Quickscan
Digitale Weerbaarheid

Gemeente Maassluis

Eindrapport

April 2025

Inhoud

1. Inleiding

1.1 Achtergrond en vraagstelling

Achtergrond

Organisaties in het publieke domein zijn in toenemende mate doelwit van digitale aanvallen. Ook gemeenten zijn steeds meer doelwit van cybercriminaliteit. De gevolgen van een succesvolle hackpoging of gijzeling van bestanden zijn zeer groot. Niet alleen loopt de dienstverlening gevaar, zijn de kosten voor herstel significant, maar tevens heeft het impact op het vertrouwen van bewoners en ondernemers in de gemeente. De Rekenkamer Maassluis heeft voor dit onderwerp gekozen gezien de actualiteit ervan.

Centrale onderzoeksvraag

Hoe goed is de digitale veiligheid binnen de gemeente Maassluis in de verschillend te onderscheiden fasen (preventie, detectie, respons)?

Deelvragen

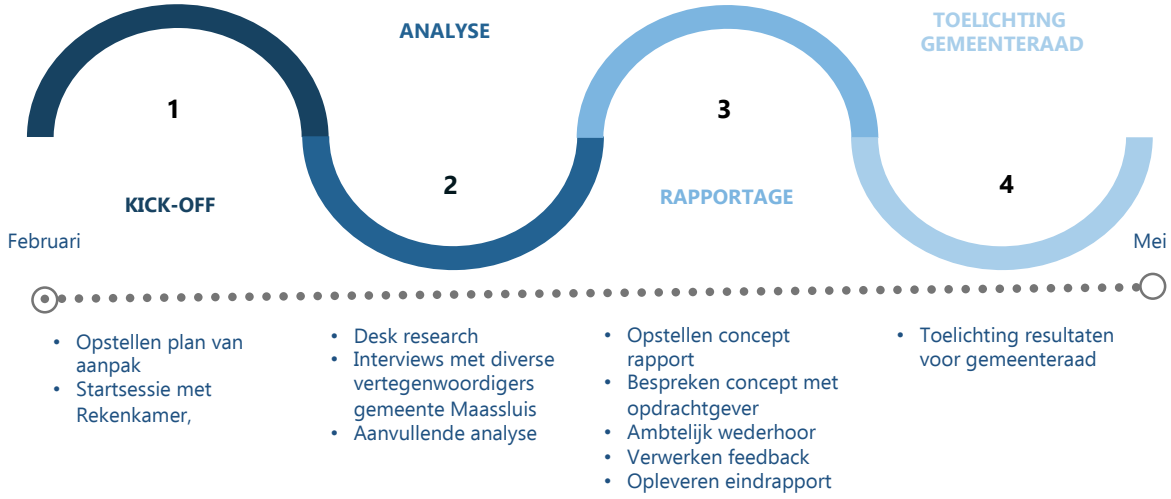
Deze centrale onderzoeksvraag is als volgt uitgewerkt:

1. Zijn er minimale vereisten op het gebied van digitale veiligheid vanuit het Rijk opgelegd aan gemeenten?
2. Is er binnen de gemeente Maassluis een beleid gericht op het borgen van de digitale veiligheid? Waar ziet dit beleid op?
3. Hoe is de verantwoordelijkheid rondom het onderwerp digitale veiligheid binnen de gemeente georganiseerd zowel binnen het college van B&W als de gemeentelijke organisatie zelf?
4. Hoe houdt de gemeente zicht op de grootste risico's ten aanzien van digitale veiligheid en de kwetsbaarheid van haar (uitbestede) systemen?
5. Hoe is de gemeente Maassluis voorbereid in het geval van mogelijke incidenten?
6. Hoe bewust zijn de medewerkers van de gemeente Maassluis als het gaat om digitale veiligheid?
7. Hoe wordt de Raad momenteel geïnformeerd door het College over het onderwerp digitale veiligheid of incidenten rondom digitale veiligheid? En welke controle- en sturingsmogelijkheden heeft de gemeenteraad bij informatiebeveiliging en worden deze ook gebruikt?

1.2 Aanpak

Het uitgevoerde onderzoek is een quickscan. Dit betekent dat het minder diepgravend is dan regulier renkameronderzoek. De resultaten van de quickscan kunnen aanleiding zijn voor verdiepend onderzoek. Basis voor de quickscan zijn desk research en interviews met vertegenwoordigers van gemeente Maassluis.

Onderstaande figuur toont de fasering van de quickscan.



2.Beantwoording onderzoeksvragen

2.1 Minimale vereisten

Zijn er minimale vereisten op het gebied van digitale veiligheid vanuit het Rijk opgelegd aan gemeenten? En in hoeverre voldoet gemeente Maassluis hieraan?

Wet- en regelgeving

Vanuit het Rijk zijn er verschillende vereisten opgelegd aan gemeenten op het gebied van digitale veiligheid. Deze vereisten vloeien voort uit verschillende wetten en regelgeving, zoals (niet uitputtend) de Gemeentewet, Belastingwet, Paspoortwet, Wet algemene bepalingen Burgerservicenummer, Wet basisregistratie personen (BRP), Wet open overheid (voorheen WOB), Wet hergebruik overheidsinformatie en de Auteurswet. Deze begrippen en afkortingen zijn tevens opgenomen in bijlage 2,

Deze wet- en regelgeving stelt eisen aan het informatiebeveiligingsbeleid van gemeenten. Zo verplichten onder andere de Algemene Verordening Gegevensbescherming (AVG), Gemeentewet en Wet BRP gemeenten om persoonsgegevens zorgvuldig te beveiligen tegen onbevoegde inzage, verlies en misbruik. De Paspoortwet en Wet algemene bepalingen Burgerservicenummer schrijven voor dat gemeenten systemen en processen implementeren die fraude met identiteitsgegevens voorkomen. De Wet open overheid en Wet hergebruik overheidsinformatie vereisen dat gemeenten digitale informatie openbaar toegankelijk maken, terwijl ze tegelijkertijd vertrouwelijkheid en privacy blijven garanderen. De Auteurswet verplicht gemeenten tot het treffen van maatregelen ter voorkoming van schending van auteursrechten in digitale systemen.

AVG, BIO(2), NIS(2), Cyberbeveiligingswet

Gemeenten verwerken dagelijks grote hoeveelheden persoonsgegevens en zijn daarbij wettelijk verplicht om deze informatie goed te beveiligen. De AVG (Algemene Verordening Gegevensbescherming) schrijft voor dat persoonsgegevens zorgvuldig moeten worden beschermd. De Wbni (Wet beveiliging netwerk- en informatiesystemen) voegt daar eisen aan toe voor de beveiliging van vitale digitale processen. Deze wettelijke verplichtingen zijn voor gemeenten vertaald naar de BIO (Baseline Informatiebeveiliging Overheid): een praktisch en verplicht normenkader voor informatiebeveiliging. Daarnaast stelt de Europese Netwerk- en Informatiesystemen-richtlijn (NIS), die recent is vervangen door de NIS2, kaders voor de cyberbeveiliging en van essentiële diensten in EU-lidstaten. De NIS2-richtlijn vergroot de reikwijdte van de NIS-richtlijn doordat het meer sectoren omvat, waaronder de sector overheid. Ook stelt de NIS2 strengere beveiligingsnormen en meldingsvereisten voor incidenten. De richtlijn moet door EU-lidstaten worden omgezet in nationale wetgeving. In Nederland gebeurt dit via de Cyberbeveiligingswet die naar verwachting medio 2025 in werking treedt. De eisen van de NIS2 worden door het ministerie van BZK vastgelegd in de vernieuwde BIO2. Concreet betekent dit dat gemeenten passende technische en organisatorische maatregelen dienen te implementeren om aan deze verplichtingen te voldoen. Dit vertaalt zich onder meer in duidelijke procedures, risicoclassificaties van informatiesystemen en het uitvoeren van periodieke risicoanalyses, evenals interne audits en controles.

Met de invoering van de NIS2-richtlijn en de ontwikkeling van de Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten worden vanaf het derde kwartaal van 2025 de verplichtingen rond digitale veiligheid verder aangescherpt. Ook zal op dat moment de vernieuwde BIO2 van kracht worden. Dit betekent concreet dat gemeenten, waaronder Maassluis, te maken krijgen met strengere eisen en aanvullende verplichtingen op het gebied van incidentmanagement, risicobeheersing en monitoring. Het is daarom essentieel dat de gemeente zich tijdig voorbereidt om te kunnen voldoen aan deze aangescherpte normen.

Bevindingen

Gemeenten zijn sinds 2017 verplicht jaarlijks verantwoording af te leggen over naleving van de BIO en bijbehorende regelgeving. Dit gebeurt horizontaal aan de gemeenteraad en verticaal aan het Rijk via de zelfevaluatietool ENSIA (Eenduidige Normatiek Single Information Audit), waarmee zij toetsen of ze voldoen aan de voorgeschreven normen van de BIO[1].

