Rekenkamer
OOST-NEDERLAND

In veilige handen?

Bestuurlijke nota informatieveiligheid Overijssel

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 Overijssel

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 Overijssel 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 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 Overijssel.

1.2 Wat is informatieveiligheid?

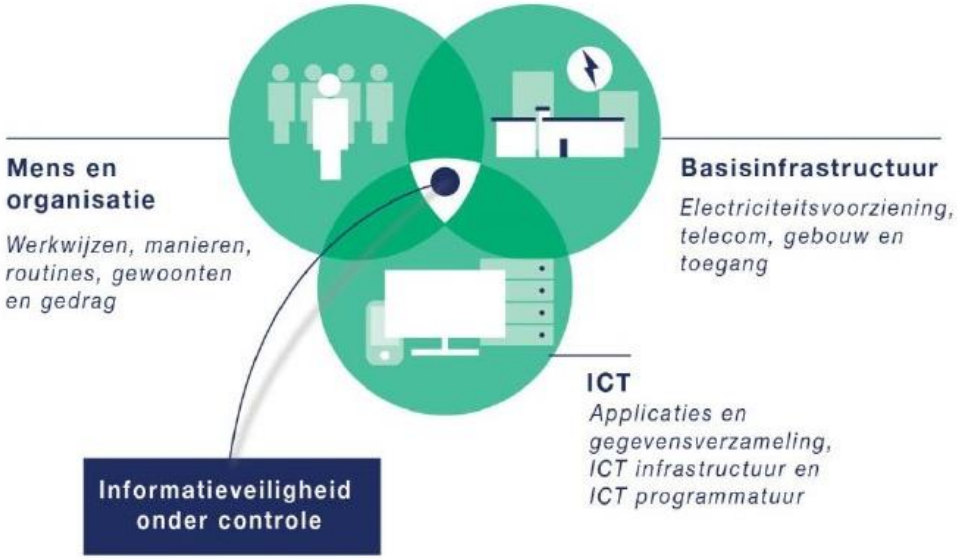
Informatieveiligheid richt zich op bescherming van informatie om de continuïteit van bedrijfsactiviteiten te waarborgen. Als de informatieveiligheid onvoldoende is gewaarborgd, ontstaan er risico's voor uitvoering van provinciale taken en het functioneren van de organisatie. De maatregelen die genomen 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

De provincie Overijssel 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 Overijsselse 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 Overijssel 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 informatieveiligheid bij de provincie Overijssel 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 Gelderland uitgevoerd. Daar waar de vergelijking relevante informatie oplevert, hebben we deze in een groen kader opgenomen.

2 Conclusies en aanbevelingen

2.1 Hoofdconclusie en aanbevelingen

Hoofdconclusie
De provincie 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 het beleid en de praktijk op meerdere - soms cruciale - punten niet op elkaar aansluiten. Zo zijn belangrijke controles niet uitgevoerd. Dit brengt onnodige risico's voor de informatieveiligheid met zich mee. De beheersing van informatieveiligheid voldoet nog niet op gebied van monitoring en verankering in de organisatie.

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 aandacht te blijven schenken aan het vergroten van bewustwording van medewerkers rondom informatieveiligheid. Besteed hierbij extra aandacht aan medewerkers die werken met vertrouwelijke informatie.
   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, bijvoorbeeld medewerkers die verantwoordelijk zijn voor 'kroonjuwelen' of voor het beheren van algemene provinciale e-mailadressen.

2. Verzoek GS meer aandacht te besteden aan de borging van het beleid zodat de uitvoering in lijn met het beleid is en het beleid actueel en volledig blijft.
Dit betekent enerzijds de uitvoering conformeren aan het beleid en anderzijds het beleid actualiseren en aanvullen, bijvoorbeeld met beleid voor patching. Bij de actualisatie is het belangrijk het hele beleid door te lichten op zaken die niet aansluiten op de praktijk.

