REKENKAMER *ZEELAND*

Aan Provinciale Staten van Zeeland

uw kenmerk:		ons kenmerk:	178070	Bijlagen:	7
behandeld door:	[redacted]	Doorkiesnummer:	0118-[redacted]	Middelburg,	15-09-2023
onderwerp:	Onderzoek cyberveiligheid				

Geachte leden van Provinciale Staten,

De rekenkamer Zeeland heeft onderzoek gedaan op het terrein van cyberveiligheid (zie kader).
In deze brief is de analyse van de onderzoeksresultaten samengevat en worden er een aantal concrete aanbevelingen gedaan aan Provinciale en Gedeputeerde Staten om de cyberveiligheid van Provinciale informatie en dienstverlening verder te versterken.

Wat is 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 hiervan.

1. Onderzoeksopzet en procedure

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.
- Westerscheldeferry BV.

Centrale Vraag

Het onderzoek geeft antwoord op de volgende 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?

Koorkerkhof 20 Middelburg **T** 0118-631841 **F** 0118-631238
Postbus 6001 4330 LA Middelburg www.rekenkamerzeeland.nl **E** rekenkamer@zeeland.nl

Werkwijze

De rekenkamer heeft de centrale vraag beantwoord door zoveel mogelijk gebruik te maken van reeds beschikbare resultaten uit onderzoeken die recent zijn of werden uitgevoerd.

Deze informatie is aangevuld met informatie uit interviews. Daarnaast is onderzoeksinformatie verkregen aan de hand van pentesten bij de verbonden partijen in de periode januari – april 2023 en de inzet van een mystery guest op de Abdij op 21 april 2023 (zie kader). Op die dag waren Provinciale Staten aanwezig waren voor een vergadering.

Pentest

Een pentest, afgeleid van het Engelse penetration test, is een technisch onderzoek waarbij ethische hackers onderzoeken of er kwetsbaarheden en beveiligingsrisico's zijn. De gebeurt vanuit twee invalshoeken:

- Extern: Onderzoeken of het mogelijk is om de netwerkomgeving van buitenaf binnen te dringen.
- Intern: Vanuit een binnengedrongen omgeving achterhalen welke andere omgevingen/systemen er benaderbaar zijn en onderzoeken of deze omgevingen/systemen weer binnengedrongen kunnen worden.

Mystery guest onderzoek

Een mystery guest test de weerbaarheid van een organisatie tegen onbevoegden die fysiek toegang proberen te krijgen tot een gebouw en onderzoekt welke schade een aanvaller mogelijk zou kunnen aanrichten, zoals het bemachtigen van fysieke en digitale data, toegang verkrijgen tot het interne netwerk, diefstal van waardevolle spullen, toegang krijgen tot risicovolle technische ruimtes, en het bemachtigen van authenticatiemiddelen zoals pasjes en wachtwoorden. De resultaten van het Mystery Guest onderzoek dragen bij aan het creëren van security awareness bij medewerkers, en biedt

Wegens de omvang van de ICT bij de Westerscheldetunnel is de pentest bij de NV Westerscheldetunnel beperkt tot het kantoorgedeelte van het netwerk. Zowel de NV Westerscheldetunnel als de Westerscheldeferry BV namen op vrijwillige basis deel aan het onderzoek.

Het onderzoek is waar mogelijk uitgevoerd door een intern onderzoeksteam van de rekenkamer. De onderzoeksopzet werd gereviewd met een extern expert. De pentesten en het mystery guest onderzoek zijn uitgevoerd door een externe partij, DONG-IT uit Leiden.

Normenkader

De bevindingen uit het onderzoek zijn waar mogelijk langs de meetlat van een normenkader gelegd. Dit normenkader is gebaseerd op het beleid van de Provincie Zeeland en algemene beginselen van behoorlijk bestuur. De toets aan het normenkader geeft de input voor sturingsaspecten die er mogelijk zijn om het beleid van de Provincie en de uitvoering daarvan verder te verbeteren.

Vertrouwelijkheid

Uit zorgvuldigheidsoverwegingen is in deze brief vertrouwelijke informatie weggelaten. Hetzelfde geldt voor de nota van bevindingen, die is te raadplegen op onze website via deze link. In deze nota wordt dieper ingegaan op de onderzoeksopzet en –bevindingen, vertrouwelijke informatie is niet gepubliceerd.