Op basis van de ENSIA-verantwoording hebben wij geïnventariseerd in welke mate gemeente Maassluis voldoet aan de normen. Daarbij hebben we gebruik gemaakt van de volgende indeling uit een de VNG-handreiking, die tevens wordt gehanteerd door de gemeente in haar managementreactie op de ENSIA-verantwoording. Deze bestaat uit de volgende vijf onderdelen:

1. ***Beleid en organisatie.*** Actueel beleid en organisatie van informatiebeveiliging en controle op naleving
2. ***Personeel en toegang.*** Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens
3. ***Continuïteit en incidenten.*** Zorgen voor de continuïteit van onze dienstverlening en opvolging van incidenten
4. ***Informatiesystemen.*** Veilige omgang met informatiesystemen en afspraken hierover met onze leveranciers
5. ***Databescherming.*** Veilige omgang met data in onze software

Bij de beantwoording van de onderzoeksvragen gaan wij in de volgende paragrafen per onderwerp nader in op achtereenvolgens de huidige situatie, geplande maatregelen en de bevindingen op basis van de gerapporteerde afwijkingen.

[1] Dit betreft onder meer BRP, PUN, DigiD, BAG, BGT, BRO, WOZ en SUWInet.

2.2 Beleid gemeente Maassluis

Is er binnen de gemeente Maassluis een beleid gericht op het borgen van de digitale veiligheid? Waar ziet dit beleid op?

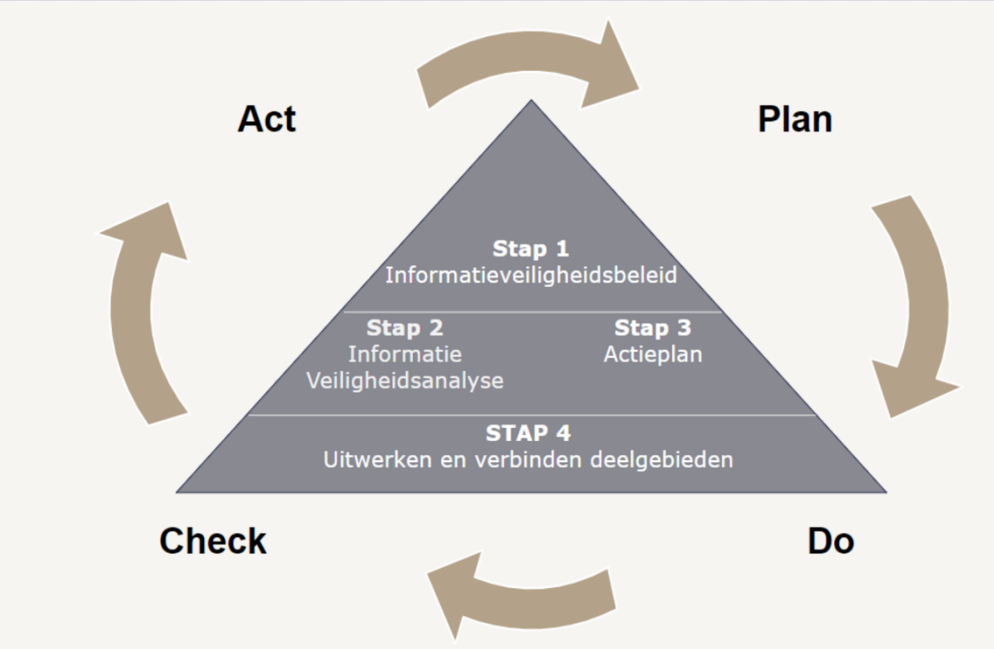
Huidige situatie

Gemeente Maassluis beschikt over een strategisch gemeentebreed informatieveiligheidsbeleid, dat in 2023 is vastgesteld door het College van B en W. De doelstelling van het beleid is als volgt gedefinieerd: "Het bieden van ondersteuning aan het bestuur, management en organisatie bij de sturing op en het beheer van informatieveiligheid."

Het beoogde resultaat is als volgt gedefinieerd: "Beleid waarin de taken, bevoegdheden en verantwoordelijkheden voor Informatieveiligheid, en het vereiste beveiligingsniveau zijn vastgelegd."

De scope van het informatieveiligheidsbeleid, op basis van de Baseline Informatiebeveiliging Overheid, omvat alle gemeentelijke informatieprocessen, zowel ambtelijk als bestuurlijk. Organisatorisch zijn de uitgangspunten uit het beleid van toepassing op zowel de ambtelijke organisatie als op (de leden van) het college. Het geldt tevens voor de Gemeenteraad en de Griffie.

Ter borging van het Informatieveiligheidsbeleid is onderstaande Plan – Do – Check – Act cyclus gedefinieerd, waarbij de resultaten van de verschillende stappen worden vastgelegd in een Information Security Management Systeem, zoals vastgelegd in onderstaande figuur overgenomen uit het Informatieveiligheidsbeleid.



Naast de maatregelen uit de Baseline Informatiebeveiliging Overheid, zijn tevens de wettelijke basis en relevante beveiligingsnormen opgenomen in het Informatieveiligheidsbeleid, waaronder: AVG, Auteurswet, Gemeentewet, Belastingwet, Wet algemene bepalingen Burgerservicenummer, Paspoortwet, Wet basisregistratie personen (Wet BRP), Wet openbaarheid bestuur (WOB) / Wet Open Overheid (WOO), Wet hergebruik overheidsinformatie, Wet politiegegevens, SUWINET, etc alsook de eisen voortkomend uit het Forum Standaardisatie, met name de 'pas toe of leg uit'-lijst, waarin voorgeschreven wordt welke technische NEN normen al dan niet van toepassing zijn voor specifieke implementaties.

In aanvulling op het Strategisch Informatieveiligheidsbeleid, heeft `de gemeente Maassluis het Handboek Informatieveiligheid en Privacy in 2024 opgesteld om het strategische beleid te vertalen naar concrete, tactische richtlijnen, procedures en maatregelen. In het handboek worden twaalf tactische beveiligingscategorieën uit de BIO beschreven, zoals veilig personeel, toegangsbeveiliging, beheer van bedrijfsmiddelen, cryptografie, fysieke beveiliging, beheer van beveiligingsincidenten en naleving. Per categorie zijn doelstellingen, uitgangspunten, richtlijnen en concrete beheersmaatregelen opgenomen. Hierin wordt tevens nader ingegaan op de uitvoering van PDCA-cyclus en de werkzaamheden die in dat kader worden uitgevoerd, zoals het opstellen en uitvoeren van een Actieplan Informatiebeveiliging. Ten slotte wordt tevens dieper ingegaan op de planning van de verantwoordingscycli in het kader van de ENSIA.

Geplande maatregelen

De CISO-organisatie heeft reeds vorig jaar voorbereidingen getroffen om de impact van de aankomende NIS2 en BIO2 richtlijnen te bepalen. De GAP-analyse is nauwgezet uitgevoerd met behulp van een stage-opdracht en geeft inzicht in de te overbruggen afwijkingen, hiermee heeft de organisatie een gedegen voorbereiding getroffen.

Bevindingen

Het informatiebeveiligingsbeleid en het Handboek Informatieveiligheid en privacy zijn opgesteld op basis van de onder 2.1 genoemde vereisten. In de interviews is aangegeven dat de toegankelijkheid van het handboek aandacht verdient. Op basis van onze ervaring kunnen we overigens stellen dat dat ook in andere organisaties vaak het geval is. Het is een beleidsstuk met een brede scope en leent zich daardoor minder om handzaam te worden opgesteld zonder aanzienlijke inspanningen.

2.3 Governance

Hoe is de verantwoordelijkheid rondom het onderwerp digitale veiligheid binnen de gemeente georganiseerd zowel binnen het college van B&W als de gemeentelijke organisatie zelf?

