Definitief

Bestuurlijk rapport Informatiebeveiliging Gemeente Den Helder

Dossiernummer 22301075

Onderzoek in opdracht van

Rekenkamercommissie gemeente Den Helder

OPENBAAR

Hoffmann
Luidsprekerstraat 10
1322 AX Almere

T 088 - 298 66 00
E info@hoffmann.nl
W www.hoffmann.nl

IBAN NL87ABNA0861616820
KvK 33170622
BTW NL006275199B01

INHOUDSOPGAVE

Managementsamenvatting

In opdracht van de rekenkamer is een IB-onderzoek uitgevoerd bij de gemeente Den Helder met als focus het beveiligingsniveau van de facetten ‘organisatie’, ‘de mens’ en techniek. Dit IB-onderzoek heeft plaatsgevonden in de periode mei 2023 t/m januari 2024.

De hoofdvraag van het onderzoek is als volgt: ‘Is de informatieveiligheid bij de gemeente Den Helder voldoende gewaarborgd?’ Om deze vraag te kunnen beantwoorden, is een integrale benadering toegepast die zich richt op een drietal segmenten: organisatie, mens en techniek. In dit rapport zijn op basis van de bevindingen de daarmee samenhangende risico’s in kaart gebracht. Om deze risico’s te mitigeren zijn concreet uitvoerbare verbetermogelijkheden geformuleerd.

In deze management samenvatting wordt het overall beeld geschetst en een samenvattende toelichting op de belangrijkste resultaten per onderdeel gegeven. Voor meer gedetailleerde bevindingen en aanbevelingen per onderdeel verwijzen wij naar hoofdstuk twee; ‘Bevindingen en aanbevelingen’.

In bijlage 5.3 is een verklarende woordenlijst opgenomen met cybersecuritytermen om bijvoorbeeld rapporten, adviezen of offertes beter te begrijpen.

Het onderzoek naar de organisatie van de informatiebeveiliging had tot doel na te gaan of de gemeente Den Helder de belangrijkste risico’s in beeld heeft, hoe het beleid is opgesteld en of dit in de praktijk wordt toegepast.

Overall beeld

In het onderzoek zijn diverse zaken geconstateerd die nadere aandacht behoeven. De onderzoekers schatten in dat de gemeente zich qua informatiebeveiliging op een volwassenheidsniveau1 tussen 1 en 2 op een schaal van 5 bevindt. Zowel op gebied van Organisatie, Mens als Techniek bevat het rapport verbetermogelijkheden. Het levert de volgende overkoepelende aanbevelingen op:

- Bepaal het volwassenheidsniveau wat je als gemeente op gebied van Informatiebeveiliging op termijn wilt bereiken inclusief een fasering en tijdspad om daar te komen.
- Heroverweeg de inrichting van de organisatie van de informatiebeveiliging. Kijk daarbij naar verdeling en scheiding van verantwoordelijkheden en taken, de nodige capaciteit en de ophanging in de organisatie.
- Onderneem extra stappen om het bewustzijn van de medewerkers met betrekking tot informatiebeveiliging te vergroten en de uitvoering van de afspraken te verbeteren. Overweeg mede in dat kader of de toegangsbeveiliging moet worden aangescherpt.
- Maak een Business Continuïteitsplan

[1] Zie Bijlage 5.8 Maturity model Informatiebeveiliging

- Herstel de geconstateerde, vooral technische, aandachtspunten vanuit de penetratietest.

Het kost tijd om het volwassenheidsniveau te verhogen. Het vervolgtraject zou kunnen beginnen met het vaststellen van het gewenste volwassenheidsniveau plus fasering en tijdspad. Zo kan stapsgewijs een steeds hoger niveau worden bereikt. In dergelijke modellen is het hoogste niveau veelal (erg) ambitieus, maar een niveau tussen 3 en 4 is aan te bevelen. Als het doel is bepaald, kunnen concrete plannen worden gemaakt om dit doel te bereiken vermoedelijk in de vorm van een verbeterprogramma.

Organisatie

Het onderzoek bestond uit het afnemen van interviews en een documentanalyse. Centraal hierbij stond het 'Informatiebeveiligingsbeleid Gemeente Den Helder'. Onderzoekers concluderen dat informatiebeveiliging binnen de gemeente Den Helder voornamelijk nog wordt gezien als I&T verantwoordelijkheid, waarbij zaken veelal bottom-up worden aangedragen. Om informatiebeveiliging te waarborgen is het van belang dat het onderdeel is van de cultuur, bedrijfsvoering en besluitvorming. Het is hierbij belangrijk dat het wordt uitgedragen als een organisatie brede verantwoordelijkheid en dat de organisatie voldoende wordt gefaciliteerd om deze verantwoordelijkheid in praktijk te brengen. Zowel op praktisch als op bestuurlijk niveau kunnen hier nog stappen in gemaakt worden. Zo kan bijvoorbeeld het beleid nog praktischer uitgewerkt worden in ondersteunende protocollen en processen, en mag men meer vanuit een visie of 'stip aan de horizon' sturing geven aan het thema informatiebeveiliging.

Mens

Het bewustzijn en gedrag van de medewerkers op het vlak van informatiebeveiliging is op de volgende manieren getest:

1. Mail-phishing test, waarbij er een e-mail is verstuurd die uitnodigde op een link te klikken en de gebruiker te verleiden om persoonlijke inloggegevens af te geven;
2. Fysieke inlooptest, waarbij een medewerker van Hoffmann heeft geprobeerd om ongeautoriseerd (zonder toestemming) toegang te krijgen tot de gemeentelijke werkplekken en vertrouwelijke informatie.

Met het versturen van een mail-phishing test is het bewustzijn en gedrag van de medewerkers ten aanzien van het herkennen van een phishing e-mail getoetst. De email is naar 542 e-mailadressen verstuurd. In totaal hebben 301 gebruikers de unieke link in de e-mail geopend (55,5% van de 542 verstuurde mails). Vervolgens hebben 235 gebruikers hun gebruikersnaam en wachtwoord ingevuld (43,4% van de 542 verstuurde mail-phishings). Dit percentage is relatief hoog vergeleken met andere gemeenten waar een soortgelijk scenario is toegepast. Gemiddeld zien de onderzoekers dat ongeveer 15% van de gebruikers hun gebruikersnaam en wachtwoord achterlaat. Het invullen van de gebruikersnaam en wachtwoord kan een kwaadwillende toegang geven tot het domein van deze medewerker. Als gevolg kan een kwaadwillende toegang krijgen tot (vertrouwelijke) informatie van de gemeente. Wij adviseren daarom doorlopend aandacht te blijven besteden aan het bewustzijn van

medewerkers en hen te voorzien van voldoende handvatten om mail-phishings te herkennen en op de juiste manier te handelen.

Het gedrag van de medewerkers is tevens onderzocht middels een fysieke inlooptest. Het was voor de Mystery Guest (MG) mogelijk om zowel het kantoorgebouw aan het adres Willemsoord 72 als het gemeentehuis aan het adres Willemsoord 66 te betreden. De MG werd hierbij niet aangesproken of bevraagd op haar aanwezigheid. Enkele medewerkers droegen een medewerkerspas en onbeheerde laptops waren vergrendeld. Het clean desk beleid mag in praktijk beter worden opgevolgd, op verschillende plekken waren onbeheerde documenten te vinden.

Techniek

Het beheer van de externe digitale infrastructuur en systemen zijn deels in handen van derde partijen. Na overleg met de gemeente, zijn die systemen getest die beheerd worden door de gemeente en die toegankelijk zijn vanaf het publieke internet. Na het achterhalen van twee accounts kon worden ingelogd op een systeem zonder 2-factor authenticatie. Onbekend is of dit systeem nog actief wordt gebruikt. Wij adviseren de gemeente dit systeem uit te schakelen of te voorzien van twee-factor authenticatie. Tevens adviseren wij de gemeente de medewerkers voor te lichten over het belang van sterke wachtwoorden.

Onze onderzoekers hebben daarnaast in een openbaar register een aantal IP reeksen gevonden die geregistreerd zijn door een persoon met een Den Helder email adres. Een aantal van deze reeksen zijn naar eigen zeggen niet bekend bij de gemeente. Dit kan erop duiden dat de gemeente niet alle systemen inzichtelijk heeft en wij adviseren de gemeente dit na te gaan.

Naast de externe systemen heeft er ook een onderzoek plaatsgevonden op de interne infrastructuur op de nieuwe locatie in Den Helder. Door de beveiligingsmaatregelen en indeling van het netwerk is het onze onderzoekers niet gelukt om interne systemen van de gemeente te benaderen. Ook na op verzoek verlenen van toegang is het de onderzoekers niet gelukt om vertrouwelijke gegevens van medewerkers of burgers te achterhalen.

Vanwege de vertrouwelijkheid zijn de technische uitkomsten en aanbevelingen van de pentesten reeds gedeeld met de ambtelijke organisatie.

1. Inleiding

De Rekenkamercommissie gemeente Den Helder (hierna genoemd: 'de Rekenkamer') heeft Hoffmann gevraagd een onderzoek uit te voeren naar de informatiebeveiliging bij de gemeente Den Helder (hierna genoemd: 'de gemeente'). Om een gedegen beeld te krijgen van de aanwezige kwetsbaarheden is tijdens het onderzoek het beveiligingsniveau van zowel organisatie, de mens als de techniek onderzocht. Maatregelen op het vlak van techniek en goed beleid valt of staat bij het gebruik en opvolging van de gebruiker (de mens). Andersom; de mens kan welwillend en bekwaam zijn, echter wanneer deze niet gefaciliteerd wordt door techniek of de organisatie, brengt dat eveneens kwetsbaarheden met zich mee. Vanwege de afhankelijkheid van deze drie facetten is er gekozen voor een integrale benadering. Op basis van de bevindingen zijn de daarmee samenhangende risico's en de concreet uitvoerbare verbetermogelijkheden (aanbevelingen) in kaart gebracht.

1.1 Doelstellingen en scope

De onderzoeksvragen zijn als volgt door de rekenkamer geformuleerd:

Hoofdvraag: 'Is de informatieveiligheid bij de gemeente Den Helder voldoende gewaarborgd?'

Per facet zijn de volgende deelvragen geformuleerd waar in hoofdstuk 2 antwoord op wordt gegeven:

1. Organisatie

a. Welk beleid heeft de gemeente vastgesteld op het gebied van informatieveiligheid?
b. Voldoet dit beleid aan de BIO?
c. Welke risico's en maatregelen heeft de gemeente benoemd?
d. Welke informatievelden van het hele gemeentelijke taakveld bestrijkt de risico-inventarisatie wel en welke niet?
e. Zijn er onderdelen die ten onrechte missen?
f. In hoeverre zijn de maatregelen geïmplementeerd en zijn daarvoor adequate middelen in de zin van geld en menskracht beschikbaar gesteld?
g. In hoeverre zijn de acties in het kader van de VNG Agenda Digitale Veiligheid uitgevoerd en wat is de voortgang daarvan?