Procedure

De concept nota van bevindingen en conclusies is voorgelegd voor een ambtelijke reactie bij de organisaties die onderzocht werden. Na ontvangst van de ambtelijke reactie is deze brief opgesteld en aangeboden aan Gedeputeerde Staten, RUD Zeeland, Westerscheldeferry BV en NV Westerscheldetunnel voor bestuurlijk commentaar.

Gedeputeerde Staten, het dagelijks bestuur van de RUD Zeeland en de directies van de Westerscheldeferry BV en NV Westerscheldetunnel hebben een reactie gegeven op het onderzoek. Deze reacties zijn opgenomen als bijlage bij deze brief en voorzien van een nawoord door de rekenkamer.

2. De rol van Provinciale Staten bij cyberveiligheid

Rol van PS met betrekking tot Provinciale organisatie

Provinciale Staten zijn als kadersteller en controleur van Gedeputeerde Staten medeverantwoordelijk voor een goede en stabiele dienstverlening en gegevensbescherming van de Provinciale organisatie. Daarnaast heeft ieder Statenlid de verantwoordelijkheid om zorgvuldig om te gaan met gegevens en zich daarover te laten informeren. Bovendien zijn Provinciale Staten een belangrijke cultuurdrager voor de organisatie als geheel.

De rekenkamer constateert het volgende:

- Het doel van de Provincie Zeeland, verwoord in de P&C cyclus, is dat de hele organisatie voldoet aan de Baseline informatiebeveiliging Overheid en ISO 27.001 is gecertificeerd (zie onderstaand kader).
- Provinciale Staten werden door Gedeputeerde Staten geïnformeerd over het gevoerde beleid met betrekking tot cyberveiligheid in de paragraaf bedrijfsvoering, onderdeel van de jaarlijkse begroting en jaarstukken van de Provincie Zeeland. De informatiewaarde van de verantwoording neemt toe wanneer daar meer SMART over gerapporteerd wordt.
- Provinciale Staten stellen in de huidige situatie geen apart budget beschikbaar voor cyberveiligheid. De continuïteit van het beleid kan worden versterkt door expliciet middelen te koppelen in de begroting aan cyberveiligheid, waarbij de hoogte van het budget afgestemd dient te zijn op de beleidsopgave.

Baseline Informatiebeveiliging Overheid (BIO) en ISO 27001

De Baseline Informatiebeveiliging Overheid (BIO) biedt het basisniveau voor adequaat veiligheidsbeleid voor het Rijk, de Provincies, gemeenten en waterschappen. In de baseline is uitgewerkt en vastgelegd wat minimaal noodzakelijk geacht wordt om informatie/dienstverlening te beschermen tegen cyberaanvallen en daarop te acteren in het kader van crisismanagement. De BIO beoogt zo de beveiliging van informatie(systemen) bij alle bestuurslagen en bestuursorganen van de overheid te bevorderen, zodat alle onderdelen erop kunnen vertrouwen dat onderling uitgewisselde gegevens, in lijn met wet- en regelgeving, passend beveiligd zijn. Het doel is continuïteit in de bedrijfsprocessen door waarborgen van juiste en tijdige informatie. In het Interprovinciaal Overleg is besloten dat alle Provincies voldoen aan het BIO per 1 januari 2023.

De BIO is afgeleid van de ISO 27.001. Deze norm vormt de internationale standaard op het gebied van informatieveiligheid in het bedrijfsleven.

Rol van PS met betrekking tot verbonden partijen

Controlerende rol

De controlerende rol van Provinciale Staten ligt bij verbonden partijen op een ander niveau dan de controlerende rol die uw Staten hebben als het gaat om de provinciale organisatie. [1] Bij verbonden partijen is het eerstelijns toezicht op de directie in de regel belegd bij een raad van commissarissen (NV Westerscheldetunnel), danwel een dagelijks/algemeen bestuur (RUD Zeeland).[2] Gedeputeerde Staten zijn op afstand betrokken vanuit de aandeelhouderrol/eigenaarspositie. Provinciale Staten controleren hoe Gedeputeerde Staten hun aandeelhouderrol/eigenaar rol vervullen.