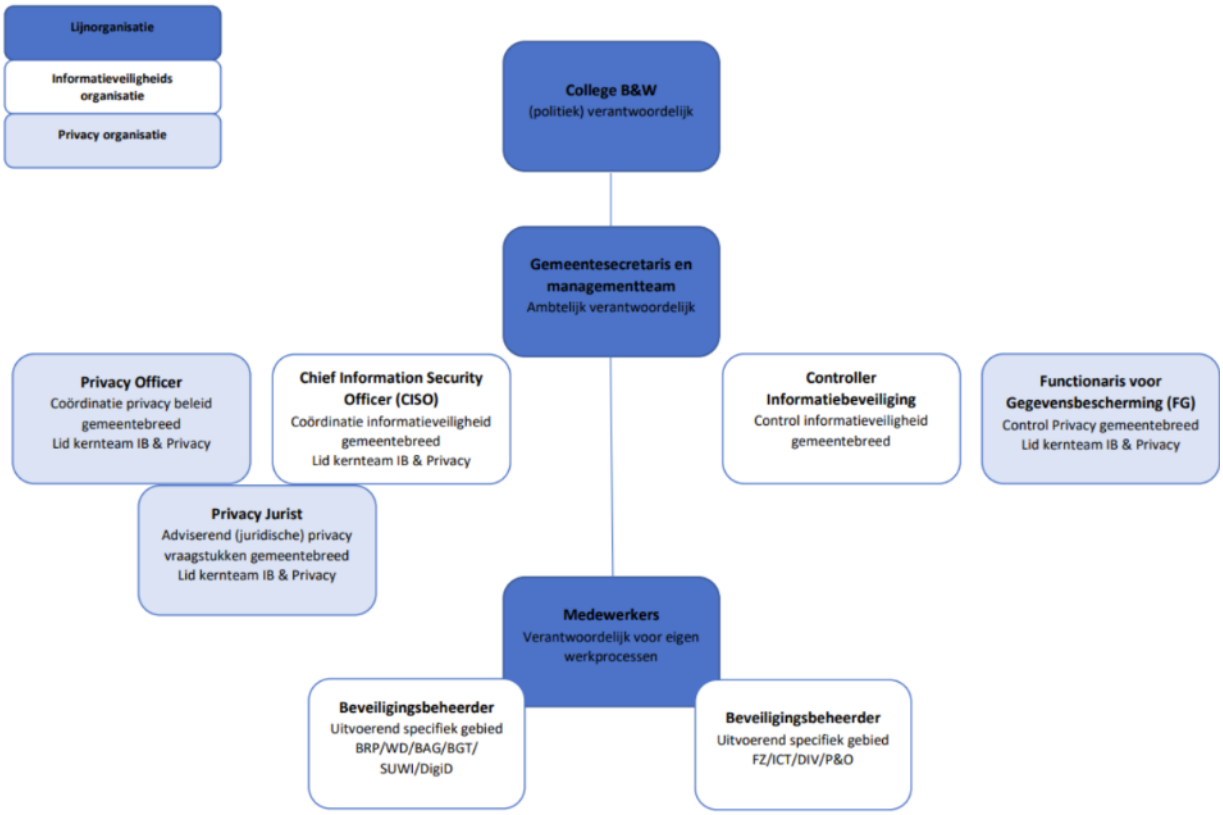
Huidige situatie

College B&W

Binnen de gemeentelijke organisatie is de verantwoordelijkheid voor digitale veiligheid gelaagd en verdeeld over zowel bestuurlijke als operationele niveaus. Het college van burgemeester en wethouders (B&W) draagt de politieke eindverantwoordelijkheid voor alle informatieprocessen en systemen. Zij stellen de beleidskaders vast en maken strategische keuzes, waarna deze verantwoordelijkheden worden gedelegeerd aan de gemeentesecretaris, die ambtelijk eindverantwoordelijk is voor de uitvoering van het vastgestelde beleid.

Ambtelijke organisatie

Onderstaande figuur uit het Strategisch Gemeentebreed Informatieveiligheidsbeleid Gemeente Maassluis 2023 geeft aan hoe de verantwoordelijkheden in de organisatie zijn belegd.



Figuur 1: Organigram (uit: Strategisch gemeentebreed Informatieveiligheidsbeleid Gemeente Maassluis 2023)

De ambtelijke organisatie vertaalt deze kaders verder door naar een aantal gespecialiseerde functies. De Chief Information Security Officer (CISO) fungeert als interne adviseur en coördinator op het gebied van informatieveiligheid. De CISO is verantwoordelijk voor het actueel houden van het informatiebeveiligingsbeleid, het ondersteunen van projecten, het coördineren van het ENSIA-traject en het adequaat afhandelen van ICT-beveiligingsincidenten zoals cyberaanvallen. Tegelijkertijd rapporteert de CISO regelmatig aan het management (in dit geval zowel de ambtelijke leiding alsook

de bestuurlijke leiding, i.c. de wethouder) over de voortgang en eventuele risico's, zodat het bestuur met regelmaat inzicht heeft in de status van de digitale veiligheid.

Naast de CISO zijn de Functionaris voor Gegevensbescherming (FG) en de Privacy Officer (PO) cruciaal voor het waarborgen van de privacy en de bescherming van persoonsgegevens. De FG houdt toezicht op de naleving van de Algemene Verordening Gegevensbescherming (AVG) en de Wet Politiegegevens (Wpg) en fungeert als aanspreekpunt voor de Autoriteit Persoonsgegevens. De PO richt zich op het ontwikkelen, coördineren en bewaken van het gemeentelijke privacybeleid, houdt belangrijke registers bij, zoals het verwerkingsregister en coördineert interne en externe audits[2].

Binnen specifieke domeinen van de gemeentelijke organisatie dragen beveiligingsbeheerders de verantwoordelijkheid voor de veiligheid van systemen zoals DigiD, de Basisregistratie Personen (BRP) of SUWI. Deze functionarissen zorgen ervoor dat de vastgestelde beveiligingsmaatregelen worden nageleefd door periodieke audits en zelfevaluaties uit te voeren en waar nodig advies te geven over de uitvoering van aanvullende maatregelen.

Op operationeel niveau zijn de cluster- en teammanagers verantwoordelijk voor de veiligheid van de informatieprocessen en -systemen binnen hun afdelingen. Zij zien toe op de correcte uitvoering van de beveiligingsmaatregelen en zorgen ervoor dat het gemeentelijke informatieveiligheidsbeleid in de praktijk wordt gebracht. De concerncontroller en de interne controleur vervullen een aanvullende controlerende rol; zij monitoren de algehele bedrijfsvoering, signaleren risico's en adviseren over verbeteringen in de beveiligingsprocessen, waarbij zij nauw samenwerken met de CISO, FG en PO.

Voorts wordt de samenwerking gezocht met soortgelijke organisaties, waaronder het MVS-verband, bestaande uit Maassluis, Vlaardingen en Schiedam. Op deze wijze kunnen relevante ontwikkelingen gezamenlijk worden gevolgd en de inspanningen worden verdeeld, zodat hieruit efficiëntie wordt behaald.

<u>Geplande maatregelen</u>
Recentelijk is een vaste medewerker aangetrokken voor de functie van Privacy Officer (PO). Voorheen werd deze functie parttime ingevuld door een externe kracht. Met het aantrekken van de nieuwe PO ontstaat meer capaciteit voor naleving van zowel BIO als privacywetgeving (AVG). Deze uitbreiding heeft positieve impact op het borgen van de informatieveiligheid en privacyaspecten.

<u>Bevindingen</u>
In de basis zijn de functies, rollen en taken belegd. Vanwege de beperkte omvang van de ambtelijke organisatie is de capaciteit echter beperkt. De organisatie is daardoor, net als andere organisaties van deze schaal, kwetsbaar voor uitval of vertrek van deze sleutelfuncties. Wel wordt opgemerkt dat de organisatie interne maatregelen heeft getroffen voor vervanging gedurende vakanties, dan wel kortdurende uitval, waardoor het risico wordt beperkt.

[2] Een gemeente is verplicht een register van verwerkingsactiviteiten bij te houden. Dit register is een overzicht van de manieren waarop een organisatie persoonsgegevens verwerkt. Het gaat onder andere om welke gegevens worden verwerkt, met welk doel, door wie, en met wie deze gegevens gedeeld worden.

2.4 Risicomanagement

Hoe houdt de gemeente zicht op de grootste risico's ten aanzien van digitale veiligheid en de kwetsbaarheid van haar (uitbestede) systemen?

Huidige situatie

Op basis van uitgevoerde risicoanalyses, controlewerkzaamheden en beveiligingsonderzoeken hebben de opeenvolgende CISO's aantoonbaar aandacht gehad voor risicomanagement. Jaarlijks voert de gemeente een dataclassificatie uit, waarbij systemen worden gekoppeld aan eigenaren en risicoclassificaties. Op basis van deze classificatie wordt vervolgens bepaald of een aanvullende risicoanalyse van processen en/of IT-systemen nodig is.

Op basis van de bevindingen uit deze onderzoeken zijn maatregelen geïnitieerd en reeds gedeeltelijk geïmplementeerd. Aanvullend vindt jaarlijks de verplichte toetsing plaats in het kader van de zelfevaluatie (ENSIA).

De risicoanalyses worden zowel in generieke zin uitgevoerd met een gemeentebrede scope, als gericht op de bedrijfskritische systemen of specifieke aspecten zoals de fysieke en digitale beveiliging van de gemeentelijke organisatie in de vorm van een red cell-onderzoek.