3. Verzoek GS vaart te maken met de implementatie van een Information Security Management System. Besteed daarbij in ieder geval aandacht aan de onderdelen 'check' en 'act' uit de Plan-do-check-act-cyclus.
Door met name de structurele monitoring (check) te verbeteren en het opvolgen van verbetermaatregelen (act) te bewaken, kan informatieveiligheid beter beheerst worden.

4. Verzoek GS regie te houden op informatieveiligheid door dit bij (externe) dienstverleners actief te (laten) controleren en de opvolging te monitoren.
Vanuit haar rol mag verwacht worden dat de provincie een vinger aan de pols houdt en periodiek laat testen of de informatieveiligheid in de praktijk op orde. Het is van belang dat de provincie bij externe dienstverleners ook zelf opdrachtgever is voor dergelijke testen dan wel als bestuur (van de bedrijfsvoeringsregeling) de opdracht geeft.

5. 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.

6. Verzoek GS de capaciteit en verankering van informatieveiligheid in de organisatie in overeenstemming te brengen met de ambities.
Voor blijvende inzet op bewustwording, uitvoering en doorontwikkeling van het beleid, monitoring en het realiseren van ambities is extra inzet nodig. Dit betekent zowel voldoende menskracht als een specialistische rol binnen de organisatie. Daarbij kan in aansluiting op de Baseline Informatiebeveiliging Overheid gedacht worden aan een (chief) information security officer. Op dit moment kent de provincie een dergelijke functie niet.

7. 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 informatieveiligheidsbeleid is met de juiste maatregelen de risico's beheersen en een afgesproken beveiligingsniveau realiseren. Om te testen of informatie bij de provincie Overijssel in de praktijk voldoende wordt beschermd tegen toegang door onbevoegden, zijn praktijktesten uitgevoerd. 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

De provincie heeft haar ICT in de praktijk over het algemeen goed beveiligd. De provincie heeft meerdere effectieve beschermingsmaatregelen genomen om weerbaar te zijn tegen cyberaanvallen. Deze maatregelen zijn bijvoorbeeld gericht op:

- het voorkomen van een hack (een hacker kan op weinig plekken naar binnen);
- moderne systemen en antivirusprogramma's waardoor de beveiliging goed is;
- het beperken van de schade van een hack, als het wel gelukt is om binnen te komen.

De maatregelen zijn effectief, zo blijkt uit de test. Zo is het via deze test niet gelukt om binnen redelijke termijn tijd bij zogenoemde 'kroonjuwelen' te komen. De term kroonjuwelen wordt vaak gebruikt als term om de belangrijkste systemen en processen van een organisatie te beschrijven. Bij de kroonjuwelen kan gedacht worden aan ondersteuning van directie en GS stukkenstroom of gevoelige informatie rondom burgemeestersbenoemingen. Deze kroonjuwelen zijn in kaart gebracht. Dit is belangrijk omdat zo passende aanvullende beveiligingsmaatregelen kunnen worden genomen. Voor de kroonjuwelen is door de provincie aangegeven hoe deze beveiligd moeten worden. Het is met praktijktesten van de systemen en netwerken niet gelukt om bij deze kroonjuwelen te komen of om de rechten van de 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

De provincie wil haar medewerkers 'bewust bekwaam' maken op het gebied van informatieveiligheid. Daarvoor organiseerde een bewustwordingscampagne in 2017 en 2018 met verschillende activiteiten: presentaties, lezingen, een quiz en het sturen van

phishingmails. Ook deelde ze informatie via intranet met medewerkers om hen bekend te maken met informatieveiligheid, zoals het informatieveiligheidsbeleid, wat er gebeurt bij datalekken en praktische tips. Dergelijke activiteiten blijven in de toekomst nodig om de bewustwording op peil te houden. Bovendien blijkt uit de praktijktesten dat de bewustwording van medewerkers op fysiek en digitaal gebied een aandachtspunt is.