2. Mens

a. Op welke manier zet de gemeente in op bewust omgaan met informatie door medewerkers, uitvoeringsorganisaties en externe adviseurs?
b. Hoe gaan medewerkers, uitvoeringsorganisaties en externe adviseurs in de praktijk om met het informatieveiligheidsbeleid?
c. In hoeverre zijn de acties in het kader van de VNG Agenda Digitale Veiligheid uitgevoerd en wat is de voortgang daarvan?

3. Techniek

a. Is data bij de gemeente voldoende beschermd tegen toegang door onbevoegde medewerkers, uitvoeringsorganisaties en externe adviseurs?

b. Is data bij de gemeente voldoende beschermd tegen toegang door onbevoegde externen?

c. Wat zijn, als vraag 3a of 3b met ‘nee’ beantwoord wordt, daarvan de gevolgen voor betrokken derden?

d. Wat zijn de technische risico’s en kwetsbaarheden?

e. In hoeverre zijn de acties in het kader van de VNG Agenda Digitale Veiligheid uitgevoerd en wat is de voortgang daarvan?

De scope van het gehele IB-onderzoek betreft:

- Afhankelijk van het ingezette middel alle medewerkers, dan wel een gericht aantal medewerkers van de gemeente Den Helder;
- Ontvangen documentatie van de gemeente Den Helder;
- De digitale en fysieke infrastructuur van de gemeente Den Helder.

Het onderzoek is een kwalitatief onderzoek en is een momentopname van de situatie zoals deze nu wordt gezien en ervaren.

2. Bevindingen en aanbevelingen

2.1 Algemeen

Het IB-onderzoek dat Hoffmann in opdracht van de rekenkamer heeft uitgevoerd, had als doel de volgende hoofdvraag te beantwoorden: *'Is de informatieveiligheid bij de gemeente Den Helder voldoende gewaarborgd?'* Voor waarborging van informatieveiligheid is het belangrijk dat dit thema onderdeel is van de organisatiecultuur. De algemene afdronk uit onderzoek is dat informatiebeveiliging binnen de gemeente Den Helder voornamelijk als I&T verantwoordelijkheid gezien wordt. Zaken worden veelal vanuit de informatiebeveiligingsorganisatie, 'bottom up', georganiseerd. Wanneer risico's worden geagendeerd, worden deze vaak teruggegeven als I&T verantwoordelijkheid. Voorbeelden hiervan zijn continuïteitsplannen en risicomanagement. Waar dit een gemeente brede verantwoordelijkheid betreft, wordt er in praktijk verwacht dat de CISO hier navolging aan geeft. De positionering van de informatiebeveiligingsorganisatie binnen het I&T team alsmede de afhankelijkheid van budget van I&T, bevestigd het beeld dat informatiebeveiliging voornamelijk wordt gezien als een I&T kwestie in plaats van een gemeente brede verantwoordelijkheid.

Om informatiebeveiliging onderdeel te maken van de organisatiecultuur is het van belang dat het bestuur een duidelijke voorbeeldrol inneemt én informatiebeveiliging c.q. risicomanagement onderdeel maakt van de algehele bedrijfsvoering en besluitvorming. Pas wanneer de gemeente zicht heeft op risico's, kan men hierop sturen en maatregelen nemen. De uitvoer van risicoanalyses is hierbij van groot belang, hier kan de gemeente Den Helder nog stappen in maken. Daarnaast is er winst te behalen in het faciliteren van de medewerkers bij het in praktijk brengen van het informatiebeveiligings- en privacybeleid. Het strategisch beleid is momenteel onvoldoende praktisch uitgewerkt, waardoor er nog veel hulpvragen terecht komen bij de CISO en de FG. Operationele richtlijnen en een aanstelling van een ISO en een PO, dragen bij aan de gewenste cultuur waarbij informatiebeveiliging 'van iedereen' is.

Het 'Maturity Model Informatiebeveiliging' helpt de inbedding van informatieveiligheid in de organisatiecultuur te duiden door een beeld te geven van het volwassenheidsniveau van een organisatie m.b.t. Informatieveiligheid (zie bijlage 6.4). Dit model geeft verschillende niveaus aan van de informatiebeveiligingscultuur binnen een organisatie. Per niveau worden verschillende kenmerken genoemd. Op basis van de kenmerken schatten de onderzoekers het huidige niveau van informatiebeveiligingscultuur van de gemeente Den Helder tussen niveau één en twee.

Hieronder volgen de bevindingen en aanbevelingen voor ieder onderzocht onderdeel: organisatie, mens en techniek voor de gemeente Den Helder. Per onderdeel worden eerst de geformuleerde onderzoeksvragen beantwoord. Vervolgens worden gedetailleerd de bevindingen en aanbevelingen op specifieke punten vermeld. Voor de uitgebreide toelichting op de bevindingen en aanbevelingen verwijzen we naar de bijlagen 5.1 en 5.2 (apart document). Op sommige plaatsen wordt verwezen naar de Baseline Informatiebeveiliging Overheid (BIO), het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen.

2.2 Organisatie

2.2.1 Onderzoeksvragen

a. Welk beleid heeft de gemeente vastgesteld op het gebied van informatieveiligheid?

Het 'Strategisch Gemeentelijk Informatiebeveiligingsbeleid 2020-2023 Den Helder' vormt de basis voor informatiebeveiliging van de gemeente Den Helder. Tevens is er een 'Beleidskader Privacy' waarin het privacybeleid van de gemeente Den Helder wordt beschreven.

b. Voldoet dit beleid aan de BIO?

Het huidige beleid is grotendeels gebaseerd op een template vanuit de Vereniging Nederlandse Gemeenten (VNG), waarmee het aan de basiseisen voldoet zoals gesteld in de BIO.[2]

c. Welke risico's en maatregelen heeft de gemeente benoemd?

Binnen de gemeente Den Helder worden weinig tot geen risicoanalyses uitgevoerd, hierdoor is er onvoldoende zicht op risico's en relevante maatregelen. Vanuit de interviews komt het gebrek aan continuïteitsbeheer naar voren als risico voor de gehele organisatie. De I&T heeft voor de kritische applicaties de risico's in kaart gebracht. Daarnaast worden de systemen jaarlijks getoetst op kwetsbaarheden en worden er preventieve maatregelen genomen tegen dreigingen vanuit buitenaf, zoals de installatie van een SIEM/SOC.

d. Welke informatievelden van het hele gemeentelijke taakveld bestrijkt de risico-inventarisatie wel en welke niet?

Rondom de kritische applicaties heeft de I&T afdeling de risico's in kaart gebracht. Er is geen sprake van een bredere risico-inventarisatie.

e. Zijn er onderdelen die ten onrechte missen?

De BIO benadrukt het belang van risicomanagement en risicogericht sturen. Dit vraagt om de uitvoer van risicoanalyses, maar ook een risicogerichte benadering binnen de bedrijfsvoering en besluitvorming. Het gebrek aan risicoanalyses maakt dat er momenteel onvoldoende zicht is op risico's, wat de sturing hierop in de weg staat.

f. In hoeverre zijn de maatregelen geïmplementeerd en zijn daarvoor adequate middelen in de zin van geld en menskracht beschikbaar gesteld?

Doordat er onvoldoende zicht is op risico's en kwetsbaarheden voor de gemeente, is het moeilijk in te schatten in hoeverre relevante risicogerichte maatregelen zijn geïmplementeerd.

Uit het onderzoek kwam naar voren dat er veel vraag is naar praktische ondersteuning rondom informatiebeveiliging en privacy. Deze hulpvragen worden momenteel opgepakt door de CISO en de

[2] Zie BIO Hoofdstuk 5 'Informatiebeveiligingsbeleid' en Hoofdstuk 6 'Organiseren van informatiebeveiliging'

FG, dit werkt echter beperkend in tijd en gewenste functiescheiding. De aanstelling van een Information Security Officer (ISO) en een Privacy Officer (PO) zou hiervoor een mogelijke oplossing zijn. Qua budget zijn zowel de CISO als de FG afhankelijk van het I&T budget. Er is geen gealloceerd budget voor informatiebeveiliging en privacy, iets wat idealiter wel het geval is.

g. In hoeverre zijn de acties in het kader van de VNG Agenda Digitale Veiligheid uitgevoerd en wat is de voortgang daarvan?

Er is een update vanuit de CISO toegevoegd aan de rapportage waarin de negen verschillende actielijnen worden toegelicht. De uitvoering en voortgang hiervan verschilt per actielijn en wordt verder toegelicht in hoofdstuk 3.

2.2.2 Bevindingen en aanbevelingen

Voor het onderzoek naar de organisatie van informatiebeveiliging is een analyse uitgevoerd op de door de gemeente Den Helder beschikbaar gestelde documentatie, rapporten en verklaringen. Daarnaast zijn er kwalitatieve (online) interviews uitgevoerd met medewerkers van de gemeente voor toelichting op het gevraagde materiaal. Het onderzoek is een kwalitatief onderzoek en is een momentopname van de situatie zoals deze nu wordt gezien en ervaren (mei 2023 t/m januari 2024). In bijlage 5.4 is een opgave van de geïnterviewden opgenomen, evenals een overzicht van de documenten die zijn meegenomen in de beoordeling.

Hieronder zijn de belangrijkste bevindingen en aanbevelingen opgenomen in een tabel. Nadere toelichting is te vinden in de bijlage 5.1.

Bijlage	Bevinding	Impact	Aanbeveling
5.1.1	Er zijn verschillende vormen/versies van de ‘Gedragsregels informatiebeveiliging’ in omloop.	De keuze voor gedragsregels verliest aan effectiviteit en duidelijkheid aangezien er geen eenduidigheid bestaat over welke gedragsregels geldend zijn.	Evalueer en actualiseer de gedragsregels. Communiceer de geldende regels. Zorg dat er in verdere documentatie naar de actuele, overkoepelende, gedragsregels wordt verwezen.
5.1.1	Het Strategisch informatiebeveiligingsbeleid is onvoldoende uitgewerkt in tactisch beleid en/of operationele richtlijnen.	De organisatie heeft weinig handvaten om het strategisch beleid in de praktijk te brengen. Mede hierdoor komen nog relatief veel praktische hulpvragen uit bij de informatiebeveiligingsorganisatie of de I&T afdeling.	Om de medewerkers te faciliteren in het nemen van verantwoordelijkheden en correct handelen op het vlak van informatieveiligheid luidt het advies om het Strategisch informatiebeveiligingsbeleid uit te werken in tactisch/operationeel beleid/richtlijnen.