Voorts wordt in het kader van de jaarlijkse financiële verantwoording door de accountant een onderzoek gedaan naar de generieke IT-controls, waarover aan de raad wordt gerapporteerd. De bevindingen uit deze rapportages vormen tevens de input van het risicomanagement.

Recentelijk is opnieuw de gemeentebrede risicoanalyse uitgevoerd, de resultaten hiervan zijn nog onderhanden en derhalve niet beschikbaar. Onderzoeken en activiteiten die voortkomen uit bovengenoemde risicoactiviteiten worden vastgelegd in de activiteitenkalender

Geplande maatregelen

Maatregelen ter mitigatie van de belangrijkste risico's zijn gepland en/of worden voorzien in de loop van 2025, zoals onlangs in de Thema-sessie ICT d.d. 28 januari 2025 aan de Gemeenteraad is gepresenteerd. Actualisatie van bestaande risicoanalyses is ook reeds in uitvoering dan wel gepland.

Belangrijkste geplande maatregel betreft de deelname aan het VNG-traject voor de implementatie van een SOC/SIEM-oplossing. Hiermee krijgt de gemeente betere mogelijkheden voor centraal beheer, logging en actieve monitoring van toegangsbeveiliging en het herkennen van beveiligingsincidenten.

Bevindingen

Hoewel de aandacht voor risico's aantoonbaar aanwezig is, zoals hierboven beschreven, merken wij op dat er geen centraal overzicht bestaat van de geconstateerde afwijkingen, bijbehorende risico's, respectievelijke aanbevelingen en adviezen. Hierdoor is niet eenduidig vast te stellen of alle risico's adequaat worden gemitigeerd, zonder alle separate onderzoeksrapportages door te nemen en vervolgens per risico te bepalen wat de mate van opvolging is.

Er is dus veel aandacht voor het verkrijgen van inzicht in risico's, de opvolging is enigszins diffuus. Wel is aangegeven dat de CISO in 2025 van plan is een overzicht van risico's op te stellen met daarin: status van de bevinding, bijbehorend risico en het betreffende advies dan wel te treffen maatregelen.

Het risicomanagement lijkt aldus voornamelijk impliciet ('het zit met name in de hoofden van betrokkenen') te gebeuren. Dat wil niet zeggen dat het niet effectief is. Dit is echter niet expliciet te toetsen.

2.5 Incidenten

Hoe is de gemeente Maassluis voorbereid in het geval van mogelijke incidenten?

Huidige situatie

De gemeente Maassluis heeft een omvangrijke set aan maatregelen getroffen om adequaat voorbereid te zijn op mogelijke digitale incidenten en calamiteiten. In lijn met het informatieveiligheidsbeleid beschikt de gemeente over een Crisisteam Informatieveiligheid, dat specifiek bijeenkomt bij ernstige incidenten of crisissituaties. Dit team komt onmiddellijk in actie om de negatieve gevolgen zoveel mogelijk te beperken en te zorgen voor duidelijke en effectieve communicatie richting betrokken partijen en belanghebbenden, met name op het niveau van de veiligheidsregio en meer gericht op de integrale beveiliging. Voorts gaan wij dieper in op de geplande maatregelen en de ontbrekende maatregelen die een impact hebben op de mate waarin gemeente Maassluis is voorbereid op mogelijke incidenten, met name gericht op ICT.

Geplande maatregelen

Op dit onderwerp staat een significant aantal maatregelen gepland. Momenteel wordt er gewerkt aan een bedrijfscontinuïteitsplan (BCP) dat in 2025 verder zal worden ontwikkeld. Als onderdeel van deze werkzaamheden zijn de uitwijktesten gepland voor Q4 2025. Het BCP-plan is bedoeld om de beschikbaarheid van essentiële processen, systemen en daarmee de dienstverlening van de gemeente tijdens en na incidenten te waarborgen. Naast het BCP-plan, is de implementatie van SOM/SIEM-dienstverlening gepland, waarmee de monitoring consistent actief kan worden uitgevoerd. Dit houdt in dat mogelijke incidenten sneller kunnen worden herkend, waardoor de gemeente sneller kan reageren.

Bevindingen

Zoals benoemd, is het bedrijfscontinuïteitsplan (BCP) op gemeentelijk niveau nog in ontwikkeling, zodoende kan eigenlijk niet worden vastgesteld in hoeverre de gemeente is voorbereid op mogelijke, serieuze incidenten, zoals een succesvolle ransomware-aanval of technische malaise. De gemeente Maassluis heeft de processen voor incidentafhandeling ingericht met behulp van TopDesk[3]. Op die wijze worden incidenten centraal vastgelegd, waarna deze worden toegewezen aan de juiste verantwoordelijken. Zodoende worden incidenten gestructureerd opgevolgd.

Voorts heeft de gemeente het niveau van beveiliging laten testen en heeft daarop aanvullende maatregelen getroffen, zodoende bestaat er wel inzicht in hoeverre de gemeente kwetsbaar is voor dergelijke incidenten (zicht op zogenaamde aanvalsvectoren). Het is echter nog niet gevalideerd of de aangetroffen kwetsbaarheden effectief zijn verholpen. Aanvullend wordt gerapporteerd door de gemeente dat niet volledig duidelijk is in hoeverre back-up en recovery-maatregelen adequaat zijn.

Hoewel logging in generieke zin is ingeregeld, wordt deze niet actief gemonitord. Hierdoor reageert de gemeente mogelijkerwijs te laat in geval incidenten. Daarnaast valt er momenteel niet te beoordelen in welke mate de gemeente op basis van onderzoek kan achterhalen wat de aard en oorzaak van een mogelijk incident was. Ten slotte is op verschillende vlakken het autorisatiebeheer onvoldoende effectief ingeregeld, waardoor risico's bestaan op onduidelijkheid en inconsistentie in toegangsbeheer.

[3] Een servicemanagementapplicatie dat binnen de organisatie wordt gebruikt, met onder andere de mogelijkheid om "tickets" aan te maken voor incidenten.

2.6 Bewustzijn ambtelijke organisatie

Hoe bewust zijn de medewerkers van de gemeente Maassluis als het gaat om digitale veiligheid?

Huidige situatie

De gemeente Maassluis heeft verschillende voorzieningen om het informatiebewustzijn van haar medewerkers te vergroten. Jaarlijks wordt per cluster een specifiek budget beschikbaar gesteld voor trainingen. Sinds september 2022 is daarnaast een online academie beschikbaar, inclusief een digitaal onboarding-programma voor nieuwe medewerkers. Alle medewerkers volgen verplicht een algemene I-bewustzijnstraining via deze academie. Nieuwe medewerkers krijgen binnen drie maanden na indiensttreding een specifieke bewustzijnstraining aangeboden. Voor functies met hogere risico's, zoals medewerkers die SUWInet Inkijk gebruiken bij Burgerzaken, zijn aanvullende trainingen verplicht. Tot slot zijn het Strategisch Informatieveiligheidsbeleid en het Handboek Informatieveiligheid en Privacy centraal toegankelijk via het serviceplein van het Social Intranet, zodat richtlijnen en beleidsinformatie eenvoudig beschikbaar zijn voor iedereen.

Geplande maatregelen

In de interviews is aangegeven dat de gemeente voornemens is om de bewustzijnstraining informatiebeveiliging uit te breiden en gespreid over het gehele jaar aan te bieden. Door medewerkers gedurende een langere periode herhaaldelijk te trainen in kortere momenten, wordt verwacht dat zij meer kennis opnemen en daarmee (nog) meer beter bewust worden van veiligheidsrisico’s en hoe ermee om te gaan.

Bevindingen

Hoewel er dus op verschillende manieren aan wordt gewerkt om het informatieveiligheidsbewustzijn van de medewerkers te vergroten, maken we uit de interviews op dat de CISO en de PO veelal op ad hoc basis en in een later stadium betrokken worden bij (nieuw) beleid en projecten. Zo is bijvoorbeeld aangegeven dat de verplichte Data Protection Impact Assessments (DPIA's) regelmatig pas uitgevoerd wanneer een project al vergevorderd is. Consequentie is dat er geen goed overzicht is van de veiligheids- en privacy-risico's, dergelijke risico’s laat worden geïdentificeerd en beveiligingsmaatregelen niet consistent worden toegepast.

2.7 Informatievoorziening, controle- en sturingsmogelijkheden gemeenteraad

Hoe wordt de Raad momenteel geïnformeerd door het College over het onderwerp digitale veiligheid of incidenten rondom digitale veiligheid? En welke controle- en sturingsmogelijkheden heeft de gemeenteraad bij informatiebeveiliging en worden deze ook gebruikt?

