is opgesteld, staat beschreven dat de jaren ervoor is gewerkt aan bevordering van bewustwording. Uit toetsing en observatie van het gedrag blijkt dat de bewustwording en het bijbehorende gedrag op dat moment niet constant op niveau blijft. Het bewustwordingsniveau wordt in 2015 omschreven als “bewust-onbekwaam”. Vele medewerkers zouden zich wel bewust zijn van de noodzaak van informatieveiligheid, maar nog niet bekwaam genoeg om dit ook in gedrag en houding vorm te geven. Om dit bewustwordingsproces te bevorderen, is het voor de provincie belangrijk dat de medewerkers actief wordt betrokken via een bewustwordingsprogramma. Doel is dat de medewerker van de provincie Overijssel bewust en bekwaam wordt.[50]

In deel 4 van het informatieveiligheidsbeleid, de projectportfolio, wordt een bewustwordingscampagne voor omgaan met persoonsgegevens als project genoemd voor het eerste en tweede kwartaal van 2016.

Bewustwordingsactiviteiten in de praktijk

De provincie is in 2017 van start gegaan met de bewustwordingscampagne waarvoor vanaf dat moment diverse activiteiten zijn uitgevoerd.[51] In 2016 is de campagne nog niet uitgevoerd door beperkte personele capaciteit.[52] Tabel 3 geeft een overzicht van activiteiten die door de provincie zijn uitgevoerd.

[49] *Provincie Overijssel (2016). Strategisch Informatieplan. Provincie Overijssel (2016) Informatiebeveiligingsbeleid.*
[50] *Provincie Overijssel (2016). Informatiebeveiligingsbeleid.*
[51] *Provincie Overijssel (2018). Awareness campagneoverzicht 2017/2018*
[52] *Interview met ambtelijk medewerkers provincie Overijssel.*

Tabel 3: Bewustwordingsactiviteiten provincie Overijssel vanaf 2017

Activiteit	Inhoud
Presentaties over bewustwording	De IB-adviseur presenteert aan de teamleiders van alle managementteams over informatieveiligheid omdat zij verantwoordelijk zijn voor hun eigen 'lijn'. Daarom worden zo tools en informatie gedeeld om hen en aan te sporen om informatieveiligheid op de agenda te houden. De teamleider moet de boodschap doorgeven aan zijn of haar mensen.[53]
Prikkelende bewustwordingsactiviteiten	2 phishing e-mails, een telefonische phishing actie, een rubber ducky actie (geprepareerde USB-stick die wordt achtergelaten).[54]
Informatieveiligheid in het inwerkprogramma	Plaats voor informatieveiligheid in gesprekken functies met prioriteit, voorlichting nieuwe medewerkers en een e-learning. Deels uitgevoerd, loopt deels nog achter op de planning. De e-learning is geannuleerd.
Quiz over informatieveiligheid	Vier quizzen via intranet met de thema's: vertrouwelijke informatie of niet?, Meldplicht datalekken, wat betekent informatiebeveiliging voor mij? en persoonsgegevens.
Set vragen voor teamleiders	Er is een setje vragen gemaakt voor teamleiders waarmee men zelf binnen het team middels een soort spel kan achterhalen waar risico's liggen.
Lezing over informatieveiligheid	Schrijfster van boek 'komt een vrouw bij de h@cker' deelt haar kennis met medewerkers. De lezing is goed bezocht.

Bron: Overzicht awareness campagne provincie Overijssel

De provincie koppelde resultaten van diverse activiteiten terug om de bewustwording te vergroten. De resultaten en aandachtspunten van de phishing test werden onder medewerkers verspreid via een filmpje, persoonlijke gesprekken en nieuwsberichten via intranet. Ook was er direct een scherm met informatie over de phishing actie te zien als medewerkers op de link klikten. Terugkoppeling naar medewerkers over de quiz verliep via nieuwsberichten op intranet. Het management werd geïnformeerd over de bewustwordingscampagne via een notitie gericht aan het bedrijfsvoeringsoverleg.[55]

Documenten en richtlijnen

Naast bovengenoemde bewustwordingsactiviteiten, heeft de provincie medewerkers in verschillende documenten en richtlijnen gewezen op hun verantwoordelijkheid bij informatieveiligheid. Via intranet heeft de provincie Overijssel een pagina 'informatieveiligheid en privacy' waarop diverse documenten en richtlijnen zijn gedeeld over informatieveiligheid waaronder:

- het informatieveiligheidsbeleid;
- meerdere documenten over datalekken waaronder de procedure voor meldplicht van datalekken. De link waarmee een datalek gemeld kan worden, werkt niet;[56]

[53] *Interview met ambtelijk medewerkers provincie Overijssel.*
[54] *Provincie Overijssel, awareness campagneoverzicht 2017/2018, stavaza aug 2018.*
[55] *Provincie Overijssel (2014). Notitie bedrijfsvoeringsoverleg bewustwordingscampagne.*
[56] *Intranet provincie Overijssel. Laatst geraadpleegd 20 november 2018.*

- praktische tips over beveiliging van mobiele apparatuur (met een link naar procedure voor wachtwoorden), verdachte e-mailberichten, social engineering, gebruik open Wifi, gebruik van applicaties en ransomware;
- links naar websites met meer informatie over informatieveiligheid;
- informatie over de procedure van de Business Impact Analyse.

Niet alle informatie gerelateerd aan informatieveiligheid is terug te vinden op deze intranetpagina. De Bring Your Own Device regeling is hier een voorbeeld van. Ook is er in de huisregels aandacht voor informatiebeveiliging, integriteit en toegang voor gebruikers, gasten en leveranciers.[57]

Aandachtsgebied ICT

Informatieveiligheidsstandaarden

Er is niet één bepaalde standaard die alle beveiligingsrisico's afdekt. Het gaat om een samenspel van meerdere standaarden.[58] In paragraaf 4.1.2 zijn we al in gegaan op uitvoering van de Interprovinciale Baseline Informatieveiligheid (gebaseerd op de ISO-27002-standaard), 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.[59] Daarnaast zijn er overheidsbreed afspraken gemaakt over de implementatie van onder meer informatieveiligheidsstandaarden.[60] Het Forum Standaardisatie toetst over overheden de informatieveiligheidsstandaarden geïmplementeerd hebben. Hun monitor liet begin 2018 het volgende beeld zien.

Tabel 4: *Toepassing informatieveiligheidsstandaarden door de provincie Overijssel (januari 2018)*

Onderdeel	Implementatie informatieveiligheidsstandaard
Web - overijssel.nl	• DNSSEC (domeinnaambeveiliging): Ja • TLS (beveiligde verbinding): Ja
Mail - @ overijssel.nl	SPF, DKIM en DMARC (anti-phishing, rapportage) • SPF: Ja • DKIM: Ja • DMARC: Ja

Bron: Halfjaarlijkse meting Informatieveiligheidstandaarden Forum Standaardisatie begin 2018 p. 15.

