Provinciale Staten

Financiële consequenties externe inhuur:
Kostensoort: n.v.t.
Bedrag: n.v.t.

Financiële consequenties opdracht/uitbesteding:
Kostensoort: n.v.t.
Bedrag: n.v.t.

Gedeputeerde belast met behandeling: drs. J.M.M. Polman

Vergadering PS: 17 november 2023
Nr: 370669
Agenda nr:
Vergadering GS: n.v.t.
Nr: 370669

Onderwerp: Rekenkamerrapport Cyberveiligheid

Aan de Provinciale Staten van Zeeland

Samenvatting

De Rekenkamer Zeeland heeft onderzoek gedaan op het terrein van cyberveiligheid. De Rekenkamer verstaat onder cyberveiligheid het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT en, indien er toch schade is ontstaan, het herstellen van de schade. In een brief heeft de rekenkamer de analyse van de onderzoeksresultaten samengevat. De Rekenkamer geeft een aantal concrete aanbevelingen aan Provinciale Staten om de cyberveiligheid van Provinciale informatie en dienstverlening verder te versterken.

De Rekenkamer beoogt met dit onderzoek bij te dragen aan de kaderstellende en controlerende rol van Provinciale Staten waar het gaat om cyberveiligheid. Dit is gedaan door inzicht te geven in welke mate Gedeputeerde Staten, Provinciale organisatie en een aantal verbonden partijen uitvoering geven aan beleidskaders en zich daarover verantwoorden. Binnen de categorie verbonden partijen heeft het onderzoek plaatsgevonden bij RUD Zeeland, NV Westerscheldetunnel en de Westerscheldeferry BV.

Aanleiding

Provinciale Staten zijn als kadersteller en controleur van het dagelijks bestuur medeverantwoordelijk voor een goede en stabiele dienstverlening en gegevensbescherming. Een cyberaanval brengt de continuïteit van de werkzaamheden van de Provincie Zeeland en het geheim houden van gegevens in gevaar. Goed cyberveiligheidsbeleid is daarom cruciaal in deze tijd waarin cyberaanvallen helaas veel voorkomen. Digitale processen vormen het zenuwstelsel van het Provinciaal bestuur, haar dienstverlening en opslag van gegevens in het kader daarvan. In de corona pandemie nam het digitaal werken sterk toe en dat effect is deels blijvend, ook nu de pandemie minder op de voorgrond staat. Bovendien is de cyberdreiging vanwege geopolitieke spanningen opgelopen.

Doelstelling

Het onderzoek heeft ten doel:

- Een bijdrage te geven aan de kaderstellende en controlerende rol van Provinciale Staten waar het gaat om de cyberveiligheid van Provinciale diensten en gegevensbeheer.
- Inzicht te geven in welke mate Gedeputeerde Staten, provinciale organisatie en RUD Zeeland, NV Westerscheldetunnel en de Westerscheldeferry BV adequaat uitvoering geven aan cyberveiligheidsbeleid en verantwoording daarover.

Centrale vraag

Wat is het niveau van cyberveiligheid bij de Provinciale organisatie, RUD Zeeland, NV Westerscheldetunnel en Westerscheldeferry BV en welke verbeteringen zijn daarin mogelijk wat betreft de doeltreffendheid van beleid?

Afbakening

De focus van het onderzoek van de rekenkamer is gebaseerd op:

- Recent uitgevoerde interne audits.
- De implementatie van de Baseline Informatiebeveiliging Overheid, die onderdeel was van het certificeringstraject voor ISO 270001/2 van de Provincie Zeeland.
- De uitvoering van Pentesten bij alle partijen, het door een Ethisch hacker de zwakke plekken van de IT-omgeving van de Provincie Zeeland bloot laten leggen.

- Het inzetten van een mystery guest bezoek bij de Provincie Zeeland, het toetsen of het fysiek mogelijk is om toegang tot ruimtes en IT-omgevingen in gebouwen van de Provincie Zeeland te krijgen.
- De uitvoering van phishing onderzoeken, het nabootsen van een phishingmail.
- Interviews met relevante betrokken personen bij alle betrokken partijen bij dit onderzoek.