Kaderstellende rol

Wat betreft kaderstelling hebben Provinciale Staten wel een positie in de eerste lijn. Provinciale Staten stellen bijvoorbeeld het deelnemingenbeleid vast, waarin de kaders gesteld zijn over hoe er wordt samengewerkt met verbonden partijen en wat de rollen en bevoegdheden zijn van Provinciale Staten, Gedeputeerde Staten en ambtelijke organisatie.

Provinciale Staten hebben specifiek op het gebied van cyberveiligheid in het deelnemingenbeleid, noch anderszins, een doel geformuleerd voor cybersecurity bij aan de Provincie verbonden partijen, zo ook niet voor de RUD Zeeland, NV Westerscheldetunnel en Westerscheldeferry BV.

3. Cyberveiligheid Provinciale organisatie

Conclusies

- 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 (BIO, zie kader) – 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 BIO, 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.

4. RUD Zeeland

Conclusies

- De rekenkamer constateert op basis van het onderzoek dat de gemeente Terneuzen en de Regionale Uitvoeringsdienst maatregelen nemen 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.

[1] De rekenkamer ging eerder uitvoerig in op de rol van Provinciale Staten bij aan de Provincie Zeeland verbonden partijen in 2019, bij het onderzoek naar externe inhuur en uitbesteden (bijlage 1: hoofdstuk 5). Provinciale Staten hebben in 2021 deelnemingenbeleid vastgesteld.

[2] Voor de Westerscheldeferry BV is er geen raad van commissarissen aangesteld wegens de geringe omvang van de BV.

- 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 BIO.
- De RUD Zeeland rapporteerde in de jaarstukken vooralsnog niet over cyberveiligheid. (meest recent op moment van schrijven: jaarstukken 2021).

5. Westerscheldeferry BV en NV Westerscheldetunnel

Conclusies

- 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 governance 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 (zie hoofdstuk 1).
- Gedeputeerde Staten voeren het beleid uit volgens de huidige 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 BIO niet van toepassing. De bedrijfsvoering van beide organisaties is tot op heden niet ISO 27.001 gecertificeerd.

6. Aanbevelingen

De rekenkamer doet <u>Provinciale Staten</u> de volgende aanbevelingen:

- 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 BIO-compliant).
- Het verbeteren van de informatiepositie over de prestaties op het gebied van cyberveiligheid via de P&C-cyclus van de RUD Zeeland.

De aanbevelingen die de rekenkamer deed aan Gedeputeerde Staten, RUD Zeeland en Westerscheldeferry BV en NV. Westerscheldetunnel zijn opgenomen in de bijlage.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,

Namens het bestuur van de Rekenkamer Zeeland

mr. G.A.A. van Rijswijk – van Mook
Voorzitter

Bijlagen:

1. **Handvaten verbeteren weerbaarheid onbevoegden.**
2. **Aanbevelingen GS en verbonden partijen**
3. **Bestuurlijk commentaar GS**
4. **Bestuurlijk commentaar RUD Zeeland**
5. **Reactie Westerscheldeferry BV.**
6. **Reactie NV. Westerscheldetunnel**
7. **Nawoord**

Bijlage 1. Handvaten verbeteren weerbaarheid tegen onbevoegden

In algemene zin dient men om tot verbetering te komen na te gaan welke risico's onacceptabel zijn voor de organisatie en op welke manier de organisatie daar in de toekomst mee om zou moeten gaan. Het is aan de organisatie in overleg met Gedeputeerde Staten om te bepalen welke acties nodig zijn, en de afweging te maken van de eventuele kosten en baten van maatregelen.

Procedures

- Houd te allen tijde vast aan de beveiligingsprocedures. Medewerkers mogen onbekenden en niet-bevoegde medewerkers geen toegang verlenen, ook al hebben ze een ogenschijnlijk plausibele verklaring. Train medewerkers hierop, ook externen.
- Creëer een cultuur waarin het openlijk dragen van een toegangspas de norm is.
- Train medewerkers om bij verdacht gedrag goed door te vragen. Laat medewerkers een daarvoor ingerichte standaardprocedure volgen, wat vaak zal beginnen bij het controleren van een toegangspas.

