Luttenbergstraat 2
Postbus 10078
8000 GB Zwolle
Telefoon 038 499 88 99
Fax 038 425 48 88

overijssel.nl
postbus@overijssel.nl

KvK 51048329
IBAN NL45 RABO 0397 3411 21

Inlichtingen bij
mw. M.G. Oosterkamp
telefoon 038 499 90 93
MG.Oosterkamp@overijssel.nl

Provinciale Staten van Overijssel

Datum	Kenmerk	Pagina
19.03.2019	2019/0071680	1 van 4

Onderwerp: Reactie op rapport Rekenkamer Oost-Nederland "In veilige handen?"

Toezending aan Provinciale Staten met oogmerk:
[X] ter informatie
[ ] anders, en wel:

Bijlagen
Geen.

De Rekenkamer Oost Nederland heeft onderzocht of de provincies Overijssel en Gelderland de informatieveiligheid voldoende hebben geborgd. Het onderzoek heeft betrekking op informatieveiligheid in de breedte. De Rekenkamer besteedt aandacht aan het beleid, de organisatie en de praktijk van de provinciale informatieveiligheid. Resultaat van het onderzoek is het rapport "In veilige handen? Bestuurlijke nota informatieveiligheid Overijssel". U ontving dit rapport op 27 februari 2019. Hierbij volgt onze reactie op het onderzoek.

Onderzoeksvraag en conclusie Rekenkamer
De centrale vraag van het onderzoek luidt als volgt:

Hebben de provincies Gelderland en Overijssel de informatieveiligheid voldoende geborgd?

Op basis van de resultaten van het onderzoek komt de Rekenkamer tot de volgende 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.

Naar aanleiding van deze hoofdconclusie heeft de Rekenkamer 3 deelconclusies geformuleerd:

Deelconclusie 1: 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

provincie Overijssel

bewustwording rondom informatieveiligheid bij haar medewerkers. De praktijktest onderstreept dat aandacht voor bewustwording nodig blijft.

Deelconclusie 2: 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.

Deelconclusie 3: 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.

Aanbevelingen Rekenkamer
De 3 hiervoor genoemde deelconclusies leiden tot de volgende aanbevelingen van de Rekenkamer voor uw Staten:

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

Reactie op het rapport
Wij zijn verheugd met de eerste conclusie van de Rekenkamer dat wij effectieve maatregelen hebben getroffen om weerbaar te zijn tegen cyberaanvallen, en dat wij op verschillende manieren aandacht geven aan bewustwording bij de medewerkers. Daarnaast herkennen wij de twee vervolgconclusies en de daaruit voortvloeiende aanbevelingen. De uitvoering van deze aanbevelingen nemen wij ter hand.

In de afgelopen jaren is op interprovinciaal niveau, ook bij de provincie Overijssel, informatieveiligheid opgepakt door pragmatisch aan de hand van best practices concrete maatregelen te nemen om in de uitvoering de informatiebeveiliging goed in te richten. Nu gaan wij de verankering in procedures en beheer verder professionaliseren. Dit doen wij aan de hand van ISO 27001. Wij hebben een ervaren specialist aangetrokken als kwartiermaker informatiebeveiliging. Dit jaar en de jaren daarna geven wij prioriteit aan het werken conform de ISO 27001 norm. Daarvoor maken wij momenteel een roadmap om zo, stap voor stap, de juiste activiteiten op het juiste moment in te plannen. Daarnaast stellen we een blauwdruk voor de informatiebeveiligingsorganisatie op en regelen wij de PDCA cyclus (Plan Do Check Act) voor informatieveiligheid op de verschillende besturingsniveaus.