[57] Intranet provincie Overijssel. Laatst geraadpleegd 20 november 2018.
[58] Forum Standaardisatie (2014). Verkennend onderzoek ISO 27001 en ISO 27002, p. 6.
[59] 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.*
[60] 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

Uit tabel 4 komt naar voren dat de provincie Overijssel alle standaarden heeft geïmplementeerd.[61]

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 drie 'basis IT-hygiënemaatregelen'. Hierbij gaat het om patchmanagement[62], toegangsbeheer en back-ups. Hieronder gaan we na wat hierover in het Overijsselse informatieveiligheidsbeleid staat en hoe dit in de praktijk geregeld is.

Patch management

De provincie heeft geen eigen patchbeleid. In het informatieveiligheidsbeleid zijn ook geen eisen opgenomen hoe vaak of snel patches uitgevoerd moeten worden. Er wordt wel in algemene zin ingegaan op onderhoud en ontwikkeling van informatiesystemen. In gesprekken is aangegeven dat het applicatielandschap niet valt onder de verantwoordelijkheid van ONS, maar onder de verantwoordelijkheid van de provincie. Omdat patching ook relevant is voor applicaties zou verwacht mogen worden dat provincie zelf ook beleid voor patching heeft. ONS is verantwoordelijk voor de uitvoering van patching voor de Overijsselse ICT-infrastructuur. ONS heeft eigen patchbeleid dat hiervoor gevolgd wordt.

Toegangsbeheer

Het beleid voor toegangsbeheer is vastgelegd in het informatieveiligheidsbeleid en het proces vastgelegd in het proces van "in- door- uitstroom". Dit proces borgt dat mensen die niet meer in dienst zijn geen toegang meer hebben tot systemen van de provincie. In het beleid staat ook dat toegangsrechten van gebruikers regelmatig gecontroleerd dienen te worden. Periodiek (tenminste ieder kwartaal) moet de functioneel beheerder en de beheerder van de Active Directory een overzicht van de gebruikers en toegangsrechten aan het Hoofd Eenheid verstrekken ter controle. In een interview wordt aangegeven dat deze periodieke controle niet plaatsvindt. Er zijn functioneel beheerders die dit wel uitvoeren, maar dit gebeurt niet structureel en er is geen totaaloverzicht. In het informatieveiligheidsbeleid staat ook dat sterke wachtwoorden geborgd moeten zijn en dat het aantal inlogpogingen beperkt moet zijn. Tijdens de uitvoering van het onderzoek hebben wij verouderde eisen voor wachtwoorden ontvangen en op intranet staan op verschillende plekken andere eisen waaraan wachtwoorden moeten voldoen. Bij navraag blijkt dat de juiste eisen op de pagina 'Tips en weetjes ICT' staat en niet bij de instructie 'Hoe kan ik mijn wachtwoord veranderen' of 'de procedure windows wachtwoord wijzigen'. Tevens kwam een verzoek naar voren van een medewerker aan een collega om het wachtwoord te delen. Ook bleek uit de praktijktest dat het mogelijk was om onopgemerkt veelvuldig geautomatiseerde inlogpogingen te doen.

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

[61] Interview met ambtelijk medewerkers provincie Overijssel.

[62] 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.

De accountant heeft in 2016 zijn opmerkingen gemaakt over toegangsbeheer.[63] De accountant merkt op dat de wachtwoordinstellingen van een applicatie nog niet voldoen aan de gewenste complexiteitseisen. Verder wordt geconstateerd dat de procedure voor toegangsbeheer nog niet is vastgelegd en dat controle van rechten dient te worden verbeterd. De procedure is dus inmiddels door de provincie vastgelegd, maar structurele controle vindt nog niet plaats. In de meest recente IBI zelfaudit (2017) wordt ook gesteld dat autorisatiebeheer een aandachtspunt is: hier worden geen controles op uitgevoerd en dit heeft als risico dat medewerkers autorisaties kunnen gaan verzamelen die ze toegekend krijgen als zij andere functies in de loop der jaren gaan bekleden.[64]

Back-ups

De externe dienstverlener, ONS, is verantwoordelijk voor het uitvoeren van back-ups. In het provinciebeleid staat dat regelmatig back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid. ONS voert het maken van back-ups uit en heeft dit vast gelegd in een uitgebreid protocol. Testen of back-ups werken gebeurt op dit moment niet.[65] Dit signaleerde de accountant ook in haar boardletter van 2016. Hierdoor bestaat het risico dat in het geval van een calamiteit data mogelijk niet (tijdig) valt te herstellen.

Aandachtsgebied basisinfrastructuur

In het informatieveiligheidsbeleid is naast organisatie en ICT ook aandacht voor de fysieke omgeving: de beveiliging van de gebouwen, werkplekken en beveiliging van het papieren archief. Er is een hoofdstuk in het beleid gewijd aan maatregelen voor fysieke beveiliging. In de audit scoort het onderdeel fysieke beveiliging 99%. Er wordt geconcludeerd dat dit onderdeel goed op orde is. Tegelijk zijn er ook nog een aantal aandachtspunten.[66] Ook uit een inlooptest die de provincie heeft laten uitvoeren bleek dat de fysieke beveiliging in de praktijk nog verbetering behoeft.[67] Hierover meer in paragraaf 4.2.

[63] *Ernst & Young, Boardletter tussentijdse controle 2016.*
[64] *Provincie Overijssel en provincie Friesland (2017). interprovinciale informatiebeveiligingsaudit conform IBI 2.0.*
[65] *Interview met ambtelijk medewerkers provincie Overijssel.*
[66] *Provincie Overijssel en provincie Friesland (2017). interprovinciale informatiebeveiligingsaudit conform IBI 2.0.*
[67] *Provincie Overijssel (2018). Rapportage Mystery Guest actie.*

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.

