Rekenkamer
OOST-NEDERLAND

In veilige handen?

Bestuurlijke nota informatieveiligheid Gelderland

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) 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 dhr. 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

De foto is afkomstig van Freepik via Catalyst Computers.

Rekenkamer
OOST-NEDERLAND

In veilige handen?

Bestuurlijke nota informatieveiligheid Gelderland

Deventer, februari 2019

Voorwoord

Digitalisering levert voordelen op voor burgers, ondernemers en overheden. Zo is het via internet aanvragen van een subsidie of een vergunning toch een stuk makkelijker dan alles op papier invullen, kopiëren en per post opsturen. Deze digitalisering kent echter ook een keerzijde door de steeds grotere en groeiende impact van incidenten. Incidenten zoals gehackte mailadressen, het verlies van USB-sticks met vertrouwelijke informatie, aanvallen op websites en verstoringen of zelfs uitschakeling van computersystemen.

Incidenten hebben al lang niet meer alleen technische of financiële gevolgen. Incidenten hebben de potentie om het imago van een overheid flink te raken en daarmee het vertrouwen van burgers in diezelfde overheid. Ze stellen de veiligheid, reputatie en zelfs de continuïteit van organisaties op de proef. Veel van de kwetsbaarheden zijn op te lossen met maatregelen. Uit ons onderzoek blijkt dat de provincie op het gebied van de systemen, netwerken en de bewustwording van medewerkers maatregelen heeft getroffen om het aantal kwetsbaarheden te beperken. Dat is goed nieuws want dat blijkt ook wel eens anders te zijn.

Het beheersen van informatieveiligheid stelt bestuurders voor nieuwe uitdagingen. Uitdagingen die verder strekken dan alleen maatregelen, maar die actieve betrokkenheid vergen van management en bestuur. Op dit punt scoort de provincie Gelderland minder goed. Gedeputeerde Staten hebben vooral aandacht voor incidenten en veel minder voor de informatieveiligheid als geheel. Ook Provinciale Staten krijgen nauwelijks informatie over het onderwerp. Vanwege de grote impact die beveiligingsincidenten kunnen hebben, is het van belang dat zowel GS als PS zich ervan vergewissen dat er binnen de organisatie voldoende aandacht is voor het thema. Informatieveiligheid is namelijk geen ‘bedrijfsvoeringdingetje’ waar alleen een afdeling Informatievoorziening & Automatisering zich mee bezig hoeft te houden.

Voor dit onderzoek hebben we ethisch hackers van Hoffmann ingeschakeld. Dit kon niet zonder medewerking van enkele personen binnen de provincie. Wij danken hen voor de open houding en het vertrouwen.

Namens de Rekenkamer Oost-Nederland,

Michael Mekel	Suzan Mathijssen
Voorzitter	*Secretaris-directeur*

Inhoudsopgave

1 Over dit onderzoek

1.1 Aanleiding voor het onderzoek

Informatie is, net als financiën en personeel, essentieel voor het functioneren van de provincie. Veiligheid van informatie is dan ook heel belangrijk. Vooral omdat de provincie werkt met gegevens en informatie van burgers, bedrijven en partners. Zij mogen erop rekenen dat 'hun' gegevens in veilige handen zijn. De provincie heeft daarin een maatschappelijke verantwoordelijkheid richting hen. Beschermt de provincie informatie onvoldoende dan bestaat het risico op het verlies van publiek vertrouwen, aantasting van privacy, fraude, vermindering van productiviteit, onvoorziene kosten, verlies van inkomsten en/of imagoschade. Dit maakt dat informatieveiligheid een politiek-bestuurlijke impact kan hebben.

Uit verschillende incidenten en publicaties in de afgelopen jaren blijkt dat de digitale veiligheid bij overheden een aantal kwetsbaarheden bevatte. Zo bleek in oktober 2017 de e-mail van kabinets- en Kamerleden niet goed beveiligd en waren in januari 2018 verschillende overheidsinstellingen slecht bereikbaar door een cyberaanval. Uit rapportages van de Autoriteit Persoonsgegevens (AP) blijkt dat duizenden datalekken zijn gemeld. En het Nationaal Cybersecurity Center (NCSC) geeft aan dat zij vele honderden cybersecurity incidenten heeft afgehandeld. Ook uit onderzoeken van rekenkamers bleek dat de informatieveiligheid bij meerdere gemeenten en provincies nog te wensen overlaat. Dit was de aanleiding om te onderzoeken hoe het gesteld is met de informatieveiligheid bij de provincie Gelderland.

