Rekenkamer
OOST-NEDERLAND

Informatieveiligheid

Onderzoeksplan

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 en de heer ir. T.J.A. Gies. De secretaris-directeur is mevrouw drs. S.W. Mathijssen RO.

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

Foto voorkant afkomstig van vl-nieuws.nl.

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

Onderzoeksplan

Deventer, juni 2019

Inhoudsopgave

1 Inleiding[1]

In dit eerste hoofdstuk beschrijven we de aanleiding voor en achtergrond bij het onderzoek naar informatieveiligheid. Ook benoemen we de focus van het onderzoek.

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.[2] 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 Wet Bescherming Persoonsgegevens, de Archiefwet en de Meldplicht datalekken. 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

[1] *Voor dit onderzoeksplan is gebruik gemaakt van de onderzoeksopzet van collega provinciale rekenkamers.*
[2] *Cibo en IPO (2010). Interprovinciale Baseline Informatiebeveiliging 1.0, p. 4.*

ervoor[3]. Ook uit onderzoeken van rekenkamers bleek dat de informatieveiligheid bij meerdere gemeenten en provincies nog te wensen overlaat. Dit is voor ons de aanleiding om het thema informatieveiligheid op te nemen in het onderzoeksprogramma 2018.

1.2 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.[4] 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.

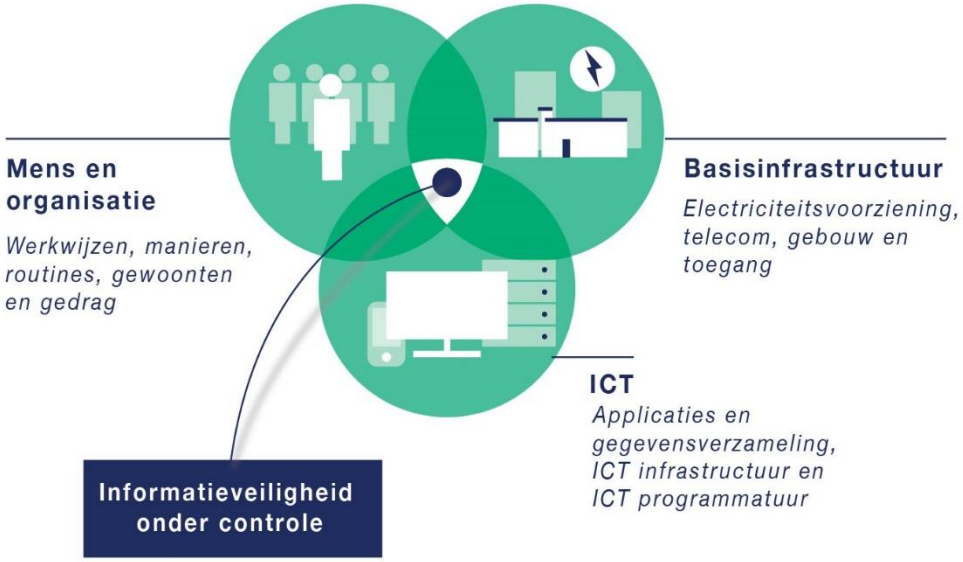
Informatieveiligheid richt zich op bescherming van informatie om de continuïteit van bedrijfsactiviteiten te waarborgen.[5] Als de informatieveiligheid onvoldoende is gewaarborgd, kunnen er risico's ontstaan bij de uitvoering van provinciale taken en het functioneren van de organisatie. De maatregelen 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 (de 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 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. [6]

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] *Nieuwsbericht Autoriteit Persoonsgegevens van 29 maart 2018.*
[4] *Cibo en IPO (feb. 2016). Interprovinciale baseline informatieveiligheid versie 2.0, p. 4.*
[5] *Cibo en IPO (2010). Interprovinciale Baseline Informatiebeveiliging 1.0.*
[6] *Combinatie van Cibo en IPO (feb. 2016). Interprovinciale baseline informatieveiligheid versie 2.0, p. 4 en Randstedelijke Rekenkamer (2015). Onderzoeksopzet, p. 6.*

Figuur 1: *Aandachtsgebieden van informatieveiligheid*



Bron: Interprovinciale Baseline Informatieveiligheid, bewerking Randstedelijke Rekenkamer & 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.[7]

Relevante ontwikkelingen

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

Figuur 2: *Tijdlijn relevante initiatieven verbetering informatieveiligheid provincies*

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

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.[8] 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: (1) sturing en verantwoordelijkheid, (2) beleid en normenkader, (3) verantwoording en toezicht en (4) 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 is afgesproken dat het Cibo zorgt draagt 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.

1.3 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.

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

2 Onderzoeksopzet

In dit hoofdstuk beschrijven we de opzet van ons onderzoek. Daarbij komen doel- en vraagstelling, het normenkader en onderzoeksmethodiek aan de orde. Ook geven we de planning van het onderzoek weer.

2.1 Doel- en vraagstelling

Doelstelling

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

De centrale vraag van dit onderzoek luidt als volgt:

> *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?

