Medemblik, 30 augustus 2022

Geachte leden van de gemeenteraad,

De rekenkamercommissie van de gemeenten Medemblik en Opmeer heeft onderzoek uit laten voeren naar het informatieveiligheidsbeleid in beide gemeenten. Het onderwerp informatieveiligheidsbeleid stond hoog op de groslijst van het onderzoeksplan 2022.

De onderzoeksvraag luidde:

**Is de informatieveiligheid bij de gemeente Medemblik respectievelijk Opmeer voldoende gewaarborgd?**

De rekenkamercommissie richt zich daarbij op drie verschillende aspecten van het beleid en beleidsuitvoering:

1. Organisatie en proces
2. Mens
3. Techniek

Het feitelijk onderzoek is uitgevoerd door de firma Hoffmann Bedrijfsrecherche B.V. Dit bedrijf is geselecteerd na een onderhandse aanbesteding waarbij drie gespecialiseerde bureaus door de rekenkamercommissie zijn uitgenodigd offerte uit te brengen. Van alle drie bureaus heeft de rekenkamercommissie offerte ontvangen. Twee bureaus hebben hun offerte in een vergadering van de rekenkamercommissie mogen toelichten, waarop de rekenkamercommissie op basis van inhoudelijke criteria de opdracht aan Hoffmann heeft gegund.

Op basis van deze bevindingen heeft de rekenkamercommissie conclusies getrokken en doet zij aanbevelingen. Die treft u hieronder. Daarna treft u de bestuurlijke reactie van het college, gevolgd door de reactie daarop van de rekenkamercommissie

**Conclusies voor de gemeente Medemblik**

Op basis van het onderzoeksrapport van Hoffmann trekt de rekenkamercommissie de volgende conclusies:

1. Het informatieveiligheidsbeleid in de gemeente Medemblik is niet op orde. Het beleid is op een te hoog abstractieniveau geschreven en daardoor moeilijk te operationaliseren en net zo moeilijk te monitoren.
2. Het bewustzijn van medewerkers – ambtelijk en bestuurlijk – is onder de maat. Zowel bij het mysterie guest bezoek als bij de penetratietest gaven medewerkers toegang tot fysieke ruimtes respectievelijk ICT-systemen.
3. Met het vertrek van de CISO in Medemblik is een extra risico ontstaan in de zin dat zijn vertrek het schrijven van een nieuw beleidsplan verder bemoeilijkt. Adequaat beleid en uitvoering daarvan laten daarmee te lang op zich wachten.
4. Het onderzoeksbureau heeft voor De Som geen afschrift van ISO-certificering in de gemeente Medemblik aangetroffen, beveiliging was niet op orde, Hoffmann heeft kunnen inbreken in de systemen. Waar Shared Service Center De Som zorgen uit handen zou moeten nemen, noemen meerdere medewerkers De Som juist als een risico.
5. De samenwerking met andere gemeenten binnen De Som - met verschillende prioritering tussen verschillende gemeenten - leidt tot trage besluitvorming, gebrek aan regie en kan daardoor leiden tot extra risico's.
6. In de uitvoering zijn op alle drie de onderzochte onderdelen mens, organisatie en techniek onvolkomenheden gevonden. Dit levert risico's op alle drie onderdelen.

**Aanbevelingen aan de gemeenteraad van Medemblik**

1. Verzoek het College het informatieveiligheidsbeleid te herijken en daarbij te voldoen aan de verplichte BIO en stel dit beleid op basis daarvan als Raad vast. Herhaal dit elke raadsperiode en heb in dit beleid oog voor mens, organisatie en techniek.
2. Verzoek het College het risicobewustzijn bij de medewerkers te verbeteren. Denk daarbij bijvoorbeeld aan thuiswerken, koop niet in zonder de CISO of de functionaris gegevensverwerking te raadplegen en verbeter de uitvoering van het toegangsbeleid voor het gemeentehuis.
3. Verzoek het College jaarlijks een risicoanalyse op het onderwerp informatieveiligheid te maken en de raad over de risico's en de acties die het College daarop onderneemt te informeren.

**Aanbevelingen aan gemeenteraad en College van Medemblik**

4. Neem de geldelijke waardering van het risico op informatieveiligheid realistisch op in de risicoparagraaf van de gemeentelijke begroting en in de jaarrekening. Denk bij het inschatten van dit risico bijvoorbeeld aan de kosten van
    a. forensisch onderzoek
    b. onderzoek welke data is nu precies gestolen is
    c. vervanging van alle buitgemaakte gegevens van documenten (bijvoorbeeld paspoorten of rijbewijzen van burgers)
    d. het inrichten van een call center
    e. het opnieuw opstarten of zelfs opnieuw inrichten van systemen
5. Eis van De Som dat zij alle relevante certificaten, normeringen en Service Level Agreement heeft en houdt. Neem hierin de bestuurlijke en financiële

verantwoordelijkheid die de eigen gemeente ook heeft. Overweeg, als De Som niet aan deze eis kan of wil voldoen, een andere partner te zoeken voor de taken die bij De Som zijn belegd.

**Bestuurlijke reactie**

De rekenkamercommissie heeft het college van de gemeente Medemblik om een reactie gevraagd op het rapport van bevindingen, de conclusies en de aanbevelingen. Deze reactie hebben wij op de volgende bladzijden integraal ingevoegd.

Rekenkamercommissie Medemblik
Per email aan de secretaris van de Rekenkamercommissie

| | |
|---|---|
| **Uw kenmerk** | |
| **Uw brief van** | 21 juni 2022 |
| **Zaaknummer** | Z-22-413927 |
| **Documentnummer** | DOC-22-553797 |
| **Bijlage(n)** | 0 |
| **Telefoonnummer** | 0229 856000 |
| **Verzonden** | Per mail 5 juli '22 |

| | |
|---|---|
| **Behandelend ambtenaar** | Manja van der Weit |
| **Onderwerp** | Bestuurlijke reactie rapport informatieveiligheid |

Geachte leden van de Rekenkamercommissie,

In opdracht van de rekenkamercommissie van Medemblik en Opmeer (hierna RKC) is er in het eerste kwartaal van 2022 een onderzoek gedaan naar de informatiebeveiliging van gemeente Medemblik. In het kader van bestuurlijke hoor en wederhoor geven wij als college graag een reactie op de onderzoeksresultaten.

Allereerst onze dank voor het onderzoeksrapport en het vele werk dat u hiervoor heeft verzet. Het onderzoek naar de organisatie van de informatiebeveiliging had tot doel om na te gaan of gemeente Medemblik de belangrijkste risico's in beeld heeft, hoe het beleid is opgesteld en of dit in de praktijk wordt toegepast. Het college heeft het rapport met belangstelling gelezen. Het college kiest ervoor om niet op elk onderdeel uit het rapport te reageren. Op dit moment volstaat het college met een reactie op hoofdlijnen.

Ondanks dat uit het onderzoek blijkt dat de informatieveiligheid op verschillende punten zorgelijk te noemen is, zijn wij blij met dit uitgebreide en zorgvuldig opgestelde rapport. Het biedt ons goede inzichten en legt de vinger op een zere plek. Hierdoor biedt het ons de kans om deze zorgelijk gebleken punten op te lossen voordat er problemen ontstaan.

Wij herkennen en erkennen de door u geschetste zorgpunten. Veel van de geconstateerde problemen zijn te herleiden naar het zich niet houden aan gemaakte afspraken en onoplettendheid. Gebrek aan awareness ligt hier dan ook vooral aan ten grondslag. Dit is niet met louter geld op te lossen. Awareness begint met het (h)erkennen van de urgentie en het onderkennen van de eigen tekortkomingen. Hierop maar ook op de andere geconstateerde gebreken, zal geïnvesteerd moeten worden.

De aanbevelingen van de Rekenkamercommissie zijn duidelijk, concreet en uitvoerbaar. Ze bieden ons duidelijke handvatten om de geschetste problematiek daadkrachtig aan te pakken.

Postbus 45, 1687 ZG Wognum / telefoon (0229) 85 60 00 / fax (0229) 85 69 99/ info@medemblik.nl / www.medemblik.nl

Het college omarmt het advies en heeft inmiddels maatregelen ingang gezet om de informatieveiligheid te verbeteren inclusief beschikbaar stellen van middelen die hiervoor nodig zijn.
Wij nemen de aanbevelingen die de Rekenkamercommissie heeft gedaan dan ook graag ter harte en hebben geen op- of aanmerkingen op het voorgelegde conceptrapport. We zien de definitieve rapport graag tegemoet en zullen vervolgens de Raad informeren over de voortgang van de genomen maatregelen en het plan van aanpak voor de nog te nemen maatregelen.

*Vragen?*
Heeft u vragen? Belt u ons dan op werkdagen (maandag t/m donderdag) tussen 08.30 en 17.00 uur of op vrijdag tussen 08.30 en 14.00 uur. Het telefoonnummer is 0229 856000. Wij zijn u graag van dienst. Houd zaaknummer en documentnummer bij de hand, dan kunnen wij u sneller helpen.

Met vriendelijke groet,
Burgemeester en wethouders van Medemblik,

| | |
|---|---|
| De secretaris, | De burgemeester, |
| A. Griekspoor | F.R. Streng |

**Reactie rekenkamercommissie op bestuurlijke reactie college**

De rekenkamercommissie neemt er met instemming kennis van dat het college de bevindingen, conclusie en aanbevelingen omarmt en wenst de gemeente succes bij de implementatie.

# Bestuurlijk rapport Informatiebeveiliging Gemeente Medemblik

22112073

Onderzoek in opdracht van

**Rekenkamercommissie gemeenten Medemblik en Opmeer**

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

# Management samenvatting

De Rekenkamercommissie gemeenten Medemblik en Opmeer (hierna genoemd: 'de Rekenkamer') heeft Hoffmann gevraagd een onderzoek uit te voeren naar de informatiebeveiliging bij de gemeente Medemblik (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.

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

Tijdens het technische onderzoek is getoetst of de informatiesystemen van de gemeente voldoende beveiligd zijn tegen het risico van hacken. Onderzoekers van Hoffmann hebben de informatiebeveiliging zowel getest vanaf het internet (externe penetratietest), als vanuit het gemeentehuis (interne penetratietest).

Het bewustzijn van de medewerkers is op de volgende manieren getest:

1. Mail-phishing, 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 heeft een medewerker van Hoffmann heeft geprobeerd om zonder toestemming toegang te krijgen tot de gemeentelijke werkplekken.

