gemeente lingewaard

Onderzoeksrapportage

Informatieveiligheid

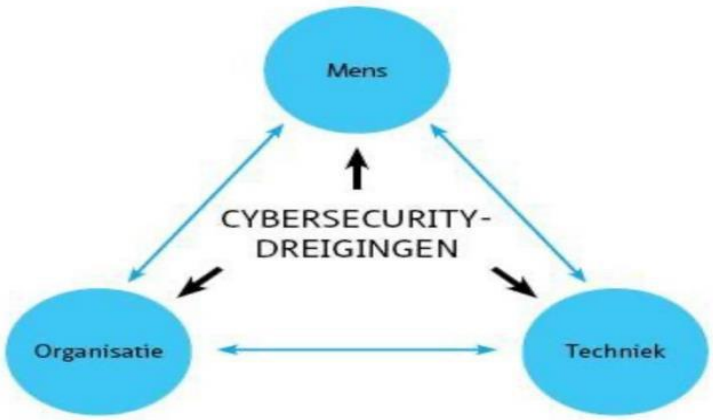
Vastgesteld in de rekenkamercommissievergadering van 12 december 2023

Inhoudsopgave

Inleiding

De rekenkamercommissie heeft Hoffmann Bedrijfsrecherche B.V. onderzoek laten uitvoeren naar het informatieveiligheidsbeleid in de gemeente Lingewaard. In dit onderzoek stond de driehoek mens-organisatie-techniek centraal. De rekenkamercommissie heeft ervoor gekozen om deze driehoek centraal te stellen, omdat wanneer één van die drie faalt de informatieveiligheid ogenblikkelijk in het geding komt.

De gevolgen van gebrekkige informatieveiligheid kunnen enorm zijn. Recent zijn meerdere gemeenten en bedrijven getroffen door hacks met als gevolg dat er data in handen van onbevoegden zijn gekomen, er soms wekenlang niet gewerkt kon worden, ICT-systemen opnieuw moesten worden ingericht en afpersing dreigde. De financiële gevolgen van een dergelijke hack kunnen voor de gemeente enorm zijn, de maatschappelijke gevolgen mogelijk nog erger.
In de rapportage staan veel praktische tips van het onderzoeksbureau. In deze bestuurlijke conclusies en aanbevelingen houdt de rekenkamercommissie het bij een meer abstract oordeel.



Hoofdvraag en deelvragen

De rekenkamercommissie heeft voor aanvang van dit onderzoek onderstaande hoofd- en deelvragen geformuleerd:

Is de informatieveiligheid bij de gemeente Lingewaard voldoende gewaarborgd?

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

1. **Organisatie en proces**
   a. Welk beleid heeft de gemeente vastgesteld op het gebied van informatieveiligheid? Voldoet dit beleid aan de BIO en zo ja, wordt dit door kwaliteitscertificaten (bijvoorbeeld BIO) ondersteund?
   b. Welke risico's en maatregelen heeft de gemeente benoemd? Past dit bij de antwoorden op a?
   c. Bestrijkt de risico-inventarisatie informatieveiligheid alle relevante taakvelden en waar blijkt dat uit? Zijn er onderdelen die ten onrechte missen?
   d. In hoeverre zijn de maatregelen geïmplementeerd en zijn daarvoor adequate middelen in de zin van geld en menskracht beschikbaar gesteld?

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?

3. **Techniek**
   a. Is data bij de gemeente voldoende beschermd tegen fysieke en technische 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?