2.2 Normenkader

Tijdens de eerste fase van het onderzoek wordt een normenkader opgesteld. De normen baseren we op ISOO27001 en voor zover (nog) relevant het Convenant Interprovinciale Regulering Informatieveiligheid, de Interprovinciale Baseline Informatieveiligheid 2.0 en het concept van Baseline Informatiebeveiliging Overheid (zie paragraaf 1.2.2).

2.3 Onderzoeksmethodiek

In tabel 1 beschrijven we de aanpak voor de beantwoording van de vier onderzoeksvragen.

Tabel 1: *Werkwijze onderzoek informatieveiligheid per onderzoeksvraag*

Vraag	Werkwijze
1.	We gaan onder andere na 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 analyseren het beleidskader informatieveiligheid (vraag 2a) en gaan na hoe er in de praktijk invulling wordt gegeven aan dit beleid (2b). Voor het beantwoorden van vraag 2c worden de waarborgen voor het beschermen van informatie voor toegang door onbevoegden door een externe partij onderzocht.
3.	We analyseren (de uitvoering van) het bewustwordingsprogramma en andere activiteiten die mogelijk worden ondernomen om bewustwording van informatieveiligheid te bevorderen. Ook dit zal de externe partij in de praktijk onderzoeken.
4.	We gaan na of informatieveiligheid een plek heeft in de P&C-documenten en of een onafhankelijke toets en zelfevaluatie wordt uitgevoerd.

Door de provincies wordt ook onderzoek gedaan naar informatieveiligheid. Deze onderzoeken nemen we – voor zover mogelijk - mee in ons onderzoek om dubbelwerk te voorkomen.

2.4 Planning

Ons onderzoek kent een aantal vaste stappen[9]. De globale planning van deze stappen voor dit onderzoek naar de provinciale informatieveiligheid vindt u in tabel 2.

Tabel 2: *Globale planning onderzoek informatieveiligheid*

Fase	Periode
Informatie verzamelen en analyseren	Juli - oktober 2018
Rapportage	November - december 2018
Afronding	Januari 2019

Voor het realiseren van deze planning zijn wij afhankelijk van een tijdige aanlevering van materiaal door de provincies.

2.5 Slotopmerkingen

- Deze onderzoeksopzet is opgesteld op basis van een globale verkenning van het onderwerp. Op basis van het verzamelde onderzoeksmateriaal kan de aanpak gedurende het onderzoek worden bijgesteld. Als deze bijstelling naar ons oordeel tot majeure aanpassingen van de opzet leidt, zal dit door ons worden gecommuniceerd.
- De Rekenkamer deelt aan PS en GS alle opmerkingen en bedenkingen mee die wij naar aanleiding van onze bevindingen van belang achten. Ook als dit niet expliciet onderdeel is van de onderzoeksopzet.
- Voor de uitvoering van het onderzoek is de Rekenkamer bevoegd alle documenten van het provinciebestuur op te vragen en mee te nemen in het onderzoek. Het provinciebestuur verstrekt desgevraagd alle inlichtingen die de Rekenkamer ter vervulling van haar taak nodig acht.[10]

[9] *Zie het volledige onderzoeksprotocol op onze website www.rekenkameroost.nl*
[10] *Artikel 184 Provinciewet.*

Bijlage 1: Geraadpleegde bronnen

Geraadpleegde bronnen

- Autoriteit Persoonsgegevens (2018). Nieuwsberichten.
- Cibo en IPO (september 2010). Interprovinciale Baseline Informatieveiligheid (versie 1.0).
- Cibo en IPO (september 2014). Convenant Interprovinciale Regulering Informatieveiligheid.
- Cibo en IPO (februari 2016). Interprovinciale Baseline Informatieveiligheid (versie 2.0).
- Follow The Money (2017, 23 oktober). Mailen uit naam van Mark Rutte? Geen probleem.
- NRC Handelsblad. (2017, 28 maart). Tweede Kamer getroffen door gijzelingssoftware.
- Randstedelijke Rekenkamer (september 2015). Onderzoeksopzet Informatiebeveiliging.
- Randstedelijke Rekenkamer (juli 2016). Eindrapporten Informatieveiligheid Flevoland, Noord-Holland, Zuid-Holland en Utrecht.
- Zuidelijke Rekenkamer (november 2017). Startnotitie informatieveiligheid van de provincies Limburg en Noord-Brabant.

Geraadpleegde websites

- (archief van) website Taskforce Bestuur en Informatieveiligheid Dienstverlening: http://taskforcebid.archiefweb.eu/#archive
- Website Randstedelijke Rekenkamer over onderzoek informatieveiligheid: http://www.randstedelijke-rekenkamer.nl/onderzoek/informatieveiligheid/
- Website Zuidelijke Rekenkamer over onderzoek informatieveiligheid: http://www.zuidelijkerekenkamer.nl/802/onderzoek/informatieveiligheid-noord-brabant-en-limburg.html