Conclusies
Gebaseerd op de bevindingen van het rekenkameronderzoek in de Nota van bevindingen, *"Better safe than sorry!"* komt de rekenkamer tot de volgende conclusies:

Provincie Zeeland
- De Rekenkamer constateert dat het beleid van de Provinciale organisatie op het gebied van cyberveiligheid en de uitvoering daarvan in hoge mate doeltreffend is geweest. De Nederlandse standaard voor cyberveiligheid bij overheden – de zogeheten Baseline Informatiebeveiliging – is op het gewenste niveau geïmplementeerd in de organisatie in de periode 2019 t/m 2023.
- De Provinciale organisatie heeft zich extern laten toetsen op de naleving daarvan middels ISO 27.001 certificering. Dit certificaat werd in februari 2023 verkregen.
- Het onderzoek van de rekenkamer bevestigt dat processen worden georganiseerd in lijn met de Baseline Informatiebeveiliging Overheid, her en der zijn er op bedrijfsvoeringniveau verbetermogelijkheden. Zo is onder andere uw rol als Staten bij een crisissituatie in het huidige continuïteitsplan beperkt uitgewerkt.
- Het aanvullende mystery guest onderzoek van de rekenkamer laat zien dat de weerbaarheid tegen onbevoegden op de Abdij een zorgpunt is. Er is zeker vooruitgang op dit punt geboekt de afgelopen jaren door het ingezette beleid, maar verdere verbetering is mogelijk en noodzakelijk.

RUD Zeeland
- De Rekenkamer constateert op basis van het onderzoek dat de Regionale Uitvoeringsdienst maatregelen neemt die het algehele risico op een cyber gerelateerde crisis omlaag brengen.
- De pentest maakt inzichtelijk dat er desondanks ook onveilige ICT-processen zijn met een dreiging voor de organisatie van de RUD Zeeland.
- Het onderzoek maakt duidelijk dat de meeste winst behaald kan worden door het aanscherpen van de reeds geïmplementeerde ICT-processen en het creëren van meer bewustzijn onder medewerkers met betrekking tot wachtwoorden en andere veiligheidsprocessen. Door de RUD Zeeland werd reeds actie ondernomen op het onderzoek van de rekenkamer door opvolging te geven aan het minimaliseren van de zwaarste geconstateerde risico's.
- Er waren geen interne evaluaties aanwezig over cyberveiligheid bij de RUD Zeeland, die bij de analyse konden worden betrokken. Het is niet inzichtelijk in welke mate de RUD Zeeland voldoet aan de Baseline Informatiebeveiliging Overheid.
- De RUD Zeeland rapporteerde in de jaarstukken vooralsnog niet over cyberveiligheid (meest recente rapportage op moment van schrijven van het onderzoek: jaarstukken 2021).

Westerscheldeferry BV en NV Westerscheldetunnel
- De Rekenkamer constateert dat de NV Westerscheldetunnel en de Westerscheldeferry in de praktijk allerlei maatregelen nemen om cyberaanvallen te voorkomen. Uit de pentest bleek dat er mogelijkheden zijn om de weerbaarheid tegen een aanval verder te vergroten.
- Het is primair aan de directies van de Westerscheldetunnel en de Westerscheldeferry om maatregelen te treffen als gevolg van de bevindingen uit het rekenkameronderzoek. Wanneer de lijn gevolgd wordt uit het huidige deelnemingenbeleid van de Provincie Zeeland, zien Gedeputeerde Staten daarop toe en zijn Provinciale Staten kaderstellend en controleur van Gedeputeerde Staten.
- Gedeputeerde Staten voeren het beleid uit in lijn met het vastgestelde governancebeleid. Ad hoc wordt met de directies gesproken over het onderwerp cyberveiligheid.
- De Westerscheldeferry BV en NV Westerscheldetunnel rapporteren in de jaarstukken niet over cyberveiligheid.
- Gezien het feit dat beide organisaties een privaatrechtelijke rechtsvorm hebben, is de Baseline Informatiebeveiliging Overheid niet van toepassing. De bedrijfsvoering van beide organisaties is tot op heden niet ISO 27.001 gecertificeerd.

Aanbevelingen rekenkamer aan de Provinciale Staten
De Rekenkamer heeft alle betrokken partijen aanbevelingen gedaan, deze zijn terug te vinden in de bijlage bij de PS brief. Hieronder de aanbevelingen van de Rekenkamer aan de Provinciale Staten:
- Spreek u, als belangrijke drager van de veiligheidscultuur van de Provincie Zeeland, uit over het dilemma tussen het verhogen van de weerbaarheid van de Provinciale organisatie tegen fysieke indringers en het behouden van de huidige openheid in de gebouwen cq. het vertrouwen dat daaruit spreekt richting bezoekers.