Conclusies

1. Het beleidskader van de gemeente Lingewaard is heel redelijk op orde. Het beleid is uitgebreid en gericht op risico's en maatregelen. Onderzoekers vinden nog verbeterpunten voor
    a. het meenemen van *alle* teams in het beleid; de decentraal belegde onderdelen van het informatieveiligheidsbeleid hebben niet in alle teams voldoende prioriteit; bijvoorbeeld risico-analyses en beheersplannen zijn nog niet voor alle teams gemaakt.
    b. aansluiting bij de meest recente standaarden
    c. het maken van een praktische handleiding voor de praktijk t.a.v. het privacybeleid
2. Uit verschillende onderdelen van het onderzoek blijken mensen de zwakke schakel:
    a. Ondanks dat technische maatregelen in combinatie met oplettendheid van medewerkers en servicedesk in praktijk goed werken zijn er toch mensen die in phishingmails tuinen.
    b. Mensen zonder medewerkerspas op de afdeling worden niet aangesproken.
    c. Clean desk policy wordt in de praktijk niet goed genoeg nageleefd.
3. De technologische beveiliging leek op orde. Het bleek wel mogelijk om ongeautoriseerde toegang te verkrijgen tot het interne draadloze 'Lingewaard-Medewerkers' netwerk van gemeente. Dit duidt op een potentiële kwetsbaarheid voor cyberaanvallen, maar dit is verder niet onderzocht. Het interne gasten netwerk bleek voldoende gesegmenteerd en voldoende beveiligd tegen hacken.

Met de antwoorden op deze drie deelvragen beantwoorden we ook de hoofdvraag of de informatieveiligheid in de gemeente Lingewaard op orde is: de informatieveiligheid is in Lingewaard redelijk op orde, maar er zijn nadrukkelijk nog wel aandachtspunten ter verbetering.

Aanbevelingen

1. Zorg voor een jaarlijkse beleidscyclus waarin aandacht is voor de gehele organisatie, jaarlijkse aansluiting bij de meest actuele standaarden en de praktische betekenis voor de uitvoering van het beleid. Maak informatieveiligheid onderdeel van de prestatieafspraken met managers en andere verantwoordelijken en creëer zo een financiële prestatieprikkel.
2. Creëer een cultuur waarin het gewoon wordt mensen aan te spreken op alledaagse dingetjes. De rekenkamercommissie begrijpt dat het lastig is collega's op het niet zichtbaar dragen van een personeelspas of het opruimen van een bureau aan te spreken. Toch vinden wij dat dat normaal zou moeten zijn in het kader van de uitoefening van de publieke functie die een gemeente heeft.
3. Blijf aandacht houden voor de technologische maatregelen die u nu ook al treft. Rapporteer daarover in bestuurlijke termen jaarlijks aan de raad, bijvoorbeeld als u het jaarverslag aanbiedt.

Bestuurlijke reactie van het College van B&W

Geachte rekenkamer,
Beste Astrid,

Hierbij de bestuurlijke reactie op het rekenkameronderzoek over Informatieveiligheid in de gemeente Lingewaard.
Het college kan zich vinden in de conclusies en aanbevelingen zoals deze zijn weergegeven. De wereld van Informatieveiligheid is echter continue in beweging. Tijdens het rekenkameronderzoek is er een grote ICT-migratie uitgevoerd waarmee de meeste technische bevindingen zijn opgelost. Hierdoor zijn de beschreven risico's al aanzienlijk kleiner dan tijdens het onderzoek het geval was. Hieronder vindt u een reactie op de conclusies en aanbevelingen zoals deze genoemd zijn in de rapportage.

Conclusies:
1. Het beleidskader van de gemeente is heel redelijk op orde. Het beleid is uitgebreid en gericht op risico's en maatregelen. Onderzoekers hebben nog wel verbeterpunten benoemd. a. *Bestuurlijke reactie*: Op dit moment wordt het beleid opnieuw beoordeeld en wordt het aangepast aan de nieuwe standaarden. Vanaf 2024 gaat de Europese wet op informatiebeveiliging (de NIS2) in en wordt het normenkader voor Nederlandse overheden (de BIO) aangepast. Wij zullen het Informatiebeveiligingsbeleid van gemeente Lingewaard hierop aanpassen en dan zullen we tevens de aanbevelingen van de rekenkamercommissie meenemen.

2. Uit verschillende onderdelen van het onderzoek blijken mensen de zwakke schakel. a. *Bestuurlijke reactie*: Dit is in de wereld van de informatieveiligheid een terugkerende conclusie, die ook bij ons van toepassing is. Dit heeft dus voortdurende aandacht nodig. Mede hierom is het specifiek toegewezen budget voor informatiebeveiliging vanaf 2024 verhoogd, zodat in deze voortdurende behoefte voorzien kan worden. Hiervoor zal ook jaarlijks een jaarplan gemaakt worden met verschillende acties om de medewerkers te blijven ondersteunen in de bewustwording.