1.2 Wat is informatieveiligheid?

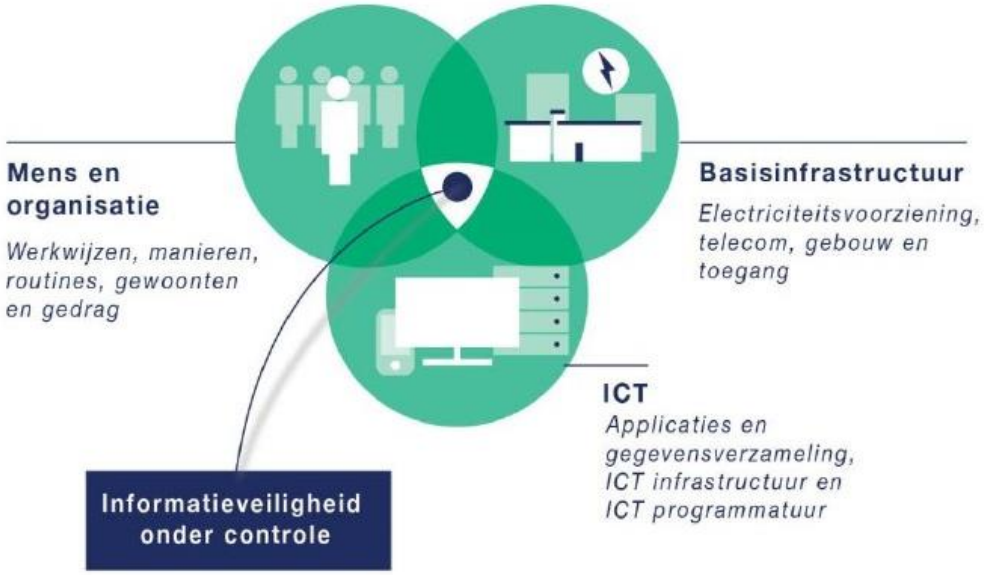
Informatieveiligheid richt zich op bescherming van informatie om de continuïteit van bedrijfsactiviteiten te waarborgen. Als de informatieveiligheid onvoldoende is gewaarborgd, ontstaan er risico's voor uitvoering van provinciale taken en het functioneren van de organisatie. De maatregelen die genomen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

brengen. Het gaat daarbij om het behouden van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie.

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

Om de risico's op schending van of inbreuk op de informatieveiligheid te verkleinen, kan een organisatie op drie verschillende aandachtsgebieden sturen en maatregelen nemen (zie figuur 1).

Figuur 1: *Aandachtsgebieden van informatieveiligheid*



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

Het is belangrijk dat de focus op het geheel van de aandachtsgebieden mens en organisatie, basisinfrastructuur en ICT ligt. Dit is waar de cirkels in figuur 1 elkaar overlappen. Vaak denkt men bij informatieveiligheid direct aan ICT, maar het nemen van technische maatregelen alleen (zoals 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 toegangsbeveiliging van gebouwen en ruimtes of de noodstroomvoorziening) zijn belangrijk.

Kaders informatieveiligheid

De provincie Gelderland beschikt over informatiebeveiligingsbeleid. Daarnaast zijn ook afspraken tussen overheden belangrijk bij informatieveiligheid. Hierbij gaat het bijvoorbeeld om een interprovinciale baseline (2010) en convenant (2014). In 2020 treedt een landelijke baseline in werking. Meer over het Gelderse beleid en de afspraken tussen overheden is te vinden in de Nota van Bevindingen.

1.3 Focus van het onderzoek

Ons onderzoek richtte zich op informatieveiligheid bij de provincie Gelderland in de breedste zin. We hebben aandacht besteed 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. De aan de provincie verbonden partijen behoren niet tot de reikwijdte van het onderzoek.
- Het verzamelen van de gegevens waarop we dit onderzoek baseren, vond plaats in de periode van juli 2018 tot november 2018. De conclusies gaan dus over de situatie in deze periode, tenzij anders aangegeven.
- Met de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) neemt de aandacht voor privacy toe, ook binnen de provincie. Privacy en informatieveiligheid zijn aan elkaar gerelateerde thema's. Voor zover het direct raakte aan informatieveiligheid namen we privacy mee. We onderzochten het echter niet als apart thema.