De gemeenteraad vormt het hoogste bestuurlijke orgaan binnen de gemeente en heeft daarom een cruciale verantwoordelijkheid voor informatiebeveiliging. Vanuit deze rol beschikt zij over belangrijke controle- en sturingsinstrumenten. In algemene zin gaat het om de volgende mogelijkheden:

- Het vaststellen van kaders en beleid, zoals bijvoorbeeld het informatieveiligheidsbeleid.
- Vanuit haar controlerende taak kan de raad toezicht en controle uitvoeren. De jaarlijkse ENSIA-verantwoording biedt hiervoor een goed aangrijpingspunt. Verder kan de raad verzoeken doen voor aanvullende onderzoeken en zich laten informeren in commissievergaderingen en raadsinformatiebijeenkomsten
- Met het budgetrecht kan de raad financiële middelen beschikbaar stellen en daarmee sturing hebben op en doelen stellen ten aanzien van de informatieveiligheid. Via de begrotings- en verantwoordingscyclus kan de raad de voortgang monitoren en bijsturen.

De primaire controlemogelijkheid is het jaarlijks uitgevoerde ENSIA-proces, waarmee de raad systematisch inzicht krijgt in de status van informatiebeveiliging binnen de gemeente, inclusief de zienswijze van de ambtelijke organisatie op deze verantwoording in de vorm van de managementreactie. Hiermee kunnen de raadsleden beoordelen of het college van B&W voldoet aan de gestelde beveiligingsnormen en -eisen. In de vorm van themasessies wordt de Raad door de ambtelijke organisatie geïnformeerd over de oplossingsrichting en voortgang van de implementatie. De raadsleden hebben hierbij tevens de mogelijkheid direct vragen te stellen aan de betrokken ambtenaren.

Op basis van een analyse van de raadsdocumenten in 2024, zoals deze beschikbaar zijn via het raadsinformatiesysteem op de website van de gemeente Maassluis, stellen wij vast dat het onderwerp in het algemeen geen specifieke aandacht krijgt, anders dan via de reguliere behandeling van beleids- en verantwoordingsdocumenten, zoals de ENSIA-verantwoording[4]. Daarnaast kreeg informatiebeveiliging veel aandacht tijdens een recent georganiseerde informatiebijeenkomst (thema-avond).

[4] Advies B en W Verantwoording ENSIA 2023 en Informatiebeveiligingsbeleid 2024, 12 maart 2024

3.Conclusie en aanbevelingen

3.1 Conclusie

Op koers maar kwetsbaar
De volgende vraag staat centraal in de quickscan:

Hoe goed is de digitale veiligheid binnen de gemeente Maassluis in de verschillend te onderscheiden fasen (preventie, detectie, respons)?

Op basis van onze bevindingen concluderen we dat de digitale veiligheid van de gemeente Maassluis in ontwikkeling is en voor een belangrijk deel voldoet aan de landelijke vereisten. Er is de afgelopen jaren behoorlijk geïnvesteerd in het op niveau brengen van de informatieveiligheid. Zo is er een actueel beleidsmatig fundament, zijn er verschillende onderzoeken en audits uitgevoerd om de risico's te inventariseren, zijn de rollen van verantwoordelijken zoals de CISO en Privacy Officer duidelijk belegd, voldoet de organisatie aan een substantieel deel van de wettelijke normen, zoals de BIO en is er structureel aandacht voor risicomanagement.

Er zijn ook kwetsbaarheden die aandacht verdienen. Dan gaat het onder andere om de implementatie van voorgenomen maatregelen die de informatieveiligheid substantieel kunnen verbeteren, zoals SOC/SIEM en bedrijfscontinuïteitsplannen. De plannen zijn er; de uitvoering en borging moeten nog plaatsvinden. Vanwege de verwachte inwerkingtreding van de Cyberbeveiligingswet ofwel NIS2-richtlijn, krijgen deze maatregelen een verplicht karakter in het kader van de zorgplicht alsmede vormen zij een essentieel onderdeel voor de meldplicht[5].

Kijken we specifiek naar de verschillende fasen, dan concluderen we als volgt:

- ***Preventie.*** De basis is op orde: er is een actueel informatiebeveiligingsbeleid dat geldt voor de hele organisatie – van college tot ambtenaren – en dit wordt aangevuld met een concreet handboek. Ook is bewustwording onder medewerkers onderdeel van het beleid, onder meer via trainingen. Toch ontbreekt het aan gestructureerde opvolging van risico's en incidenten en worden beveiligingsmaatregelen nog niet consequent vooraf meegenomen in projecten.
- ***Detectie.*** De detectie van digitale risico's en incidenten is nog niet volledig ingericht. Logging en met name monitoring zijn (nog) onvoldoende operationeel en er is geen centrale tool voor overzicht en alarmering. Hierdoor is het moeilijk te achterhalen wat er precies is gebeurd bij een incident.
- ***Respons.*** Hoewel er een crisisteam is en incidenten via een intern systeem worden opgevolgd, ontbreekt een uitgewerkt en getest bedrijfscontinuïteitsplan (BCP). Hierdoor is de voorbereiding op ernstige incidenten, zoals een ransomware-aanval, beperkt. Hoewel back-ups regelmatig worden getest, wordt niet de gehele keten getest, wat het risico op dataverlies vergroot.

Ten aanzien van de deelvragen uit de quickscan concluderen we het volgende:

[5] NCSC Cyberbeveiligingswet (NIS2-richtlijn): https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie

1. *Zijn er minimale vereisten op het gebied van digitale veiligheid vanuit het Rijk opgelegd aan gemeenten?* Ja, het Rijk stelt via wet- en regelgeving zoals de BIO, AVG en de opkomende NIS2-richtlijn eisen aan gemeenten. Maassluis voldoet hier grotendeels aan.
2. *Is er binnen de gemeente Maassluis een beleid gericht op het borgen van de digitale veiligheid? Waar ziet dit beleid op?* Er is actueel informatiebeveiligingsbeleid (2023) en een handboek (2024). De scope is breed; de toegankelijkheid van het handboek vraagt aandacht.
3. *Hoe is de verantwoordelijkheid rondom het onderwerp digitale veiligheid binnen de gemeente georganiseerd zowel binnen het college van B&W als de gemeentelijke organisatie zelf?* De verantwoordelijkheden zijn belegd bij het college, gemeentesecretaris, CISO, PO en FG. Er is wel sprake van kwetsbaarheid door beperkte capaciteit en afhankelijkheid van sleutelfunctionarissen.
4. *Hoe houdt de gemeente zicht op de grootste risico's ten aanzien van digitale veiligheid en de kwetsbaarheid van haar (uitbestede) systemen?* Er worden risicoanalyses uitgevoerd, onder andere via ENSIA, DPIA's en audits. Er is echter geen centraal overzicht van risico's en opvolging, waardoor het moeilijk is om consistentie en volledigheid te beoordelen.
5. *Hoe is de gemeente Maassluis voorbereid in het geval van mogelijke incidenten?* Er is een crisisteam en incidentenregistratie (TopDesk), maar het bedrijfscontinuïteitsplan (BCP) is nog in ontwikkeling en actieve monitoring ontbreekt nog grotendeels.
6. *Hoe bewust zijn de medewerkers van de gemeente Maassluis als het gaat om digitale veiligheid?* Trainingen en een online academie zijn ingericht, maar borging van veiligheid in gedrag is nog beperkt. De CISO/PO worden vaak te laat betrokken bij projecten en DPIA's worden ad hoc uitgevoerd.
7. *Hoe wordt de Raad momenteel geïnformeerd door het College over het onderwerp digitale veiligheid of incidenten rondom digitale veiligheid?* En welke controle- en sturingsmogelijkheden heeft de gemeenteraad bij informatiebeveiliging en worden deze ook gebruikt? Het college stelt de ENSIA-verantwoording jaarlijks vast en dit besluit is te vinden op het raadsinformatiesysteem bij de collegevergaderingen. De gemeenteraad krijgt hierover echter geen actieve informatie van het college. De inhoud van de adviezen, toelichting en onderbouwing is echter geheim geclassificeerd vanwege de vertrouwlijkheid in het kader van informatieveiligheid en privacy. In themabijeenkomsten wordt de raad daarentegen geïnformeerd over de te treffen maatregelen. Alles overziend benut de Raad haar mogelijkheden voor actieve sturing en controle nog beperkt.