Toegang

- Richt het gebouw zo in dat zoveel mogelijk van de toegangspunten tot het beveiligde gedeelte zich in het direct zicht van een receptiebalie of beveiligingspost bevinden. Waar dit niet mogelijk is, zorg voor cameratoezicht dat voortdurend gemonitord wordt.
- Overweeg om meer deuren standaard gesloten te houden zodat deze alleen met een toegangspas geopend kunnen worden, bijvoorbeeld tussen verdiepingen of afdelingen.
- Kijk bij het verlaten van een beveiligde ruimte achterom of de deur wel goed in zijn slot valt, en of niemand mee naar binnen loopt voor de deur sluit.
- Mogelijk gevoelige ruimtes, zoals technische ruimtes en opslagruimtes, dienen altijd op slot te zijn. Automatisch sluitende deuren met paslezers kunnen hierbij helpen.
- Herhaal de mysteryguest acties. Oefening baart kunst. De ervaring is dat de scherpte van de organisatie en daarmee de weerbaarheid en veiligheid aanzienlijk verbetert wanneer mysteryguest worden herhaald.

Onbeheerd achterlaten van informatie en informatiedragers

- Laat medewerkers de aan hen toegewezen systemen zelf actief vergrendelen zodra ze er geen gebruik meer van maken, bijvoorbeeld als ze de werkplek verlaten. Er zijn positieve manieren om medewerkers te attenderen op het feit dat zij een werkplek onbeheerd en toegankelijk hebben achtergelaten. Hiermee wordt het belang van het vergrendelen onder de aandacht gebracht om het gedrag positief te verbeteren. Denk hierbij bijvoorbeeld aan het plaatsen van een opvallende tekst of plaatje op het werkblad van een onbeheerde computer, onder het mom van 'security-awareness' (https://www.troyhunt.com/40-inappropriate-actions-to-take/).
- Laat medewerkers vertrouwelijke documenten opbergen. Kasten dienen afgesloten te worden na vertrek, en sleutels veilig opgeborgen, zoals in een sleutelkast.

ICT en het interne netwerk

- Pas network access control toe op alle Ethernetaansluitingen, ook op aansluitingen van VoIP-telefoons, Teams-PCs, en andere apparaten.
- Implementeer, waar mogelijk, fysieke beveiliging van apparaten en netwerkaansluitingen.
- Pas striktere monitoring toe, het ontkoppelen van een netwerkkabel moet een signaal laten afgaan in de securityoplossing van de ICT-beheerder, des te meer als dit gepaard gaat met een vreemd MAC-adres van het verbindende apparaat, en verdacht netwerkverkeer zoals een port scan.
- Vreemd gedrag op een PC, zoals het triggeren van antivirus software, moet eveneens een signaal laten afgaan. Des te meer als dit gedeelde PCs betreft waar gebruikers alleen toegang hebben tot een gelimiteerde interface, zoals de Teams-PCs.
- Verifieer tevens of het uitvoeren van malware op de computer van de werknemer tot een signalering heeft geleid.
- Bij het signaleren van vreemd computergedrag in een bepaalde ruimte wordt het aangeraden om de beveiliging fysiek in te schakelen, om te verifiëren wat er aan de hand is.

Algemeen

- Betrek de medewerkers bij de beveiliging van hun eigen deel van het gebouw.
- Deel de resultaten van dit onderzoek op gepaste wijze met de medewerkers binnen de organisatie. Praktijkvoorbeelden uit de directe werkomgeving in combinatie met een security awareness training hebben meer effect dan een algemene security awareness training. Uiteraard verdient juist handelen een groot compliment.
- Maak medewerkers bewust van hoe verschillende delen van het gebouw zijn opgedeeld. Hiermee wordt het een binnendringer veel moeilijker gemaakt om met een dekmantel van een andere afdeling elders zomaar de waarheid te verkopen.
- Wijs per afdeling of vloer eventueel beveiligingstaken toe aan een specifiek persoon. In de praktijk scheelt het al heel veel als een klein percentage van de medewerkers waakzaam is (maar zorg hierbij uiteraard wel voor een goede verdeling over de organisatie).