Interprovinciaal werken wij samen in het Centraal Informatiebeveiligingsoverleg (Cibo). Het Cibo ziet samenwerking niet alleen op provinciaal niveau, maar ook met andere overheidslagen zoals gemeenten, waterschappen en de ministeries BZK, EZK en J&V. Het Cibo houdt ook actief contact met de Informatiebeveiligingsdienst voor gemeenten IBD (het kenniscentrum voor informatiebeveiliging bij gemeenten), en de hiervoor genoemde overheidslagen. In 2019 werken wij binnen het Cibo aan een sjabloon voor een informatiebeveiliging beleidskader.
Het Cibo zet zich in 2019 en de jaren daarna in voor de ondersteuning van de ISO 27001 implementaties bij de provincies. De provincies willen certificeerbaar zijn binnen een termijn van 5 jaar. Onze ambitie is om te onderzoeken of het werken conform de ISO 27001 norm kan leiden tot een certificering.

Alle betrokken overheidslagen (Rijk/ZBO's, provincies, gemeenten en waterschappen) hebben zich gecommitteerd aan een op de Code voor Informatiebeveiliging gebaseerde baseline per sector of

overheidslaag. Voor de provincies is dat momenteel de interprovinciale Baseline Informatiebeveiliging (IBI). De overheden streven gezamenlijk naar een baseline informatiebeveiliging (BIO) die de huidige baselines binnen de overheid vervangt. Dat voornemen wordt ook door de provincie Overijssel gedragen.

Alle aanbevelingen van de Rekenkamer worden met de uitvoering van het plan voor de ISO certificering opgepakt. Wij informeren u over een jaar over de implementatie van de aanbevelingen.

Reactie op de aanbevelingen

Ad 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.
In de roadmap naar het werken conform de ISO27001 norm krijgt bewustwording een prominente plaats. Informatie-veiligheid staat en valt immers met de manier waarop mensen er mee omgaan. Jaarlijks maken we een awarenessplan. Uitvoering doen we door inzet van interne medewerkers en externe gespecialiseerde partijen die onder onze regie de juiste middelen op de juiste momenten inzetten. De samenwerking met het Shared Service Centrum ONS is daarbij belangrijk. Waar mogelijk trekken we gelijk op.

Ad 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.
In 2019 gaan we het informatieveiligheidsbeleid actualiseren. Aansluitend leveren we een informatiebeveiligingsplan op. Dit plan gaan we jaarlijks actualiseren en bijstellen.

Ad 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.
Het implementeren van een ISMS, een managementsysteem voor informatiebeveiliging, is onderdeel van de ISO 27001 certificering. Met een ISMS krijgen we meer grip op control en regie op beveiliging. Een ISMS is een continu verbeterproces, een manier van werken waarbij een systematische aanpak wordt gehanteerd om (vertrouwelijke) informatie te managen. Een ISMS kan leiden tot het aanpassen van de processen en de organisatie rondom informatieveiligheid.

Ad 4: Verzoek GS regie te houden op informatieveiligheid door dit bij (externe) dienstverleners actief te (laten) controleren en de opvolging te monitoren.
Wij geven de komende jaren meer aandacht aan monitoring. In de roadmap nemen wij op hoe we daar het beste invulling aan kunnen geven. We denken momenteel aan risico-gebaseerd controle uitoefenen waarbij de leveranciers op zowel strategisch, tactisch, als operationeel niveau worden gemonitord.

Ad 5: Verzoek GS verantwoording af te leggen over informatieveiligheid en dat ook binnen de organisatie beter te borgen.
We gaan de organisatie van informatieveiligheid aan de hand van een blauwdruk opnieuw inrichten. Daarbij besteden we ook aandacht aan rapportages en het afleggen van verantwoording. De taken, verantwoordelijkheden en bevoegdheden gaan we helder benoemen.

Ad 6: Verzoek GS de capaciteit en verankering van informatieveiligheid in de organisatie in overeenstemming te brengen met de ambities.
In lijn met de blauwdruk gaan we ook de governance van informatieveiligheid herzien. Daarin gaan we rollen en verantwoordlijkheden verder uitwerken alsook de capaciteit die daarvoor nodig is.

Ad 7: Verzoek GS een jaar na de behandeling van dit rapport inzicht te geven in de implementatie van de aanbevelingen.
Wij informeren u een jaar na behandeling van de bestuurlijke nota over de implementatie van de aanbevelingen.

Gedeputeerde Staten van Overijssel,

voorzitter,

secretaris,