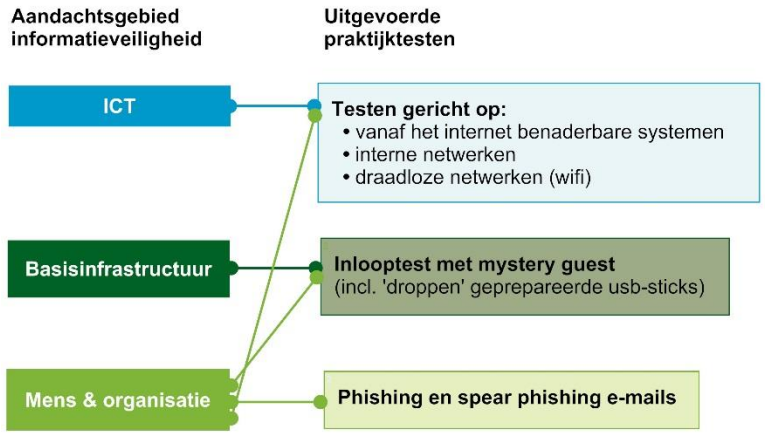
Bevindingen

- In opdracht van de Rekenkamer zijn in oktober 2018 praktijktesten uitgevoerd op de aandachtsgebieden ict en mens & organisatie. De provincie heeft in 2018 een inlooptest en phishing-campagne laten uitvoeren.
- Uit de testen blijkt dat de provincie meerdere effectieve beschermingsmaatregelen heeft genomen om weerbaar te zijn tegen cyberaanvallen.
- Er zijn een aantal kwetsbaarheden gevonden die een risico vormen voor de informatieveiligheid. Het ging in één geval om een kritisch risico. Via malware is toegang verkregen tot meerdere systemen waardoor vertrouwelijke informatie toegankelijk werd.
- Het doel van de provincie is dat medewerkers bewust bekwaam zijn over het thema informatieveiligheid. Uit de inloop- en phishingtesten bleek dat dit nog niet het geval is. Het versturen van spear phishing e-mails leidde tot het verkrijgen van toegang tot accounts en bestanden en tot het verkrijgen van inloggegevens. Bij de inlooptest is ongeautoriseerd toegang tot niet-publieke ruimtes, systemen en gegevens verkregen. Meer dan 100 medewerkers klikten op een kwaadaardige link in een phishing e-mail.
- Uit de test komen enkele kwetsbaarheden naar voren die ook uit de vorige penetratietest (april 2018) naar voren kwamen.

In deze paragraaf gaan we in op het resultaat van het informatieveiligheidsbeleid en de uitvoering daarvan. Wordt informatie bij de provincie Overijssel door de genomen maatregelen voldoende beschermd tegen toegang door onbevoegden? Om deze vraag te kunnen beantwoorden, maken we gebruik van praktijktesten uit 2018. Een penetratie- en spear phishingtest[68] test zijn in opdracht van de Rekenkamer uitgevoerd. Daarnaast wordt gebruik gemaakt van een inloop- en phishingtest die de provincie zelf in 2018 heeft laten uitvoeren. In figuur 7 hebben we schematisch weergegeven wat voor soort praktijktesten in 2018 zijn uitgevoerd. Na de figuur volgen de uitkomsten.

[68] *Spear phishing is een gerichte phishing actie waarbij een geïnfecteerde e-mail naar een specifiek geselecteerde groep wordt gestuurd.*

Figuur 7: *Uitgevoerde praktijktesten 2018 naar aandachtsgebied*



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 penetratietesten (voornamelijk aandachtsgebied ICT)

Uit de test komt naar voren dat de provincie Overijssel meerdere effectieve beschermingsmaatregelen 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[69] en filtering;[70]
- gebruik te maken van moderne besturingssystemen en antivirus.

Het lukte de onderzoekers niet om binnen de beschikbare tijdsperiode de rechten van de systeembeheerder[71] te verwerven.

Ondanks deze maatregelen zijn er wel mogelijkheden aangetroffen om via het internet toegang te krijgen tot systemen en gegevens van enkele gebruikers. Dit lukte door kwetsbaarheden in de zogenoemde authenticatievoorzieningen[72] te gebruiken. Hierdoor konden de onderzoekers bij vertrouwelijke documenten. Verder zijn best practices en

[69] *Netwerksegmentatie betekent dat het netwerk ingedeeld is in verschillende zones. Wanneer er sprake is van netwerksegementatie dan heeft een hacker of malware wanneer het toch is gelukt binnen te komen niet gelijk vrij spel binnen het hele netwerk.*
[70] *Filtering betekent dat de 'verkeersstromen' tussen de verschillende segmenten van het netwerk wordt beperkt.*
[71] *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.*
[72] *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.*

'hardening'[73] 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. Zo maken niet alle websites gebruik van versleutelde verbindingen.[74] Dit punt was ook in eerdere testen van de provincie naar voren gekomen.[75] Opvallend is dat de provincie Overijssel bij het forum standaardisatie wel positief scoort op het punt beveiligde verbinding (zie paragraaf 4.1.3). Naast het punt van de beveiligde verbinding, worden nog enkele andere bevindingen gedaan die ook in de vorige penetratietest naar voren kwamen.

Op het interne netwerk is het gelukt om restricties te omzeilen en in beperkte mate toegang te krijgen tot gegevens. Verder zijn er inlogcombinaties achterhaald via mobiele apparaten. Deze inlogcombinaties bleken niet te voldoen aan het beleid van de provincie.[76] Hiermee kon toegang verkregen worden tot e-mails en bestanden van de gebruikers van die apparaten.

Uitkomsten inlooptest (aandachtsgebied basisinfrastructuur en mens & organisatie)
In mei 2018 is een inlooptest uitgevoerd bij het provinciehuis. De mystery guest kon ongeautoriseerde toegang krijgen tot niet-publieke ruimten. Tijdens zijn bezoek is hij een aantal maal aangesproken, maar werd er niet doorgevraagd. De mystery guest kon zich daardoor vrij door het gebouw begeven. Er werden niet vergrendelde computersystemen, niet afgesloten lockers met gegevens, onbewaakte devices (smartphones en tablets) en toegangspassen aangetroffen. Ook bleek het mogelijk toegang tot krijgen tot de afdeling van ONS. Het is niet gelukt om toegang te krijgen tot technische ruimten zoals de serverruimte. Het lukte de mystery guest zich toegang te verschaffen tot niet-publieke ruimten, waaronder de afdeling van ONS, door mee te lopen met medewerkers.

Uitkomsten (spear)phishing (aandachtsgebied mens & organisatie)
In oktober/november 2017 en maart 2018 heeft de provincie zelf phishingtesten laten uitvoeren. In figuur 8 zijn de resultaten van de phisingtesten weergegeven. Het doel van deze testen was om het bewustzijn van betrokkenen te verhogen, de reacties van medewerkers kwantitatief in kaart te brengen en dit te benchmarken met andere door het onderzoeksbureau getoetste organisaties. Doel was bovendien met de resultaten een positieve boodschap aan de medewerkers te richten met als onderwerp informatieveiligheid en bewustwording in het algemeen, met phishing in het bijzonder.[77]

[73] *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).

[74] *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.*

[75] *ONS (2017 en 2018). Rapportage penetratietesten.*

[76] *Provincie Overijssel, Procedure windows wachtwoord wijzigen.*

[77] *Provincie Overijssel (2017 en 2018). Rapporten 1e en 2e phishing-linkactie.*

Figuur 8: *'Ruwe' phishing-resultaten provincie Overijssel (maart 2018)*

Actie	Totaal aantal e-mails	Totaal aantal hits	Inlogpercentage
1ste actie	1458	104 (7%)	n.v.t.
2de actie	1458	154 (11%)	94 (7%)

Bron: Overijssel (2017 en 2018) Rapporten 1e en 2e Phishlink-actie.