1.4 Opbouw van dit rapport

In deze bestuurlijke nota geven we de conclusies en aanbevelingen van ons onderzoek naar de informatieveiligheid bij de provincie Gelderland weer. De onderbouwing in de Nota van Bevindingen vindt u op onze website. In bijlage 1 van de Nota van Bevindingen leest u de opzet van het onderzoek.

Dit onderzoek is ook voor de provincie Overijssel uitgevoerd.

2 Conclusies en aanbevelingen

2.1 Hoofdconclusies en aanbevelingen

Hoofdconclusie
De provincie Gelderland treft verschillende effectieve maatregelen voor systemen en netwerken om informatie te beveiligen en schenkt aandacht aan de bewustwording van haar medewerkers. Tegelijkertijd constateren we dat beleid en praktijk op meerdere - soms cruciale - punten niet op elkaar aansluiten. Zo zijn belangrijke controles niet (goed) uitgevoerd. Dit brengt onnodige risico's met zich mee. De beheersing van informatieveiligheid voldoet nog niet op gebied van monitoring en verantwoording.

In de volgende paragrafen werken we de hoofdconclusie in deelconclusies uit met daarbij onze aanbevelingen. Hieronder volgt het totaaloverzicht van de aanbevelingen.

Aanbevelingen

1. Verzoek GS om aandacht te blijven schenken aan het vergroten van de bewustwording van medewerkers rondom informatieveiligheid.
   De provincie zet al in op de bewustwording van medewerkers. De praktijktest onderstreept dat aandacht nodig blijft. Het gaat om aandacht voor de algehele bewustwording van alle medewerkers, maar ook om aandacht voor medewerkers die functies vervullen waarin zij in het bijzonder te maken kunnen krijgen met pogingen tot inbreuk of schending van de informatieveiligheid. Denk aan het beheer van algemene mailadressen.

2. Verzoek GS meer aandacht te besteden aan de borging van het beleid zodat het beleid actueel en de uitvoering in lijn met beleid blijft.
   Dit betekent enerzijds de uitvoering conformeren aan het beleid (bijvoorbeeld het doen van testen) en anderzijds het beleid actualiseren. Bij de actualisatie is het belangrijk om rekening te houden met ontwikkelingen als de AVG en het hele beleid door te lichten op zaken die niet aansluiten op de praktijk. Een deel van de uitvoering

ligt sinds kort bij een externe dienstverlener. Onderdeel van het in lijn brengen van de uitvoering met het beleid is daarmee dat de provincie zicht houdt op nakoming van de gemaakte afspraken. De provincie blijft immers verantwoordelijk voor de informatieveiligheid, ook al ligt de uitvoering deels elders.

3. Verzoek GS de controle op informatieveiligheid te versterken door:
   a. te zorgen voor een goede monitoring waardoor zicht ontstaat op de daadwerkelijke uitvoering van beveiligingsmaatregelen.
   b. regelmatig testen uit te laten voeren om te bezien of de beveiligings-maatregelen in de praktijk voldoende bescherming bieden.

   Om te voldoen aan haar ambitie ('in control zijn') en landelijke afspraken is een goed managementsysteem voor informatieveiligheid van belang. Monitoring van maatregelen is hier een onderdeel van. Ook het uitvoeren van testen is daarvoor belangrijk. Testen bieden zicht op het niveau van beveiliging en/of bewustwording. Daarnaast leggen testen kwetsbaarheden bloot. Zo ontstaat inzicht in de maatregelen waarmee je risico's kunt reduceren. Het is dan ook belangrijk met regelmaat testen te doen. Ook in tijden van verandering moet er zekerheid zijn over dat de informatiebeveiliging op orde is.

4. Verzoek GS verantwoording af te leggen over informatieveiligheid en dat ook binnen de organisatie beter te borgen.
   De verantwoording kan verbeterd worden door afspraken over rapportage aan directie en rapportage via de P&C-cyclus op te volgen. Verantwoording naar directie en bestuur over informatieveiligheid is noodzakelijk vanwege het belang van informatie voor het functioneren en de continuïteit van de provincie en de mogelijk grote gevolgen wanneer die informatie niet voldoende beschermd of gewaarborgd is. Cybercriminaliteit kan een grote politieke-bestuurlijke impact hebben en daarmee is het belangrijk dat PS zich er van vergewissen dat de informatieveiligheid op orde is.