In dit hoofdstuk worden de resultaten samengevat. Voor gedetailleerde bevindingen en aanbevelingen verwijzen wij naar:

- Hoofdstuk 2. Conclusies en aanbevelingen;
- Hoofdstuk 3. Organisatie;
- Hoofdstuk 4. Mens;
- Hoofdstuk 5. Techniek;
- Hoofdstuk 6. Bijlagen.

In de bijlage (6.1) is een verklarende woordenlijst opgenomen met cybersecuritytermen om bijvoorbeeld rapporten, adviezen of offertes beter te begrijpen.

### Organisatie

Onderzoek naar de organisatie en het beleid op het gebied van informatiebeveiliging bestond uit interviews en documentanalyse. Centraal hierbij stond het 'Gemeentelijk Informatiebeveiligingsbeleid 2020-2023' (vigerend beleid ten tijde van het onderzoek). Het beleid geeft een hoog over beschrijving van informatiebeveiliging in het algemeen. Het is weinig voorschrijvend of richtinggevend voor de organisatie en medewerkers. Hierdoor sluit het minder goed aan bij de praktijk, iets wat naleving bemoeilijkt. Het informatiebeveiligingsbeleid en de praktijk zijn nog niet in lijn met de BIO-richtlijnen. In combinatie met het ontbreken van risicoanalyses heeft de gemeente de risico's en de benodigde maatregelen onvoldoende in beeld. Door een capaciteits- en continuïteitsuitdaging binnen het team kunnen de functionarissen zich minder richten op overstijgende/toekomstige risico's, controles of beleidsmatige thema's. Zij houden zich bezig met urgente vragen vanuit de praktijk en prioriteiten zoals wettelijke verplichtingen. Informatiebeveiliging lijkt binnen de gemeente daarmee vrij ad-hoc georganiseerd. Op verschillende onderdelen zijn aandachtspunten geconstateerd: zo mogen informatiebeveiligings- en privacyeisen bij inkooptrajecten en leveranciersmanagement sterker vertegenwoordigd worden. Het komt voor dat er tot een aanschaf of verwerking wordt overgegaan zonder beoordeling vanuit de CISO, FG of PO óf dat een advies vanuit de één van deze functionarissen niet wordt overgenomen bij besluitvorming. De gemeente beschikt over een incident management en responseplan, echter is deze verouderd en niet geïmplementeerd in de praktijk. Bij gebrek aan een responseteam worden incidenten via SSC DeSom en de CISO ad hoc en via informele lijnen opgepakt. Vanuit een gezamenlijke regeling is SSC DeSom de ICT dienstverlener voor zeven deelnemende gemeenten. Tijdens de interviews benoemen meerdere functionarissen deze samenwerking als risico, het gebrek aan eigen regie en consensus besluitvorming zijn punten van zorg binnen de organisatie. Wat betreft logisch toegangsbeleid is een deel ondergebracht in processen in de praktijk, echter is er geen eenduidigheid of beleid. De gemeente is voornemend om dit jaar een meer-jaren actieplan op te stellen met als doen de bewustwording bij de medewerkers op het vlak van informatiebeveiliging te verhogen. Nu beperkt zich dit tot kennisdeling via intranet.

### Mens (social engineering)

Met het versturen van een phishing mail is het bewustzijn van de medewerkers ten aanzien van het herkennen van een nep-e-mail getoetst. Bij de 727 verstuurde phishing e-mails hebben 63 gebruikers (9%) de unieke link in de e-mail geopend. In totaal zijn er 47 inlogpogingen van unieke gebruikers met geldige e-mailadressen geregistreerd (6%). Met een enkele geldige gebruikersnaam en wachtwoord kan een kwaadwillende verbinding maken met het draadloze netwerk en zo de multifactor authenticatie omzeilen.

De bovengenoemde percentages zijn relatief laag in vergelijking met andere gemeenten waar dit scenario is toegepast, maar laat zien dat een deel van medewerkers toch gevoelig is voor dergelijke aanvallen. Wij adviseren om medewerkers via een gedragsprogramma te 'leren' hoe zij phishing e-mails kunnen herkennen en ervoor te zorgen dat medewerkers weten hoe te handelen in geval van twijfel.

Op de servicepunten in Wognum (gemeente Medemblik) was het mogelijk om meerdere dagen als mystery guest (hierna genoemd: 'MG') de verschillende gebouwen te betreden. Door de afwezigheid van tourniquets en een openstaande deur konden de MG's onopgemerkt doorlopen. De MG's hebben zichzelf toegang kunnen verschaffen tot afgesloten ruimtes en afdelingen.

### Techniek (penetratietesten)

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

#### Externe penetratietest

De pentest bij de gemeenten Medemblik is blackbox onderzocht. Blackbox wil zeggen dat de onderzoeker niet over achtergrondinformatie beschikt, zoals een gebruikersaccount, relevante informatie, of informatie over de netwerk infrastructuur van beide gemeentes en Shared Service Center (SSC DeSom.) De onderzoeker is er extern in geslaagd om ongeautoriseerde toegang te verkrijgen tot de systemen van beide gemeentes en SSC DeSom.

Via (semi-)openbare bronnen zijn er e-mailadressen verzameld van de gemeente Medemblik, welke vervolgens zijn gebruikt voor password spraying aanvallen op de omgeving ADFS en Exchange. Met succes heeft de onderzoeker meerdere gebruikersaccounts bemachtigd. De wachtwoorden die voor deze accounts werden gebruikt waren zeer eenvoudig te raden (bijvoorbeeld: 'Lente2022!'). Doordat het ontbrak aan multifactor authenticatie (MFA) was het mogelijk om toegang te krijgen tot de webapplicatie 'blik.medemblik.nl'.

Op de Wie-is-wie website konden medewerkers van de gemeente Medemblik gevonden worden, waardoor nog meer e-mailadressen verzameld werden. Ook deze e-mailadressen zijn gebruikt voor password spraying aanvallen en op deze manier werden er nieuwe gebruikersaccounts bemachtigd. Ook konden er op dezelfde website documenten worden geraadpleegd, die op OneDrive stonden opgeslagen. Zo had de onderzoeker toegang tot:

- Asbest dossiers (Word document);
- Instructie thuiswerken (Handleiding);
- Werkinstructie alarm in en uitschakelen (Piket);
- Informatie inbraak installatie en toegangscontrole systeem (Piket).

Ook ontbrak het op een aantal algemene e-mailaccounts aan MFA. Hierdoor was de onderzoeker in staat zijn eigen telefoon te configureren voor Microsoft authenticatie meldingen. Op deze manier kon er ook toegang verkregen worden tot de 'Global adreslijst', een lijst waar alle e-mailadressen van de deelnemende partijen in staan. Tevens is er toegang verkregen tot de Citrix omgeving van een aantal balie werkplekken van de gemeente Medemblik, waardoor informatie van de burgers zichtbaar werd zoals:

- Rijbewijzen;
- Identiteitsbewijzen;
- Uittreksels van het basisregistratie personen.

Bij de e-mailaccounts van de balie werkplekken, maar ook bij andere accounts (Opmeer en SSC De-Som) zijn wachtwoorden aangetroffen in de mailbox. Niet alleen in de mailbox zijn wachtwoorden aangetroffen, maar ook in TopDesk (door in te loggen als behandelaar).

### Interne penetratietest

De onderzoeker is met de extern bemachtigde credentials intern ingelogd op de thin clients. Vanuit de gemeente Medemblik zijn er geen accounts verstrekt voor de pentest. De onderzoeker is er intern in geslaagd om ongeautoriseerd de volledige controle te verkrijgen tot de systemen van SSC DeSom en de deelnemende gemeenten waaronder Medemblik en Opmeer, maar ook indirect tot de Gemeente Stede Broec, Gemeente Enkhuizen, Gemeente Drechterland, Gemeente Koggenland en Werkzaam West-Friesland.

Door de laptop aan te sluiten op een netwerkkabel op beide locaties (gemeenten Medemblik en Opmeer) kreeg de onderzoeker via DHCP een IP-adres toegewezen. [redacted] was alles benaderbaar en werd er geen gebruik gemaakt van [redacted]
Middels een kwetsbaarhedenscan (Nessus) zijn er verouderde applicaties aangetroffen die kwetsbaarheden bevatten. Er is geprobeerd om enkele van deze kwetsbaarheden te exploiteren. Dit is echter door ingrijpen van de virusscanner niet gelukt.

Doordat de onderzoeker toegang had verkregen tot een aantal medewerker accounts kon er in Outlook, via de browser en op de netwerkshares gezocht worden naar wachtwoorden. Zowel in Outlook, de browser als op de netwerkschijven zijn een aantal wachtwoorden aangetroffen, waarvan een aantal serviceaccounts met hogere rechten. Met een serviceaccount, welke in de mailbox van een medewerker van SSC DeSom was gevonden, was het mogelijk om de volledige controle te krijgen over het netwerk. In theorie zou het bijvoorbeeld mogelijk kunnen zijn om de data te stelen en/of te gijzelen. Vergelijkbare situaties hebben zich in het verleden helaas voorgedaan bij de gemeente Hof van Twente (2020) en de gemeente Buren en Neder-Betuwe (2022).

Middels de verkregen beheerrechten zijn alle NTLM-hashes van de domaincontroller achterhaald. Dit zijn de versleutelde waardes van de wachtwoorden gebruikt in de Windows accounts. Met een wachtwoordkraker (Hashcat) zijn er hashes gekraakt. In totaal waren er 2469 hashes waarvan er 1339 zijn gekraakt (65,82%). Wat hierbij opvalt is dat er een hoop zwakke wachtwoorden worden gebruikt, bijvoorbeeld wachtwoorden zonder speciaal leesteken zoals 'Welkom01'.

Middels verkregen beheerrechten was ook het masterwachtwoord van de wachtwoordkluis van het technisch beheer verkregen. Dit wachtwoord stond namelijk in leesbare tekst in een word document In de wachtwoordkluis (KeePass) stonden ook de wachtwoorden van andere wachtwoordkluizen en de digitale infrastructuur (printer, servers, switches ect) van alle deelnemers van SSC DeSom.

Wat verder opviel is dat het mogelijk was om bepaalde programma's (cmd.exe en mstsc.exe) te draaien op de Citrix omgeving. Het is onwenselijk dat iedere medewerker deze programma's kan draaien, omdat kwaadwillenden hier mogelijk gebruik van kunnen maken om hun rechten hogerop te werken. Het downloaden en starten van eigen executables was niet mogelijk. Het was voor de onderzoeker mogelijk om via een Excel bestand een (authenticatie) aanval uit te voeren. Hierbij zijn negen serviceaccounts[1] bemachtigd maar waren niet te kraken (er is hierbij gebruik gemaakt van Hashcat).