Figuur 8 laat zien dat de campagne is uitgevoerd bij 1.458 medewerkers. Daarvan hebben in de eerste actie in een tijdsbestek van 7 dagen 104 mensen op de link in de e-mail geklikt. Bij beide acties vonden de meeste reacties plaats kort na het versturen van de e-mail. In een interview wordt aangegeven dat na de eerste phishingmail medewerkers melding deden van de verdachte mail. Bij een echte phishingmail was daarom wel veel eerder actie ondernomen. Dat is nu niet gedaan omdat het doel van de actie was het vergroten van bewustzijn en niet het testen van procedures.[78] Er werd niet gevraagd om in te loggen. De eerste actie wordt getypeerd als 'makkelijk'. Er waren twee cruciale herkenningspunten waaraan te zien was dat het om een phishing e-mail ging. In de tweede actie klikten in een tijdsbestek van ongeveer 11 dagen 154 personen op de phishing-link. 97 personen hebben hun gegevens ingevuld. De tweede phishing e-mail valt in de moeilijkheidsgraad "gemiddeld" en is dus lastiger te onderscheiden van een echte e-mail.

Bij beide acties scoort de provincie met deze cijfers beter dan het gemiddelde van vergelijkbare acties van het onderzoeksbureau. Er zijn bij de acties geen kwetsbare of mogelijk verouderde besturingssystemen aangetroffen bij de medewerkers. Wel werden er bij medewerkers plug-ins aangetroffen die bekend staan om kwetsbaarheden en werd er in een geval gebruik gemaakt van een verouderde browserversie.[79]

In september 2018 zijn er in opdracht van de Rekenkamer twee "gerichte" spear phishing e-mails gestuurd met een kwaadaardige bijlage. 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 dan groter is dat de aanval dan opgemerkt en/of afgeslagen wordt. De spear phishing mails hebben in beide gevallen geleid tot volledige toegang tot de accounts en gegevens van een drietal medewerkers die de bijlage hebben geopend. Hierbij ging het om een medewerker die verantwoordelijk is of is geweest voor de afhandeling van vertrouwelijke stukken. Hierdoor is toegang verkregen tot beveiliging en configuratiebestanden van applicatiebeheer. Ook is toegang verkregen tot een zogenoemde 'scanstraat' waar documenten gedigitaliseerd worden. Zodoende werden alle documenten die hier gedigitaliseerd worden toegankelijk. Zo konden kroonjuwelen van de provincie Overijssel benaderd worden.

[78] *Interview met ambtelijk medewerkers provincie Overijssel.*
[79] *Rapporten phishing-linkacties.*

Uitkomsten achtergelaten USB-stick (aandachtsgebied mens & organisatie)

Om de bewustwording van medewerkers te testen is er een USB-stick achtergelaten. Op de USB-stick staan geprepareerde bestanden. Die bestanden nemen contact op met een systeem op internet zodat gezien kan worden of de bestanden geopend worden. Via een achtergelaten USB-stick met daarop kwaadaardige bestanden kunnen kwaadwillenden toegang tot systemen verschaffen. De USB-stick die bij de provincie Overijssel is achtergelaten is noch gebruikt, noch ingeleverd bij de verantwoordelijke afdeling.[80]

[80] *Interview met ambtelijk medewerker provincie Overijssel.*

5 Toezicht en verantwoording

In dit hoofdstuk gaan we in op de wijze waarop de provincie Overijssel 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 informatieveiligheidsbeleid.
- De provincie voert zelfevaluaties uit.

Bevindingen

- Onafhankelijke toetsen vinden periodiek plaats in de vorm van een DigiD-audit en een jaarlijks onderzoek van de accountant.
- De provincie voert zelfevaluaties uit. Dit gebeurt niet jaarlijks zoals in het beleid staat.
- De provincie laat incidenteel praktijktesten uitvoeren zoals inloop-, phishing- en penetratietesten. ONS is verantwoordelijk voor het uitvoeren van de penetratietesten.
- In 2018 hebben nulmetingen plaatsgevonden van de implementatie van de ISO 27001. Op een aantal punten scoort de provincie Overijssel goed. Op een aantal punten voldoet de provincie nog niet, met name als het gaat om de monitoring en beheersing.
- ONS rapporteert via documenten en overleg aan de provincies over informatieveiligheid. De provincie monitort zelf niet structureel of externe leveranciers informatieveiligheid in de praktijk waarborgen.

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.[81]

In deze paragraaf gaan we eerst in op wat in het beleid staat over toezicht. Daarna bekijken we hoe dit er in de praktijk uitziet. Hiervoor hebben we uitgezocht in hoeverre de provincie Overijssel onafhankelijke onderzoeken heeft laten uitvoeren naar het beveiligingsniveau en de implementatiestatus van het informatieveiligheidsbeleid. Daarnaast hebben we gekeken in hoeverre de provincie Overijssel zelf onderzoek doet naar 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 staat dat onafhankelijke auditing noodzakelijk is om na te gaan of de provincie voldoet aan wet- en regelgeving en normen voor informatieveiligheid. Daarnaast wil de provincie periodiek haar eigen normen toetsen op het gebied van relevantie, actualiteit, naleving en uitvoering. Toetsing moet gebeuren door de wettelijk verplichte audit en een tweejaarlijkse zelfaudit aan de hand van ISO-normen. Ook wordt beschreven dat jaarlijks implementatie van beheersmaatregelen wordt getoetst via de Cibo-monitor. Het beleid is niet eenduidig over controles van de provincie. In het beleid wordt gesproken van een tweejaarlijkse zelfaudit en van een jaarlijkse zelfaudit. Hiermee wordt hetzelfde bedoeld. Navraag leert dat het doel is om jaarlijks een zelfaudit uit te voeren.[82]

Door de zelfaudit moet de aanpak van de organisatie en de implementatie (bijv. beheersdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatieveiligheid), onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen worden beoordeeld. Er is beschreven dat op een aantal specifieke onderdelen van informatieveiligheid regelmatig controles plaatsvinden. In paragraaf 4.1 kwamen hier al een drietal voorbeelden van terug:

- controle op uitvoering van maatregelenpakketten die voortkomen uit impactanalyses[83];
- elk kwartaal een controle op toegangsrechten van gebruikers;
- back ups regelmatig testen.

Daarnaast is beschreven dat de DigiD voorziening jaarlijks getest wordt. In het beleid is niet gespecificeerd dat testen en controles voor de praktische stand van

[81] *Overgenomen uit: Randstedelijke Rekenkamer (juli 2016). Eindrapporten informatieveiligheid Flevoland, Nood-Holland, Utrecht en Zuid-Holland. Paragraaf 5.2 Onafhankelijke toets op informatieveiligheid.*
[82] *Provincie Overijssel (december 2018). Reactie ambtelijk hoor en wederhoor.*
[83] *Provincie Overijssel (november 2017). Business Impact Analyse, procedure en handleiding.*

informatieveiligheid in de vorm van penetratietesten of inlooptesten regelmatig dienen plaats te vinden.[84]

Toezicht en testen in de praktijk

De provincie Overijssel heeft diverse onderzoeken, controles en testen uitgevoerd of laten uitvoeren op verschillende onderdelen van informatieveiligheid. Tabel 5 geeft hiervan een overzicht.