- Bij de inlooptest (voorjaar 2018) is ongeautoriseerd toegang verkregen tot niet-publieke ruimtes door met medewerkers mee naar binnen te lopen en toegang tot computersystemen en gegevens verkregen. Ook werd op dezelfde manier toegang verkregen tot de afdeling van Overheid en Service (ONS). Dit is de dienstverlener die een groot deel van de ICT van de provincie beveiligt. Het lukte niet om toegang te krijgen tot de serverruimte.
- Het versturen van spear-phishingmails[1] leidde tot toegang tot accounts, bestanden en inloggegevens. Bij dit type aanval wordt geprobeerd om inloggegevens van medewerkers met een specifieke functie te krijgen, omdat zij toegang hebben tot specifieke vaak vertrouwelijke informatie. Er werd zo toegang verkregen tot een account waarmee kroonjuwelen benaderd konden worden.
- Bij de meest recente phishingtest (voorjaar 2018) klikten 154 mensen op de kwaadaardige link in een van de 1458 verstuurde e-mails. 94 Mensen vulden ook hun inloggegevens in. Deze score is overigens beter dan de gemiddelde score bij vergelijkbare acties bij andere organisaties.

Aanbevelingen

1. Verzoek GS aandacht te blijven schenken aan het vergroten van bewustwording van medewerkers rondom informatieveiligheid. Besteed hierbij extra aandacht aan medewerkers die werken met vertrouwelijke informatie.

2.3 Beleid en praktijk sluiten niet op elkaar aan

Het beleid sluit op meerdere - soms cruciale - punten niet aan op de praktijk. Enerzijds zijn belangrijke controles niet uitgevoerd terwijl dit wel in het beleid staat. Anderzijds is het beleid niet volledig en op onderdelen niet actueel. Dit brengt onnodige risico's met zich mee.

Beleid op - soms cruciale - punten niet uitgevoerd

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

Allereerst voert de provincie een aantal belangrijke controles niet uit zoals deze in het beleid omschreven zijn. De Rekenkamer onderzocht drie essentiële onderdelen van het informatieveiligheidsbeleid. Het gaat om zogenaamde IT-basishygiënemaatregelen: patching (tijdig uitvoeren van updates), toegangsbeheer en back-ups. Voor twee van de

[1] *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.*

drie onderdelen wordt het beleid voor controles niet gevolgd. De provincie beschrijft in haar beleid dat ze de toegangsrechten regelmatig wil controleren en back-ups regelmatig wil testen. In de praktijk doet ze beide niet. Deze zijn overigens bekende aandachtspunten waar de accountant in 2016 al op wees. Het controleren van toegangsrechten kwam ook uit de meest recente zelfaudit (2017) als aandachtspunt naar voren. Een andere controle die de provincie niet uitvoert is de opvolging van Business Impact Analyses. Deze analyse bepaalt of voor applicaties en systemen extra beveiligingsmaatregelen nodig zijn. Voor het beschermen van de 'kroonjuwelen' moeten altijd extra maatregelen genomen worden. Het beleid beschrijft dat de implementatie van deze beveiligingsmaatregelen steekproefsgewijs getest moet worden. Ook dit gebeurt in de praktijk niet. Testen en controles zijn belangrijk omdat ze inzicht geven in het niveau van beveiliging en kwetsbaarheden blootleggen, zodat maatregelen genomen kunnen worden om risico's te reduceren.

Een aantal andere punten die niet conform beleid zijn uitgevoerd:

- Er wordt niet jaarlijks gerapporteerd aan de directie.
- In plaats van in 2016 startte de bewustwordingscampagne in 2017.
- Een zelfaudit is niet jaarlijks uitgevoerd.
- Informatiebeveiliging is nog niet geïmplementeerd in de Planning & Control cyclus en een Information Security Management System is nog niet gerealiseerd. De provincie beschrijft in het beleid van 2016 dat ze zo regie wil houden op informatieveiligheid. Hierover meer in paragraaf 2.4.