5.1.2	De CISO valt hiërarchisch onder de teammanager I&T en is afhankelijk van het budget van het I&T-team.	Naast het feit dat deze afhankelijkheid het onafhankelijke opereren op het gebied van informatiebeveiliging in de weg kan staan, geeft de positionering en het gealloceerde budget een belangrijk signaal over het belang dat wordt gehecht aan informatiebeveiliging.	Idealiter heeft een CISO een onafhankelijke positie ten opzichte van lijnmanagement en een eigen budget voor informatiebeveiliging. Evalueer de huidige positionering en mogelijke risico's, pas waar nodig aan.[3]
5.1.3	Het jaarlijks gemeentelijk informatiebeveiligingsplan en PDCA plan van aanpak zijn niet beschikbaar voor de jaren 2022 en 2023.	Een jaarlijks informatiebeveiligingsplan en PDCA plan van aanpak draagt bij aan een proactieve bedrijfsvoering en continue verbetering op het vlak van informatiebeveiliging. Daarnaast geeft het plan een mogelijkheid tot het delen van de visie en geeft het handvaten voor sturing.	Herpak het werken volgens een jaarlijks informatiebeveiligingsplan. Beleg de verantwoordelijkheid hiervoor op de juiste plek. Volgens het gemeentelijk Strategisch informatiebeveiligingsbeleid is het niet enkel de verantwoordelijkheid van de CISO, maar wordt het jaarlijks informatiebeveiligingsplan opgesteld onder leiding van directie.
5.1.4	Door het gebrek aan risicoanalyses hebben niet alle teams goed zicht op risico's en nodige maatregelen.	Het niet tijdig in te spelen op (toekomstige) dreigingen maakt niet alleen afdelingen, maar ook de gehele organisatie kwetsbaar en vergroot het risico op het ontstaan van blinde vlekken.	Maak risicomanagement onderdeel van de bedrijfsvoering en beleg de verantwoordelijkheid voor de uitvoering van risicoanalyses duidelijk bij het (lijn) management. Bekijk of het (lijn)management voldoende gefaciliteerd wordt voor de uitvoering hiervan, stel zo nodig een ISO aan.
5.1.5	Bij de aanschaf van (IT) producten en diensten wordt de IB organisatie soms niet, of (te) laat betrokken, waardoor eisen m.b.t. informatiebeveiliging niet altijd voldoende worden meegenomen.	Er worden mogelijk producten en diensten aangeschaft of ontwikkeld en in gebruik genomen die niet voldoen aan het IB-beleid en de gestelde beveiligingseisen. Bij gebrek aan zicht op de aangekochte producten of diensten ontstaat tevens het risico op (onbeheerd) schaduw-IT.	Bij elke aanschaf moet worden voldaan aan de eisen m.b.t. informatiebeveiliging.[4] Duidelijke werkprocessen moeten ervoor zorgen dat de IB organisatie, en waar nodig tevens de inkooporganisatie, wordt betrokken.
5.1.5	Onder medewerkers is een wisselende bekendheid met de eisen en procedures rondom inkoop. Hierdoor worden de inkoopadviseurs soms niet of te laat betrokken.	Bij gebrek aan zicht op de aangekochte IT producten of diensten ontstaat het risico op schaduw-IT.	De geldende eisen en procedures mogen breder bekend worden onder medewerkers. Evalueer de huidige procedures in het kader van het risico op schaduw-IT en pas deze eventueel aan.

[3] Opmerking ambtelijke afstemming: *'In de huidige fase van volwassenheid biedt positionering in team I&T de meerwaarde van korte lijnen tussen de CISO en de beheerders en adviseurs van de digitale techniek.'*
[4] Zie hiervoor BIO "Leveranciersrelaties". Hoofdstuk 15.1

5.1.5	Tijdens de looptijd van een contract wordt niet gecontroleerd of het product/de leverancier voldoet aan de door de gemeente gestelde (in het contract opgenomen) eisen m.b.t. informatiebeveiliging.	De aangeschafte (IT) producten en diensten en/of de leverancier voldoet mogelijk niet aan het IB-beleid en de gestelde beveiligingseisen.	Het is raadzaam om periodiek (minimaal jaarlijks) een controle uit te voeren op de naleving van eisen door leveranciers m.b.t. informatiebeveiliging.[5] Leveranciersmanagement kan bijdragen aan een juiste opvolging binnen dit proces.
5.1.6	De gemeente beschikt niet over continuïteit /crisismanagementplannen.	De gemeente Den Helder is momenteel onvoldoende voorbereid om de continuïteit van de meest kritische bedrijfsprocessen en dienstverlening te garanderen in het geval van een (cyber)crisis.	Stel continuïteit/crisismanagement plannen op en formaliseer een crisisteam. Evalueer de plannen periodiek en plan een periodieke oefening (inclusief evaluatie) om te waarborgen dat de plannen en het team in praktijk functioneren.
5.1.7	De FG valt hiërarchisch onder de teammanager I&T.	De huidige positionering van de FG vormt een mogelijk risico voor de onafhankelijkheid van deze positie.	Idealiter rapporteert de FG aan het hoogst leidinggevend orgaan binnen de gemeente om de onafhankelijk te kunnen waarborgen. Evalueer de huidige positionering en mogelijke risico's, pas waar nodig aan.
5.1.7	Het privacybeleid sluit onvoldoende aan bij de behoeften van de organisatie. Er worden doelstellingen en uitgangspunten uiteengezet, echter ontbreekt het aan praktische handleidingen of richtlijnen voor medewerkers.	Omdat het beleid onvoldoende voorschrijft wat het verwacht van de organisatie, blijft de opvolging en naleving van het beleid in de praktijk veelal uit.	Herschrijf en actualiseer het privacybeleid, zodat het de praktische uitvoering hiervan ondersteund. De aanstelling van een PO werkt tevens faciliterend in de uitvoering van het beleid en kan een rol spelen in herschrijven en actualiseren.
5.1.7	Het verwerkingsregister van de gemeente Den Helder wordt niet systematisch bijgewerkt waardoor deze niet up to date is.	De gemeente voldoet hiermee nog niet geheel aan de verantwoordingsverplichting zoals gesteld in de AVG.	Werk het verwerkingsregister bij en richt de organisatie zo in dat een continu doorlopend proces wordt. Rapporteer de status richting het college, dit faciliteert sturing en monitoring.

[5] Zie hiervoor BIO "Beheer van dienstverlening van leveranciers". Hoofdstuk 15.2

5.1.8	Binnen de gemeente Den Helder zijn er geen bestaande processen aangaande dataclassificatie. Hierdoor ontbreekt duidelijkheid over het vertrouwelijkheidsniveau van een document	De gemeente heeft onvoldoende zicht op de vertrouwelijkheid van informatie en waar deze informatie zich bevindt. Hiermee bestaat het risico dat er onvoldoende beveiligingsmaatregelen worden genomen voor gevoelige informatie.	Specificeer beleid/processen rondom dataclassificatie en besteed aandacht aan de inbedding van het classificatiebeleid in de praktijk. Doe dit door bewustwording en voorbeeldgedrag.
5.1.10	Informatiebeveiliging is nog onvoldoende onderdeel van de organisatiecultuur binnen de gemeente. Zowel op bestuurlijk niveau als op praktische inbedding.	Een reactieve bedrijfsvoering, veel verantwoordelijkheid bij de IB-organisatie en onvoldoende praktische inbedding maakt dat er momenteel onvoldoende zicht en sturing is op risico's en maatregelen in het kader van informatieveiligheid.	Creëer een visie op informatieveiligheid, maak het thema onderdeel van besluitvorming en faciliteer de praktische inbedding. Evalueer de positie van de informatiebeveiligingsorganisatie.[6]

2.3 Mens

2.3.1 Onderzoeksvragen

a. *Op welke manier zet de gemeente in op bewust omgaan met informatie door medewerkers, uitvoeringsorganisaties en externe adviseurs?*

De gemeente beschikt over een online leeromgeving waarin e-learnings en wekelijkse quizvragen op het vlak van informatiebeveiliging worden gedeeld. Daarnaast worden door de informatiebeveiligingsorganisatie presentaties gegeven binnen diverse teams en heeft de CISO een start gemaakt met het plannen van mystery guest bezoeken om het bewustzijn in de praktijk te toetsen. Uitvoeringsorganisaties dienen bij aanvang te voldoen aan een vaste set eisen aangaande informatiebeveiliging, echter worden niet periodiek getoetst op de gemaakte afspraken.

b. *Hoe gaan medewerkers, uitvoeringsorganisaties en externe adviseurs in de praktijk om met het informatieveiligheidsbeleid?*

De onderzoekers bemerken een duidelijke behoefte aan operationele ondersteuning om het beleid in de praktijk te brengen. De gemeente Den Helder beschikt over een strategisch informatiebeveiligingsbeleid en een set aan gedragsregels waarin wordt beschreven wat er op bepaalde thema's wordt verwacht van de medewerkers. Tussen beiden zit echter nog een inhoudelijke gap, namelijk een uitwerking in tactisch beleid of operationele richtlijnen. Deze vertaling draagt bij aan het vermogen van medewerkers om het beleid in de praktijk te brengen en verantwoordelijkheid te nemen aangaande informatieveiligheid. De eerdergenoemde aanstelling van een ISO en een PO draagt hier eveneens aan bij.

[6] Opmerking vanuit ambtelijke afstemming: *'In de huidige fase van volwassenheid biedt positionering in team I&T de meerwaarde van korte lijnen tussen de CISO en de beheerders en adviseurs van de digitale techniek.'*

c. *In hoeverre zijn de acties in het kader van de VNG Agenda Digitale Veiligheid uitgevoerd en wat is de voortgang daarvan?*

Er is een update vanuit de CISO toegevoegd aan de rapportage waarin de negen verschillende actielijnen worden toegelicht. De uitvoering en voortgang hiervan verschilt per actielijn en wordt verder toegelicht in hoofdstuk 3.

2.3.2 Bevindingen en aanbevelingen

Maatregelen op het vlak van techniek en goed beleid valt of staat bij het gebruik en opvolging van de gebruiker (de mens). De mens is een onmisbare schakel op het vlak van informatiebeveiliging en daarom een belangrijk onderdeel van dit IB-onderzoek.

Het bewustzijn en gedrag van de medewerkers zijn getest op de volgende manieren:

1. Mail-phishing test, waarbij er een e-mail is verstuurd die uitnodigde op een link te klikken en de gebruiker te verleiden om persoonlijke inloggegevens af te geven;
2. Fysieke inlooptest, waarbij een medewerker van Hoffmann heeft geprobeerd om ongeautoriseerd toegang te krijgen tot de gemeentelijke werkplekken en vertrouwelijke informatie.

In dit hoofdstuk worden de bevindingen en aanbevelingen beschreven. Nadere toelichting is te vinden in de bijlage 5.2 (apart document).

2.3.2.1 Phishing-mail

Gedurende het onderzoek traject hebben onderzoekers van Hoffmann in overleg met gemeente Den Helder een mail-phishing verstuurd naar alle medewerkers. De e-mail werd verstuurd vanuit het domein ‘denhelder@feestdagen-geschenken.nl’. Op 28 november 2023 om 13:00 uur werd de mail naar 542 unieke e-mailadressen verstuurd.

Gedurende de looptijd van de test (6 dagen)[7] zijn er in totaal 301 unieke bezoekers geregistreerd (55,5% van de 542 verstuurde mail-phishings) waarvan 235 gebruikers hun gebruikersnaam en wachtwoord hebben ingevuld (43,4% van de 542 verstuurde mail-phishings).[8] Dit percentage is relatief hoog vergeleken met andere gemeenten waar een soortgelijk scenario is toegepast. Gemiddeld zien de onderzoekers dat ongeveer 15% van de gebruikers hun gebruikersnaam en wachtwoord achterlaat.