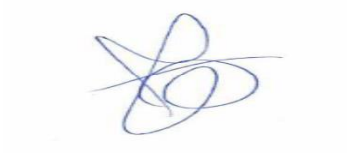
3. De technologische beveiliging leek op orde. Het bleek wel mogelijk om ongeautoriseerd toegang te verkrijgen tot het interne draadloze 'Lingewaard-medewerkers' netwerk van de gemeente. Dit duidt op een potentiële kwetsbaarheid voor cyberaanvallen, maar dit is verder niet onderzocht. Het interne gasten netwerk bleek voldoende gesegmenteerd en voldoende beveiligd tegen hacken. a. *Bestuurlijke reactie*: Het college heeft eind 2022 nog een uitgebreide penetratietest (PENtest) laten uitvoeren en daarbij hebben wij de conclusie gekregen dat ons netwerk goed beveiligd is voor aanvallen van buitenaf. Daarnaast is in de migratie van de ICT de inrichting van de draadloze netwerken opnieuw ingericht en is geen toegang van buitenaf meer te krijgen zonder multi-factor authenticatie. Dit is geheel volgens de richtlijnen van de NIS2, de BIO en de VNG. Daarmee is het genoemde risico ook geminimaliseerd. In november is er een nieuwe PENtest uitgevoerd om het nieuwe ICT-landschap te toetsen op de beveiliging. De bevindingen hieruit zullen opgenomen worden in het uitvoeringsplan informatiebeveiliging van het team Informatie Voorziening (IV).

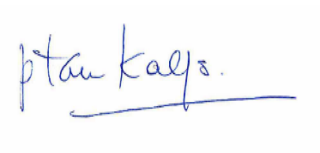
Aanbevelingen:
Alle drie de aanbevelingen worden door ons onderschreven en zullen worden opgenomen in het IB-beleid. Tevens zullen we periodiek het beleid blijven toetsen op actualiteit. Dit zal conform de bestaande standaarden gedaan worden, zodat we blijven voldoen aan de wetgeving en de normenkaders die voor de gemeente gelden.

Naast de algemene aanbevelingen uit het rekenkameronderzoek zullen we de aanbevelingen uit het onderzoeksrapport, voor zover nu nog van toepassing, meenemen in de uitvoeringsplannen van 2024. Zodat we daarmee ook voldoen aan de beveiligingsstandaarden en de wetgeving.
Algemeen concluderend kunnen we zeggen dat wij de zorgen van de rekenkamercommissie delen. Mede dankzij een stevige investering in onze ICT en daarmee in onze informatieveiligheid, hebben we het afgelopen jaar grote stappen gezet in het verhogen van de kwaliteit van zowel ICT als van de beveiliging hiervan. Om de beveiliging in zowel techniek als mens voldoende aandacht te blijven geven is het gealloceerde budget Informatiebeveiliging voor de komende jaren verhoogd, zodat ook de stijgende kans op cyberincidenten het hoofd geboden kan worden.
Mede hierdoor herkennen wij de conclusie op pagina 19 **"de bedrijfsvoering is veelal reactief en de bestuurlijke betrokkenheid en bereidheid straalt onvoldoende uit dat informatieveiligheid belangrijk is**" niet. We hebben de afgelopen jaren veel geïnvesteerd in informatiebeveiliging en wij hebben vanuit het college en het management veel aandacht voor de ontwikkeling van de informatieveiligheid.
Bemmel, 28-11-2023

Hoogachtend,

burgemeester en wethouders van de gemeente Lingewaard,
de secretaris, de burgemeester,





drs. I.P. van der Valk dr. P.T.A.M. Kalfs

Rekenkamerreactie op de bestuurlijke reactie van het College van B&W

De rekenkamer heeft in haar vergadering van 12 december 2023 kennisgenomen van de reactie van het college en daarop onderstaande reactie geformuleerd.

De rekenkamer is verheugd te constateren dat het college zich grotendeels in de rapportage herkent en bereid is de aanbevelingen op te volgen. De rekenkamer wenst u daar veel succes bij.