Beleid op onderdelen niet volledig en actueel

Het beleid dat het CMT in 2016 vaststelde, blijkt op onderdelen niet volledig. Op een groot aantal plekken staat dat de verantwoordelijke voor een onderdeel 'nader te bepalen' is. Bovendien zijn in de tekst nog opmerkingen opgenomen die erop duiden dat het document nog niet definitief is. Daarnaast heeft de provincie geen beleid voor patching terwijl dit wel een belangrijke hygiënemaatregel voor bescherming tegen cyberaanvallen is. Wordt een update niet gedaan, dan kan dit een kwetsbaarheid opleveren die een hacker kan gebruiken om binnen te komen.

Daarnaast is het beleid sinds vaststelling in 2016 niet meer geactualiseerd. Terwijl twee onderdelen ervan, een actieplan en monitor, waren bedoeld als levende documenten die jaarlijks geactualiseerd worden. Deze documenten zijn daardoor verouderd. Ook andere onderdelen van het beleid zijn niet meer actueel, zoals een stappenplan voor passende beveiligingsmaatregelen. Dit stappenplan wordt niet gevolgd, omdat de praktische uitvoering van enkele stappen voor de provincie niet noodzakelijk of uitvoerbaar bleken. Tenslotte bleken er verouderde richtlijnen met eisen voor wachtwoorden te circuleren op intranet en binnen de organisatie.

Dat onderdelen van het beleid niet zijn uitgevoerd of geactualiseerd, komt mede door te beperkte personele capaciteit. Op de organisatie van informatieveiligheid gaan we volgende paragraaf verder in.

Aanbevelingen

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

2.4 Beheersing informatiebeveiliging voldoet nog niet

De beheersing van de informatieveiligheid bij de provincie voldoet nog niet. Zo wordt informatieveiligheid wel getest, maar is de structurele monitoring op onderdelen te beperkt en is de verankering van informatieveiligheid in de organisatie niet op alle niveaus goed geregeld.

Een manier om te laten zien dat de beheersing van informatieveiligheid op orde is, betreft ISO27001 certificering. De provincie wil in 2023 gecertificeerd zijn. De ISO27001-standaard bevat eisen waar het managementsysteem voor informatieveiligheid (een Information Security Management System) aan moet voldoen. Bij een goed managementsysteem hoort een Plan-do-check-act (PDCA)-cyclus waarmee je de kwaliteit van informatiebeveiliging verhoogt.

De provincie voldoet op dit moment nog niet aan alle eisen van de IS27001-standaard. Op sommige punten al wel, maar op de meeste moet ze zich nog verbeteren. Al in 2016 wil de provincie regie houden op informatieveiligheid door middel van een Information Security Management System. In 2018 is dit nog niet gerealiseerd. De provincie liet in november 2018 wel een plan van aanpak voor ISO27001 certificering opstellen door externe adviseurs. De Rekenkamer constateert dat nog een aantal belangrijke stappen nodig zijn om de ISO certificering te realiseren. Om informatieveiligheid voldoende te beheersen, kan op dit moment zowel monitoring als verankering van informatieveiligheid in de organisatie verbeterd worden.

Op onderdelen beperkte monitoring

De onderdelen waarop de provincie niet goed scoort, hebben met name betrekking op het onderdeel ‘check’ en ‘act’ van de PDCA-cyclus. Om haar informatieveiligheid beter te beheersen en aan de ambities te voldoen, is het nodig monitoring (check) te verbeteren. De provincie besteedt hier wel aandacht aan, maar dit gebeurt nog niet structureel. Zowel de interne monitoring als monitoring van de externe leveranciers is beperkt.