5. Verzoek GS een jaar na de behandeling van dit rapport inzicht te geven in de implementatie van de aanbevelingen.

2.2 Effectieve maatregelen voor systemen en netwerken, aandacht voor bewustwording blijft nodig

Uit de praktijktesten van de systemen en netwerken blijkt dat de provincie meerdere effectieve beschermingsmaatregelen heeft genomen om weerbaar te zijn tegen cyberaanvallen. Het is binnen redelijke termijn niet gelukt om bij de 'kroonjuwelen' te komen noch de rechten van systeembeheer te verwerven.
De provincie schenkt op verschillende manieren aandacht aan het vergroten van de bewustwording rondom informatieveiligheid bij haar medewerkers. De praktijktest onderstreept dat aandacht voor bewustwording nodig blijft.

Het doel van de provincie Gelderland is om met passende maatregelen haar informatie te beschermen en waarborgen. Voor dit onderzoek lieten we testen of de informatie van de provincie in de praktijk voldoende is beschermd tegen toegang voor onbevoegden. Hierbij is er gekeken naar systemen en netwerken (aandachtsgebied ICT) en naar de bewustwording van medewerkers (alle aandachtsgebieden, voornamelijk mens & organisatie).

Effectieve maatregelen voor systemen en netwerken

Uit de test blijkt dat de provincie haar systemen en netwerken met diverse maatregelen beschermt tegen de aanval van een hacker. Deze maatregelen zijn gericht op:

- het voorkomen van een hack (een hacker kan op weinig plekken naar binnen);
- het tijdig signaleren van een hack;
- het beperken van de schade van een hack.

De maatregelen zijn effectief, zo blijkt uit de test. Zo is het niet gelukt om binnen redelijke termijn bij zogenoemde 'kroonjuwelen' te komen. De term kroonjuwelen wordt vaak gebruikt als term om de belangrijkste systemen en processen van een organisatie te beschrijven.[1] Denk hierbij aan het account van de Commissaris van de Koning of gevoelige informatie rondom burgemeestersbenoemingen. Ook lukte het niet om de rechten van systeembeheerder te verwerven. Daarmee krijgt een hacker toegang tot alle systemen en applicaties en kan hij/zij grote schade aanrichten. Uit recent rekenkameronderzoek bleek dit bij verschillende andere provincies wel mogelijk.

Aandacht voor bewustwording blijft nodig

Daarnaast is gekeken hoe het gesteld is met de bewustwording van medewerkers rondom informatieveiligheid. De provincie vergroot de bewustwording actief met bijvoorbeeld workshops, berichten op intranet en het neerleggen van kaartjes bij niet afgesloten computers. Daarnaast maakt de provincie medewerkers via een aantal documenten bekend met hun verantwoordelijkheid bij informatieveiligheid. Denk hierbij aan een eed/belofte, de gedragscode integriteit en de gebruiksvoorwaarden voor mobiele apparaten. Alle geïnterviewden gaven aan dat bewustwording een belangrijk aandachtspunt voor de provincie is. Onlangs is een programma rondom digitale vaardigheden gestart en hierop wil de provincie in de toekomst meer inzetten. Dergelijke activiteiten blijven in de toekomst nodig om de bewustwording op peil te houden. Bovendien blijkt uit de praktijktest dat de bewustwording van medewerkers op fysiek en digitaal gebied een aandachtspunt is:

- Bij de inlooptest kreeg de mystery guest ongeautoriseerd toegang tot niet-publieke ruimtes en beperkte toegang tot dossiers en gegevens. Tijdens zijn bezoek is hij niet opgemerkt of aangesproken.
- Het versturen van spear phishing e-mails[2] leidde tot het verkrijgen van toegang tot accounts en bestanden. Ook werden inloggegevens verkregen.
- Bij een phishing-actie in opdracht van de provincie om de bewustwording van medewerkers te testen, klikte ongeveer vier op de tien medewerkers op de link. Eén derde van de medewerkers vulde zijn of haar inloggegevens in.

[1] *De provincie gebruikt de term kroonjuwelen zelf niet. Zij spreekt voor ICT liever van 'mission critical systems'.*

[2] *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. Spear-phishing is een phishing-variant die gericht is op (een) specifieke (groep) personen.*

Uit de inlooptest blijkt ook dat de fysieke bescherming van de serverruimte geborgd is. Twee van de vijf achtergelaten geprepareerde usb-sticks werden gevonden en adequaat afgehandeld.

Aanbeveling

1. Verzoek GS om aandacht te blijven schenken aan het vergroten van de bewustwording van medewerkers rondom informatieveiligheid.