[1] Een serviceaccount is een gebruikersaccount dat is gemaakt om een service of toepassing te isoleren.

# 1. Inleiding

In opdracht van de rekenkamer is een informatiebeveiligingsonderzoek (hierna genoemd: IB-onderzoek) uitgevoerd bij de gemeente Medemblik (hierna genoemd: 'de gemeente') met als focus het beveiligingsniveau van zowel organisatie, 'de mens' en techniek. Dit IB-onderzoek heeft plaatsgevonden in de periode januari t/m 4 mei 2022.

## 1.1 Doelstellingen en scope

De onderzoeksvragen zijn als volgt door de rekenkamer geformuleerd:

Hoofdvraag: 'Is de informatieveiligheid bij de gemeente Medemblik voldoende is gewaarborgd?'

Per deelgebied zijn de volgende deelvragen geformuleerd waar in paragraaf 2.1 antwoord op wordt gegeven:

1. Organisatie en proces
a. Welk beleid heeft de gemeente vastgesteld op het gebied van informatieveiligheid?
b. Welke risico's en maatregelen heeft de gemeente benoemd?
c. Welke informatievelden van het hele gemeentelijke taakveld bestrijkt de risico-inventarisatie wel en welke niet?
d. In hoeverre zijn de maatregelen geïmplementeerd en zijn daarvoor adequate middelen in de zin van geld en menskracht beschikbaar gesteld?
e. Evaluatie en actualisatie (zijn rollen en rechten geïmplementeerd?)

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. Hoe gaan medewerkers, uitvoeringsorganisaties en externe adviseurs in de praktijk om met het informatieveiligheidsbeleid als ze thuiswerken?

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. Voldoet de techniek aan de eisen die Rijk en beleid daaraan stellen?

De scope van het gehele IB-onderzoek betreft:

- afhankelijk van het ingezette middel alle medewerkers, dan wel een gericht aantal medewerkers van de gemeente Medemblik;
- de digitale en fysieke infrastructuur van de gemeente Medemblik.

## 1.2 Contactinformatie

| Naam | Functie | E-mail | Telefoon |
|---|---|---|---|
| Mathijs van der Pol | Security Consultant | [redacted] | |
| Esther Kraan | Consultant Riskmanagement | | |
| Mo Ballari | Sales Consultant | | |
| Maarten IJzermans | Director Riskmanagement | | |
| Jeroen van Oort | Ambtelijk-Secretaris | | |

## 1.3 Versies

| Versie | Datum | Status |
|---|---|---|
| 1.0 | 26-04-2022 | Conceptversie |
| 1.3 | 06-05-2022 | Conceptversie bijgewerkt techniek + opmerkingen rekenkamer |
| 2.0 | 21-0-2022 | Definitieve rapport aangepast n.a.v. wederhoor |

# 2. Conclusies

## 2.1 Conclusies

Het onderzoek dat Hoffmann in opdracht van de rekenkamer heeft uitgevoerd, had als doel de volgende hoofdvraag te beantwoorden: 'Is de informatieveiligheid bij de gemeente Medemblik voldoende gewaarborgd?' De onderzoekers hebben moeten constateren dat de informatieveiligheid bij de gemeente Opmeer onvoldoende is gewaarborgd. Op alle drie van de onderzoeksgebieden (organisatie, mens en techniek) zien de onderzoekers risico's en onvoldoende risicogerichte maatregelen. Hieronder volgen de conclusies voor ieder onderzocht onderdeel: organisatie, mens en techniek voor de gemeente Medemblik.

### 2.1.1 Organisatie en proces

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

Het 'Gemeentelijk Informatiebeveiligingsbeleid 2020-2023' vormt de basis voor informatiebeveiliging van de gemeente Medemblik. Daarnaast is er nog een 'Privacybeleid Raad Medemblik 2020'. Vaststelling evenals auteur en versie bij het informatiebeveiligingsbeleid zijn niet terug te vinden in het beleidsdocument zelf.

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

De gemeente heeft geen risicoanalyse uitgevoerd op het vlak van informatiebeveiliging. Een gestructureerde risicobeoordeling en het vervolgens implementeren van relevante maatregelen is daarom lastig. In de interviews kwamen een aantal risico's naar voren, waarbij de afhankelijkheid van SSC DeSom (en [redacted] vaak wordt genoemd. Het gebrek aan capaciteit en continuïteit in de informatiebeveiligingsorganisatie werd tevens als risico aangemerkt. Wat betreft de implementatie van de BIO is er een 'stip aan de horizon' gezet, maar nog geen start in de praktijk gemaakt.

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

De gemeente heeft geen risicoanalyses uitgevoerd op het vlak van informatiebeveiliging.

*d. 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 relevante risico's en kwetsbaarheden voor de gemeente, is het moeilijk in te schatten in hoeverre er risicogerichte maatregelen zijn benoemd en geïmplementeerd. Het is zodoende eveneens moeilijk om de aanwezige maatregelen te categoriseren en op waarde te schatten.

De organisatie voldoet niet aan de richtlijnen van de BIO, implementatie zal een eerste stap betekenen naar het nemen van relevante maatregelen. Het gebrek aan capaciteit en continuïteit van de informatiebeveiligingsorganisatie is de hoofdreden waardoor informatiebeveiliging onvoldoende zichtbaar is

binnen de gemeente. Dit is een belangrijk punt van aandacht. Wat betreft SSC DeSom werkt de consensus besluitvorming vertragend en soms belemmerend bij het doorvoeren van maatregelen. Het budget en de belangen van de deelnemende gemeenten loopt uiteen.

*e. Evaluatie en actualisatie; zijn rollen en rechten geïmplementeerd?*

In praktijk is er deels sprake van een logisch toegangsbeleid (in-dienst proces). Ten tijde van het onderzoek was er een interne audit gaande om te kijken hoe de werking van dit proces in praktijk is. De onderzoekers hebben de resultaten hiervan niet ontvangen om deze te kunnen beoordelen. Wat betreft uit-dienst en wijzigingen betreft is er geen eenduidigheid. In de interviews komt naar voren dat er onvoldoende vastlegging plaats vindt tussen de betrokken afdelingen waardoor het onduidelijk is wie welke rechten heeft. Er vindt geen periodieke controle uit op rechten en verantwoordelijkheden. Onderzoekers hebben geen beleidsstukken ontvangen aangaande logisch toegangsbeleid.

### 2.1.2 Mens (social engineering)

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

De gemeente maakt gebruik van intranet (intern) voor wat betreft informatie en kennisdeling rondom informatieveiligheid richting medewerkers. Uitvoeringsorganisaties worden gedurende de looptijd van het contract niet periodiek gecontroleerd op de gemaakte afspraken aangaande informatieveiligheid. De gemeente is voornemend om dit jaar een meerjaren actieplan op te stellen met als doen de bewustwording bij de medewerkers op het vlak van informatiebeveiliging te verhogen.

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

Het huidige informatiebeveiligingsbeleid sluit onvoldoende aan bij de praktijk van de gemeente. Het beleid is weinig tactisch/operationeel voorschrijvend voor de organisatie en medewerkers. Er worden geen procedures, protocollen, maatregelen of verwachtingen voor de praktijk beschreven of daarnaar verwezen. Het maakt het daarmee lastig voor de organisatie om bij onduidelijkheid terug te vallen op het beleid of in beginsel zich hier aan te houden.

*c. Hoe gaan medewerkers, uitvoeringsorganisaties en externe adviseurs in de praktijk om met het informatieveiligheidsbeleid als ze thuiswerken?*

Zoals hierboven omschreven geeft het huidige informatiebeveiligingsbeleid weinig sturing voor omgang in de praktijk. Er is tevens geen specifiek thuiswerkbeleid of protocol aanwezig.

### 2.1.3 Techniek

Tijdens het onderzoek zijn meerdere kritieke kwetsbaarheden geconstateerd die onmiddellijk met het Shared Service Center, SSC DeSom, zijn gedeeld. Vanwege de diepgang en vertrouwelijkheid zijn de technische uitkomsten en aanbevelingen van de pentesten gedeeld met de ambtelijke organisatie.

De detailbevindingen en specifieke aanbevolen maatregelen van de penetratietesten zijn beschreven in het document: 22112073 – Rekenkamercommissie_Medemblik&Opmeer_*techniek.pdf'.*
Dit document is geheim verklaard, door de zeer gevoelige inhoud en de waarde van dit document voor kwaadwillenden, die het als handleiding kunnen gebruiken.

*a. Is data bij de gemeente voldoende beschermd tegen toegang door onbevoegde medewerkers, uitvoeringsorganisaties en externe adviseurs?*
Nee, de data bij de gemeente is niet voldoende beschermd. Het is de onderzoeker gelukt om de volledige controle te krijgen over het netwerk van de gemeente Medemblik, Opmeer en SSC DeSom.

*b. Is data bij de gemeente voldoende beschermd tegen toegang door onbevoegde externen?*
Nee, het was mogelijk om met het wachtwoord 'Welkom01' extern toegang te krijgen tot het netwerk van de gemeente Medemblik en SSC DeSom.

*c. Wat zijn, als vraag 3a of 3b met 'nee' beantwoord wordt, daarvan de gevolgen voor betrokkenderden?*
Persoonlijke en gevoelige informatie van de gemeente Medemblik en deelnemende gemeentes (via SSC DeSom) kan gestolen worden door een kwaadwillende. Denk hierbij bijvoorbeeld aan de situatie dat een ransomware groepering de data gijzelt. Dit specifieke scenario heeft zich al eerder voorgedaan bij de gemeente Hof van Twente (2020) en de gemeente Buren en Neder-Betuwe (2022).

*d. Wat zijn de technische risico's en kwetsbaarheden?*
Tijdens het onderzoek zijn meerdere kritieke kwetsbaarheden geconstateerd die onmiddellijk met het Shared Service Center zijn gedeeld. Vanwege de diepgang en vertrouwelijkheid zijn de technische uitkomsten en aanbevelingen van de pentesten gedeeld met de ambtelijke organisatie.

*e. Voldoet de techniek aan de eisen die Rijk en beleid daaraan stellen?*
Nee, de techniek voldoet niet aan alle eisen die in de Baseline informatiebeveiliging Overheid (BIO) staan [2]. Zo voldoen niet alle wachtwoorden aan de wachtwoordlengte van minimaal 8 posities en complexiteit qua samenstelling. Ook zijn er accounts die niet beschikken over multifactor authenticatie. Hierdoor kan een kwaadwillende vanuit een ongeauthenticeerde zone, toegang worden verleend naar de vertrouwde zone.