Tabel 5: *Uitgevoerde onderzoeken, controles en testen door / in opdracht van provincie Overijssel*

Uitvoerder	Scope en frequentie
Provincie	• Cibo-monitor over de implementatie van de IBI (2014 en eerder, 2017). • Doorlopende monitoring van (verbetering) maatregelen.
Extern (onafhankelijke toetsing)	• Structureel: o Aandacht van accountant voor thema in boardletters en jaarverslagen, in het bijzonder in 2016; o DigiD-audit. • Incidenteel: o test bewustwording medewerkers via phishingmail in 2017 en 2018; o Inlooptest 2018 (daarvoor inlooptesten in 2011 en 2012); o penetratietest in 2017 en 2018 (in 2015 en 2016 geen testen uitgevoerd); o nulmeting ISO 27001 in 2018.[85]
Concerncontrol	• 2017a onderzoek concerncontrol over beheersing van informatiebeveiliging (2018).

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

Periodieke toetsing door provincie

Cibo-monitor

Uit de tabel blijkt dat de provincie Overijssel voor 2014 en in 2017 een zelfaudit heeft uitgevoerd. In 2015, 2016 en 2018 heeft de provincie Overijssel geen zelfaudit uitgevoerd. De zelfaudit heeft dus niet jaarlijks plaatsgevonden, zoals in het beleid staat. Ook de provincies hadden afgesproken de interprovinciale Cibo-monitor jaarlijks in te vullen. Dit hebben zij tot en met 2014 gedaan. Omdat de provincies binnen het Cibo 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.[86] De provincie Overijssel heeft hier dus niet voor gekozen. Eind 2016 hebben de provincies de monitor ingevuld

[84] *Provincie Overijssel (2016). Informatiebeveiligingsbeleid.*
[85] *Formele opdrachtgever is Bij12. Bij12 is de uitvoeringsorganisatie voor de samenwerkende provincies.*
[86] *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).*

op basis van de nieuwe IBI. Dit heeft de provincie Overijssel niet gedaan in verband met beperkte beschikbare capaciteit.[87] In 2017 is de Cibo-monitor niet ingevuld door de provincies, maar heeft de provincie Overijssel wel een zelfaudit uitgevoerd.[88] In 2018 is de zelfaudit niet uitgevoerd. De zelfaudit is in 2018 vervangen door en 0-meting van de ISO27001-standaard.[89]

Doorlopende monitoring en dossiervorming provincie

Naast de zelfaudit houdt de adviseur informatiebeveiliging een excelbestand bij waarin de voortgang en aandachtspunten van beheersmaatregelen worden bijgehouden. De provincie heeft het voornemen dit bestand te vervangen door een ander systeem. De mogelijkheden van het excelbestand zijn beperkt. Zo kunnen acties niet via het excelbestand gedeeld kunnen worden met collega's die ook taken hebben voor informatieveiligheid, bijvoorbeeld afdeling facilitair.[90] Ook Concerncontrol concludeert in haar 217a-onderzoek dat de huidige tooling (excel) onvoldoende geschikt is voor monitoring en beheersing. Het is arbeidsintensief, foutgevoelig en de continuïteit van gegevens onvoldoende geborgd. Advies van Concerncontrol is op korte termijn over te gaan op nieuwe standaard tooling.[91] Aanbevelingen die voortkomen uit audits en praktijktesten worden niet structureel bijgehouden via het excelbestand. De adviseur informatiebeveiliging is in grote lijnen wel op de hoogte van opvolging van aanbevelingen, maar een totaaloverzicht hiervan bestaat niet.

In eerdere hoofdstukken kwam al naar voren dat in het informatieveiligheidsbeleid op onderdelen specifieke beleidslijnen worden geformuleerd voor monitoring. Voor alle specifieke onderdelen die in dit onderzoek bekeken zijn, blijkt deze monitoring niet plaats te vinden zoals in het beleid beschreven is:

- er worden geen streekproeven gehouden of (aanvullende) maatregelen worden uitgevoerd die voortkomen uit impactanalyses;
- toegangsrechten worden niet structureel elk kwartaal gemonitord middels een overzicht van gebruikers en toegangsrechten
- back ups worden op dit moment niet getest.

In interviews wordt aangegeven dat de onderdelen 'check' en 'act' uit de PDCA-cyclus nog verbetering behoeven. Hierbij worden ook het verbeteren van checks of iedereen zijn taak uitvoert en het rapporteren over informatieveiligheid genoemd.[92]

Periodieke externe toetsing

Accountant

Uit de boardletters en verslagen van de accountant blijkt dat deze de afgelopen jaren aandacht hebben gehad voor (aspecten van) informatieveiligheid bij de provincie Overijssel. Deze aspecten van informatiebeveiliging (bijvoorbeeld wijzigingsbeheer, toegangsbeveiliging) kwamen veelal aan bod bij de aandacht die de accountant had voor algemene IT-controles bijvoorbeeld rondom het financieel systeem van de provincie. De

[87] *Interview met ambtelijk medewerker provincie Overijssel.*
[88] *Provincie Overijssel en provincie Friesland (2017), interprovinciale informatiebeveiligingsaudit conform IBI 2.0.*
[89] *Provincie Overijssel (december 2018). Reactie ambtelijk hoor en wederhoor.*
[90] *Interview met ambtelijk medewerkers provincie Overijssel.*
[91] *Provincie Overijssel, Concerncontrol (2018). Art. 217a onderzoek beheersing informatiebeveiliging.*
[92] *Interview met ambtelijk medewerkers provincie Overijssel.*

accountant had met name in 2016 veel aandacht voor cybersecurity. PS hadden dit toen ook als één van de drie aandachtspunten voor de accountant meegegeven.

DigiD

De provincie Overijssel wordt jaarlijks getoetst voor DigiD-certificering. Voor DigiD geldt de verplichting om te voldoen aan een beveiligingsnorm en dit via een jaarlijkse ict-beveiligingsnorm te laten toetsen.[93]

Incidentele externe toetsing

Praktijktesten

De provincie Overijssel heeft incidenteel testen laten uitvoeren die de stand van informatieveiligheid in de praktijk testen. De provincie heeft in 2017 en 2018 phishing acties laten uitvoeren. In 2011, 2012 en 2018 werd een inlooptest uitgevoerd. Daarnaast heeft ONS in 2017 en 2018 penetratietesten laten uitvoeren. Voorheen werden dergelijke testen in opdracht van de provincie uitgevoerd. Tegenwoordig worden deze in opdracht van ONS uitgevoerd omdat ze daarbij aansluiting kan zoeken bij testen die voor de gemeenten Zwolle en Kampen gedaan worden[94]. In de overige jaren vonden geen phishing-, inloop- of penetratietesten plaats.