3.2 Aanbevelingen

Op basis van de conclusies komen we tot de volgende aanbevelingen:

1. ***Versnel implementatie van monitoring en incidentdetectie.*** Gemeente Maassluis heeft momenteel geen centrale monitoring ingeregeld, wat snelle detectie van incidenten en reconstructie belemmert. De implementatie van SOC/SIEM biedt een uitstekend handvat om grip te krijgen op de monitoring van essentiële onderdelen van het IT-landschap en stelt de gemeente in staat incidentdetectie adequaat uit te voeren. De omvang en complexiteit van een SOC/SIEM-implementatie kan echter tegenvallen in de praktijk. Het is daarom aan te bevelen deimplementatie van het SOC/SIEM-traject te versnellen en zorg voor continue monitoring van toegang en netwerkverkeer. Overweeg een vervolgonderzoek naar de

implementatie van logging & monitoring: zijn systemen actief, effectief en structureel ingezet? Maak hierbij gebruik van bijvoorbeeld de gezamenlijke basisprincipes voor digitale weerbaarheid van het Nationaal Cyber Security Centrum[6]. Daarnaast geldt voor gemeenten, net als andere overheidsinstanties onder de NIS2-implementatiewet, zorgplicht, toezicht en een meldplicht[7]. Hierdoor wordt een tijdige detectie van incidenten essentieel.

2. ***Rond het bedrijfscontinuïteitsplan (BCP) af en test back-up voorzieningen.*** Zonder een getest BCP en back-upstrategie is de gemeente kwetsbaar bij verstoringen of aanvallen. Ontwikkel het BCP met scenario's voor kritieke processen en test jaarlijks uitwijkscenario's en back-up hersteloperaties. Overweeg vervolgonderzoek naar de crisisgereedheid en weerbaarheid bij verstoringen: hoe functioneert het BCP in de praktijk? Dit is mede van belang vanwege de tien zorgplichtmaatregelen waaraan gemeenten ten minste aan dienen te voldoen in het kader van de Cyberbeveiligingswet (NIS2)[8].

3. ***Borg capaciteit en sturing op de implementatie van maatregelen.*** Gemeente Maassluis is voornemens verschillende maatregelen te implementeren om de informatieveiligheid (nog) beter te borgen. Dit doet een behoorlijk beroep op capaciteit en budget en er is een grote afhankelijkheid van enkele sleutelfunctionarissen. Het is daarom van belang dat de organisatie over voldoende middelen (financieel, personeel) beschikt, implementatieprojecten realistisch prioriteert en de voortgang actief monitort en waar nodig bijstuurt. Overweeg een vervolgonderzoek op de haalbaarheid en risico's van de implementatie van de voorgenomen maatregelen.

4. ***Versterk bewustzijn, houding en gedrag in de ambtelijke organisatie.*** De mens is een van de belangrijkste factoren in de informatieveiligheid. Gemeente Maassluis biedt trainingen en is gestart met een nieuwe bewustzijnscampagne. Afgevraagd kan worden of er in dit verband in de reguliere bedrijfsvoering voldoende aandacht is. Denk aan het in een vroeg stadium betrekken van de CISO en/of PO bij de start van projecten, nieuw beleid of (veranderingen) in de uitvoering; het opnemen van informatieveiligheid als thema in functioneringsgesprekken; voorbeeldgedrag van leidinggevenden en het uitbreiden van bewustzijnscampagnes met kort-cyclische bewustzijnstrainingen door het jaar heen. Overweeg vervolgonderzoek naar de cultuur rond informatieveiligheid: hoe bewust, handelend en verantwoordelijk voelen ambtenaren zich in de praktijk?

5. ***Activeer de sturingsrol van de gemeenteraad.*** De gemeenteraad beschikt over formele sturingsmiddelen, maar benut deze beperkt. De ENSIA-verantwoording biedt een goede basis om invulling te geven aan de controlerende taak. Daarbij is het van belang dat de actief en op een toegankelijke wijze geïnformeerd wordt. Denk bijvoorbeeld aan een compacte raadsinformatiebrief met daarin de kern van de ENSIA-verantwoording. Daarnaast is het van belang dat de gemeenteraad goed geïnformeerd wordt over de voortgang van de

[6] website: https://www.ncsc.nl/actueel/nieuws/2025/04/04/ncsc-en-dtc-lanceren-gezamenlijke-basisprincipes-voor-digitale-weerbaarheid
[7] NIS2 nieuws VNG: https://vng.nl/artikelen/cyberbeveiligingswet-nis2-nieuws-en-updates
[8] Zorgplicht: tien zorgplichtmaatregelen: https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/hoe-kan-uw-organiseren-zich-voorbereiden-op-de-nis2-richtlijn

implementatie van (voorgenomen) maatregelen, incidenten en oplossingsacties, bijvoorbeeld in de vorm van een vast rapportageformat en -cyclus. En organiseer periodiek een themabijeenkomst waarin de ambtelijke organisatie (manager informatievoorziening, CISO en Privacy Officer) de gemeenteraad op actualiteit en specifieke onderwerpen bijpraten. Ten aanzien van de kaderstellende rol van de gemeenteraad adviseren we de raad actief te betrekken bij het bepalen van de meerjarenvisie en (operationele) doelstellingen op het gebied van informatieveiligheid, inclusief het budgettair beslag. Zeker in het licht van de toenemende (cyber)dreigingen en de druk op de begroting vanwege het verwachte 'Ravijnjaar' is het essentieel de gemeenteraad te betrekken bij prioriteitsstelling. Overweeg, tot slot, vervolgonderzoek naar de governance. Centrale vragen daarin zijn: hoe functioneert de horizontale verantwoording over digitale veiligheid en is de controlerende rol van de gemeenteraad effectief?

Reactie van college van B&W

gemeente Maassluis

Postbus 55
3140 AB Maassluis

T 14 010
E gemeente@maassluis.nl
I www.maassluis.nl

Aan de Rekenkamercommissie van de
gemeente Maassluis

ons kenmerk		datum	21 mei 2025
uw kenmerk	857545	uw brief van	April 2025
contactpersoon	Schippers, S.M.	doorkiesnummer	0103127209
onderwerp	Reactie op het eindrapport "Quickscan Digitale Weerbaarheid Gemeente Maassluis	bijlage(n)	0

Geachte leden van de Rekenkamercommissie van de gemeente Maassluis,

Naar aanleiding van het door de Rekenkamer opgestelde eindrapport inzake de quickscan digitale weerbaarheid van de gemeente Maassluis, biedt het college van burgemeester en wethouders u hierbij onze bestuurlijke reactie aan. Het onderwerp informatieveiligheid is van cruciaal belang, gezien de toenemende dreigingen op het gebied van cybercriminaliteit en de verplichtingen die voortvloeien uit nationale en Europese regelgeving.

Het rapport biedt een actueel beeld van de stand van zaken op het gebied van digitale weerbaarheid binnen onze gemeente. Wij waarderen de inspanningen van de Rekenkamer om een grondige analyse te maken en dragen de conclusies en aanbevelingen met zorg over aan de gemeentelijke organisatie. Hieronder vindt u onze reactie op de belangrijkste bevindingen en aanbevelingen.

1. Conclusies uit het rapport
Uit de quickscan blijkt dat de gemeente Maassluis in de afgelopen jaren belangrijke stappen heeft gezet om haar digitale weerbaarheid te verbeteren. De ontwikkeling en implementatie van een strategisch informatieveiligheidsbeleid, de aanstelling van sleutelfunctionarissen zoals de CISO en Privacy Officer, en het uitvoeren van risicoanalyses zijn belangrijke mijlpalen.

Tegelijkertijd erkent het college dat er nog stappen te nemen zijn, zoals:

- Het ontbreken van een volledig operationeel bedrijfscontinuïteitsplan (BCP).
- Het nog niet volledig ingeregelde proces rondom logging, monitoring en incidentdetectie.
- De beperkte capaciteit in relatie tot de omvang van de taken en de afhankelijkheid van cruciale sleutelfunctionarissen.
- Het ontbreken van een centraal overzicht van risico's en opvolging.

2. Reactie op aanbevelingen
Het college herkent zich in de aanbevelingen uit het rapport en zet zich in voor de verdere versterking van de digitale weerbaarheid. Hieronder een reactie per aanbeveling:

a. Versnel de implementatie van monitoring en incidentdetectie
Het college onderschrijft het belang van centrale monitoring en incidentdetectie. De implementatie van SOC/SIEM-diensten wordt actief opgepakt en is reeds onderdeel van een lopend traject binnen het VNG-programma. Wij streven ernaar om de inventarisatie van wensen en eisen met prioriteit af te ronden in 2025.

b. Rond het bedrijfscontinuïteitsplan (BCP) af en test back-up voorzieningen
Het testen van back-up voorzieningen werd al gedeeltelijk gedaan en zal worden uitgebreid. Het ontwikkelen en testen van een BCP staat daarnaast hoog op de agenda. Wij streven ernaar om het BCP uiterlijk in het vierde kwartaal van 2025 operationeel te hebben.

c. Vergroot capaciteit en borging van maatregelen
Wij onderkennen het belang van continuïteit op sleutelposities, maar achten de huidige borging binnen onze organisatie voldoende. In situaties waarin dit noodzakelijk is, kunnen de betreffende functies adequaat worden waargenomen door andere daartoe bekwame medewerkers. Hiermee is een passende mate van continuïteit gewaarborgd. Het aantrekken van een vaste Privacy Officer is recent een belangrijke stap geweest.

d. Versterk bewustzijn en gedrag binnen de organisatie
Het college onderschrijft het belang van een versterkte bewustzijnscultuur. Wij breiden de huidige trainingsprogramma's verder uit en maken bewustwording een integraal onderdeel van de reguliere bedrijfsvoering. Er zal worden ingezet op een manier door bewustzijn frequenter onder de aandacht te brengen.

e. Activeer de sturingsrol van de gemeenteraad
Wij zien het als onze taak om de gemeenteraad actief en toegankelijk te informeren. Naast de jaarlijkse ENSIA-verantwoording, die reeds beschikbaar wordt gesteld, zal het college een halfjaarlijkse raadsinformatiebrief introduceren waarin de voortgang van maatregelen, incidenten en risico's worden toegelicht.