[2] https://www.bio-overheid.nl/media/1572/bio-versie-104zv_def.pdf

# 3. Organisatie

Voor het onderzoek naar de organisatie van informatiebeveiliging is een analyse uitgevoerd op de door de gemeente Medemblik beschikbaar gestelde documentatie, rapporten en verklaringen en daarnaast door het uitvoeren van verschillende interviews 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. In bijlage 6.2 is een opgave van de geïnterviewden opgenomen, evenals een overzicht van de documenten die zijn meegenomen in de beoordeling.

## 3.1 Bevindingen en aanbevelingen

| Paragraaf | Bevinding | Impact | Aanbeveling |
|---|---|---|---|
| 3.1.1 | Vaststelling, auteur en versie van het IB-beleid zijn niet terug te vinden in het beleidsdocument zelf. | Voor de lezer is het onduidelijk wat de status van het document is en of dit door de organisatie is vastgesteld. | Het is raadzaam om de vaststelling van een beleid door het College en de directieraad in het document zelf op te nemen. Zo is voor de lezer duidelijk wat de status van het document is. |
| 3.1.1 | Het IB-beleid sluit niet (voldoende) aan bij de praktijk van de organisatie. Er worden strategische uitgangspunten en ambities uiteengezet, echter mist het kaders en richtlijnen voor de actuele praktijk. | Omdat het beleid onvoldoende voorschrijft wat het verwacht van de organisatie, blijft de opvolging en naleving van het beleid in de praktijk uit. | Een IB-beleid werkt het best als het aansluit bij de actuele praktijk, cultuur en uitgangspunten van de organisatie. Aangepast/nieuw beleid mag meer aansluiten op het normenkader van de BIO en de praktische opvolging hiervan. |
| 3.1.1 | In het IB-beleid wordt geen frequentie en proces beschreven hoe en wanneer het IB-beleid geactualiseerd wordt. | Het beleid veroudert waardoor het mogelijk niet meer aansluit bij huidige risico's. | Het is raadzaam om het beleid periodiek (jaarlijks) te evalueren en waar nodig te actualiseren. |
| 3.1.1 | Informatiebeveiligingsbeleid is nog niet in lijn met BIO. Er is een 'stip op de horizon' gezet wat betreft implementatie. | Gemeente voldoet niet aan BIO en loopt mogelijk risico's door het gebrek aan beleid en maatregelen conform BIO. | De organisatie zal zo snel mogelijk stappen moeten zetten naar een implementatie van de BIO en een nieuw, op de BIO gebaseerd, informatiebeveiligingsbeleid. |

| | | | |
|---|---|---|---|
| 3.1.1 | Er is geen werking van het ISMS geconstateerd bij de gemeente Medemblik, waarmee er structureel een PDCA aanpak op informatiebeveiliging (IB) wordt geborgd. | Door het missen van een ISMS, ontstaat het risico dat IB op ad-hoc basis wordt georganiseerd en dat (nieuwe) dreigingen en risico's onvoldoende adequaat worden (h)erkent en beheerst | Een ISMS dient aan te sluiten op het beleid en de strategie van de organisatie en dient geïntegreerd te worden in de bestaande processen. Het doel van een ISMS is (vertrouwelijke) informatie beter te beveiligen. |
| 3.1.2 / 3.1.8 | Op het vlak van informatiebeveiliging en privacy is er weinig (personele) capaciteit en continuïteit aanwezig. Functionarissen hebben dubbelrollen, weinig beschikbare uren of zijn extern ingehuurd. | Risico: onvoldoende waarborging kennis, weinig/geen achtervang en focus op ad-hoc zaken in plaats van beleid, verbetering of overkoepelende risico's. | Meer uren per gemeente, verdeeld over meer functionarissen. |
| 3.1.2 | Te weinig afbakening tussen strategisch, tactisch en praktisch niveau. Medewerkers op strategische functies acteren op operationeel niveau en andersom vanwege het capaciteitsprobleem. | Te veel focus op ad-hoc zaken en wettelijke verplichtingen, te weinig aandacht voor strategische thema's en uitwerken van een visie op structurele verbeteringen en vernieuwingen, en mogelijke demotivatie van verantwoordelijke medewerkers. | Heldere verdeling en afbakening van taken en verantwoordelijkheden op strategisch, tactisch en operationeel niveau en een formele vastlegging hiervan. |
| 3.1.2 | Voor bepaalde functies geldt dat taken en verantwoordelijkheden niet helder zijn afgebakend of dat er geen officiële benoeming is. | Wanneer taken en verantwoordelijkheden niet helder zijn afgebakend, kan het voorkomen dat medewerkers elkaar overlappen in verantwoordelijkheden of dat zaken juist niet worden opgepakt, omdat niemand verantwoordelijk is. | Taken en verantwoordelijkheden (m.b.t. informatiebeveiliging en privacy) duidelijk beleggen en mandateren. |
| 3.1.4 | Onvoldoende inzicht in en sturing op risico's en (toekomstige) dreigingen. Risicoanalyses worden niet uitgevoerd. | Het niet tijdig in kunnen spelen op (toekomstige) dreigingen maakt de organisatie kwetsbaar. | Implementatie van risicomanagement en uitvoeren van dreigingsanalyses en deze periodiek actualiseren. |

| | | | |
|---|---|---|---|
| 3.1.5 | Bij de aanschaf van (IT) producten en diensten worden CISO en de privacyorganisatie niet, of (te) laat betrokken, waardoor eisen m.b.t. informatiebeveiliging niet voldoende worden gewaarborgd. | Er worden producten en diensten aangeschaft of ontwikkeld en in gebruik genomen die niet voldoen aan het IB-beleid en de gestelde beveiligingseisen. | Bij elke aanschaf moet worden voldaan aan de eisen m.b.t. informatiebeveiliging[3].<br>De eisen dienen voor het sectorhoofd/de inkoper helder en vindbaar te zijn. Werkprocessen moeten ervoor zorgen dat de CISO/privacyorganisatie worden betrokken. |
| 3.1.5 | 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 die het levert voldoen niet aan het IB-beleid en de gestelde beveiligingseisen. | Periodiek (minimaal jaarlijks) dient er een controle uitgevoerd te worden op de naleving van eisen m.b.t. informatiebeveiliging[4]. |
| 3.1.6 | Het incidentmanagement en responseplan van de gemeente is verouderd en vindt geen werking in de praktijk. Er is geen responseteam aangewezen, calamiteiten worden ad hoc en via informele lijnen opgepakt. | Tijdens een calamiteit worden niet de juiste medewerkers geïnformeerd en/of is er niet voldoende mandaat om beslissingen te nemen. | Stel up to date en complete informatiebeveiligingscontinuïteit plannen op te welke aansluiten bij huidige de praktijk. Stel een responseteam samen. Plan een periodieke oefening (inclusief evaluatie) om te waarborgen dat het plan in praktijk functioneert. |
| 3.1.7 | Afhankelijkheid en consensus besluitvorming binnen SSC DeSom werkt vertragend en soms belemmerend. | Het nemen van maatregelen of het doorvoeren van verbeteringen of innovatie vindt niet altijd doorgang of laat lang op zich wachten. Hierdoor loopt de Gemeente mogelijk risico's. | Voer een risicoanalyse uit om in kaart te brengen welke risico's er beheerst worden door SSC DeSom en welke niet. Op deze manier kan een risicobeoordeling plaatsvinden en gekozen worden voor de juiste maatregelen. |
| 3.1.8 | De Gemeente voert weinig tot geen 'DPIA's uit. | Verwerkingen die worden gestart zonder dat er een DPIA is opgesteld, zijn mogelijk onrechtmatig en voldoen niet aan eisen m.b.t. informatiebeveiliging en privacy. | Maak een inhaalslag met DPIA's en monitoren van reeds gestarte verwerkingen. Tijdig opstellen van DPIA's in processen formaliseren. |

[3] Zie hiervoor BIO "Leveranciersrelaties". Hoofdstuk 15.1
[4] Zie hiervoor BIO "Beheer van dienstverlening van leveranciers". Hoofdstuk 15.2

| | | | |
|---|---|---|---|
| 3.1.8 | Er is geen duidelijk classificatie proces, waarbij het op documenten van de gemeente niet helder is welke vertrouwelijkheid het document heeft. | Het risico hiervan is dat vertrouwelijke documenten die beschikbaar zijn bij medewerkers, niet als zodanig worden (h)erkent en ze mogelijk onbedoeld en onrechtmatig worden gedeeld. | Voer een helder beleid op gebied van classificatie van documenten in en zorg dat zichtbaar wordt op de documenten welke rubricering van toepassing is. |
| 3.1.9 | In praktijk is er deels sprake van een logisch toegangsbeleid (in-dienst proces). Verder is er geen eenduidigheid en ontbreekt beleid en controle. | De toekenning van rechten bij de juiste rollen en verantwoordelijkheden (in-dienst/uit-dienst en wijzigingen) is niet beschreven en wordt niet gecontroleerd. | Beleid formaliseren, procedures inrichten en rollen<br>En verantwoordelijkheden uitwerken en vastleggen.<br>Er dient periodiek controle uitgevoerd te worden op de naleving. |

## 3.2 Overzicht van de bevindingen

### 3.2.1 Beleid

Het 'Gemeentelijk Informatiebeveiligingsbeleid 2020-2023' vormt de basis voor informatiebeveiliging van de Gemeente Medemblik. Het geeft een omschrijving van informatiebeveiliging in het algemeen, bespreekt een aantal thema's en de ambities daarbij. Het geeft een hoog over en vrij beknopt beeld van een grotendeels 'soll' situatie aangaande informatiebeveiliging. Door de algemeenheid van het stuk sluit het minder goed aan bij de 'ist' situatie van de Gemeente. Het beleid is tevens weinig tactisch/operationeel voorschrijvend voor de organisatie en medewerkers. Er worden geen procedures, protocollen, maatregelen of verwachtingen voor de praktijk beschreven of daarnaar verwezen. Het maakt het daarmee lastig voor de organisatie om bij onduidelijkheid terug te vallen op het beleid of in beginsel zich hier aan te houden. Onderdelen als een clean desk beleid, beleid over gebruik van hardware, thuiswerken en dataclassificatie ontbreken.

Er wordt in het beleid verwezen naar de implementatie van de BIO (Baseline Informatieveiligheid Overheid). Er worden verder nog geen stappen of maatregelen omschreven voortkomende uit de BIO. Uit de interviews komt naar voren dat risicogerichte maatregelen op basis van de BIO-richtlijnen tevens in de praktijk (grotendeels) ontbreken.