De provincie liet onlangs wel de informatieveiligheid van de eigen organisatie op verschillende niveaus (mens & organisatie, ICT en infrastructuur) testen. Dit vindt de Rekenkamer positief. Op dit moment vindt structurele interne monitoring echter nog beperkt plaats:

- Enkele belangrijke controles voert de provincie niet uit (bijvoorbeeld voor toegangsbeheer, back-ups en aanvullende maatregelen), zie ook de vorige paragraaf.
- De adviseur informatiebeveiliging monitort beheersmaatregelen. Het instrument waarmee dit gebeurt is verouderd en heeft beperkte mogelijkheden.

- De provincie voert niet jaarlijks een zelfaudit uit om te toetsen of voldaan wordt aan de Interprovinciale Baseline Informatiebeveiliging.
- De provincie monitort niet structureel of opvolging wordt gegeven aan aanbevelingen en verbetermaatregelen worden niet altijd uitgevoerd (act). Uit de praktijktesten kwamen ook kwetsbaarheden naar voren die al bekend waren uit eerder uitgevoerde testen.

Ook de monitoring van (externe) dienstverleners is beperkt, zowel als het gaat om de beheerder van ICT-infrastructuur als beheerders van applicaties. Voor de informatieveiligheid is de provincie in de uitvoering in grote mate afhankelijk van externe leveranciers. De ICT-infrastructuur is belegd bij bedrijfsvoeringsorganisatie Overheid en Service (ONS). In overleggen met ONS komt het onderwerp informatieveiligheid terug. Sinds 2018 rapporteert ONS maandelijks. ONS voert zelf (onafhankelijke) praktijktesten uit en koppelt over opvolging van aanbevelingen terug aan de provincie via ambtelijke overleggen. Voor de uitvoering daarvan vertrouwt de provincie op de expertise van ONS. De provincie kiest er voor om applicaties onder te brengen bij andere externe leveranciers. In die gevallen is informatieveiligheid in de uitbesteding meegenomen, maar wordt meestal niet gemonitord of informatieveiligheid in de praktijk voldoet. De provincie is echter zelf eindverantwoordelijke. Voor het beheersen van informatieveiligheid is goede monitoring van deze leveranciers daarom dus belangrijk. Vanuit haar rol als opdrachtgever mag verwacht worden dat de provincie zelf een vinger aan de pols houdt en ook zelf regelmatig test hoe de informatiebeveiliging in de praktijk verzorgd is.

Aanbevelingen

3. Verzoek GS vaart te maken met de implementatie van een Information Security Management System. Besteed daarbij in ieder geval aandacht aan de onderdelen ‘check’ en ‘act’ uit de Plan-do-check-act-cyclus.
4. Verzoek GS regie te houden op informatieveiligheid door dit bij (externe) dienstverleners actief te (laten) controleren en de opvolging te monitoren.

Verankering informatieveiligheid in organisatie kan beter

Om informatieveiligheid goed te kunnen beheersen, is verankering in de organisatie belangrijk. Dit kan in Overijssel zowel op bestuurlijk als op ambtelijk niveau beter. In de ISO27001-standaard is betrokkenheid van de leiding één van de onderdelen waar aan voldaan moet worden. 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.

De betrokkenheid van het bestuur en de directie bij het thema informatieveiligheid is op dit moment echter beperkt en vooral incidentgedreven. De directie stelde het beleid vast, maar laat zich niet regelmatig informeren over de stand van zaken. Een structurele

verantwoordingsmethodiek is er niet, ondanks dat in het beleid staat dat jaarlijks aan de directie gerapporteerd wordt. Ook het rapporteren over informatieveiligheid in de P&C-cyclus gebeurt niet, terwijl dat dit in 2014 interprovinciaal is afgesproken. PS worden niet structureel geïnformeerd over informatieveiligheid, waardoor zij hun controlerende taak niet kunnen invullen. Informatieveiligheid krijgt op dit moment vooral op niveau van bedrijfsvoering aandacht. In de praktijk liggen de verantwoordelijkheden lager in de organisatie dan in het beleid is beschreven, namelijk bij het Hoofd Bedrijfsvoering, bedrijfsvoeringsoverleg en de teamleider informatie. Het is logisch dat op uitvoeringsniveau de verantwoordelijkheden lager in de organisatie liggen. Maar structurele rapportage aan het bestuur en directie is daardoor extra belangrijk en nodig om bij te kunnen sturen.