3. Tot slot
Het college is zich bewust van de urgentie en het belang van digitale weerbaarheid in het licht van de toenemende dreigingen en de aangescherpte eisen vanuit de NIS2-richtlijn en de BIO2-norm. Wij zullen de voortgang van de verbetermaatregelen nauwgezet volgen en hierover via een raadsinformatiebrief rapporteren aan de raad.

Wij vertrouwen erop dat deze reactie u voldoende inzicht biedt in de inspanningen en voornemens van het college. Wij blijven graag in gesprek over dit belangrijke onderwerp en zien eventuele vragen of opmerkingen met belangstelling tegemoet.

Hoogachtend,
het college van Burgemeester en Wethouders van Maassluis,

de secretaris,	de burgemeester
Ing. P.D. Verstoep	drs. J.G. de Vries

Dit document is digitaal ondertekend.

Bijlage 1 - Geïnterviewde personen en bestudeerde documenten

Geïnterviewde personen gemeente Maassluis

- Denise Mulder-Solleveld, portefeuillehouder Informatisering & Automatisering
- Sander Schippers, Chief Information Security Officer
- Michel van den Thoorn, Teammanager Informatievoorziening
- Irma Visser, Privacy Officer

Bestudeerde documenten

Beleidsdocumenten

- Strategisch gemeentebreed informatieveiligheidsbeleid Maassluis 2023
- Handboek Informatieveiligheid en privacy Maassluis 2024
- Werkplan privacy (AVG) Maassluis
- Toezichtsbeleid Wpg Maassluis

Rapportages

- Aanvullende risicoanalyse Maassluis, aanvullende risicoanalyse MAPGOOD & Heronderzoek toegankelijkheidzaaksysteem
- Procedure Controle Plan BIO-2, IST analyse verslag 2024 & Controleplan BIO-2.xlsx (Scriptie onderzoek)
- Gemeente Maassluis BIO-rapportage ENSIA 2023 & 2024
- Gemeente Maassluis Management IB en privacy 2023 & 2024
- Gemeentebrede risicoanalyse Informatieveiligheid gemeente Maassluis 2023
- Gemeente-Maassluis-RedCell-RAPPORT-v1.0
- IT audit 2023 & 2024

PDCA documenten

- Activiteitenkalender
- Kernteam IB en privacy overleggen: bewijsstukken van plaatshebben overleggen Kernteam IB en Privacy.
- Opzet awareness informatieveiligheid V3: presentatie voor de bewustwordingssessie
- C 08 - Topdesk periodieke controle Zaaksysteem
- overzicht Incidentmeldingen PinkRoccade 2024
- Overzicht verwerking en registratie Topdesk releasenotes iBurgerzaken 2024
- Dataclassificatie Maassluis
- Kritieke-processen-gemeenten
- Bewijsstukken TPM-verklaringen

Bijlage 2 – Begrippen en afkortingenlijst

Afkorting	Betekenis	Referentie
2-FA	2-Factor Authenticatie	Onderdeel van Multi-Factor Authenticatie, vereist meerdere bewijsmiddelen voor toegang - BIO
AFAS	AFAS Software (bedrijfssoftware voor HR, Finance)	Gemeente-specifieke leverancierreferentie
AVG	Algemene Verordening Gegevensbescherming	https://autoriteitpersoonsgegevens.nl
BAG	Basisregistratie Adressen en Gebouwen	Kadaster, Wet BAG
BCP	Business Continuity Plan	BIO, VNG, NEN-ISO 22301
BGT	Basisregistratie Grootschalige Topografie	Kadaster, Wet BGT
BIO	Baseline Informatiebeveiliging Overheid	https://bio-overheid.nl, VNG, IBD
BRO	Basisregistratie Ondergrond	Ministerie van BZK - https://www.basisregistratieondergrond.nl
BRP	Basisregistratie Personen	Wet BRP - https://www.rvig.nl
BSN	Burgerservicenummer	Wet algemene bepalingen BSN
CISO	Chief Information Security Officer	BIO, gemeentelijke informatiebeveiligingsstructuur
DPIA	Data Protection Impact Assessment (Gegevensbeschermingseffect–beoordeling)	AVG, verplicht bij gegevensverwerkingen met hoog risico - https://autoriteitpersoonsgegevens.nl
DigiD	Digitale Identiteit	Logius - https://www.digid.nl
ENSIA	Eenduidige Normatiek Single Information Audit	VNG, Informatiebeveiliging en ENSIA - https://www.vngrealisatie.nl/ensia
FG	Functionaris Gegevensbescherming	AVG, verplicht bij overheden
GBA	Gemeentelijke Basisadministratie	Historisch, vervangen door BRP
IBD	Informatiebeveiligingsdienst voor gemeenten	https://www.informatiebeveiligingsdienst.nl

Afkorting	Betekenis	Referentie
IOAW	Inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers	Participatiewet, UWV
IOAZ	Inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen	Participatiewet, UWV
MVS-verband	Maassluis, Vlaardingen en Schiedam	Samenwerkingsverband tussen de gemeenten Maassluis, Vlaardingen en Schiedam
NEN	Nederlandse Normen (zoals NEN-ISO 27001)	https://www.nen.nl
NIS	Netwerk- en Informatiebeveiligingsrichtlijn	Europese richtlijn NIS1, Wbni
NIS2	Netwerk- en Informatiebeveiligingsrichtlijn 2	EU NIS2, implementatie in nationale wetgeving 2024-2025
PDCA-cyclus	Plan-Do-Check-Act cyclus (verbetercyclus)	BIO, ISO 27001, VNG
PO	Privacy Officer	Gemeentelijke uitvoering van AVG
PTOLU-lijst	Pas toe of Leg uit-lijst, in het kader van onderbouwen van implementatie van standaarden	IBD, VNG
PUN	Persoonsgebonden Uitkering naar Normbedrag	Participatiewet / Gemeentelijk beleid
SOC/SIEM	Security Operations Center / Security Information and Event Management	IBD, NCSC, BIO-richtlijnen
SUWINET	Systeem Uitwisseling Informatie Sociale Zekerheid	SUWI-wet, Rijksoverheid - https://www.rijksoverheid.nl
TPM-verklaring	Third Party Mededeling (assurance-verklaring door externe partij)	Norea - https://www.norea.nl
TopDesk	TopDesk (servicemanagementsysteem)	Software voor IT- en facilitaire serviceprocessen binnen o.a. gemeenten - https://www.topdesk.com
VNG	Vereniging van Nederlandse Gemeenten	https://www.vng.nl
WOB	Wet Openbaarheid van Bestuur	Vervallen, vervangen door WOO

Afkorting	Betekenis	Referentie
WOO	Wet open overheid	https://www.rijksoverheid.nl/onderwerpen/open-overheid
WOZ	Waardering Onroerende Zaken	Wet WOZ, Gemeentelijke belastingen
WPG	Wet Politiegegevens	
Wbni	Wet beveiliging netwerk- en informatiesystemen	Implementeert de Europese NIS-richtlijn in Nederland - https://wetten.overheid.nl/BWBR0040988

Bijlage 3 – Mate waarin voldaan is aan de BIO-normen

In onderstaande tabel zijn de afwijkingen nader geduid. Belangrijk is op te merken dat het voornamelijk afwijkingen betreft ten aanzien van de BIO-norm. Afwijkingen ten opzichte van de andere genoemde richtlijnen zoals de SUWINET, Politiewet, IOAZ of IOAW zijn beperkt tot normen die te maken hebben met het ontbreken van een SOC/SIEM voorziening.