In het huidige beleid wordt verwezen naar een ISMS (Information Security Management System) en PDCA cyclus. Vanuit de interviews blijkt dat er geen sprake is van werking in de praktijk, dit blijkt tevens vanuit het ontbreken van bijvoorbeeld versiebeheer van het informatiebeveiligingsbeleid zelf. Het beleid beschrijft tevens geen frequentie waarmee het beleid wordt geëvalueerd. Het is conform BIO vereist om

het beleid periodiek (voorkeur jaarlijks) te evalueren en waar nodig te actualiseren[5]. De Gemeente beschikt over een ISMS-tool (Cyber Manager), echter wordt hier nog niet actief mee gewerkt. Ten tijde van het onderzoek werd het systeem in gebruik genomen om actiepunten ten aanzien van informatiebeveiliging in op te nemen ('stip aan de horizon t.a.v. implementatie BIO). Vanwege capaciteitsproblemen is het echter nog niet mogelijk om deze taken te beleggen. Een goed werkend ISMS zal de gemeente helpen bij het opzetten en onderhouden van de informatiebeveiliging, het advies is dan ook om deze in de praktijk in gebruik te nemen.

### 3.2.2 Informatiebeveiligingsorganisatie

De informatiebeveiligingsorganisatie bestaat uit de CISO, twee privacy officers (PO's) en een functionaris gegevensbescherming (FG). De vacature voor het afdelingshoofd Informatiebeveiligingsbeheer is vacant. De CISO valt binnen het team Informatiemanagement. De FG valt onder Advies en Dienstverlening binnen de gemeente Medemblik. Voorheen was er sprake van privacy medeweker(s) (benoemd in privacy beleid), maar deze positie(s) zijn niet ingevuld op dit moment. De FG treed toezichthoudend op en werkt in de praktijk veel samen met de PO's. De CISO treed meer solistisch op en heeft minder contact met de FG en PO's. Idealiter zouden de CISO en de FG meer moeten samenwerken op overkoepelende thema's en zichtbaarheid van informatiebeveiliging in het algemeen.

De verschillende functionarissen zijn verantwoordelijk voor meerdere gemeenten. Zo verdeelt de CISO de tijd en aandacht over drie gemeenten (Opmeer, Medemblik, Koggenland) en is de FG tevens in dienst bij de gemeente Koggenland en SSC DeSom. De PO's hebben een dubbelrol en zijn niet officieel in deze functie benoemd. Continuïteit en capaciteit zijn zodoende een uitdaging voor het team. De CISO houdt zich in de beschikbare tijd (16 uur) bezig met strategische thema's, de ENSIA verantwoording en ad-hoc vraagstukken. Door het verdere tijdsgebrek is informatiebeveiliging als thema weinig zichtbaar in de organisatie. Doordat de functies binnen de informatiebeveiligingsorganisatie vaak gegroeid zijn vanuit dubbelrollen mist het soms aan ervaring en focus. Hierbij speelt eveneens mee dat de PO's en de CISO niet officieel benoemd zijn (CISO is officieel Adviseur Informatiebeveiliging). Het is hierdoor in de praktijk niet altijd duidelijk waar welke verantwoordelijkheden liggen en wie welk mandaat heeft. Wij raden de organisatie aan hier duidelijkheid in te scheppen door verantwoordelijkheden te beleggen en rollen en functies te formaliseren.

### 3.2.3 Verantwoording

Jaarlijks legt de Gemeente verantwoording af op het vlak van informatieveiligheid door het uitvoeren van de ENSIA audit. Binnen de Gemeente Medemblik is de CISO belegd met deze taak. Het college is op de hoogte gebracht van de status en bijbehorende risico's aangaande de uitkomsten van de verschillende onderdelen van de ENSIA. Naast de ENSIA audit is er geen sprake van andere vaste periodieke rapportages op het vlak van informatieveiligheid.

[5] Zie BIO; Informatiebeveiligingsbeleid 5.1.2.

### 3.2.4 Risicoanalyse

In het informatiebeveiligingsbeleid wordt verwezen naar de BIO en de daarin beschreven risicogerichte benadering van informatieveiligheid. Er wordt omschreven wat het belang is risico- en GAP-analyses. In de praktijk vinden er echter geen risico- of GAP-analyses plaats. De processen zijn niet duidelijk in kaart gebracht waardoor er onvoldoende zicht is op mogelijke risico's en gevolgen voor de organisatie. Omdat er niet aan risicobeoordeling gedaan wordt, heeft de gemeente Medemblik onvoldoende zicht op risico's, en de reeds genomen en nog nodige beheersmaatregelen. Het advies luidt dan ook om een risicoanalyse op het gebied van informatiebeveiliging uit te voeren en deze jaarlijks te evalueren.

### 3.2.5 Inkoop- en leveranciersmanagement

Idealiter worden eisen m.b.t. informatiebeveiliging en privacy aan producten, diensten en leveranciers gesteld in de selectiefase vóór de aanschaf. Deze eisen zijn opgesteld op basis van het beleid en geïdentificeerde risico's van het product en worden adequaat getoetst, zodat men enige zekerheid heeft dat de aan te schaffen diensten en producten en de leverancier die deze levert voldoet aan de eisen die de gemeente stelt.

De gemeente Medemblik hanteert de 'handreiking inkoopvoorwaarden' van de IBD als eisen voor leveranciers. Specifieke eisen met betrekking tot informatiebeveiliging en privacy worden door CISO (mits deze beschikbaar is i.v.m. beperkte capaciteit) en PO's of FG (ad hoc) geformuleerd wanneer zij betrokken worden bij inkooptrajecten en leveranciersselecties. Het inkoopproces wordt in de praktijk echter niet altijd gevolgd, vooral wanneer het gaat om investeringen onder €10.000,-. Het gevolg is dat de informatiebeveiligingsorganisatie niet, of soms te laat in het proces betrokken worden. Het komt ook voor dat functionarissen wel worden betrokken bij het proces, echter dat de gegeven adviezen niet worden meegenomen in de uiteindelijke besluitvorming. Het risico wat de gemeente hier loopt is dat informatiebeveiligings- en privacy eisen niet (volledig) worden meegenomen bij de aanschaf van diensten en producten, waardoor deze in gebruik worden genomen zonder aan de eisen te voldoen.

Er vindt geen tussentijdse controle of beoordeling plaats op lopende contracten of bestaande leveranciers. Het is onduidelijk wie hiervoor verantwoordelijk zou moeten zijn binnen de gemeente. Wij raden de organisatie aan hier duidelijkheid te scheppen door de verantwoordelijkheid te beleggen en te formaliseren.

### 3.2.6 Incidentmanagement

De gemeente beschikt over een incident management plan (Incident management en responseplan Gemeente Medemblik). Dit beleidsdocument dateert uit 2016 en is in de tussentijd niet herzien of geëvalueerd. Uit de interviews blijkt dat het plan geen werking heeft in de praktijk. Afhankelijk van het incident wordt dit gemeld bij SSC DeSom en/of de CISO, waarna er ad hoc wordt geacteerd op de situatie. Betrekken van andere functionarissen gebeurt via de informele lijnen, er is geen vast responsteam. Bij gebrek aan responsteam vindt tevens de training hiervan (zoals benoemd in het incident management en responseplan) in de praktijk niet plaats.

Het advies is om up to date en complete informatiebeveiligingscontinuïteit plannen op te stellen welke aansluiten bij de praktijk. Deze plannen dienen de crisis- en incidentmanagement teams met hun taken en bevoegdheden te omschrijven, inclusief duidelijke crisis scenario's met bijbehorende actieplannen. Het is van belang dat deze plannen periodiek (jaarlijks) worden geëvalueerd. Om tot een optimale situatie te komen, dienen deze plannen en het managen van een crisis ook periodiek te worden getraind.

### 3.2.7 ICT organisatie

De gemeente Medemblik is aangesloten bij SSC DeSom, een ICT dienstverlener voor 7 deelnemende gemeenten. De deelname aan DeSom en de gevolgen daarvan worden door de gesproken functionarissen genoemd als een mogelijk risico voor de gemeente Medemblik. Dit komt door meerdere punten. Zo zijn er zorgen over het gebrek aan technische maatregelen ten behoeve van informatiebeveiliging, [redacted] Dit levert een groot risico op wanneer bijvoorbeeld één van de deelnemende organisaties wordt geraakt door een aanval van buitenaf, zoals ransomware. Dit wordt eveneens door de gesproken functionarissen als groot risico gezien. Daarnaast werkt vereiste consensus besluitvorming tussen meerdere gemeenten werkt vertragend of zelfs belemmerend. De verschillende budgetten, invalshoeken en belangen bemoeilijkt het nemen van bepaalde stappen in het kader van verbetering of innovatie.

Tijdens de interviews kwam tevens naar voren dat DeSom, als belangrijkste ICT dienstverlener, zelf niet ISO 27002[6] gecertificeerd is. Daarbij is het voor de gemeente lastig om inzage te krijgen in auditresultaten, genomen informatiebeveiligingsmaatregelen of uitkomsten van bijvoorbeeld kwetsbaarhedenscans. Omdat DeSom zelf geen onderdeel uitmaakt van dit onderzoek is hier verder geen documentatie van ontvangen door de onderzoekers. Het is voor de onderzoekers zodoende moeilijk in te schatten waar de regie ligt met betrekking tot het functioneren van SSC DeSom. Echter gezien de invloed op eventuele risico's voor de gemeente aangaande informatieveiligheid is dit een serieus punt van aandacht. Wij raden de organisatie aan om, samen met SSC DeSom, een risicoanalyse uit te voeren om in kaart te brengen welke risico's er worden beheerst door SSC DeSom en welke niet. Op deze manier kan men een goede risicobeoordeling maken en eventueel extra maatregelen nemen.

### 3.2.8 Privacy

Het ontvangen 'Privacybeleid Raad Medemblik 2020' staan strategische kaders beschreven voor de Raad voor het verwerken van privacygevoelige informatie, oftewel persoonsgegevens, de bescherming van deze gegevens en de omgang met deze gegevens. Dit zou nog uitgebreid mogen worden met werkinstructies en protocollen voor de praktijk.