[7] De mail-phishing actie is gestopt op 4 december 2023 omstreeks 13:00 uur.
[8] Het wachtwoord is niet opgeslagen, ook zijn de inloggegevens niet getest op geldigheid.

Aanbevelingen
Blijf medewerkers voortdurend bewust maken van mail-phishing-technieken en consequenties door praktijktoetsen, bewustwordingsprogramma's en het delen van actuele voorbeelden.
Communiceer duidelijk wat er van medewerkers wordt verwacht aangaande informatieveilig gedrag en hoe te handelen in het geval van phishing c.q. social engineering.
Zorg ervoor dat medewerkers weten welke domeinnamen van de gemeente zijn en communiceer dat men geen gebruik moet maken van andere domeinen.

2.3.2.2 Fysieke inlooptest – Mystery Guest

Op 20 november 2023 heeft een Mystery Guest van Hoffmann, hierna te noemen 'MG', een fysieke inlooptest verricht bij het kantoorgebouw (Willemsoord 72) en het gemeentehuis (Willemsoord 66) van de gemeente Den Helder.

Bevindingen
Het lukte de MG om de gebouwen op Willemsoord van de gemeente Den Helder te betreden zonder zich te melden of een medewerkerspas te tonen.
MG is geruime tijd aanwezig geweest in beide gebouwen van de gemeente Den Helder op Willemsoord. Gedurende die tijd is de MG niet aangesproken door enige medewerker op haar aanwezigheid.
Het viel MG op dat enkele aanwezige personen een medewerkerspas droegen.
Het viel MG op dat op de onbemande werkplekken, de laptops vergrendeld waren.
Het viel MG op dat op de onbemande werkplekken, onbeheerde documenten lagen.
Het viel MG op dat enkele postvakken open waren.
Het viel MG op dat de papierbakken op de afdeling documenten bevatten.
Het viel MG op dat er geen onbeheerde documenten in de printerruimtes aanwezig waren.

Aanbevelingen
De (effectiviteit van de) beheersmaatregelen in overeenstemming brengen met de risico's in relatie tot de beveiligingsdoelstellingen van de kantoorgebouwen van de gemeente Den Helder. Bijvoorbeeld: Indien de gemeente niet wil dat onbevoegden tijdens kantooruren het kantoorgebouw kunnen betreden en informatie kunnen bereiken, dienen de beheersmaatregelen dit te ondersteunen. Denk in dat geval aan: ○ Het nemen van (effectieve) toegangsbeheersmaatregelen, zoals het actief monitoren en verifiëren van binnenkomende personen die het kantoor willen betreden. Een andere maatregel zou mogelijk kunnen zijn om meerdere compartimenten met toegangsbeveiliging toe te voegen om de toegang tot beveiligde ruimten te bemoeilijken. Bijvoorbeeld: men dient een pas aan te bieden om toegang te krijgen tot de eerste en tweede verdieping; ○ het afgesloten bewaren van (vertrouwelijke) documentatie; ○ het verhogen van het risicobewustzijn van personen in het kantoorgebouw van de gemeente (zodat zij voor hen onbekende personen aanspreken en een sluitende verificatie verrichten naar de reden van hun aanwezigheid).
Het (laten) verrichten van een risicoanalyse in verband met de fysieke veiligheid van de gemeente Den Helder, om tot een evenwichtig securitymanagement te komen (zie ook bovenstaande punten).
Risicobewustzijn van medewerkers te verhogen: ○ Laat ongeautoriseerde c.q. onbekende personen zonder pas niet meeliften door de deur/toegangspoorten. ○ Spreek onbekenden aan wanneer zij geen toegangspas dragen. ○ Zorg voor een clean desk wanneer je het kantoor of het bureau verlaat. ○ Bewaar gevoelige documentatie op plekken die vergrendeld kunnen worden en vergrendel deze wanneer je het kantoor/de werkplek verlaat. ○ Maak gebruik van de afgesloten papierbakken voor het weggooien van vertrouwelijke documenten.

2.4 Techniek

2.4.1 Onderzoeksvragen

a. *Is data bij de gemeente voldoende beschermd tegen toegang door onbevoegde medewerkers, uitvoeringsorganisaties en externe adviseurs?*

De gegevens die benaderbaar zijn op het externe systeem waar zonder meer-factor op kan worden ingelogd zijn dit mogelijk niet. Wachtwoorden kunnen via phishing achterhaald worden en door het ontbreken van deze tweede factor is het de vraag of er gesproken kan worden over "behoorlijke

beveiliging" van deze gegevens. Naast deze bevinding zijn er door onze onderzoekers geen aanwijzingen of bewijzen gevonden dat de gegevens onvoldoende beschermd zijn.
In hoeverre autorisaties voor verschillende rollen en functies voldoende zijn afgedwongen door middel van techniek is door onze onderzoekers zeer beperkt onderzocht. Er zijn echter geen aanwijzingen en/of bewijzen gevonden dat de gegevens onvoldoende zijn beschermd.

b. Is data bij de gemeente voldoende beschermd tegen toegang door onbevoegde externen?

Hier is hetzelfde antwoord van toepassing als bij 2.4.1.a.

c. Wat zijn, als vraag 2.4.1.a of 2.4.1.b met 'nee' beantwoord wordt, daarvan de gevolgen voor betrokken derden?

Omdat vraag 2.4.1.a en 2.4.1.b niet stellig met "nee" zijn beantwoord, is deze vraag niet van toepassing. Tijdens het onderzoek zijn er geen gegevens achterhaald die betrekking hebben op burgers, en zijn conclusies hierover speculatief.

d. Wat zijn de technische risico's en kwetsbaarheden?

Als risico zien wij het kennelijk gebruik van voorspelbare wachtwoorden gecombineerd met het ontbreken van meer factor authenticatie. Overige technische risico's uit de interne test zijn relatief eenvoudig te verhelpen en moeilijk te exploiteren.

e. In hoeverre zijn de acties in het kader van de VNG Agenda Digitale Veiligheid uitgevoerd en wat is de voortgang daarvan?

Er is een update vanuit de CISO toegevoegd aan de rapportage waarin de negen verschillende actielijnen worden toegelicht. De uitvoering en voortgang hiervan verschilt per actielijn en wordt verder toegelicht in hoofdstuk 3.

2.4.2 Bevindingen en aanbevelingen n.a.v. Penetratietest

De detailbevindingen en specifieke aanbevolen maatregelen van de penetratietest zijn beschreven in het document: "Pentestrapport Den Helder.docx.

Om te voorkomen dat kwaadwillenden de geconstateerde kwetsbaarheden kunnen misbruiken, is dit document als geheim geclassificeerd. De tijdens het onderzoek geconstateerde kritische kwetsbaarheden zijn onmiddellijk met de CISO gedeeld.

3. VNG agenda actielijnen

De VNG Agenda Digitale Veiligheid 2020-2024 biedt via 10 actielijnen handelingsperspectief voor de bestuurlijke praktijk. De VNG ondersteunt hiermee gemeenten bij de beveiliging van hun informatiesystemen en de gegevens over inwoners en ondernemers. De hoofdonderwerpen zijn: bewustwording, governance, risicogericht handelen en werken als één overheid.[9]

De rekenkamer heeft Hoffmann verzocht om de status van de in de agenda genoemde actielijnen op te halen en te rapporteren. Hieronder een toelichting vanuit de CISO per actielijn, onderverdeeld in de hoofdonderwerpen.

3.1.1.1 Awareness

Actielijn 1: Bewustzijn vergroten

Sinds 2021 is er een interne bewustzijnscampagne bij de gemeente Den Helder. De volgende onderdelen komen hierin naar voren:

1. Wekelijkse vraag (Recourse – Sir Askalot); onderdeel van de campagne is een wekelijkse vraag over informatiebeveiliging en privacy.
2. Online leeromgeving (Recourse); medewerkers hebben allemaal een account bij Recourse waarin ze e-learnings kunnen maken om meer kennis op te doen van thema's zoals phishing, 'achter je scherm', cloud, en privacy. Bij nieuwe medewerkers wordt aangegeven dat zij de e-learnings over informatiebeveiliging en privacy dienen te maken binnen drie maanden van indiensttreding.
3. Presentaties worden ad hoc gedaan met diverse teams. Momenteel worden de meeste presentatie gegeven bij het sociaal domein vanwege de gevoeligheid van de data waarmee gewerkt wordt. Meestal wordt naar aanleiding van een verzoek een presentatie voorbereidt gericht op de specifieke risico's binnen dat team.
4. Vorig jaar heeft de gemeente een mystery guest ingezet om te kijken hoe de fysieke beveiliging in combinatie met informatiebeveiliging geregeld is. De ambitie is om deze test jaarlijks te laten terugkeren.

Externe bewustzijn wordt gecreëerd door team Openbare Orde en Veiligheid door het gesprek aan te gaan met MKB-bedrijven.

Actielijn 2: Weerbare organisatie

Wat betreft de actielijn 'weerbare organisatie' spreekt gemeente Den Helder intern van three-lines-of-defense of de beveiligingsstrategie volgens het ui-model. Eigenlijk is het gehele doel van informatiebeveiliging en privacy om schillen en afscheidingen te creëren, zodat risico's worden beperkt.

[9] Voor meer informatie zie: https://vng.nl/publicaties/agenda-digitale-veiligheid-2020-2024

Voorbeelden van maatregelen in het kader van de weerbare organisatie zijn:

- Firewall + IDS systemen;
- Anti-spam filters;
- Autorisatiebeheerbeleid;
- Procedures en beleid voor werken;
- Afscheiding van netwerken;
- SIEM/SOC beveiliging;
- Back-ups met ransomware beveiliging;
- Bewustzijn van medewerkers.

Actielijn 3: De digitale brandoefening

Crisisoefeningen of een digitale brandoefening hebben nog niet plaatsgevonden binnen de gemeente. Intern wordt er jaarlijks wel een uitwijktest gedaan om te testen of er bij problemen goed overgeschakeld kan worden van het ene datacenter naar het andere datacenter. Resultaten uit de uitwijktest worden vervolgens besproken en indien nodig verbeterd.

3.1.1.2 Governance

Actielijn 4: Decentrale verantwoording waar kan, centraal toezicht waar moet

De jaarlijkse externe audit wordt gezien als een decentrale verantwoording met centraal toezicht. Hier moeten de gemeente aan voldoen en dit zorgt er onder andere voor dat verbeteringen worden getroffen. Daarnaast wordt een zelfevaluatie voor de BIO uitgestuurd door de CISO via het ISMS. De tekortkomingen die hieruit komen, worden geprioriteerd en besproken.

Actielijn 5: OOV bevoegdheden en rollen voor de lokale bestuurders

Team OOV en de burgemeester zijn verantwoordelijk voor de veiligheid in de gemeente Den Helder. Dit valt buiten scope van de informatiebeveiligingsorganisatie (CISO en FG).