ISO27001

Waar de Cibo-monitor toetst of voldaan wordt aan de IBI (gebaseerd op de ISO27002), is ook onderzocht of de provincie voldoet aan de ISO27001. De IBI is meer tactisch en operationeel van aard en gericht op het implementeren van technische en procedurele maatregelen. De ISO27001 bevat eisen waar het managementsysteem voor informatieveiligheid aan moet voldoen. De focus bij de ISO27001 is gericht op het aantoonbaar managen en beheersen van informatiebeveiliging. Dit 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 aan het voorbereiden. Onderdeel van die voorbereiding was een nulmeting, om bij elke provincie te kijken hoe het er nu voor staat. Ook Concerncontrol heeft een nulmeting uitgevoerd.

Concerncontrol heeft deze nulmeting in de eerste helft van 2018 uitgevoerd. Figuur 9 geeft de resultaten weer.

[93] *Dit is landelijk bepaald: op 2 februari 2012 heeft de toenmalig minister Spies dit in een brief aan de Tweede Kamer aangegeven. Die brief is hier te vinden: https://kennisopenbaarbestuur.nl/media/111360/kamerbrief-over-ict-beveiligingsassessments-bij-digid-gebruikende- organisaties.pdf*

[94] *Interview met ambtelijk medewerkers provincie Overijssel.*

Figuur 9: *Self-assessment IS27001*

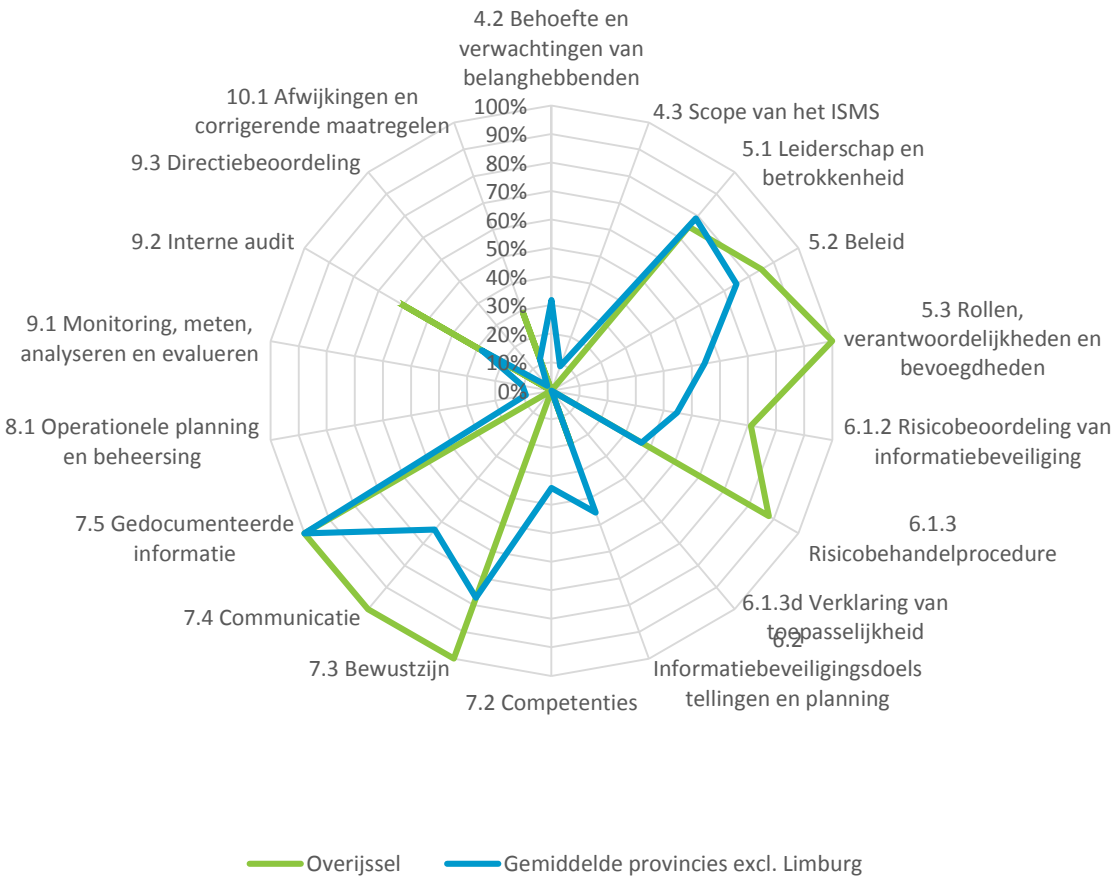
Bron: Provincie Overijssel, concerncontrol (2018). Art.217A Onderzoek beheersing informatiebeveiliging

De rode lijn is de minimumscore om te voldoen aan certificering. Deze ligt op 65%. De blauwe lijn geeft de resultaten van de provincie Overijssel weer. De conclusie van Concerncontrol is dat de provincie het voor een aantal onderwerpen, zoals leiderschap, beveiligingsbeleid en risicoanalyses, goed op orde heeft. [95] Tegelijkertijd moeten er voor veel onderdelen nog stappen gezet worden. Zo moet een Information Security Management System (ISMS) nog worden vormgegeven. Daarnaast zal documentatie en de PDCA cyclus op het ISMS aan moeten gaan sluiten.[96] De provincie heeft al langer het doel een ISMS in te richten. In het informatieveiligheidsbeleid wordt beschreven dat de provincie regie wil houden door middel van een ISMS. Voor 2015/2016 is het inrichten van een ISMS als één van de drie projecten beschreven.[97] Navraag bij de provincie leert dat dit er niet van gekomen is vanwege beperkte capaciteit. Andere grote ontwikkelingen zoals invoering van de AVG namen veel capaciteit in beslag.[98]

In 2018 heeft een extern bureau getoetst in hoeverre alle provincies, waaronder de provincie Overijssel, de ISO 27001 heeft geïmplementeerd. De resultaten van deze nulmeting zijn weergegeven in figuur 10.

[95] *Provincie Overijssel (2016). Informatiebeveiligingsbeleid.*
[96] *Provincie Overijssel Concerncontrol (2018). Art. 217a onderzoek beheersing informatiebeveiliging.*
[97] *Provincie Overijssel (2016). Informatiebeveiligingsbeleid.*
[98] *Interview met ambtelijk medewerkers provincie Overijssel.*

Figuur 10: *Uitkomst nulmeting provincie Overijssel (in relatie tot gemiddelde provincies) (nov. 2018)*



Bron: Presentatie Digitrust Nulmeting ISO27001 BIJ12 + 12 provincies (november 2018).