1. BELEID EN ORGANISATIE Actueel beleid en organisatie van informatiebeveiliging en controle op naleving	32	- 28 normen voldoen - 4 normen voldoen niet

Het onderwerp Beleid en Organisatie omvat de hoofdstukken 5 Informatiebeveiligingsbeleid, 6 Organiseren van Informatiebeveiliging en 18 Naleving. De geconstateerde afwijkingen hebben betrekking op:

Mobile device management (H6): Op dit moment zijn de mobiele apparaten zoals mobiele telefoons nog niet volledig ingericht zodanig dat niet langer vertrouwelijke informatie op het apparaat wordt opgeslagen. Hiertoe is een project opgezet dat reeds in 2023 in gang is gezet om deze apparaten met behulp van Mobile device management (hierna: MDM) beter te beveiligen. Alle laptops zijn reeds opgenomen in MDM, dat geldt tevens voor het grootste gedeelte van de in gebruik zijnde telefoons. Een beperkt aantal telefoons wordt dus nog niet beschermd met Mobile Device Management.

Naleving (H18): Ten aanzien van de toetsing op naleving van het beleid zijn drie afwijkingen geconstateerd. Hoewel aan het merendeel van de maatregelen wordt voldaan, word de logging van de verwerking van persoonsgegevens niet regelmatig gecontroleerd op rechtmatig gebruik. Daarnaast wordt niet expliciet getoetst of de cyrptografische beheersmaatregelen expliciet voldoen aan de Pas-to-of-Leg-uit-lijst van het Forum van Standaardisatie (PTOLU-lijst). Ten slotte beschikt de organisatie niet over een vastgesteld auditplan.

2. PERSONEEL EN TOEGANG Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens	60	- 52 normen voldoen - 8 normen voldoen niet

Het onderwerp Personeel en Toegang beslaat de hoofdstukken 7 Veilig personeel, 9 Toegangsbeveiliging en 11 Fysieke beveiliging en beveiliging van de omgeving. De geconstateerde afwijkingen hebben betrekking op:

Toegangsbeveiliging (H9): Beoordeling van speciale bevoegdheden (bijvoorbeeld beheeraccounts) vindt momenteel niet plaats voor de generieke ICT-systemen noch voor AFAS. De beoordeling vindt wel plaats voor het Zaaksysteem en het BRP. Daarnaast worden de generieke toegangsrechten niet volledig gecontroleerd, deze controle is wel opgenomen in het interne controle plan voor 2025. Afwijkingen/incidenten worden altijd geregistreerd in Topdesk en ook afgehandeld. Meerdere disciplines binnen de ambtelijke organisatie doen hier een beoordeling op vanuit hun perspectief en expertise. Aanvullend is op dit moment niet vastgelegd hoe moet worden omgegaan met mislukte inlogpogingen, deze maatregel is gepland als onderdeel van de geplande SOC/SIEM implementatie (Q3 2025). Ten slotte wordt de logging van het gebruik van systeemhulpmiddelen wel gelogd, maar is deze niet conform norm voor de periode van een half jaar beschikbaar voor eventueel nader onderzoek.

Fysieke beveiliging en beveiliging van de omgeving (H11): In beginsel is er geen rekening gehouden met de gevolgen van rampen, wel zijn uitwijkvoorzieningen beschikbaar deze zijn echter nog in ontwikkeling. Apparaten en informatiedragers worden vernietigd nadat deze niet langer worden gebruikt. De registratie hiervan echter is niet sluitend, waardoor de norm niet volledig voldoet.

3. CONTINUÏTEIT EN INCIDENTEN Zorgen voor de continuïteit van onze dienstverlening en opvolging van incidenten	21	- 16 normen voldoen - 5 normen voldoen niet

Het onderwerp Continuïteit en Incidenten beslaat de hoofdstukken 16 Beheer van informatiebeveiligingsincidenten en 17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer. De geconstateerde afwijkingen hebben betrekking op:

Beheer van Informatiebeveiligingsincidenten (H16): Het beheer van Informatiebeveiligingsincidenten is vastgelegd in het beleidskader en nader uitgewerkt in het handboek Informatieveiligheid en Privacy. De enige geconstateerde afwijking ten opzichte van de norm betreft de maandelijkse rapportage over de opvolging van informatiebeveiligingsincidenten, deze rapportage vindt niet periodiek plaats, doch in voorkomende gevallen op ad-hoc basis.

Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer (H17): Hoewel op het niveau van de veiligheidsregio een crisisplan bestaat waarop actief wordt getraind, is het Business Continuity Plan (BCP) voor de gemeente in ontwikkeling. Derhalve wordt het BCP nog niet jaarlijks getest noch kan worden gegarandeerd dat de dienstverlening van bedrijfskritische onderdelen binnen uiterlijk een week kunnen worden hersteld.

4. INFORMATIESYSTEMEN Veilige omgang met informatiesystemen en afspraken hierover met onze leveranciers	61	- 38 normen voldoen - 23 normen voldoen niet

Het onderwerp Informatiesystemen omvat de volgende hoofdstukken 12 Beveiliging bedrijfsvoering, 14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen en 15 Leveranciersrelaties. De geconstateerde afwijkingen hebben betrekking op:

Beveiliging bedrijfsvoering (H12): Op dit onderwerp betreft het een significant aantal afwijkingen, veertien van de tweeëndertig normen voldoen niet. De afwijkingen hebben betrekking op drie aspecten van de bedrijfsvoering:

- *Beheer Productieomgeving:* Conform de BIO dient te worden getest in een testomgeving en niet in de productieomgeving. Dit gebeurt in de praktijk wel, omdat niet in alle gevallen een testomgeving beschikbaar is. Wel wordt gebruik gemaakt van vastgestelde testprocedures.
- *Back-up en restore:* Hoewel een vastgesteld back-up beleid bestaat waarin de eisen voor het bewaren en beschermen is gedefinieerd, is dit behoudens voor de GBA niet op basis van een expliciete risicoafweging bepaald. Dit houdt in dat het restore beleid niet voldoet aan de norm, noch dat het back-proces aan de norm voldoet. Ten slotte wordt de restore-procedure niet minimaal jaarlijks getest, behoudens die voor de GBA.
- *Logging en Monitoring:* In beginsel is er op dit moment geen centrale aanpak of tool voor logging en monitoring geïmplementeerd, dat wil niet zeggen dat er geen logging wordt vastgelegd, deze voldoet echter niet structureel aan het beleid. Zo wordt er wel gelogd op de centrale firewalls, maar is er geen monitoring ingeregeld, noch worden gedetecteerde aanvallen centraal gemeld bij de Informatiebeveiligingsdienst (IBD) van VNG. Deze afwijkingen zijn onderkend en worden opgevolgd met implementatie van SOC/SIEM als onderdeel van de VNG-aanbesteding. Hierbij dient te worden opgemerkt dat voorgaande geldt voor de infrastructuur en systemen in eigen beheer. Voor de bedrijfskritische bedrijfsapplicaties geldt het niet, deze worden conform norm gemonitord.

Acquisitie, ontwikkeling en onderhoud van informatiesystemen (H14): De geconstateerde afwijkingen hebben met name betrekking op het ontbreken van gestructureerde testprocedures door de beperkte omvang van de organisatie en het ontbreken van testomgevingen. Hierdoor vinden ongestructureerd testen plaats dan wel wordt gebruik gemaakt van productiegegevens voor testdoeleinden in plaats van geanonimiseerde testgegevens.

Leveranciersrelaties (H15): In het kader van acquisitie van nieuwe informatiesystemen en diensten is de Informatiebeveiligingsorganisatie doorgaans niet nauw betrokken, waardoor beveiligingseisen niet structureel worden opgenomen in de aanbestedingstrajecten. Aanvullend wordt gemeld dat wijzigingen in de dienstverlening van leveranciers niet consistent worden beoordeeld op hun impact ten aanzien van de informatiebeveiliging.

5. DATABESCHERMING Veilige omgang met data in onze software	34	- 27 normen voldoen - 7 normen voldoen niet

Het onderwerp Databescherming beslaat de volgende hoofdstukken 8 Beheer van bedrijfsmiddelen, 10 Cryptografie en 13 Communicatiebeveiliging. De geconstateerde afwijkingen hebben betrekking op:

Beheer van bedrijfsmiddelen (H8): Het ontbreekt aan een vastgestelde procedure voor het fysieke transport van media, denk hierbij aan harde schijven of USB-sticks.

Cryptografie (H10): Voor de belangrijkste diensten en koppelingen met bijvoorbeeld het zaaksysteem en iBurgerzaken zijn de verbindingen adequaat ingericht, zoals vastgesteld op basis van de beoordeelde TPM-rapportages. Wel wordt opgemerkt dat het cryptografiebeleid op onderdelen aanvulling vereist.

Communicatiebeveiliging (H13): De interne netwerken worden beheerd door een derde partij en deze voert basis monitoring uit, vanaf het derde kwartaal 2025 wordt deze dienst aangesloten op de SOC/SIEM dienstverlening. Op dit moment voldoet de monitoring van het netwerk nog niet volledig aan de BIO-normen.