3.1.1.3 Risicogericht handelen

Actielijn 6: Lokale vitale processen bepalen vanuit maatschappelijke taken

Voldoen aan de BIO en ISO27001 is een doelstelling op zich, maar het beschermen van de data van burgers en de gemeente heeft de hoogste prioriteit voor de CISO. Vitale processen worden daarbij gecategoriseerd en bekeken, waarbij de focus vooral ligt op informatie en data van de burgers. Vitale infrastructuur is belangrijk, maar qua taken en uren is er onvoldoende ruimte om bedrijven in de vitale infrastructuur binnen de gemeente Den Helder ook te controleren. Om dit thema hoger op de agenda te zetten, zal de gemeente Den Helder extra FTE vrij moeten maken en extra financiële middelen beschikbaar moeten stellen.

Actielijn 7: Krachtige partner in de keten

De gemeente Den Helder werkt nauw samen met de VNG en de Informatiebeveiligingsdienst (IBD). Cyberdreigingen worden door het Nationaal Cyber Security Centrum (NCSC) en de IBD met de

gemeente gedeeld. Daarnaast is de CISO van de gemeente Den Helder onderdeel van een maandelijks overleg en Signal-groep waarin kennis, dreigingen en beleid worden gedeeld. Ook worden projecten in samenwerking met andere gemeenten opgepakt om bijvoorbeeld samen leveranciersmanagement op te zetten.

Actielijn 8: Risicomanagement geeft focus

Bij nieuwe projecten wordt er door middel van een DPIA gecontroleerd wat de risico's voor de privacy zijn. Daarnaast wordt de CISO betrokken om te bepalen of er grote beveiligingsrisico's zijn bij de aanschaf van nieuwe applicaties. Dit proces is vooral ingericht voor de interne organisatie.

3.1.1.4 Eén overheid/samen organiseren

Actielijn 9: Versterken gemeentelijke weerbaarheid

Onderdeel van actielijn 9 zijn de voorgaande actielijnen. Informatiebeveiliging is een pakket van organisatorische en technische maatregelen om te voorkomen dat de gemeente data of informatie kwijt raakt. Jaarlijks moeten maatregelen worden aangepast om te alle tijde mee te bewegen met de nieuwe risico's. Door meldingen van de IBD worden kwetsbaarheden van applicaties sneller opgelost.

Actielijn 10: Eén overheid

Door een gemeenschappelijk normenkader wordt het makkelijker om als gemeente samen te werken met andere gemeenten. Informatie en kennis delen staat hierin centraal en wordt regelmatig gedaan.

4. Disclaimer

De volgende medewerkers van Hoffmann hebben het onderzoek uitgevoerd en deze rapportage opgemaakt:

Oscar Vermaas,
Security Consultant

Esther Kraan,
Consultant Riskmanagement

Ondergetekende is vanuit zijn rol als leidinggevende eindverantwoordelijk voor dit onderzoek.

Johan van Slooten
Directeur Cybersecurity & Security Risk management

Ondanks het feit dat onze onderzoekers zeer zorgvuldig onderzoek verrichten, bestaat de mogelijkheid dat zij niet iedere kwetsbaarheid detecteren in de IT-infrastructuur van onze opdrachtgever. Dit komt mede doordat onze medewerkers gebonden zijn aan een budget- en tijdslimiet (een penetratietest is altijd een momentopname).

Dit rapport is geschreven voor de opdrachtgever, zodat hij of zij staat wordt gesteld om maatregelen te nemen teneinde de cyberweerbaarheid van zijn/haar organisatie te verhogen. Wij kunnen geen aansprakelijkheid aanvaarden voor acties of maatregelen die door opdrachtgever of diens vertegenwoordigers op basis van het rapport worden ondernomen. Tenslotte verwijzen wij naar de van toepassing zijnde dienstverleningsvoorwaarden.

Almere, 8 april 2024

5. Bijlagen

5.1 Bijlage Toelichting op bevindingen & aanbevelingen onderdeel Organisatie

5.1.1 Beleid

Het 'Strategisch informatiebeveiligingsbeleid 2020-2023 is op het moment van onderzoek vigerend binnen de gemeente Den Helder. Dit beleid omschrijft op hoog over niveau de scope, uitgangspunten en rollen en verantwoordelijkheden van informatiebeveiliging binnen de gemeente Den Helder. De gemeente heeft ervoor gekozen om verantwoordelijkheden zo laag mogelijk in de organisatie te beleggen, zo ook wanneer het informatiebeveiliging betreft. Passend bij deze bedrijfsvoering is in plaats van een tactisch beleid of operationele richtlijnen, gekozen voor gedragsregels. Concreet en bondig wordt er in het document 'Gedragsregels informatiebeveiliging' beschreven wat er wel óf juist niet op bepaalde thema's wordt verwacht van alle medewerkers. In andere documenten[10] wordt tevens verwezen naar gedragsregels, echter lijken er meerdere versies van deze regels in omloop te zijn. Hierdoor is het voor de onderzoekers, en daarmee aannemelijk ook voor medewerkers, niet duidelijk welke gedragsregels er van kracht zijn. Hiermee verliest het aan effectiviteit en duidelijkheid.

In de interviews komt naar voren dat er losse beleidsstukken beschikbaar zijn op verschillende deelthema's (zoals autorisaties, wachtwoorden en incidenten) en dat er momenteel wordt gewerkt aan het lees- en vindbaar maken van deze stukken. Men geeft echter aan dat er te weinig tijd is om een overkoepelend tactisch beleid uit te werken. Er is tevens een gebrek aan uitwerking in procedures of operationele richtlijnen waardoor veel vragen nu uitkomen bij de I&T afdeling of de CISO. Ook ontbreekt het 'Gemeentelijk informatiebeveiligingsplan' voor 2022 en 2023, het gebrek aan tijd wordt hier tevens genoemd als reden.

Met het besluit om de verantwoordelijkheden laag in de organisatie te beleggen, is het van een nóg groter belang om de medewerkers te faciliteren met duidelijke handvaten. Er is nu een inhoudelijke gap tussen het strategisch informatiebeveiligingsbeleid en de gedragsregels. Een volledige en tactische c.q. operationele uitwerking van strategisch beleid draagt sterk bij aan het vermogen van de medewerkers om het beleid in praktijk te brengen. Duidelijke richtlijnen kunnen er tevens voor zorgen dat medewerkers minder vaak een beroep hoeven te doen op de informatiebeveiligingsorganisatie of I&T afdeling.

In de interviews wordt aangegeven dat er ten tijde van het onderzoek wordt gewerkt aan een nieuwe versie van het strategisch beleid. Het huidige beleid komt op bepaalde vlakken niet (meer) overeen met de praktijk binnen de gemeente. Zo wordt er bijvoorbeeld geschreven over een controller informatieveiligheid en privacybeheerders, echter zijn deze geen onderdeel van de informatiebeveiligingsorganisatie. Daarnaast is het strategisch beleid een uitgelezen plek om visies van

[10] 'Wachtwoordbeleid gemeente Den Helder' en 'Informatie bezoek Mystery Guest gemeente Den Helder 2022'

de gemeente Den Helder op informatiebeveiliging toe te lichten. Het huidige beleid is grotendeels gebaseerd op een template vanuit de Vereniging Nederlandse Gemeenten (VNG) waardoor het geheel vrij algemeen is en minder aansluit bij de situatie binnen de gemeente. De actualisatie is een mooi moment om te evalueren hoe het beleid beter kan aansluiten bij de praktijk en meer gekleurd kan worden met de visie, ambities en speerpunten van de gemeente op informatiebeveiliging.

5.1.2 Informatiebeveiligingsorganisatie

De informatiebeveiligingsorganisatie van de gemeente Den Helder bestaat uit de chief informatie security officer (hierna genoemd: CISO) en de functionaris gegevensbescherming (hierna genoemd: FG). De CISO rapporteert op het vlak van informatiebeveiliging aan de wethouder, eveneens portefeuillehouder. De CISO en de FG hebben een vast wekelijks overleg en regelmatig vindt er afstemming plaats met collega's van bijvoorbeeld inkoop, technische IT-adviseurs en informatiemanagers. Daarnaast overleggen de CISO en FG periodiek met CISO's en FG's van anderen gemeenten ten behoeve van kennisdeling en een gezamenlijke aanpak in grotere projecten. Gezien het belang van het thema informatiebeveiliging, is het wenselijk om een vast periodiek overleg te hebben met de portefeuillehouder, iets wat momenteel niet het geval is.

De CISO voert verschillende taken uit binnen de gemeente. Zo heeft hij de rol van ENSIA-coördinator, beveiligingsfunctionaris voor Suwinet en is hij verantwoordelijk voor de informatiebeveiligingsbewustwording onder medewerkers. Inhoudelijk is er soms sprake van rolonduidelijkheid. Conform de BIO ligt de verantwoordelijkheid voor de uitvoering van het informatiebeveiligingsbeleid formeel bij de teammanagers en treed de CISO adviserend op. De CISO heeft in dat kader de teammanagers en applicatiebeheerders toegevoegd aan het ISMS, waarin middels een PDCA-vragenlijst wordt uitgevraagd hoe de organisatie ervoor staat aangaande informatiebeveiliging. In de praktijk blijkt echter dat het ISMS voornamelijk nog iets 'van de CISO' is en wordt op het vlak van informatiebeveiliging vanuit de organisatie nog veel praktische ondersteuning gevraagd. De gemeente zou kunnen overwegen om een ISO (Information Security Officer) aan te stellen om de CISO alsmede de organisatie te ondersteunen bij deze praktische werkzaamheden en hulpvragen.

Aangaande de positionering van de CISO zijn een aantal zaken die opvallen. Idealiter heeft een CISO een onafhankelijke positie ten opzichte van lijnmanagement en een eigen budget voor informatiebeveiliging. Binnen de gemeente Den Helder valt de CISO hiërarchisch onder de teammanager I&T en is hij tevens afhankelijk van het budget van het I&T-team. De teammanager I&T en de CISO zitten op dezelfde lijn aangaande de nodige investeringen, waardoor de CISO momenteel geen belemmering ervaart. Echter, kent ook dit budget zijn beperkingen en hangt er een mogelijk risico aan deze afhankelijkheid, bijvoorbeeld in het geval van een personele wisseling.

5.1.3 Verantwoording

Jaarlijks legt de gemeente verantwoording af op het vlak van informatieveiligheid door het uitvoeren van de ENSIA-audit. Binnen de gemeente Den Helder is de CISO verantwoordelijk als coördinator, hij wordt hierin bijgestaan door een externe partij. De CISO maakt daarnaast een halfjaarlijkse rapportage voor het MT en wethouders waarin thema's als Suwinet, incidenten en bewustzijn behandeld worden. In aparte rapportages wordt het bestuur meegenomen in eventuele incidenten.