De privacyorganisatie van de Gemeente Medemblik bestaat uit de FG en twee PO's. De FG heeft 12 beschikbare uren voor de gemeente Medemblik en is tevens werkzaam voor de gemeente Koggenland

[6] De ISO 27002 is een Code voor Informatiebeveiliging. Deze geeft richtlijnen en normen voor het opstellen, implementeren, onderhouden en het verbeteren van informatiebeveiliging binnen een organisatie. De ISO 27002 dient vaak als een praktische richtlijn voor het ontwerpen van veiligheidsstandaarden binnen een organisatie.

en SSC DeSom. De twee PO's hebben een dubbelrol en zijn niet officieel benoemd in de rol van Privacy Officer. Zij hebben een wisselend aantal uren beschikbaar, één keer acht uur en bij de tweede PO is het aantal beschikbare uren afhankelijk van wat overblijft naast de functie van Secretaris Bezwarencommissie. Daarnaast is er geen opleidingsbudget voor deze twee functionarissen.

In het beleid wordt beschreven dat er één tot twee privacy medewerkers (PM'ers) zijn om privacy structureel te borgen. Op dit moment is dit in praktijk niet als zodanig ingeregeld. Al met al zijn capaciteit en continuïteit zijn een uitdaging voor het team. Praktisch heeft dat zijn weerslag, zo zijn de jaarrapportage 2021 en het jaarplan 2022 nog niet beschikbaar. De focus ligt voornamelijk op ad-hoc zaken in plaats van overstijgende thema's of beleid. Daarnaast worden er, mede door tijdgebrek weinig tot geen DPIA's uitgevoerd op eigen initiatief van de privacyorganisatie (in 2018 was er nog een functionaris fulltime aangesteld voor het uitvoeren van DPIA's). Doordat er weinig advies-uitvragen gedaan worden en de privacyorganisatie vaak te laat of zelfs niet betrokken worden bij nieuwe of wijzigingen in verwerkingen komen hier ook weinig DPIA's uit voort. Het komt voor dat er verwerkingen worden gestart zonder dat er een toetsing plaatsvind vanuit de privacyorganisatie (en CISO). Duidelijke werkinstructies/protocollen, meer capaciteit binnen het team en budget voor bewustwording zouden de betrokkenheid van de privacyorganisatie in de praktijk kunnen waarborgen.

### 3.2.9 Logisch toegangsbeleid

In de praktijk wordt er een in-dienstprocedure gevolgd die via verschillende afdelingen loopt. Op netwerkgebied gaat het toekennen van rechten via SSC DeSom. Voor de toegang tot overige applicaties geeft het afdelingshoofd en P&O een opdracht naar de functioneel applicatiebeheerder welke bepaald welke rechten van toepassing zijn. In afstemming met het afdelingshoofd worden de autorisaties door de functioneel applicatiebeheerder gegeven. Ten tijde van het onderzoek was er een interne audit gaande om te kijken hoe de werking van dit proces in praktijk is. De onderzoekers hebben de resultaten hiervan niet ontvangen om deze te kunnen beoordelen. Wat betreft uit-dienst en wijzigingen betreft is er geen eenduidigheid. In de interviews komt naar voren dat er onvoldoende vastlegging plaats vindt tussen SSC DeSom, P&O en de afdelingshoofden waardoor het onduidelijk is wie welke rechten heeft. Er vindt geen periodieke controle uit op rechten en verantwoordelijkheden. Onderzoekers hebben geen beleidsstukken ontvangen aangaande logisch toegangsbeleid. Het advies luidt om beleid op te stellen, procedures in te richten en rollen en verantwoordelijkheden uit te werken en vast te leggen. Een periodieke controle zal helpen de procedures in de praktijk te bestendigen.

### 3.2.10 Bewustwording medewerkers

De Gemeente Medemblik beschikt niet over een tool of platform ten behoeve van de bewustwording van medewerkers aangaande (informatie)veiligheid. In samenwerking met SSC DeSom is er in het verleden een mail-phishing test uitgevoerd om te kijken hoe medewerkers hierop reageerden. Momenteel wordt er voornamelijk gebruik gemaakt van intranet om medewerkers te informeren en kennis te delen. De gemeente is voornemend om dit jaar een meerjaren actieplan op te stellen met als doen de bewustwording bij de medewerkers op het vlak van informatiebeveiliging te verhogen.

# 4. Mens

In dit hoofdstuk worden de bevindingen in detail beschreven en zijn schermafdrukken opgenomen ter illustratie.

Het bewustzijn van de medewerkers is getest door middel van de volgende manieren:

1. Mail-phishing, 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 heeft een medewerker van Hoffmann heeft geprobeerd om zonder toestemming toegang te krijgen tot de gemeentelijke werkplekken.

## 4.1 Mail-phishing aanval

De onderzoekers waren in eerste instantie niet in staat om met de phishing-mail direct door de beveiliging (spamfilter) van de gemeente te komen. De gemeente heeft hierop de beveiliging specifiek en alleen voor deze actie aangepast (via SSC DeSom) zodat de phishing test uitgevoerd kon worden.

Onze onderzoekers hebben zelf een lijst met e-mailadressen samengesteld. Het aantal e-mailadressen was 727. Naar deze e-mailadressen is op maandag 2 mei 2022 vanaf 10:34 uur tot ongeveer 11:03 een phishing e-mail verstuurd. De onderzoeker heeft het domein ‘SSC DeSom.com’ geregistreerd. Via dit domein zijn vanaf het e-mailadres ‘servicedesk@sscdesom.com’ de e-mails verstuurd. De e-mail had de volgende inhoud:

do 14-4-2022 16:43

IT Servicedesk <servicedesk@sscdesom.com>

Autorisatie netwerkapparatuur vereist

Aan Mathijs van der Pol

Opvolgen. Voltooid op vrijdag 29 april 2022.

Beste collega,

Om ons draadloze netwerk te beschermen tegen ongeautoriseerde apparaten dienen alle apparaten waarop je draadloos Wi-Fi gebruikt eenmalig geregistreerd te worden. Door in te loggen met je laptop, smartphone of iPad wordt je account toegevoegd aan de database van geautoriseerde systemen.

**Hoe koppel ik mijn apparaat?**
Om toegang tot het draadloos Wi-Fi netwerk te behouden klik je op de onderstaande link naar het Wi-Fi portaal van de Gemeente Medemblik en log je in om het apparaat te registreren.

https://medemblik.sscdesom.com

**Waarom?**
Een niet veilig Wi-Fi bedrijfsnetwerk kan tot gevolg hebben dat anderen toegang krijgen tot het gemeentenetwerk. De Gemeente Medemblik loopt dan het risico dat de bedrijfsinformatie en persoonsgegevens in handen van anderen kunnen komen.

**Let op, actie vereist!**
Indien je geen actie onderneemt, zal de toegang tot het draadloos netwerk verlopen binnen enkele dagen.

Met vriendelijke groet,

ICT Servicedesk

DeSom

Shared Service Centrum West-Friesland

DATA PRO CERTIFIED

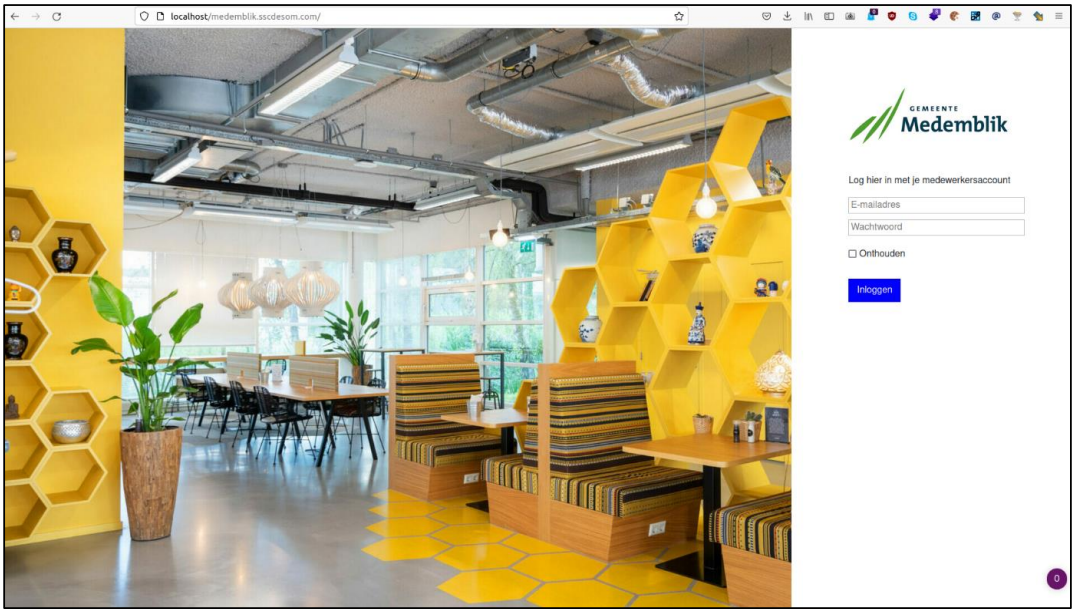
0229-856666

www.sscdesom.nl

Correspondentie: SSC DeSom, Postbus 45, 1687 ZG Wognum

Bezoek: Dick Ketlaan 1, 1687 CD Wognu

Figuur 1: Phishing e-mail 'medemblik.SSC DeSom.com', met als onderwerp 'Autorisatie netwerkapparatuur vereist'.




Figuur 2: Phishing website gemeente 'medemblik.SSC DeSom.com'.

Doordat de link naar de website een uniek ID bevat, kon worden geregistreerd hoeveel unieke gebruikers de website bezochten en/of hun gebruikersnaam en wachtwoord invulden. De wachtwoorden van gebruikers zijn niet geregistreerd tijdens de mail phishing.

Er zijn in totaal 63 unieke bezoekers geregistreerd (9%) waarvan 47 gebruikers (6%) hun gebruikersnaam en wachtwoord hebben ingevuld. Het wachtwoord is niet opgeslagen, ook zijn de credentials niet getest op geldigheid. De mail-phishing campagne is gestopt op woensdag 4 mei 2022 omstreeks 18:00.

### Aanbevelingen

- Maak medewerkers bewust van mail-phishing-technieken door bewustwording en gedragsveranderingsprogramma's;
- Zorg ervoor dat medewerkers weten welke domeinnamen van de gemeente zijn en dat ze geen gebruik moeten maken van andere domeinen.