Ook op ambtelijk niveau kan de verankering beter. De ISO-standaard vereist dat de organisatie de middelen vaststelt en beschikbaar stelt die nodig zijn voor het inrichten, implementeren, onderhouden en continu verbeteren van het managementsysteem voor informatiebeveiliging. Daar voldoet de provincie op dit moment niet aan. Een adviseur informatie is in de uitvoering de belangrijkste schakel voor informatieveiligheid. Deze rol is niet uitgewerkt in het informatieveiligheidsbeleid, terwijl dit wel verwacht mag worden gezien deze cruciale rol. De provincie kent in de organisatie geen (Chief) Information Security Officer die rechtstreeks aan het management rapporteert. In de praktijk is informatieveiligheid één van de taken van de adviseur. In de vorige paragraaf bleek al dat onderdelen van het beleid niet uitgevoerd of geactualiseerd worden. Daarvoor is beperkte personele capaciteit mede oorzaak. Concerncontrol constateerde al in het voorjaar van 2018 dat de capaciteit voor informatieveiligheid onvoldoende is om de minimale structurele taken uit te voeren en om aan toekomstige ambities te voldoen. Bovendien constateert de Rekenkamer dat de provinciale organisatie kwetsbaar is bij afwezigheid van de adviseur informatie. De provincie heeft per februari 2019 wel een externe adviseur aangesteld die ISO certificering moet vormgeven. Ook moet hij een blauwdruk voor de organisatie voor informatiebeveiliging en PDCA-cyclus op alle bestuursniveaus opstellen.

Vergelijking (Chief) Information Security Officer Gelderland

De provincie Gelderland kent een rol van Information Security Officer. Deze rapporteert direct aan directie en management.

De Informatiebeveiligingsdienst (een gezamenlijk initiatief van alle Nederlandse Gemeenten) concludeert dat een sterke inbedding van informatiebeveiliging in de organisatie vraagt om een Chief Information Security Officer (CISO) met voldoende mogelijkheden om effectief te zijn. Zij adviseren te investeren in de CISO, de CISO strategisch en onafhankelijk binnen de organisatie te positioneren, de CISO voldoende ruimte, mandaat en middelen te geven en bij voorkeur iedere maand bij directie of het bestuur aan tafel te zitten om hen bij te praten (Bron: Informatiebeveiligingsdienst 2018).

Bovendien is in de concept-Baseline Informatiebeveiliging Overheid (BIO) vastgelegd dat een CISO aangesteld moet zijn volgens een CISO functieprofiel. De BIO wordt vanaf 2020 de opvolger van de Interprovinciale Baseline Informatiebeveiliging (IBI). Het wordt een formeel basisnormenkader voor alle overheden en bevat richtlijnen op het gebied van informatieveiligheid.

Aanbevelingen

5. Verzoek GS verantwoording af te leggen over informatieveiligheid en dat ook binnen de organisatie beter te borgen.
6. Verzoek GS de capaciteit en verankering van informatieveiligheid in de organisatie in overeenstemming te brengen met de ambities.

Bijlage 1: Bronnenlijst

- Rekenkamer Oost-Nederland (2019). Nota van bevindingen informatieveiligheid Overijssel.
- Baseline Informatiebeveiliging Overheid, versie 1 (juni 2018).
- Informatiebeveiligingsdienst (2018). Dreigingsbeeld 2019/2020.
- Informatiebeveiligingsdienst (2018). Dreigingsbeeld 2018.
- Cibo en IPO (2016). Interprovinciale Baseline Informatieveiligheid 2.0.
- Randstedelijke Rekenkamer (2015). Onderzoeksopzet Informatieveiligheid.