Figuur 10 laat zien dat de provincie Overijssel op een aantal onderdelen net als in het onderzoek van Concerncontrol goed scoort: leiderschap, beveiligingsbeleid, risicoanalyses en risicobehandelprocedure. In vergelijking met de uitkomsten van Concerncontrol wordt er op een aantal andere onderdelen ook goed gescoord: rollen, bewustzijn, communicatie en gedocumenteerde informatie. Tegelijkertijd scoort zij net zoals veel andere provincies op verschillende onderdelen in de nulmeting nog laag. Bijvoorbeeld op informatiebeveiligingsdoelstellingen en planning, operationele planning en beheersing en monitoring, meten, analyseren en evalueren. Uit beide figuren valt dus af te leiden dat vooral op het onderdeel 'check' van de PDCA-cyclus nog winst te behalen valt. Dit beeld werd in interviews bevestigd. In november 2018 is in opdracht van de provincie door een extern bureau een plan van aanpak opgesteld om te komen tot ISO27001 certificering. Om gecertificeerd te raken moeten ook de 'check' en 'act' activiteiten bewezen worden uitgevoerd.[99]

[99] *Provincie Overijssel (december 2018). Reactie ambtelijk hoor en wederhoor.*

Geen van de provincies voldeed aan alle hoofdstukken van de ISO 27001. Er waren negen provincies die gemiddeld onder de 50% scoorden. De provincie Overijssel scoorde gemiddelde 46%. Zij behoort daarmee tot de middenmoot.

Toezicht en testen externe leveranciers

Beleid externe leveranciers

Wanneer gegevens buiten het netwerk van de provincie staan, eist de provincie dat leveranciers en bewaarders aan de maatregelen van de provincie Overijssel voldoen. Dit moet worden vastgelegd in contracten. In het informatieveiligheidsbeleid staat beschreven dat provincie auditrapporten vraagt aan leveranciers en bewaarders om dit te kunnen monitoren. De provincie Overijssel acht dit noodzakelijk om regie te houden op de uitvoering. De regie willen ze houden door middel van een zogenaamde PDCA-cyclus voor informatieveiligheid en het information security management system (ISMS).

Monitoring op de taken van ONS

Zoals in paragraaf 3.2 aangegeven, is belangrijkste externe dienstverlener voor de provincie ONS. Toezicht op ONS verloopt via rapportages en overleg. In het overleg worden lopende zaken besproken aan de hand van een jaarplan. Ook worden recente ontwikkelingen besproken. Op basis van de input van partners kan de planning van ONS aangepast worden.[100]

Verantwoording vindt plaats via een maandelijkse rapportage van ONS aan de partners.[101] Sinds dit jaar zit daar een paragraaf over informatieveiligheid in, omdat het onderdeel van de SLA is geworden.[102] In interviews wordt aangegeven dat de rapportage over informatieveiligheid voor die tijd beperkt was, maar dat is verbeterd doordat ONS in 2018 heeft ingezet op het neerzetten van de PDCA-cyclus.[103]

De resultaten van een penetratietest worden besproken in het eerdergenoemde breed tactisch overleg (BTO). Verbeteringen die voortkomen uit de penetratietesten pakt ONS grotendeels zelf op. De verbeterpunten worden in Topdesk gezet en met dat systeem kan door ONS ook gekeken worden hoe het met de opvolging staat.[104] Terugkoppeling van opvolging van aanbevelingen van ONS aan de provincie verloopt via het BTO. Uit interviews met de provincie blijkt dat de terugkoppeling verloopt op hoger abstractieniveau. Op detailniveau is de opvolging van aanbevelingen voor de provincie moeilijk te controleren omdat de aanbevelingen daarvoor vaak te technisch van aard zijn. Voor de uitvoering van technische aanbevelingen wordt daarom op de expertise van ONS vertrouwd.[105]

Monitoring van overige externe leveranciers

Naast de diensten van ONS maakt de provincie ook gebruikt van diensten van andere leveranciers. Zo zijn er diverse applicaties ingekocht bij externen. In de uitvraag voor

[100] *Interviews met ONS en ambtelijk medewerkers.*
[101] *ONS (2018) maandrapportage ICT dienstverlening juli/augustus.*
[102] *ONS (2018). Service Level Agreement generiek*
[103] *Interviews met ONS en ambtelijk medewerkers.*
[104] *Interview met ONS.*
[105] *Interview met ambtelijk medewerkers provincie Overijssel.*

applicaties stelt de provincie voorwaarden aan informatieveiligheid. In de praktijk wordt er bij een tweetal applicaties ook gerapporteerd over de uitvoering van informatieveiligheid.[106] In overige gevallen gebeurt dat niet. Eerder in deze paragraaf bleek al dat de wijze waarop de provincie dit vorm wil geven, via het ISMS[107], nog niet opgezet is.

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.
- Informatieveiligheid maakt nog geen deel uit van de P&C-cyclus. Er wordt niet over gerapporteerd in de begroting en de jaarstukken. Wel is in de begroting van 2019 aandacht voor ISO27001 certificering.

Het principe van verplichtende zelfregulering bij de borging van informatieveiligheid door provincie, betekent ook dat er geen sprake is van een vrijblijvend proces en 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 informatieveiligheid 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 aan betrokkenheid van GS, directie en management bij informatieveiligheid. Hierbij is ook de verantwoording richting deze actoren aan bod gekomen. In de kern is hierover aangegeven dat volgens het informatieveiligheidsbeleid eenmaal per jaar kort en bondig gerapporteerd moet worden aan de directie. Dit is in de praktijk niet gebeurd. Structurele rapportage vindt niet plaats. Wel komt informatieveiligheid regelmatig ter sprake in het bedrijfsvoeringsoverleg als onderwerpen daartoe aanleiding geven.[108] In interviews wordt aangegeven dat rapportage aan directie en management nog verbeterd kan worden. Verbetering kan door structureel te gaan rapporteren, los van een expliciete

[106] *Interviews met ambtelijk medewerkers.*
[107] *Provincie Overijssel (2016). Informatiebeveiligingsbeleid.*
[108] *Diverse notities bedrijfsvoeringsoverleggen.*

aanleidingen. Nu gebeurt dit vooral wanneer er bijzonderheden zijn. Ook GS worden vooral betrokken als er aanleiding voor is. Er is geen structurele rapportage aan GS.

In het beleid staat ook dat de directie door procesverantwoordelijken wordt geïnformeerd bij beveiligingsincidenten.[109] Grote incidenten hebben afgelopen periode niet plaatsgevonden.[110]

Provinciale Staten

De verwachting bij ambtelijk medewerkers is dat PS vooral geïnformeerd zullen worden over informatieveiligheid bij incidenten. Deze incidenten zijn er niet geweest. Tabel 6 geeft een overzicht van verantwoording die heeft plaatsgevonden aan PS. In de P&C-cyclus valt informatieveiligheid onder het thema digitalisering: duurzaam toegankelijke informatie. Daar is de afgelopen jaren niet ingegaan op informatieveiligheid. In de begroting van 2019 is voorbeiding van implementatie van de ISO27001 norm een actie. In de accountantsverslagen en de boardletters, die ook naar PS gaan, was wel structureel aandacht voor (aspecten van) informatieveiligheid. Zie voor de inhoudelijke toelichting de vorige paragraaf.