Bijlage 2. Aanbevelingen GS en verbonden partijen

De rekenkamer Zeeland deed GS en de verbonden partijen de volgende aanbevelingen:

Aanbevelingen GS

- Zet in het nieuw op te stellen beleidskader voor cyberveiligheid 2023-2027 in op het behouden van de ISO 27.001 certificering bij de Provinciale organisatie.
- Blijf streven naar het voldoen aan de BIO.
- Scherp het veiligheidsbeleid van de Provinciale organisatie gericht aan om de weerbaarheid tegen (fysieke) indringers te versterken. Gebruik hiervoor de handvatten die volgen uit het rekenkameronderzoek (zie bijlage)
- Betrek in het overleg over cyberveiligheid met de RUD Zeeland en overige deelnemers in deze gemeenschappelijke regeling uw positieve ervaringen met externe ISO 27001 certificering.
- Zie vanuit uw aandeelhouderrol erop toe dat Westerscheldeferry BV en NV Westerscheldetunnel de verbeterpunten uit het rekenkameronderzoek adequaat oppakken.

Aanbevelingen RUD Zeeland

- Stel voor de RUD Zeeland SMART een ambitie voor cyberveiligheid op, betrek deze ambitie bij de contractverlenging over de PIOFACH-taken met de gemeente Terneuzen vanaf 1 januari 2024 en verzoek deelnemers om voldoende budget beschikbaar te stellen om BIO-compliant te worden.
- Overweeg in gesprek met de deelnemers bij het vorige punt ook externe ISO 27.001 certificering, neem kennis van de positieve ervaringen daarmee bij de Provincie Zeeland en betrek dat in het gesprek.
- Ga met de gemeente Terneuzen op beleidsniveau nader het gesprek aan om slimme combinaties te maken op het gebied van cyberveiligheid, zoals het gezamenlijk uitvoeren van pentesten en mystery guest onderzoek en het verbeteren van de veiligheidscultuur.
- Pak in samenspraak met de gemeente Terneuzen de lessen uit het technische rapport van de pentest op, voor zover dat nog niet heeft plaatsgevonden en verlaag daarmee de kwetsbaarheid van de organisatie.
- Agendeer periodiek cyberveiligheid op de agenda's van dagelijks en algemeen bestuur.
- Start met het verantwoorden over de stand van zaken met betrekking tot cyberveiligheid in de bedrijfsvoeringsparagraaf van de begroting en jaarstukken.

Aanbevelingen Westerscheldeferry BV.

- Bepaal gelet op de resultaten van de pentest welke risico's onacceptabel zijn voor uw organisatie en op welke manier uw organisatie daar in de toekomst mee om zou moeten gaan. Ga daarover indien noodzakelijk het gesprek aan met de provincie Zeeland als aandeelhouder.
- Overweeg om in de toekomst uw organisatie extern te laten certificeren volgens ISO 27.001, waarbij het vast onderdeel voor uw organisatie wordt om zich extern op het gebied van cyberveiligheid te laten beoordelen.

Aanbevelingen NV. Westerscheldetunnel

- Bepaal gelet op de resultaten van de pentest welke risico's onacceptabel zijn voor uw organisatie en op welke manier uw organisatie daar in de toekomst mee om zou moeten gaan. Ga daarover indien noodzakelijk het gesprek aan met de provincie Zeeland als aandeelhouder.
- Overweeg om in de toekomst uw organisatie extern te laten certificeren volgens ISO 27.001, waarbij het vast onderdeel voor uw organisatie wordt om zich extern op het gebied van cyberveiligheid te laten beoordelen.

Bijlage 3. Bestuurlijke reactie GS

Gedeputeerde Staten

Provincie Zeeland

Abdij 6 4331BK Middelburg
Postbus 6001 4330 LA Middelburg
+31 118631011
IBAN NL08 BNGH 0285010557

Rekenkamer Zeeland
Postbus 6001
4330 LA MIDDELBURG

Onderwerp	Zaaknummer	Behandeld door	Verzonden
Onderzoek cyberveiligheid rekenkamer Zeeland	251792	[redacted]	21 JUN 2023

Middelburg, 20 juni 2023

Geacht bestuur,

Wij hebben uw brief van 2 juni 2023 met het kenmerk REK in goede orde ontvangen.
De aanbevelingen die u in de brief zelf doet kunnen we onderschrijven.