De CISO beoogt te werken volgens een jaarlijks gemeentelijk informatiebeveiligingsplan (volgens het beleid opgesteld onder leiding van directie) en een plan van aanpak met een PDCA-cyclus. Door een te grote (ad-hoc) belasting lukt dit in praktijk niet altijd. Onderzoekers hebben vernomen dat deze documenten daarom voor 2022 en 2023 niet beschikbaar zijn. Het uitblijven van de plannen zorgt niet voor vragen vanuit de organisatie, iets waaruit afgeleid kan worden welk belang hieraan wordt gehecht.

5.1.4 Risicomanagement

Met de komst van de BIO in 2019 ligt er meer nadruk op risicomanagement binnen informatiebeveiliging. Op basis van risicoanalyses dienen de juiste en relevante maatregelen getroffen te worden[11]. Het strategisch beleid van de gemeente Den Helder zegt hier het volgende over: "Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid." Kijkende naar de praktijk binnen de gemeente komt echter naar voren dat binnen de gemeente Den Helder nog niet overal proactief op risico's wordt gestuurd.

Rondom de kritische applicaties heeft de I&T afdeling de risico's goed in kaart gebracht. Daarnaast laat men de systemen jaarlijks toetsen door de uitvoer van penetratietesten en audits en worden diverse (preventieve) maatregelen genomen, zoals bijvoorbeeld de installatie van een SIEM/SOC[12]. Van de systemen en applicaties die onder het I&T beheer vallen, worden de updates en patches bijgehouden. Voor de systemen en applicaties welke niet bekend zijn bij I&T, bestaat het risico op onvoldoende beheer, wat kwetsbaarheden in de beveiliging kan opleveren. De I&T afdeling is momenteel bezig met een project om onbeheerde systemen in kaart te brengen en, waar servicecontracten en updates ontbreken, deze te verwijderen. Binnen de gemeente mag echter door medewerkers zelf software aangekocht worden, waarbij I&T of inkoop niet altijd wordt betrokken. Dit houdt het risico op het ontstaan van zogenaamde 'schaduw-IT' in stand.

Risicomanagement beperkt zich niet tot IT, het is een overstijgend thema wat voor alle bedrijfsprocessen belangrijk is. De lijnmanager kent de eigen werkprocessen en de daarbij te beschermen informatie het beste. Het is daarom ook de verantwoordelijkheid van het lijnmanagement om een inschatting te maken van de risico's en af te wegen in hoeverre deze risico's acceptabel zijn. Deze risicoanalyses helpen om

[11] Zie hiervoor BIO "Informatiebeveiliging bij de overheid" Hoofdstuk 1.2
[12] Zie de verklarende woordenlijst in bijlage 5.3

de juiste maatregelen te nemen om risico's te mitigeren. Op dit moment worden er weinig tot geen risicoanalyses uitgevoerd en is er daardoor onvoldoende zicht op (mogelijke) risico's en (eventuele) maatregelen. Uit de interviews komt naar voren dat de organisatie moeite heeft met het stuk verantwoordelijkheid en eigenaarschap op dit vlak. De CISO geeft aan te weinig ruimte te hebben om dit zelf te organiseren, los van de vraag of dit wenselijk zou zijn. Het is raadzaam om deze verantwoordelijkheid duidelijk in de lijn te beleggen, deze eventueel te faciliteren door de aanstelling van een ISO, en de risicoanalyses een onderdeel te maken van besluitvorming.

5.1.5 Inkoop- en leveranciersmanagement

De gemeente Den Helder heeft twee inkoopadviseurs in dienst welke de organisatie ondersteunen in het aanbestedingenproces. Ten tijde van het interview is er een vacature voor een derde inkoopadviseur. Het team is verantwoordelijk voor beleid, formats en advies op het vlak van het inkoopproces, zij adviseren niet inhoudelijk over de aan te kopen dienst of product.

Met betrekking tot informatiebeveiliging en privacy worden de eisen aan producten, diensten en leveranciers idealiter gesteld in de selectiefase, vóór de aanschaf. De gemeente Den Helder werkt daarom met een vaste set aan eisen aangaande informatiebeveiliging, welke is opgenomen in een standaard offerte aanvraag. Voor verdiepende vragen of advies aangaande de eisen kan men bij de informatiebeveiligingsorganisatie terecht.

Ook op het vlak van inkoop zijn verantwoordelijkheden zo laag mogelijk binnen de organisatie belegd. Dit betekent in de praktijk dat iedereen een inkooptraject mag starten. Vanaf een bedrag van €50.000,- kijken de inkoopadviseurs mee. Er is echter geen centraal inkoopsysteem en de inkoopadviseurs merken dat er bij de medewerkers nog een wisselende bekendheid is met de eisen en procedures rondom inkoop. Het resultaat is dat de inkoopadviseurs en/of de informatiebeveiligingsorganisatie soms niet of te laat worden betrokken bij een inkooptraject. Daarmee bestaat het risico dat de informatiebeveiligingseisen onvoldoende in acht worden genomen en eventuele toetsing daarop ontbreekt. Het in de vorige paragraaf genoemde risico op 'schaduw-IT' is tevens een risico dat blijft bestaan met de huidige organisatie van inkoop.

Leveranciersmanagement helpt grip te krijgen op mogelijke risico's bij reeds afgenomen diensten en producten. Een actueel en volledig overzicht kan helpen om het beheer van systemen en applicaties juist te beleggen, en daarmee het risico op 'schaduw-IT' te verkleinen. Daarnaast kan leveranciersmanagement bijdragen aan risicomanagement op het vlak van informatiebeveiliging door gebruik te maken van het 'recht op audit' bij bestaande contracten. Op deze manier kan tijdens looptijd bekeken worden of er nog aan de gestelde informatiebeveiligingseisen wordt voldaan. Momenteel is er geen sprake van leveranciersmanagement binnen de gemeente en worden afspraken tijdens looptijd niet getoetst.

5.1.6 Continuïteitsbeheer

De BIO heeft een focus op risicomanagement en stelt daarom ook eisen aan het continuïteitsbeheer van een gemeente.[13] Onderzoekers hebben inzicht gekregen in het 'Incidentmanagement en response beleid' van de gemeente. Hierin wordt beschreven hoe informatiebeveiligingsincidenten, zoals bijvoorbeeld datalekken en uitval van systemen, worden gemanaged. Het doel van het beschreven proces is om informatiebeveiligingsincidenten zo veel mogelijk te voorkomen óf de schade zo veel mogelijk te beperken. De CISO en/of de FG zijn volgens het beleid bij dergelijke incidenten in de lead. Dit komt overeen met de registraties in de door de onderzoekers ontvangen incidentenregisters (2022 en 2023).

Bedrijfscontinuïteitsbeheer gaat echter verder dan het informatiebeveiligingsaspect en de I&T afdeling, het raakt de hele gemeente. Neem bijvoorbeeld een ransomware aanval waarbij meerdere gemeentelijke processen verstoord worden. Een omschreven aanpak van een dergelijke calamiteit of crisis, in de vorm van een Business Continuity plan (BCP), hebben de onderzoekers niet ontvangen. Tijdens de interviews wordt bevestigd dat deze plannen ontbreken en dat er op dit vlak nog een stap te maken is. Het bestuur (college) en de portefeuillehouder hebben hier, als eindverantwoordelijken voor de bedrijfscontinuïteit, een belangrijke rol en verantwoordelijkheid.

5.1.7 Privacy

De FG is drie dagen beschikbaar voor de gemeente Den Helder en werkt één dag voor de gemeente Hollands Kroon. Binnen de gemeente Den Helder valt zij, net als de CISO, onder de teamleider I&T. Idealiter rapporteert de FG aan het hoogst leidinggevende orgaan binnen de gemeente om de onafhankelijkheid te kunnen waarborgen. In het interview geeft de FG weliswaar aan zich vrij genoeg te voelen om zonder last en ruggespraak (ongevraagd) advies te geven.

Volgens de FG is er voldoende bewustzijn bij de medewerkers over het belang van vertrouwelijkheid van de persoonsgegevens. Het loopt echter spaak op de uitvoering van het beleid en de toepassing in het werk. Het privacybeleid van de gemeente Den Helder beschrijft de doelstellingen, uitgangspunten, taken en verantwoordelijkheden en maatregelen rondom privacy. Het ontbreekt aan praktische handleidingen of richtlijnen voor medewerkers. Daarnaast wordt de organisatie op tactisch/operationeel niveau niet ondersteund door bijvoorbeeld een privacy officer, er komen daarom veel praktische hulpvragen bij de FG terecht. Formeel is de FG een toezichthouder, een controlerend orgaan om toe te zien op de naleving van de algemene verordening gegevensbescherming (AVG). Een strikte functiescheiding is vanwege bovenstaande echter lastig te hanteren. De FG is zich hiervan bewust en beperkt zich zo veel mogelijk tot advisering, waarbij het lijnmanagement beslist. Aanstelling van een privacy officer (PO) maakt de functiescheiding gemakkelijker te handteren en beperkt de ad-hoc druk bij de FG.

[13] Zie BIO: Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer 17.1

Omdat de informatiebeveiligingsorganisatie niet altijd (op tijd) betrokken wordt bij een nieuwe verwerking komt het voor dat verwerkingen worden gestart zonder uitvoer van een Data Protection Impact Assessment (hierna: DPIA). Bij de uitvoeringing van een DPIA wordt meestal om ondersteuning van de FG gevraagd. Gemeente Den Helder beschikt over een uitgebreid verwerkingsregister, echter is dit een statisch in plaats van dynamisch verwerkingsregister. Het verwerkingsregister wordt bijgehouden middels een periodieke uitvraag bij de teams. De laatste (en tevens ook eerste) uitvraag is vier jaar geleden gedaan. Het verwerkingsregister is daarmee niet up to date, waardoor de gemeente niet volledig voldoet aan de verantwoordingsverplichting zoals gesteld door in de AVG.[14] Onderzoekers raden aan dit register bij te werken en een continu doorlopend proces in te richten zodat het een dynamisch register wordt. Daarnaast is het van belang dat de status van dit document wordt meegenomen in de rapportages richting het college zodat hierop gestuurd kan worden.

5.1.8 Logisch toegangsbeleid

Om te voorkomen dat onbevoegden toegang krijgen tot informatie, is het wenselijk om de toegang tot die informatie te baseren op verantwoordelijkheden en/of functie.[15] Het toekennen van autorisaties gaat bij de gemeente Den Helder op aanvraag van de manager, op basis van een functieprofiel. Ten tijde van het onderzoek is de gemeente Den Helder in de opstartfase van een autorisatiemanagementproject. De eerste stap is om voor de vijf belangrijkste kernapplicaties autorisatiematrixen te maken en zo inzicht te creëren in de toegangsrechten.[16] Met dit inzicht wordt er een periodieke controle opgezet naar autorisaties (indienst, uitdienst en doorstroom).[17] De ambitie is tevens om een automatische koppeling tussen functiehuis en rollen vast te leggen in Topdesk, zodat autorisaties niet meer handmatig toegekend hoeven te worden. Het standaardiseren hiervan draagt bij aan de informatieveiligheid binnen de organisatie.