Omdat ONS (de externe dienstverlener) sinds 2018 een Gemeenschappelijke Regeling bedrijfsvoeringsorganisatie is, stuurt ONS haar begroting sinds 2018 naar PS. In de begroting is aandacht voor informatieveiligheid.

Tabel 6: *Informatievoorziening aan Provinciale Staten over informatieveiligheid*

Wat	Onderwerp	Datum
Besluitenlijst GS (PS/2018/350)	Vaststelling 217a-onderzoek en beknopte terugkoppeling conclusie.	8 mei 2018
Begroting ONS (PS/2018/274)	Kaderbrief en concept-programmabegroting ONS	9 april 2018
Besluitenlijst GS (PS/2017/923)	Start 217a-onderzoek naar monitoring en beheersing informatiebeveiliging	27 november 2017
Statenvragen Dhr. Joosten (VVD) (PS/2017/797)	Schriftelijke vragen over Shared Service Centrum - ICT en het Lysias rapport	16 oktober 2017
Lysias rapport (PS/2017/755)	Over problemen toegankelijkheid van informatie, met name bij de gemeenten Kampen en Zwolle, door problemen bij Shared Service Centrum/ONS	28 september 2017
Verzoek Provinciale Staten aan accountant	Verzoek informatieveiligheid één van de drie aandachtspunten te maken bij controle 2016	2016

Bron: samengesteld door de Rekenkamer Oost-Nederland

[109] *Provincie Overijssel (2016). Informatiebeveiligingsbeleid.*
[110] *Interviews met ambtelijk medewerkers.*

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 Overijssel hebben we het volgende normenkader opgesteld:

Tabel 7: *Normen onderzoek informatieveiligheid*

Thema	Norm	Bron
Beleid	• De provincie heeft een beleidskader informatieveiligheid: o dat is vastgesteld op minimaal directieniveau, o maximaal vier jaar oud is en gewijzigd is bij belangrijke ontwikkelingen en o 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. o 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 o 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) • Streefbeeldafsprak en 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 Overijssel in de praktijk voldoende wordt beschermd tegen toegang door onbevoegden. Dit praktijkonderzoek vond in september - oktober 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 spear phishing.

Bijlage 2: Afkortingen en begrippen

Tabel 9: *Gebruikte afkortingen*

Afkorting	Uitleg
AP	Autoriteit Persoonsgegevens
AMT	Afdelingsmanagementteam
BIA	Business Impact Analyse
BIO	Baseline Informatiebeveiliging Overheid
Cibo	Centraal Informatiebeveiligingsoverleg
CMT	Concern managementteam
CSR	Cyber Security Raad
GS	Gedeputeerde Staten
IBI	Interprovinciale Baseline Informatieveiligheid
ICT	Informatie- en Communicatietechnologie
IPO	Interprovinciaal Overleg
IRI	Interprovinciale Regulering Informatieveiligheid
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
ONS	Overheid en Service (externe dienstverlener
P&C	Planning & Control
PDCA	Plan, Do, Check, Act
PS	Provinciale Staten

Tabel 10: 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 door bijvoorbeeld 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. 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
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 3: Bronnenlijst

Geraadpleegde personen

- Mw. Steinprinz, teamleider informatie.
- Dhr. Schaafsma, teamleider faciliteiten.
- Dhr. Hepp, adviseur informatiebeveiliging.
- Dhr. Lammerts van Bueren, Chief Information Security Officer a.i. ONS.
- Dhr. van der Werf, IT-architect ONS.

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 Overijssel 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.
- Zuidelijke Rekenkamer (juli 2018). Bestuurlijke nota en nota van bevindingen informatieveiligheid Limburg.

Provincie Overijssel

- Provincie Overijssel. Accountantsverslagen 2015 t/m 2017.
- Provincie Overijssel. Boardletters 2015 t/m 2017.
- Provincie Overijssel. Procedure windows wachtwoord wijzigen.
- Provincie Overijssel (2012). Notitie bedrijfsvoeringsoverleg procedure account- en wachtwoordwijziging.
- Provincie Overijssel (PS/2013/450). Besluit gemeenschappelijke regeling shared service centrum bedrijfsvoering.
- Provincie Overijssel (2014). Notitie bedrijfsvoeringsoverleg bewustwordingscampagne.
- Provincie Overijssel (oktober 2014). Notitie portefeuilleoverleg.
- Provincie Overijssel (november 2014). Strategisch Informatieplan 2015-2019, informatie voor participatie.
- Provincie Overijssel (2016) proces in-, door-, uitstroom medewerker.
- Provincie Overijssel (2016). Besturings- en managementconcept.
- Provincie Overijssel (2016). Notitie bedrijfsvoeringsoverleg proces datalekken.
- Provincie Overijssel (2016). Procesplaat meldplicht datalekken.
- Provincie Overijssel (maart 2016). Memo risicoanalyse 2015.
- Provincie Overijssel (februari 2016). CMT extract informatiebeveiligingsbeleid.
- Provincie Overijssel (2016). Informatiebeveiligingsbeleid deel 1, 2, 3, en 4.
- Provincie Overijssel (2017). Beweerkersovereenkomst ONS.
- Provincie Overijssel (2017), Eenheid bedrijfsvoering, werkplan 2018.
- Provincie Overijssel (november 2017). Business Impact Analyse, procedure en handleiding.
- Provincie Overijssel en provincie Friesland (2017), interprovinciale informatiebeveiligingsaudit conform IBI 2.0.
- Provincie Overijssel (2017 en 2018). Rapporten 1e en 2e phishing-linkactie.
- Provincie Overijssel (2018), awareness campagne 2017/2018.
- Provincie Overijssel (2018). Besluitenlijst Gedeputeerde Staten 8 mei 2018.
- Provincie Overijssel, Concerncontrol (2018). Art. 217a onderzoek beheersing informatiebeveiliging.
- Provincie Overijssel (2018). Rapportage Mystery Guest actie.

Documenten ONS

- ONS (2016) Servicecatalogus ONS-ICT.
- ONS (2017). Beleidsplan informatiebeveiliging Shared Service Centrum ONS Zwolle 2016-2021.
- ONS (2017) Dossier Afspraken & Procedures.
- ONS (2017 en 2018). Rapportage penetratietesten.
- ONS (2018). Informatieveiligheid & privacy. Programmaplan 2018-2021. Jaarplan 2017.
- ONS (2018). Strategisch beleid informatieveiligheid & privacy.
- ONS (2018). Concernarchitectuur informatieveiligheid & privacy.
- ONS (2018). Information security Management System.
- ONS (2018). Rollen en profielen voor informatieveiligheid en privacy.
- ONS (2018). Service Level Agreement 2018.

Websites

- www.autoriteitpersoonsgegevens.nl/
- www.cip-overheid.nl
- www.forumstandaardisatie.nl
- Intranet Provincie Overijssel