Ook hebben we de conceptbrief aan Provinciale Staten als bijlage bij uw brief ontvangen.

Uiteraard zijn we verheugd dat onze organisatie blijk geeft van een groot veiligheidsbewustzijn en zijn we trots om de eerste volledig ISO 27001-gecertificeerde overheidsorganisatie in Nederland te zijn. We willen deze status zeker vasthouden en onze weerbaarheid blijven verbeteren.

U geeft terecht aan dat de weerbaarheid tegen onbevoegde toegang op de Abdij een zorgpunt is. Daar zijn we ons als gedeputeerde staten ook zeker van bewust en daar wordt ook al actie op ondernomen. Een nieuw Beleid Toegangsbeveiliging wordt al voorbereid en zal op korte termijn worden vastgesteld en de bijbehorende maatregelen zullen zo spoedig mogelijk daarna worden ingevoerd.

Aan uw aanbeveling om ook de statenleden mee te nemen in bewustwording en training, op het gebied van informatiebeveiliging, wordt ook gevolg gegeven: Er is al overleg tussen CISO en statenadviseur om een en ander voor te bereiden.

Uw brief aan provinciale staten geeft duidelijke conclusies en aanbevelingen.
De aanbevelingen die u geeft zijn zinvol; als gedeputeerde staten kunnen we die onderschrijven.

Met vriendelijke groet,

Gedeputeerde Staten van Zeeland,

[redacted]

drs. J.M.M. Polman, voorzitter

[redacted]

drs. M.C.J. Franken, secretaris-algemeen directeur

Noem in uw contact met ons steeds het zaaknummer. Dit staat bovenaan deze brief.

Bijlage 4. Bestuurlijke reactie RUD Zeeland

DE OMGEVINGSDIENST VOOR EEN SCHOON EN VEILIG ZEELAND

Rekenkamer Zeeland
Postbus 6001
4330 LA MIDDELBURG

Terneuzen, 11 september 2023

Betreft: Bestuurlijk commentaar onderzoek cyberveiligheid RUD Zeeland 2023

Geachte mevrouw Van Rijswijk-Van Mook,

Op 20 juni 2023 hebben wij uw brief met kenmerk REK ontvangen waarin u verzoekt om een bestuurlijke reactie te geven op het door Donglt uitgevoerde onderzoeksrapport.

Het onderzoek heeft zich gericht op de cyberveiligheid bij onder andere RUD Zeeland. Het heeft geleid tot het vertrouwelijke rapport met kenmerk:

Pentest report RUD Zeeland, External & Internal Network, version 2023-04-06 15:15:41.

Reactie
Wij hebben de rapportage met belangstelling gelezen en kunnen ons vinden in de uitkomst hiervan.

Onze Chief Information Security Officer (CISO) heeft de rapportage eveneens tot zich genomen en de nodige acties in gang gezet. De hoge risico bevindingen zijn door ons uiteraard met de hoogste prioriteit opgepakt. De zogenaamde quick-wins zijn deels al afgerond of zijn nog in behandeling. In ieder geval zijn alle grote risico's direct geëlimineerd.
Concreet gaat dit om:

- Een bewustwordingscampagne welke momenteel al voor alle medewerkers loopt en verder uitgebreid gaat worden. Denk daarbij aan nep-fishingmails, nieuwsberichten, een nulmeting, wachtwoordenbeheer, enz.
- Diverse processen worden aangepast en zo nodig aangescherpt.
- Voor de overige maatregelen wordt/is een planning gemaakt.

Hoewel wij ons reeds bewust waren van alle digitale gevaren welke we anno 2023 lopen, heeft het onderzoek hier ons zeker nog meer bewust van gemaakt. Reeds lopende acties zijn daardoor in een stroomversnelling geraakt, andere hebben hierdoor een hogere prioriteit gekregen.