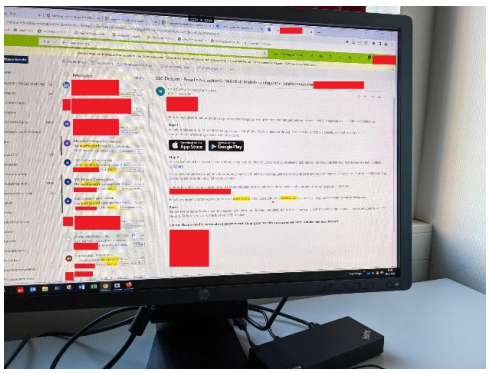
## 4.2 Mystery guest bezoek

Op woensdag 23 maart 2022 omstreeks 13:45 heeft Mystery Guest 3 (hierna genoemd: 'MG3') het pand betreden voor een verkenning. Langs de Servicedesk gaat MG3 via het trappenhuis naar de bovenste etage. Op de deuren is een paslezer aanwezig en de deuren kunnen niet open gemaakt worden.

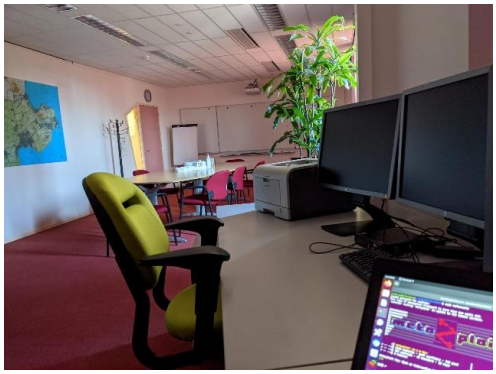
Rond 13:50 loopt MG3 langs de griffie voorbij de postvakken. Om vervolgens zich op te houden in een vergaderzaal en daar gebruik te maken van de thin clients (met de extern bemachtigde credentials) en de netwerkkabel. De detailbevindingen van de penetratietesten zijn vanwege de gevoeligheid beschreven in het document: *'22112073 – Rekenkamercommissie_Medemblik&Opmeer_techniek.pdf'*.

Rond 16:05 verlaat MG3 het pand via de lobby.

Figuur 3: Postvakken.



Figuur 4: Ingelogd op thinclient als medewerker. Wachtwoord extern buitgemaakt.



Figuur 5: Werkplek MG3.

Op vrijdag 25 maart 2022 omstreeks 12:33 heeft MG3 het pand betreden. Hij loopt rechtstreeks door naar de vergaderzaal op de begane grond. Om vervolgens zich op te houden in een vergaderzaal en daar gebruik te maken van de thin clients ( met de extern bemachtigde credentials ) en de netwerkkabel. De detailbevindingen van de penetratietesten zijn vanwege de gevoeligheid beschreven in het document: *'22112073 – Rekenkamercommissie_Medemblik&Opmeer_techniek.pdf'.*

Rond 15:45 verlaat MG3 het pand via de lobby. Wat hierbij opvallend is dat de schuifdeur al dicht is, maar dat deze wel van binnenuit bediend kan worden met een lichtschakelaar.

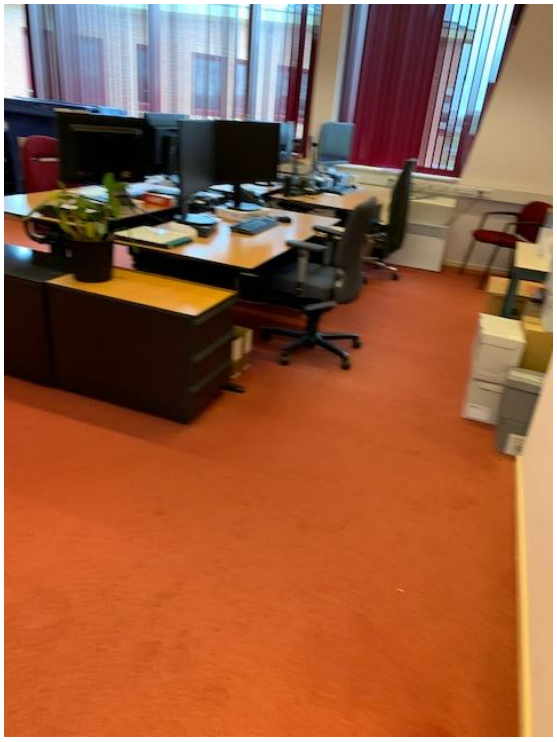

Figuur 6: Servicedesk niet bemand.

Op dinsdag 5 april 2022 omstreeks 10:10 heeft Mystery Guest 1 (hierna genoemd: 'MG1') het pand betreden voor een eerste verkenning. De hal is open met een balie en een wachtruimte. De hal geeft toegang tot de lift en de trap is vrij toegankelijk. MG1 loopt een rondje door de hal en wordt niet aangesproken op aanwezigheid. Vervolgens loopt MG1 terug naar buiten en verkent de rest van het pand, er lijkt verder geen achteringang/personeelsingang te zijn waar gebruik van gemaakt kan worden.

MG1 en Mystery Guest2 (hierna genoemd: 'MG2') overleggen kort, waarna MG2 rond 10:20 het pand betreed. MG2 begroet de receptie en loopt door naar de lift. Onderweg naar de tweede verdieping stopt de lift op de eerste verdieping, daar stappen 3 medewerkers de lift binnen. MG2 maakt kort contact en stapt bij de tweede verdieping uit. De deuren richting de afdelingen zijn op slot en beveiligd met een paslezer.

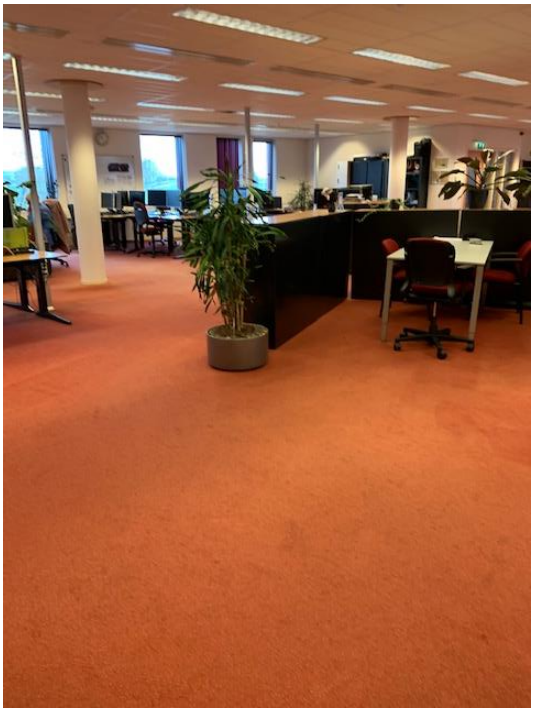

Figuur 7: Paslezer afdeling.

Al vrij snel komt er een medewerker aanlopen welke de deur opent naar de afdeling. MG2 loopt met de medewerker mee naar binnen. Op de afdeling waren niet veel werkplekken bezet, de vergaderruimte is leeg. MG2 loopt over de afdeling en wordt begroet, maar wordt niet aangesproken op aanwezigheid. Voor zover de MG2 heeft kunnen zien, waren de onbemande plekken voorzien van schermbeveiliging of uitgeschakeld (niet toegankelijk).



Figuur 8: Afdeling tweede verdieping.

MG2 besluit om naar de eerste verdieping te gaan. Op de gang is weinig beweging. MG2 houdt zich al bellend een tijdje op bij de wc voor afgesloten deur naar een afdeling. Na even gewacht te hebben komt er een medewerker aanlopen welke de deur opent waardoor MG2 de mogelijkheid heeft om te volgen mee de afdeling op. Aan de linkerkant is een vergaderruimte, MG2 besluit zich daar te installeren. Na ongeveer 10 minuten loopt MG2 de afdeling op, maar wordt niet aangesproken op aanwezigheid.



Figuur 9: vergaderruimte en afdeling eerste verdieping.

Rond 10:40 verlaat MG2 het pand via de lobby. Voor zover MG2 heeft kunnen zien waren de onbemande plekken voorzien van schermbeveiliging of uitgeschakeld (niet toegankelijk). MG2 heeft niet direct toegang gehad tot documenten, echter was er niet overal zichtbaar sprake van clean-desk.

# 5. (Techniek) penetratietesten

De (werking van) de informatiebeveiliging is onderzocht met behulp van de volgende penetratietesten:

- Externe penetratietest;
- Interne penetratietest;

De penetratietesten hebben plaatsgevonden in de periode van 1 maart 2022 tot 4 mei 2022

## 5.1 Rapportage penetratietesten

De detailbevindingen en specifieke aanbevolen maatregelen van de penetratietesten zijn beschreven in het document: 22112073 – Rekenkamercommissie_Medemblik&Opmeer_*techniek.pdf*'

Om te voorkomen dat kwaadwillenden de geconstateerde kwetsbaarheden kunnen misbruiken, is dit document als geheim geclassificeerd. Tijdens het onderzoek zijn meerdere kritieke kwetsbaarheden geconstateerd die onmiddellijk met de opdrachtgever en de CISO zijn gedeeld.

# Disclaimer

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

Mathijs van der Pol,
Security Consultant

Esther Kraan,
Consultant Riskmanagement

Nina Verhoeven,
Consultant Riskmanagement

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

Maarten IJzermans
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, 21 juni 2022

# 6. Bijlagen

## 6.1 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

Hieronder een opsomming van cybersecuritytermen die voorkomen in deze rapportage.