De BIO stelt dat informatie door middel van een risicoafweging geclassificeerd dient te worden, zodat duidelijk is wat een passend beschermingsniveau is. Met inzicht in het type data, de locatie van de informatie en het belang hiervan voor de organisatie kunnen de juiste beveiligingsmaatregelen genomen worden.[18] Binnen de gemeente Den Helder zijn er nog geen bestaande processen op het vlak van dataclassificatie. In het contact met andere gemeentes wordt hier kennis gedeeld en worden best practices uitgewisseld. Het is uiteindelijk aan de teammanagers, als eigenaar van de informatie, om hier verantwoordelijkheid in te nemen.

[14] Zie: https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/verantwoordingsplicht#een-verwerkingsregister-bijhouden

[15] Zie BIO: Toegangsbeveiliging van systeem en toepassing 9.4.1.2

[16] Het betreft hier de volgende applicaties: Suwinet, Suite4SocialeRegie/Suite4SocialeDomein, BRP, XxIlnce – zaaksysteem, Cognos.

[17] Uit ambtelijk wederhoor komt naar voren dat er een half-jaarlijkse autorisatiecontrole door teammanagers is opgezet.

[18] Zie BIO: Informatieclassificatie 8.2

5.1.9 Bewustwording medewerkers

De BIO geeft aan dat de organisatie een verantwoordelijkheid heeft voor het bewustzijn, opleiding en training van medewerkers ten aanzien van informatiebeveiliging.[19] De gemeente Den Helder maakt gebruik van een online leeromgeving (Recourse) om kennis te delen op het vlak van informatiebeveiliging en privacy. Via dit platform krijgen de medewerkers een wekelijkse vraag toegestuurd en kan men e-learnings maken op het vlak van informatiebeveiliging en privacy. Deelname aan de e-learnings is niet verplicht, in de praktijk is ongeveer 50% van de medewerkers actief. Bewustwording behoort binnen de gemeente Den Helder tot de verantwoordelijkheid van de CISO, hij rapporteert het aantal deelnemers en past de inhoud aan waar nodig of relevant. Naast de e-learning zijn er ook initiatieven als presentaties, nieuwsbrieven en themaweken zoals 'Week van de privacy' om het bewustzijn op het vlak van privacy en informatiebeveiliging te verhogen.

De hierboven genoemde initiatieven en e-learnings worden ingezet om het bewustzijn van de medewerkers te verhogen. Het einddoel is echter informatieveilig gedrag terug te zien in de praktijk. Helaas geeft het hebben van de juiste kennis nog niet de garantie op het gewenste gedrag. Om het leereffect te versterken is het aan te raden om kennis te combineren met oefening in de praktijk. De ambitie van de gemeente is daarom om periodiek phishing e-mails te versturen en jaarlijks een mystery guest bezoek te laten uitvoeren. Daarnaast kan de gemeente onderzoeken op welke manier zij de medewerkers zo goed mogelijk kunnen faciliteren om het gewenste informatieveilige gedrag in de praktijk te laten zien.

5.1.10 Organisatiecultuur

In het ideale geval is informatiebeveiliging onderdeel van de cultuur. Iedereen is eigenaar en risicomanagement is onderdeel van de bedrijfsvoering. Kijkende naar de praktijk binnen de gemeente Den Helder zien we dat deze organisatorische inbedding van informatiebeveiliging nog niet op orde is. De gemeente heeft ervoor gekozen om verantwoordelijkheden laag in de organisatie te beleggen, echter is te merken dat men in de praktijk meer behoefte heeft aan ondersteuning om deze verantwoordelijkheid op te kunnen pakken. Duidelijke richtlijnen, protocollen en processen kunnen hierbij helpen. Eveneens zou men kunnen overwegen om iemand in de rol van ISO en PO aan te stellen ter ondersteuning van het in praktijk brengen van beleid.

Wellicht van een nog groter invloed is de attitude van het bestuur ten opzichte van informatiebeveiliging. Wanneer men informatiebeveiliging onderdeel van de cultuur wil maken, is het van belang dat het bestuur de noodzaak van informatiebeveiliging uitdraagt en het juiste voorbeeld geeft in visie en besluitvorming.[20] Tijdens het onderzoek is geen duidelijke visie of 'stip op de horizon' op het vlak van informatiebeveiliging naar voren gekomen. Het gebrek aan visie draagt bij aan een voornamelijk reactieve bedrijfsvoering. Zaken worden veelal 'bottom up' vanuit de IB-organisatie georganiseerd, thema's worden van onderaf aangedragen. Hierop volgen weinig vragen of initiatieven van bovenaf. De

[19] Zie BIO: Veilig personeel 7.2.2

[20] Opmerking uit ambtelijk wederhoor: "In de gemeenteraad van 7 maart 2022 zijn extra middelen voor ICT beschikbaar gesteld. Het aspect veiligheid is in het raadsvoorstel en uitvoeringsplan nadrukkelijk benoemd."

bestuurlijke betrokkenheid kan gemeten worden aan de hand van de vragen of verzoeken vanuit raad, college en directie, maar ook door te kijken naar organisatie en budget. De positionering van de IB-organisatie binnen het I&T team alsmede de afhankelijkheid van budget van I&T, bevestigt het beeld dat informatiebeveiliging voornamelijk wordt gezien als een I&T kwestie in plaats van een gemeente brede verantwoordelijkheid.

5.2 Toelichting op bevindingen & aanbevelingen onderdeel Mens

De toelichting op de uitgevoerde test met phishing mail en het bezoek van de mystery guest bevat detailinformatie over hoe deze tests zijn uitgevoerd. Deze informatie kan door mogelijk kwaadwillende lezers gebruikt worden tegen de gemeente Den Helder. Om dit te voorkomen is bijlage 5.2. op verzoek van de Rekenkamer in een apart document opgenomen en als geheim geclassificeerd.

5.3 Verklarende woordenlijst

Onder leiding van Cyberveilig Nederland (https://www.cyberveilignederland.nl/) hebben ruim 60 organisaties, overheidspartijen en private partijen meegewerkt aan de samenstelling van het cybersecurity woordenboek. Er is een verklarende woordenlijst opgesteld met bijna 600 cybersecuritytermen om bijvoorbeeld rapporten, adviezen of offertes beter te begrijpen.

Voor het complete woordenboek verwijzen wij graag naar: www.cyberveilignederland.nl/woordenboek

Begrip	Betekenis
Account	Element van een digitaal systeem dat een gebruiker representeert. Bij een account hoort informatie over de gebruiker, zoals persoonlijke gegevens, inloggegevens en informatie waar de gebruiker bij mag. Er bestaan verschillende soorten accounts, zoals een gebruikersaccount of een administratoraccount voor beheerders. In het spraakgebruik wordt deze term vaak gebruikt om lidmaatschap bij een dienst aan te duiden - "ik heb een account bij ...
Authenticatie	Wat men doet om vast te stellen of een ander wel is wie hij zegt te zijn. De ander kan een persoon zijn, maar ook bijvoorbeeld software of een apparaat.
Autorisatie	De bevoegdheden die een gebruiker van een computersysteem heeft om toegang te krijgen tot gegevens of handelingen te mogen uitvoeren. Bijvoorbeeld het opstarten van programma's of het inzien, wijzigen of wissen van informatie.

Begrip	Betekenis
AVG	Algemene Verordening Gegevensbescherming. In Europa wordt dit geregeld in de GDPR. De AVG is de Nederlandse uitwerking van de Europese GDPR. De GDPR zorgt ervoor dat er in de hele EU dezelfde basis/ minimum regels voor de bescherming van persoonsgegevens zijn. De AVG is in Nederland de opvolger van de Wet Bescherming persoonsgegevens.
Business continuity plan (BCP)	Gedocumenteerde informatie die een organisatie richting geeft om te reageren op een verstoring en de levering van producten en diensten conform haar doelstellingen voor bedrijfscontinuïteit te hervatten en herstellen.
CISO	Chief Information Security Officer. Verantwoordelijk voor informatiebeveiligingsbeleid evenals de implementatie en toezicht op uitvoering. Tevens verantwoordelijk voor strategie op het gebied van informatiebeveiliging.
Crisismanagement	Gecoördineerde activiteiten om een organisatie te leiden, te sturen en te controleren met betrekking tot crisis .Een crisis is een abnormale of buitengewone gebeurtenis of situatie die een organisatie of gemeenschap bedreigt en een strategische, adaptieve en tijdige reactie vereist om de levensvatbaarheid en integriteit te behouden.
Domeinnaam	Een unieke naam op internet. Meestal geldt een domeinnaam voor websites, maar men kan ook een domeinnaam aanvragen voor een persoonlijk mailadres.
DPIA	Data Protection Impact Assessment. Een organisatie onderzoekt vooraf wat de risico's van gegevensverwerking zijn voor de privacy van personen. Dit is vaak verplicht volgens de Algemene verordening Gegevensbescherming.
FG	Functionaris Gegevensbescherming. Verantwoordelijk voor toezicht op toepassing en naleving van de AVG.
Firewall	Hardware of software om computers en netwerken te beschermen tegen aanvallen. Een firewall bekijkt alles wat over het netwerk gaat en blokkeert bepaald verkeer op het netwerk.
Gebruikersnaam	Naam waarmee een gebruiker in een computersysteem kan inloggen.
Intrusion detection system (IDS)	Een systeem dat alle data controleert die door een computernetwerk gaan of die een digitaal systeem verstuurt en ontvangt. Het systeem geeft een waarschuwing als er iets niet in orde lijkt.

Begrip	Betekenis
Informatiebeveiliging (IB)	Alles wat men doet om ervoor te zorgen dat men bij informatie kan komen wanneer men dat wil, dat de informatie klopt en dat de informatie niet bij anderen terecht komt. Het gaat daarbij vaak om een computersysteem, maar dat hoeft niet. Het gaat om maatregelen, procedures en processen die beveiligingsproblemen voorkomen, opsporen, onderdrukken en oplossen. Ontstaat er wel een probleem met de informatie? Dan zorgt informatiebeveiliging ervoor dat de gevolgen zoveel mogelijk beperkt worden.
Informatiebeveiligingsbeleid	Algemene regels waarmee een organisatie beveiligingsrisico's zo klein mogelijk wil maken. Van tevoren spreekt men af hoe groot de beveiligingsrisico's mogen zijn.
IP reeksen	Een IP adres is het “telefoonnummer” van een computer, waardoor systemen met elkaar kunnen communiceren binnen netwerken en het internet. Een IP reeks is een reeks van opvolgende IP adressen.
Information Security Management System (ISMS)	Managementsysteem voor de beveiliging van informatie. Met dit systeem bewaakt men het proces van informatiebeveiliging.
ISO	Information Security Officer. Verantwoordelijk voor informatiebeveiligingsbeleid evenals de implementatie en toezicht op uitvoering. Tevens verantwoordelijk voor strategie op het gebied van informatiebeveiliging.
Multifactor Authenticatie (MFA) / 2-factor authenticatie	Multifactor Authenticatie (MFA) is een methode om de authenticiteit van een gebruiker te verifiëren op meer dan één enkele manier.
Mystery guest bezoek	Beveiligingstest waarbij een daartoe aangewezen persoon op bezoek gaat bij een organisatie. Daar probeert hij in ruimtes te komen waar hij niet mag komen. En hij probeert bij informatie te komen waar hij niet bij mag komen. Zo test de persoon deze organisatie. Men kan deze test combineren met een penetratietest. Bij deze test gaat de mystery guest een beveiligde ruimte in. Daar probeert hij in te breken op het lokale computernetwerk.
PDCA	Plan-Do-Check-Act (cyclus). Stappen ter verbetering van bijvoorbeeld een proces of beleid.