Wij zien het onderzoek dan ook als een goede bijdrage om onze digitale omgeving op het gewenste niveau van veiligheid te brengen.

Hoogachtend,

Het Dagelijks Bestuur van Regionale Uitvoeringsdienst Zeeland,
namens dezen,

A. van der Maas
Voorzitter

A. van Leeuwen
Secretaris

De Regionale Uitvoeringsdienst (RUD) Zeeland voert sinds 1 januari 2014 milieu- en veiligheidstaken uit namens de Zeeuwse gemeenten, Waterschap Scheldestromen en Provincie Zeeland.

RUD Zeeland
Postbus 35, 4530 AA Terneuzen

Bezoekadres
Stadhuisplein 1 4531 GZ Terneuzen

E-mail: info@rud-zeeland.nl
Internet: www.rud-zeeland.nl

Bij beantwoording a.u.b. onderwerp, datum en kenmerk van deze brief vermelden.

Bijlage 5. Reactie Westerscheldeferry BV.

Westerschelde Ferry

Bezoekadres
Westerhavenweg 2a
4382 NM Vlissingen

Postadres
Postbus 13
4460 AA Goes

T: 085-0401 800
E: klantenservice@westerscheldeferry.nl

Website : www.westerscheldeferry.nl

KvK nr. : 61547336
BTW : NL854 385 381 B01
IBAN : NL26 ABNA 0830 3607 35
BIC : ABNA NL 2A
Facturen : digifactuurwsf@movenience.nl

Rekenkamer Zeeland

Mr. G.A.A. van Rijswijk – van Mook

Postbus 6011

4330 LA Middelburg

Datum : 13 juni 2023
Behandeld door : Leo Wolterman
Email : [redacted]
Onderwerp : [redacted]

Geachte Mr. Van Rijswijk – Van Mook,

De rekenkamer Zeeland heeft onlangs onderzoek gedaan naar cybervelligheid. De resultaten van dit onderzoek uitgevoerd door Dong IT en uw conclusies en aanbevelingen naar aanleiding van dit rapport zijn met ons gedeeld.

Wij hebben kennis genomen van uw conclusies en onderschrijven deze.

Wij zullen uw aanbevelingen ter harte nemen en ze in de eerstvolgende aandeelhoudersvergadering bespreken.

Ik vertrouw erop dat ik u hiermee voldoende heb geïnformeerd.

[redacted]

Hoogachtend,

[redacted]

Leo Wolterman
Algemeen Directeur Westerschelde Ferry B.V.

Iedere overtocht is een belevenis op zich.

Bijlage 6. Reactie NV. Westerscheldetunnel

WESTERSCHELDE TUNNEL

MEER MOGELIJK MET DE SLUISKILTUNNEL

Rekenkamer Zeeland
mr. G.A.A. van Rijswijk - van Mook
Postbus 6001
4430 LA MIDDELBURG

Datum	13 juni 2023
Onze referentie	NVWST/2023.53134
Onderwerp	Onderzoek cyberveiligheid
Behandeld door	[redacted]
Telefoonnummer	
E-mailadres	

Geachte Mr. Van Rijswijk – Van Mook,

De rekenkamer Zeeland heeft onlangs onderzoek gedaan naar cyberveiligheid. De resultaten van dit onderzoek uitgevoerd door Dong IT en uw conclusies en aanbevelingen naar aanleiding van dit rapport zijn met ons gedeeld.

Wij hebben kennis genomen van uw conclusies en onderschrijven deze.

Wij zullen uw aanbevelingen ter harte nemen en ze in de eerstvolgende aandeelhoudersvergadering bespreken.

Ik vertrouw erop dat ik u hiermee voldoende heb geïnformeerd.

Hoogachtend[redacted]

drs. H.T.W.J.M Schoenmakers MMO,
algemeen directeur

N.V. Westerscheldetunnel
Westerscheldetunnelweg 1
4454 PD Borssele
Postbus 303
4460 AS Goes

KvK nr. 220400203
IBAN: NL74ABNA0256718555
BIC: ABNANL2A
BTW nr.: NL 8073.05.509.B.01

tel. 088 9969000
www.westerscheldetunnel.nl
info@westerscheldetunnel.nl
WSTVerkeer