2.3 Beleid en praktijk sluiten niet op elkaar aan

De afgelopen jaren ging er veel tijd en aandacht naar de uitbesteding van de IT-taken en daardoor minder naar andere zaken rondom informatieveiligheid. Dat zien we ook terug in het beleid en de praktijk die op meerdere - soms cruciale - punten niet op elkaar aansluiten. Enerzijds is het beleid op onderdelen niet uitgevoerd waar dit wel wenselijk is. Zo zijn enkele belangrijke controles niet (goed) gedaan. Anderzijds is het beleid op onderdelen niet actueel. Dit brengt onnodige risico's met zich mee.

De afgelopen jaren besteedde de provincie veel tijd en aandacht aan de uitbesteding van de IT-taken. Dit ging ten kostte van de tijd en aandacht voor andere zaken omtrent informatieveiligheid. Dat zagen we ook terug bij het beleid dat op meerdere - soms cruciale - punten niet is uitgevoerd en op onderdelen niet actueel is.

Beleid op punten niet uitgevoerd

In de praktijk blijkt de provincie haar informatiebeveiligingsbeleid op verschillende punten niet te volgen, terwijl dit wel wenselijk is.

Een aantal belangrijke controles zijn niet (goed) uitgevoerd. Zo testte de provincie tussen 2013 en 2018 de informatieveiligheid op de verschillende aandachtsgebieden (mens & organisatie, ICT en basisinfrastructuur) niet in de praktijk. De accountant wees hier vanuit zijn rol ook al eens op. Als redenen hiervoor noemt de provincie de overgang van IT-taken naar een externe dienstverlener en de verbouwing van het provinciehuis. De provincie vond het niet zinvol om in die periode testen uit te voeren. De Rekenkamer is van mening dat de informatiebeveiliging en het testen daarvan altijd aandacht verdient. *'Als je je huis verbouwt, controleer je toch ook of het slot op de deur wel werkt?'* Testen bieden zicht op het niveau van beveiliging en/of bewustwording. Daarnaast leggen testen kwetsbaarheden bloot. Zo ontstaat inzicht in de maatregelen waarmee je risico's kunt reduceren.

Daarnaast voerde de provincie de afgelopen jaren geen periodieke back-up testen uit. Dit is essentieel om het verlies van informatie te voorkomen. Volgens het Gelderse informatiebeveiligingsbeleid is dit ten minste één keer per jaar nodig. De provincie deed dat in het verleden niet. Met de overgang van de IT-diensten naar een externe

dienstverlener zijn de back-ups ook anders geregeld. Deze nieuwe situatie is wel getest. De provincie sprak met de externe dienstverlener af dat zij de back-up periodiek testen en daarover rapporteren. Het is zaak dat de provincie in de gaten houdt of dit in de praktijk ook gebeurt.

Ook is de controle op het zogenoemde patchen niet optimaal. Patchen is het uitvoeren van updates. Wordt een update niet gedaan, dan kan dit een kwetsbaarheid opleveren die een hacker kan gebruiken om binnen te komen. In het Gelderse informatie-beveiligingsbeleid is er aandacht voor patching en het is een onderdeel van de uitbesteding van de IT-taken. Toch werd bij de praktijktest toegang verkregen tot informatie omdat een beveiligingsupdate niet was toegepast. Het niet volgen van het beleid leidde hier dus tot een kritisch risico in de praktijktest. Dit betekent niet automatisch dat andere patches en updates ook niet zijn gedaan. Wel geeft het aan dat de controle op de daadwerkelijke uitvoering van patches en updates niet optimaal is. Het is voor de toekomst dan ook zaak hier goed op te letten.

Een aantal andere punten die niet conform beleid zijn uitgevoerd:

- Het beleid is niet vastgesteld door de directie maar door het managementteam van de afdeling Informatievoorziening & Automatisering.
- De provincie heeft geen beveiligingsdocumentatiedossier aangelegd en onderhouden waaruit blijkt of kan worden aangetoond dat aan de beveiligingseisen is voldaan.
- De directie ontvangt geen jaarlijkse rapportages over informatieveiligheid.
- Er wordt niet gerapporteerd over informatieveiligheid in de P&C-cyclus.

Bovenstaande punten raken aan de beheersing van informatieveiligheid. Meer hierover in paragraaf 2.4.