Begrip	Betekenis
Penetratietest	Handmatige controle waarbij men zo diep mogelijk wil binnendringen in een systeem om zwakke plekken te vinden en de gevolgen hiervan te kennen. Men gebruikt de zwakke plekken om nog wat dieper in het systeem te komen. Doel van de test is niet om zoveel mogelijk zwakke plekken te vinden. Dat gebeurt wel bij een vulnerability scan.
Phishing/Mail-phishing	Aanval waarbij de aanvaller iemand verleidt om belangrijke informatie te geven, zoals bijvoorbeeld inloggegevens of creditcardgegevens. Phishing gebeurt vaak via e-mails. Maar aanvallers proberen het ook via de telefoon, een sms of een app-bericht.
Privacybeleid	Met een privacybeleid brengt een organisatie in kaart welke maatregelen zij heeft genomen om de persoonsgegevens van bijvoorbeeld klanten, patiënten, cliënten te beschermen. Daarnaast is het een manier om als organisatie aan zowel de doelgroep als aan de Autoriteit Persoonsgegevens te laten zien dat ze voldoet aan de AVG.
Privacy Officer / PO	Privacy Officer. Verantwoordelijk voor het ontwikkelen en bewaken van het privacybeleid en ondersteuning bieden bij uitvoering van het beleid.
Ransomware	Ransomware is een samenvoeging van de woorden ransom (losgeld) en software. De aanvallers gijzelen data van het slachtoffer en gebruiken drukmiddelen om het slachtoffer over te halen te betalen. Die gijzeling bestaat vaak uit het versleutelen van de gegevens van het slachtoffer.
Risicoanalyse	Methode om inzicht te krijgen in de risico's die je loopt. De onderzoeker kijkt daarbij onder andere naar het volgende: - hoe groot is de kans dat iets gebeurt? - hoe groot zijn de gevolgen als dat gebeurt?
Schaduw IT (shadow IT)	Shadow IT is hardware of software binnen een onderneming die niet ondersteund wordt en opgezet is door de IT afdeling, maar wel een rol speelt in de bedrijfsvoering.
Security Information and Event Management (SIEM)	Systeem waarin men informatie uit computersystemen verzamelt en analyseert. Het doel is om verdacht gedrag te ontdekken. Of zien dat iemand dingen in het systeem heeft veranderd, terwijl hij dat niet mocht.
Security Operations Center (SOC)	Afdeling of team dat informatiesystemen controleert of bewaakt. Dit doen zij voor de eigen organisatie of voor klanten.

Begrip	Betekenis
Social engineering	Als een aanvaller iemand misleidt door bijvoorbeeld in te spelen op nieuwsgierigheid of behulpzaamheid. Op deze manier probeert de aanvaller bijvoorbeeld aan informatie te komen om in een digitaal systeem in te breken.
Vitale infrastructuur	Die diensten, producten of onderdelen van de infrastructuur van een land die door de Nederlandse overheid als essentieel zijn bestempeld. Worden deze onderdelen uitgeschakeld, of vallen ze uit? Dan is de kans op economische en/of maatschappelijke ontwrichting groot.
Wachtwoord	Reeks van letters, cijfers en of andere karakters waarmee een gebruiker in een computersysteem kan komen. Het is de bedoeling dat een gebruiker dit wachtwoord niet aan anderen geeft en een sterk wachtwoord kiest zodat dit moeilijk te kraken is door aanvallers.

5.4 Overzicht geïnterviewden

Functie	Datum interview
CISO	26 juni 2023 + 14 december 2023
Functionaris gegevensbescherming / Awareness coördinator	27 juni 2023
Technisch IT adviseur	27 juni 2023
Adviseur Inkoop	4 juli 2023
Wethouder	20 juli 2023

5.5 Overzicht bestudeerde documenten

Onderstaande tabel bevat de documenten die zijn ontvangen vanuit de gemeente Den Helder en bestudeerd ten behoeve van het onderzoek naar de organisatie van informatiebeveiliging.

Document	Versie	Datum
Incidentmanagement en response beleid	1.1	08-06-2022
Autorisatiebeheerbeleid	1.0	15-02-2023
Proces wijzigingsbeheer	1.1	21-09-2023
309520 Informatiebeveiligingsbeleid gemeente Den Helder – Getekend	2.0	14-06-2021
AVG inproces verwerkingsregister excelrapportage 2023	-	-

Document	Versie	Datum
Gedragsregels informatiebeveiliging	-	-
Incidentregister 2022	-	-
Informatie bezoek Mystery Guest gemeente Den Helder 2022	-	11-10-2022
PDCA-plan van aanpak informatiebeveiligingsbewustzijn 2021	1.0	17-12-2020
Presentatie informatiebeveiliging Q2-2022	-	-
Privacybeleid gemeente Den Helder	2.0	Juli 2020
Privacyprotocol afvalvinzameling	1.0	23-10-2020
Privacyreglement e-mail- en internetgebruik	-	-
Richtlijnen Social Media gemeente Den Helder	-	-
Strategisch informatiebeveiligingsbeleid 2020-2023	3.0	03-12-2019
Incidentenregister 2023	-	-
Wachtwoordbeleid gemeente Den Helder	1.0	29-09-2020
Proces melden beveiligingsincidenten en datalekken	-	-
2022.FG.Jaarrapportage.College.GemDH	-	-

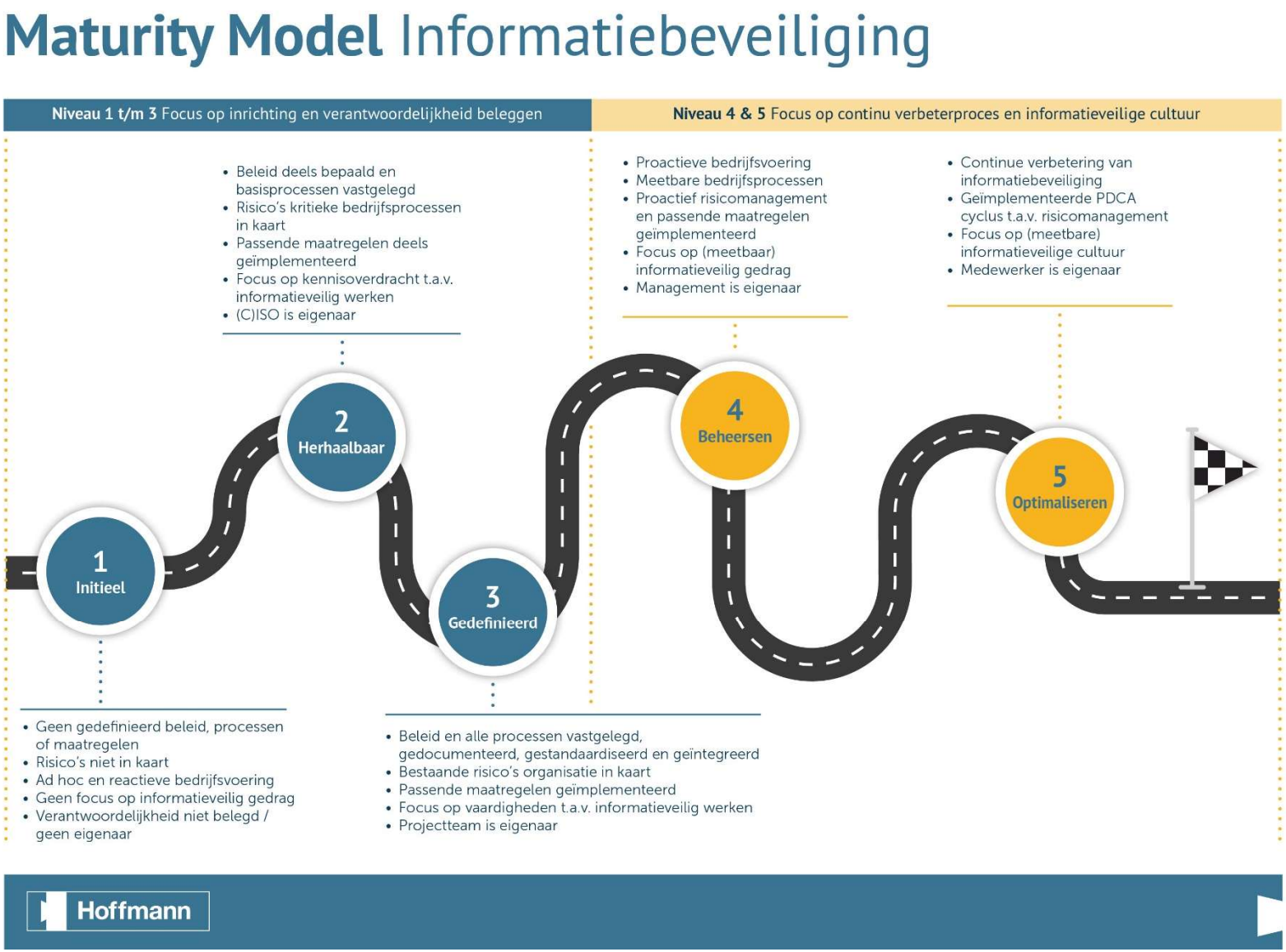
5.6 Contactinformatie

Naam	Functie	E-mail	Telefoon
Oscar Vermaas	Security Consultant	o.vermaas@hoffmann.nl	06-53410213
Laurens Kolfschoten	Security Consultant	l.kolfschoten@hoffmann.nl	06-11769892
Esther Kraan	Consultant Riskmanagement	e.kraan@hoffmann.nl	06-21330432
Mo Ballari	Sales Consultant	m.ballari@hoffmann.nl	06-47384377
Robert Molenaar	Teamleider ICT-security	r.molenaar@hoffmann.nl	06-25716990
Johan van Slooten	Director Riskmanagement	j.vanslooten@hoffmann.nl	06-11003083
Harmannus Kruizinga	Voorzitter RK	-	-
Martine Klaassen Bos	Secretaris Rekenkamer	m.klaassenbos@denhelder.nl	06-22410585

5.7 Versies

Versie	Datum	Status
1.1	25-01-2024	Conceptversie RKC
1.2	01-03-2024	Conceptversie inclusief ambtelijk wederhoor en opmerkingen RKC
Definitief	05-03-2024	Bestuurlijk rapport Informatiebeveiliging Gemeente Den Helder Definitief
Definitief V2	08-04-2024	Bestuurlijk rapport Informatiebeveiliging Gemeente Den Helder Definitief inclusief aanpassingen t.b.v bestuurlijk wederhoor

5.8 Maturity model




Hoffmann
VERTROUWEN IS GOED,
HOFFMANN IS BETER