| BEGRIP | BETEKENIS |
|---|---|
| 2-stapsverificatie | Tweefactor authenticatie |
| 2FA | Tweefactor authenticatie |
| Aanvaller | Iemand die met opzet de beveiliging probeert uit te schakelen of te omzeilen om in een digitaal systeem te komen |
| 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 ... |
| Administrator | Beheerder van een computersysteem of computernetwerk. Deze persoon heeft meer rechten dan een gewone gebruiker. Zo kan hij bijvoorbeeld instellingen aanpassen. En hij bepaalt wat gebruikers in een computernetwerk mogen doen en wat niet. |
| ADFS | ADFS is een flexibel, gebruiksvriendelijk systeem waarmee organisaties de accounts van hun werknemers kunnen beheren. |
| 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 |

| BEGRIP | BETEKENIS |
|---|---|
| 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. |
| Blackbox test | Veiligheidstest die aangeeft dat de tester geen voorkennis van het systeem heeft. Je kunt ook op andere manieren testen:<br>- Heeft de tester een beetje kennis? Dan heet het greybox test.<br>- Bij veel voorkennis, zoals bijvoorbeeld toegang to de broncode, is het een white-box test of crystalbox test. |
| BIOS | Het basic input/output system, meestal afgekort tot BIOS, is een bibliotheek met een aantal stuurprogramma's voor de aansturing van de hardware die nodig is om een besturingssysteem op te starten. |
| Besturingssysteem | Een besturingssysteem is een programma dat na het opstarten van een computer in het geheugen geladen wordt en de hardware aanstuurt. Het fungeert als medium tussen de hardware en de computergebruiker. |
| CISO | Chief Information Security Officer. Verantwoordelijk voor informatiebeveiligingsbeleid evenals de implementatie en toezicht op uitvoering. Tevens verantwoordelijk voor strategie op het gebied van informatiebeveiliging. |
| Citrix | Citrix Workspace is een digitale werkplek waar medewerkers vanaf elk apparaat bij kunnen |
| Credentials | De gegevens waarmee een gebruiker of ander computersysteem bij een computersysteem kan aantonen dat hij is wie hij zegt dat hij is. Bijvoorbeeld een gebruikersnaam in combinatie met een wachtwoord of een via SMS opgestuurde code. |
| Domeinnaam | Een unieke naam op internet. Meestal geldt een domeinnaam voor websites, maar men kan ook een domeinnaam aanvragen voor een persoonlijk mailadres. |
| DHCP | Dynamic Host Configuration Protocol is een computerprotocol dat beschrijft hoe een computer dynamisch zijn netwerkinstelling (IP-adres) van een DHCP-server kan verkrijgen. |

| BEGRIP | BETEKENIS |
|---|---|
| Diskencryptie | Schijfencryptie is een technologie waarbij een harde schijf wordt voorzien van encryptie met als doel het ontoegankelijk maken van gegevens die op het schijfstation zijn opgeslagen |
| Exchange | Exchange is een stuk software wat ontwikkeld is door Microsoft, de intentie van de software is om op alle apparaten contacten, agenda punten en email te hebben. |
| End-of-life | Het moment dat een leverancier de software of hardware niet meer ondersteunt. Meestal voert hij dan geen updates of andere aanpassingen meer uit |
| Exploit | Programmacode of reeks acties waarmee iemand een zwakke plek in een digitaal systeem misbruikt. Het doel hiervan kan zijn om toegang te krijgen tot het systeem, om informatie te stelen of te veranderen of om te zorgen dat anderen niet meer bij informatie kunnen. Men kan een exploit gebruiken als onderdeel van malware |
| FG | Functionaris Gegevensbescherming. Verantwoordelijk voor toezicht op toepassing en naleving van de AVG. |
| Gebruikersnaam | Naam waarmee een gebruiker in een computersysteem kan inloggen. |
| IP-adres | Internet Protocol adres. Adres dat de bron of bestemming van verkeer op Internet aangeeft. |
| ISMS | Information Security Management Tool. Verzameling van alle onderling samenhangende elementen op het vlak van informatiebeveiliging. Helpt beleid, procedures en doelstellingen te formuleren, implementeren, communiceren en evalueren om de algehele informatiebeveiliging te verbeteren/garanderen. |
| ISO | Information Security Officer. Verantwoordelijk voor informatiebeveiligingsbeleid evenals de implementatie en toezicht op uitvoering. Tevens verantwoordelijk voor strategie op het gebied van informatiebeveiliging. |
| Kerberoasting | Bij Kerberoasting worden TGS-tickets uit het geheugen gehaald of afgeluisterd van het netwerk. Zodoende kan de wachtwoordhash van het serviceaccount verkregen worden. |
| KeePass | KeePass is een wachtwoordmanager waarin je wachtwoorden versleuteld kan bewaren. |

| BEGRIP | BETEKENIS |
|---|---|
| Kwetsbaarhedenscan | Een kwetsbaarheidsscanner is een computerprogramma dat is ontworpen om computers, netwerken of applicaties te beoordelen op bekende zwakheden. Deze scanners worden gebruikt om de zwakke punten van een bepaald systeem te ontdekken. |
| Kroonjuwelen | Informatie en informatiesystemen die het allerbelangrijkst zijn voor een organisatie. Het heeft grote gevolgen voor de organisatie als men niet meer bij deze informatie kan komen wanneer men dat wil. Of als de informatie niet meer klopt, of als die ongewild bij anderen terechtkomt. Intellectueel eigendom is voorbeeld van een kroonjuweel. |
| Malware | Kwaadaardige software die aanvallers op een digitaal systeem zetten om er op afstand bij te kunnen, het te vernielen of informatie te stelen. Malware is een samentrekking van het Engelse malicious software. |
| Man-in-the-middle aanval | Een aanval waarbij een aanvaller zich tussen twee partijen bevindt. De partijen denken direct met elkaar te communiceren. Echter de aanvaller is in staat informatie af te luisteren en/of te wijzigen en hier misbruik van te maken |
| Metadata | Gegevens die de eigenschappen van andere gegevens beschrijven. Bijvoorbeeld van wie de gegevens zijn, of wie ze verstuurd heeft, of wanneer ze voor het laatst gewijzigd zijn. |
| Mitigerende maatregel | Een activiteit met als doel om de oorzaak of het gevolg van een ongewenste gebeurtenis weg te nemen, of te verkleinen. |
| Monitoring | Continu bewaken van een computer of digitaal netwerk. Bijvoorbeeld of het nog helemaal goed werkt, of er fouten voorkomen, enzovoort. |
| 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. |

| BEGRIP | BETEKENIS |
|---|---|
| Multifactor Authenticatie (MFA) | Multifactor Authenticatie (MFA) is een methode om de authenticiteit van een gebruiker te verifiëren op meer dan één enkele manier. |
| [redacted] | |
| Patch | Nieuwe versie van software. In deze nieuwe versie heeft de leverancier kwetsbaarheden in het systeem hersteld. Hij heeft geen nieuwe functies toegevoegd. |
| Patch management | Proces waarbij men indien mogelijk patches installeert op een digitaal systeem. Het proces dat zorgt voor het verwerven, testen en installeren van patches (wijzigingen ter opheffing van bekende beveiligingsproblemen in de code) op (verschillende softwarecomponenten van) een computersysteem |
| PDCA | Plan-Do-Check-Act (cyclus). Stappen ter verbetering van bijvoorbeeld een proces of beleid. |
| 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 |
| PO | Privacy Officer. Verantwoordelijk voor het ontwikkelen en bewaken van het privacybeleid en ondersteuning bieden bij uitvoering van het beleid. |

| BEGRIP | BETEKENIS |
|---|---|
| Poortscan | Scan van openstaande poorten op een digitaal systeem waarmee inzichtelijk wordt gemaakt welke poorten openstaan. Een poort is een manier om via een netwerk te communiceren met een digitaal systeem. Aanvallers gebruiken de informatie uit de poortscan om te beslissen hoe zij het systeem kunnen binnendringen of beschadigen. |
| Ransomware | Ransomware is malware die de databestanden van gebruikers versleutelt, met als doel om deze later te ontsleutelen in ruil voor losgeld. |
| Shared Service Center | Een Shared Service Center (SSC) is een (semi-)autonome eenheid die verantwoordelijk is voor de afhandeling van een aantal operationele taken van één of meerdere organisaties. |
| Script | Computerprogramma met instructies die voor mensen leesbaar zijn. Men gebruikt vaak scripts als men webapplicaties wil bouwen en beheren. Aanvallers gebruiken onder andere scripts om onderdelen van een cyberaanval te automatiseren. |
| Server | Krachtige computer die in een netwerk de gemeenschappelijke voorzieningen regelt zoals authenticatie, autorisatie. |
| Switch | Een apparaat dat onderdelen van een netwerk met elkaar verbindt. |
| Shell | Computerprogramma waarmee een gebruiker met een commandoregel opdrachten kan geven aan het besturingssysteem van een computer. |
| TopDesk | TopDesk is een service management-provider. De kernactiviteit draait om het beheer van meldingen, middelen, wijzigingen, workflows en reserveringen in de infrastructuur van organisaties |
| Thin client | Het is een naam voor een relatief lichte computer die uitsluitend beeldinformatie, toetsaanslagen en muisacties uitwisselt tussen de gebruiker en een centrale computeromgeving |
| Fat client | Een fat client is een computer in een client-serverconfiguratie die onafhankelijk van de server kan functioneren. Veel applicaties worden lokaal op de harde schijf van de client geïnstalleerd. |

| BEGRIP | BETEKENIS |
|---|---|
| Time box | Vaste tijd waarin men bepaalde geplande activiteiten uitvoert. Is de tijd om, dan stopt het. Ook als de activiteiten nog niet klaar zijn. |
| Update | Aanpassing van een bestaande versie van hard- of software. Deze repareert bekende zwakke plekken, zorgt eventueel voor nieuwe beveiliging en extra functies |
| 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 |
| Wachtwoordmanager<br>Wachtwoordkluis | Software waarin een gebruiker de combinatie van wachtwoord en gebruikersnaam kan opslaan. Dit is een soort digitale kluis. Vaak kan de software ook zelf wachtwoorden aanmaken, websites herkennen en automatisch invullen. Ook geeft de wachtwoord manager vaak aan of een wachtwoord sterk genoeg is, en of je deze al eerder hebt gebruikt. |

## 6.2 Overzicht geïnterviewden

| Functie | Datum interview |
|---|---|
| CISO | 14 maart 2022 |
| Functionaris gegevensbescherming | 10 maart 2022 |
| Privacy officers (2) | 11 maart 2022 |
| Senior beleidsmedewerker informatiemanagement | 7 april 2022 |
| Senior financieel beleidsadviseur | 14 maart 2022 |
| Interim Directeur Bedrijfsvoering en Kwaliteitsontwikkeling | 10 maart 2022 |

## 6.3 Overzicht bestudeerde documenten

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

| Document | Versie | Datum |
|---|---|---|
| Gemeentelijk Informatieveiligheidsbeleid 2020-2023 | - | 14-10-2020 |
| 2.2 Privacybeleid gemeenteraad getekend | - | 09-04-2020 |
| 2.2 Raadsbrief privacybeleid | - | 15-07-2019 |
| Privacybeleid Raad Medemblik 2020 | - | 19-03-2019 |
| Gemeente Medemblik Afdelingsplan 2022 Informatiebeveiliging | - | - |
| Dataclassificatie iBurgerzaken gemeente Medemblik | - | - |
| Incidentmanagement en responsplan Gemeente Medemblik | 1.1 | 01-07-2016 |
| Jaarrapportage Gegevensbescherming Gemeente Medemblik 2020 | - | Feb. 2021 |
| Verwerkingsregister export | - | 30-11-2021 |


Hoffmann
VERTROUWEN IS GOED,
HOFFMANN IS BETER
www.hoffmann.nl