Beleid op een aantal onderdelen niet actueel

Het provinciale beleid is tevens op enkele onderdelen niet actueel. Zo staat er niets in het beleid over de (verantwoordelijkheden en taken) van het security team. Dit team bestaat sinds ongeveer vier jaar en houdt zich bezig met operationele zaken op het aandachtsgebied ICT. Het bespreekt bijvoorbeeld de informatiebeveiligingsjaarplannen en testresultaten. Daarnaast heeft de provincie de uitbesteding van een groot deel van de IT-taken nog niet in het informatiebeveiligingsbeleid verwerkt. Formeel zijn deze IT-taken in juli 2017 overgenomen door een externe dienstverlener. De accountant adviseerde eerder al om het informatiebeveiligingsbeleid periodiek te actualiseren en daarbij de nieuwe wet- en regelgeving mee te nemen. De provincie gaf aan van plan te zijn om het beleid na de afronding van de overgang van de IT-taken te actualiseren.

Aanbeveling

2. Verzoek GS meer aandacht te besteden aan de borging van het beleid zodat het beleid actueel en de uitvoering in lijn met beleid blijft.

2.4 Beheersing informatieveiligheid voldoet nog niet

De beheersing van de informatieveiligheid bij de provincie voldoet nog niet. Zo is het beleid niet vastgesteld door de directie, was de monitoring van maatregelen de afgelopen jaren beperkt en is er niet structureel verantwoording afgelegd aan directie en bestuur.

Een manier om te laten zien dat de beheersing van informatieveiligheid op orde is, betreft certificering. Zo is de ISO 27001-standaard gericht op het aantoonbaar beheersen en managen van informatiebeveiliging. De provincie heeft nog niet op bestuurlijk niveau besloten dat zij het ISO 27001-certificaat wil halen, maar er is in inter-provinciaal verband wel op ambtelijk niveau besloten dat men klaar wil zijn voor certificering. Dit sluit aan bij de algemene ambitie zoals die in Gelderse beleid is geformuleerd: 'in control' zijn bij informatieveiligheid. Monitoring en verantwoording zijn belangrijke onderdelen van het in control zijn. Het gevolg geven aan verbeterpunten op deze twee onderdelen is niet alleen nodig om de ambitie meer te realiseren, maar ook om te gaan voldoen aan landelijke afspraken.

Monitoring van maatregelen beperkt

De provincie Gelderland noemt informatieveiligheid een continu verbeterproces en geeft aan dat de 'plan, do, check, act'-methodiek het managementsysteem van informatiebeveiliging vormt. Vorig jaar is een externe nulmeting naar het managementsysteem voor informatieveiligheid uitgevoerd. Hieruit kwam dat er verschillende verbeterpunten waren. Deze lagen vooral op het onderdeel 'check'.
Wij zagen in ons onderzoek dat de monitoring van maatregelen de afgelopen jaren beperkt was. Er was geen totaaloverzicht van de stand van zaken en voortgang van de maatregelen uit het beleid. Daarnaast werd de naleving van de aanvullende maatregelen (Business Impact Analyses)[3] niet standaard gevolgd. Het is belangrijk om dit te verbeteren om informatieveiligheid meer te gaan beheersen. Dit geldt ook voor het uitvoeren van testen waarover we in de vorige paragraaf al constateerden dat de provincie dit niet heeft gedaan tussen 2013 en 2018.

Voor informatieveiligheid is de provincie in de uitvoering in grote mate afhankelijk van externe leveranciers. Zij blijft eindverantwoordelijk voor informatieveiligheid. Daarom is het van belang om de dienstverlening van leveranciers te monitoren en beoordelen. Dit is ook onderdeel van de landelijke afspraken. Het is nog te vroeg om te beoordelen in hoeverre de provincie Gelderland haar IT-dienstverlener adequaat monitort. Deze taken worden namelijk pas sinds kort extern uitgevoerd. Wel zagen we dat er in de aanbesteding aandacht was voor monitoring, testen en verantwoording. Bij andere externe leveranciers houdt de provincie er geen goed zicht op dat zij audits aanleveren.

[3] *Het doel van een Business Impact Analyse is om tot een classificatie van de gegevens en/of processen te komen. Daarvoor wordt nagegaan hoe groot de schade is die geleden zou worden als de integriteit, vertrouwelijkheid of beschikbaarheid van betreffend proces en gegevens geschonden zou worden. Na de Business Impact Analyse worden soms naar eigen inzicht (maatwerk) aanvullende maatregelen bepaald.*

Wel eist en wenst de provincie bepaalde certificeringen die aantonen dat de betreffende dienstverlener informatieveiligheid in control heeft.