- Verzoek de griffie om Statenleden goed op de hoogte te houden over cyberveiligheid en hen daarin te trainen waar nodig in afstemming met de Chief Information Security Officer van de Provincie Zeeland.
- Geef Gedeputeerde Staten opdracht om in de begroting expliciet middelen te reserveren voor cyberveiligheid van de Provinciale organisatie, waarvan de hoogte van het budget wordt gebaseerd op het realiseren van de ambitie en prestaties die daarbij horen.
- Geef Gedeputeerde Staten opdracht om uw Staten jaarlijks via de jaarstukken te blijven informeren over de geleverde prestaties aan de hand van een (beperkte) set indicatoren gericht op de speerpunten van het beleid.
- Geef Gedeputeerde Staten opdracht om uw rol als Provinciale Staten bij een crisissituatie verder in het continuïteitsplan uit te werken en uw Staten zo nodig te betrekken bij oefeningen als gevolg daarvan.
- Overweeg in overleg met Gedeputeerde Staten om in het deelnemingenbeleid waar nodig en mogelijk een norm te stellen voor cyberveiligheid bij aan de Provincie Zeeland verbonden partijen, bijvoorbeeld ISO 27.001 en dat de partijen daarvoor indien noodzakelijk budget beschikbaar te stellen en Gedeputeerde Staten u periodiek over de voortgang te laten informeren.
- Geef Gedeputeerde Staten opdracht om met de andere deelnemers van de RUD Zeeland afstemming te zoeken over:
    - Het meer SMART maken van de ambitie op het gebied van cyberveiligheid, waarbij de inzet dient te zijn dat, waar dat nog niet het geval is, de gegevens die de RUD namens de Provincie Zeeland in beheer heeft/gebruikt zo snel mogelijk op hetzelfde veiligheidsniveau beschermd worden als dat voor de eigen provinciale organisatie geldt (aantoonbaar Baseline Informatiebeveiliging Overheid -compliant).
    - Het verbeteren van de informatiepositie over de prestaties op het gebied van cyberveiligheid via de P&C-cyclus van de RUD Zeeland.

Bestuurlijke reactie
In hun reactie van 20 juni 2023 geven Gedeputeerde Staten aan, de concept brief van de Rekenkamer over het onderzoek over cyberveiligheid ontvangen te hebben. De brief geeft duidelijke conclusies en aanbevelingen en de Gedeputeerde Staten onderschrijven deze aanbevelingen.

Wij stellen u voor te besluiten overeenkomstig bijgevoegd ontwerpbesluit.

het presidium van Provinciale Staten van Zeeland,

drs. J.M.M. Polman, voorzitter

drs. F.J. van Houwelingen MPA, statengriffier

Onderwerp:
Rekenkamerrapport Cyberveiligheid

Ontwerpbesluit

De staten der provincie Zeeland,
gelezen het voorstel van het Presidium d.d. 30 oktober 2023

besluiten:

1. Kennis te nemen van het rekenkamerrapport “Onderzoek cyberveiligheid”.
2. De griffier te verzoeken om Statenleden goed op de hoogte te houden over cyberveiligheid en hen daarin te trainen in afstemming met de Chief information security officer van de Provincie Zeeland.
3. Gedeputeerde Staten opdracht te geven om in de begroting expliciet middelen te reserveren voor cyberveiligheid van de Provinciale organisatie, waarvan de hoogte van het budget wordt gebaseerd op het realiseren van de ambitie en prestaties die daarbij horen.
4. Gedeputeerde Staten opdracht te geven om Provinciale Staten jaarlijks via de jaarstukken te blijven informeren over de geleverde prestaties aan de hand van een (beperkte) set indicatoren gericht op de speerpunten van het beleid.
5. Gedeputeerde Staten opdracht te geven om uw rol als Provinciale Staten bij een crisissituatie verder in het continuïteitsplan uit te werken en uw Staten te betrekken bij oefeningen als gevolg daarvan.
6. Gedeputeerde Staten opdracht te geven om te bespreken of het mogelijk is om in het deelnemingenbeleid een norm te stellen voor cyberveiligheid bij aan de Provincie Zeeland verbonden partijen, waarbij aan deze partijen daarvoor indien noodzakelijk budget beschikbaar wordt gesteld en Gedeputeerde Staten de staten periodiek informeren over de voortgang .
7. Gedeputeerde Staten opdracht te geven om met de andere deelnemers van de RUD Zeeland afstemming te zoeken over:
    a. Het meer SMART maken van de ambitie op het gebied van cyberveiligheid, waarbij de inzet dient te zijn dat, waar dat nog niet het geval is, de gegevens die de RUD namens de Provincie Zeeland in beheer heeft/gebruikt zo snel mogelijk op hetzelfde veiligheidsniveau beschermd worden als dat voor de eigen provinciale organisatie geldt (aantoonbaar Baseline Informatiebeveiliging Overheid compliant).
    b. Het verbeteren van de informatiepositie over de prestaties op het gebied van cyberveiligheid via de P&C-cyclus van de RUD Zeeland.