Aanbeveling

3. Verzoek GS de controle op informatieveiligheid te versterken door:
   a. te zorgen voor een goede monitoring waardoor zicht ontstaat op de daadwerkelijke uitvoering van beveiligingsmaatregelen.
   b. regelmatig testen uit te laten voeren om te bezien of de beveiligings-maatregelen in de praktijk voldoende bescherming bieden.

Geen structurele verantwoording aan directie en bestuur

Informatie is een basisvoorwaarde voor het functioneren en de continuïteit van een overheidsorganisatie. Dit geldt ook voor de veiligheid van die informatie. Burgers, bedrijven en overheidspartners moeten er op kunnen rekenen dat hun gegevens veilig zijn bij de provincie. Inbreuken op de informatieveiligheid kunnen bovendien leiden tot financiële en/of imagoschade, bijvoorbeeld wanneer gevoelige informatie in verkeerde handen valt of een cyberaanval de organisatie raakt. Informatieveiligheid kan daardoor een politiek-bestuurlijke impact hebben. Daarom is bestuurlijke betrokkenheid bij informatieveiligheid essentieel.

Uit ons onderzoek blijkt dat er in de afgelopen jaren geen sprake was van structurele verantwoording aan directie en bestuur.

- *De directie* ontvangt geen periodieke rapportages over informatieveiligheid, zoals wel staat in het beleid. In overleg met de directie is afgesproken dat zij informatie ontvangen bij incidenten, uitkomsten van praktijktesten of via gerelateerde projecten (bv. AVG).
- *Gedeputeerde Staten* laten zich niet regelmatig informeren over de stand van zaken van de informatieveiligheid. Zij worden alleen geïnformeerd bij een incident zoals een datalek.
- *Provinciale Staten* krijgen geen informatie over informatieveiligheid via de P&C-cyclus terwijl dit wel in landelijke afspraken staat. Hierdoor kunnen PS hun controlerende rol niet invullen.

De provincie gaf aan dat zij haar wijze van verantwoorden in 2019, na afronding van de overgang van de IT-taken, wil herzien.

Tot slot bleek uit het onderzoek dat het managementteam van de afdeling Informatievoorziening & Automatisering van de provincie Gelderland het beleid vaststelde. Dit is niet in lijn met landelijke afspraken. Daarin staat namelijk dat de directie cq de leiding van de organisatie dit moet vaststellen.

Aanbeveling

4. Verzoek GS verantwoording af te leggen over informatieveiligheid en dat ook binnen de organisatie beter te borgen.

3 Reactie GS en nawoord

3.1 Reactie GS Gelderland

Wij ontvingen uw rapport “Bestuurlijke nota informatieveiligheid Gelderland” en de bijbehorende bestuurlijke brief. In het rapport zijn de door u gesignaleerde bevindingen opgenomen over de maatregelen en beleid rondom informatiebeveiliging.

Het rapport van bevindingen is zeer feitelijk van aard en geeft ons inziens een getrouw beeld van de huidige situatie en inrichting van onze informatiebeveiliging en van de (ontwikkel) fase waarin dit zich bevindt. In zijn algemeenheid kunnen wij ons vinden in de constateringen die u hebt opgenomen in het rapport. Wij zijn verheugd te vernemen dat onze maatregelen als totaal een adequaat niveau van beveiliging hebben laten zien. Het is een uitdaging voor de provincie om adequaat te digitaliseren, dit om als overheid bij de tijd te blijven. Digitalisering is de bredere context waarbinnen informatieveiligheid een uitermate belangrijk thema is. Wij onderschrijven dan ook uw aanbevelingen. Het belang van digitalisering/informatieveiligheid is van dien aard dat wij er voor willen zorgen dat de verantwoordelijkheid hiervoor breder gedragen wordt, met name ook door de hele ambtelijke top.

In uw rapport hebt u een aantal aanbevelingen opgenomen. Deze hebben wij hieronder genoemd en daaraan onze reactie toegevoegd.

1. *Verzoek GS om aandacht te blijven schenken aan het vergroten van de bewustwording van medewerkers rondom informatieveiligheid.*

Reactie: Het vergroten van het bewustzijn over informatiebeveiliging is een blijvend aandachtspunt, hier worden elk jaar diverse acties voor opgezet, altijd doelgroepgericht en de actualiteit als achtergrond. Daarnaast is het creëren van bewustzijn ook een vast onderdeel van het introductieprogramma voor nieuwe medewerkers.

2. *Verzoek GS meer aandacht te besteden aan de borging van het beleid zodat het beleid actueel en de uitvoering in lijn met beleid blijft.*

Reactie: Wij onderschrijven het belang van een actueel beleid, wij kiezen ervoor om gezamenlijk met andere provincies in de komende maanden te komen tot een nieuw standaard beleid. Hierin worden actuele thema's als AVG, werken in de Cloud en Internet of Things uiteraard ook meegenomen. Het samen optrekken met de andere provincies zal er voor zorgen dat de overheden in deze gelijkwaardig zijn, het zelfde opereren, wat gezien de open netwerksamenleving sowieso aan een beter geborgde informatieveiligheid zal bijdragen.

Om onze informatiebeveiliging op een gewenst niveau te krijgen zal provincie Gelderland zich aansluiten op een interprovinciaal initiatief om binnen enkele jaren te gaan voldoen aan de ISO 27001 standaard voor informatiebeveiliging. Dit sluit ook aan op de verplichting te moeten gaan voldoen aan de Baseline Informatiebeveiliging Overheid (BIO). De borging van informatiebeveiligingsbeleid is een fundamenteel onderdeel van de ISO 27001 methodiek en zal daarmee in de komende jaren worden ingevuld.

3. *Verzoek GS de controle op informatieveiligheid te versterken door:*
   a. *te zorgen voor een goede monitoring waardoor zicht ontstaat op de daadwerkelijke uitvoering van beveiligingsmaatregelen.*
   b. *regelmatig testen uit te laten voeren om te bezien of de beveiligings-maatregelen in de praktijk voldoende bescherming bieden.*

Reactie: Het gaan voldoen aan de ISO 27001 standaard zal gaan zorgen voor een permanent actueel beeld over de uitvoering van onze beveiligingsbeleid. Over de voortgang van dit traject zal GS gaan rapporteren. Met onze ICT leverancier wordt gewerkt om naast het uitvoeren van maatregelen op het gebied van informatiebeveiliging ook structureel testen uit te voeren op de werking van deze maatregelen.

De monitoring op de werking van informatiebeveiliging en de daarbij behorende maatregelen zullen onderdeel gaan worden van de PDCA cyclus waarover zal worden gerapporteerd. Om dit ook praktisch te toetsen wordt er naast testen vanuit de accountant en de Auditdienst Rijk ook regelmatig gebruik maakt van penetratie testen door derden. De daar gevonden bevindingen zullen leiden tot verbeteringen op, of de implementatie van nieuwe, maatregelen.

4. *Verzoek GS verantwoording af te leggen over informatieveiligheid en dat ook binnen de organisatie beter te borgen.*

Reactie: De verantwoordingscyclus zal dit jaar worden herzien en in lijn worden gebracht met geldende standaarden. Hierbij is het van belang dat het nieuwe informatiebeveiligingsbeleid zal worden vastgesteld door GS.

Op grond van betere monitoring zullen we in staat zijn om een regelmatige rapportage aan bestuur en directie te realiseren. Daarnaast willen we via bewustwording bewerkstelligen dat de verantwoording voor de informatieveiligheid breder gedragen wordt, met name door het ambtelijk management.

5. *Verzoek GS een jaar na de behandeling van dit rapport inzicht te geven in de implementatie van de aanbevelingen.*

Reactie: Wij zullen deze aanbeveling uitvoeren.

3.2 Nawoord Rekenkamer

De Rekenkamer dankt het College van Gedeputeerde Staten voor de reactie op het onderzoek ‘In veilige handen?’. GS gaan vooral in op de aanbevelingen, welke ze onderschrijven. Hieruit leiden wij af dat de conclusies over de tekortkomingen in het beleid en de uitvoering daarvan eveneens worden herkend. Gezien de mogelijke risico’s hiervan roepen we GS op de aanbevelingen voortvarend ter hand te nemen en niet te afwachtend te zijn van landelijke ontwikkelingen bij de uitvoering van het eigen beleid.

Bijlage 1: Bronnenlijst

- Rekenkamer Oost-Nederland (2019). Nota van bevindingen informatieveiligheid Gelderland.
- Baseline Informatiebeveiliging Overheid, versie 1 (juni 2018).
- Cibo en IPO (2016). Interprovinciale Baseline Informatieveiligheid 2.0.
- Randstedelijke Rekenkamer (2015). Onderzoeksopzet Informatieveiligheid.