Voorzitter
Jeroen van Oort

Secretaris-Onderzoeker
Astrid Boin

Rapport van bevindingen door Hoffmann B.V.

Op de volgende bladzijden treft u het rapport van bevindingen dat in opdracht en onder verantwoordelijkheid van de rekenkamercommissie is opgesteld door Hoffmann. De rekenkamer baseert zijn conclusies en aanbevelingen op basis van dit rapport.

Bestuurlijk rapport Informatiebeveiliging Gemeente Lingewaard

Dossiernummer 22212023

Onderzoek in opdracht van

Rekenkamercommissie gemeente Lingewaard

Vertrouwelijk

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

In opdracht van de rekenkamer is een informatiebeveiligingsonderzoek (hierna genoemd: IB-onderzoek) uitgevoerd bij de gemeente Lingewaard (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 april 2023.

De hoofdvraag van het onderzoek is als volgt: 'Is de informatieveiligheid bij de gemeente Lingewaard voldoende gewaarborgd?' Deze vraag wordt beantwoord aan de hand van de bevindingen uit de facetten organisatie, mens en techniek welke hieronder staan beschreven.

In deze management samenvatting worden de belangrijkste resultaten van het onderzoek 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.

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

Organisatie

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

Het onderzoek bestond uit het afnemen van interviews en een documentanalyse. Centraal hierbij stond het 'Informatiebeveiligingsbeleid Gemeente Lingewaard' (vigerend beleid ten tijde van het onderzoek). Onderzoekers concluderen dat de inbedding van informatieveiligheid in de praktijk het grootste aandachtspunt is voor de gemeente. Op een aantal vlakken voldoet de informatiebeveiliging al aan een hoger volwassenheidsniveau, maar wordt dit bijvoorbeeld niet door de gehele organisatie gedragen (bijvoorbeeld risicoanalyses). Op andere vlakken mag de informatiebeveiliging nog groeien aan volwassenheid (bijvoorbeeld op het vlak van privacy). Informatiebeveiliging mag meer onderdeel worden van de organisatiecultuur om zo de informatieveiligheid te kunnen waarborgen. Belangrijke stappen zijn o.a.;

beleid actualiseren en aanvullen, processen inzichtelijk maken, werken aan een meer pro-actieve bedrijfsvoering en draagvlak creëren door een duidelijke bestuurlijke betrokkenheid en bereidheid.

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 nep-e-mail getoetst. Bij de 492 verstuurde e-mails hebben 14 gebruikers de unieke link in de e-mail geopend. In totaal zijn er 5 inlogpogingen van unieke gebruikers met geldige e-mailadressen geregistreerd.

Uit de test is gebleken dat de technische maatregelen, in combinatie met oplettendheid van medewerkers en servicedesk in praktijk goed werken. Dit heeft ertoe geleid dat de mail snel opgemerkt en ondervangen is, waardoor niet alle medewerkers de mail hebben ontvangen. Echter, wanneer slechts één iemand op een mail-phishing link klikt en een gebruikersnaam en wachtwoord achterlaat, kan een kwaadwillende al toegang krijgen tot het apparaat van deze medewerker. Wat als gevolg kan hebben dat een kwaadwillende toegang krijgt tot vertrouwelijke informatie van de gemeente. Wij adviseren daarom om doorlopend aandacht te blijven besteden aan het bewustzijn van medewerkers, zodat bijvoorbeeld ook nieuwe collega's weten hoe zij moeten handelen in geval van twijfel.

Het gedrag van de medewerkers is tevens onderzocht middels een fysieke inlooptest. Het was voor de Mystery Guest (hierna genoemd: 'MG') mogelijk om het gemeentehuis en de daarin beveiligde zones te betreden. Opvallend was dat veel van de aanwezige personen een personeelspas droegen, echter werd de MG (zonder pas) niet aangesproken. Op de onbemande werkplekken waren de computers vergrendeld. Het clean desk beleid mag in praktijk beter worden opgevolgd, er was namelijk op verschillende plekken (op bureaus en in kasten) informatie in te zien.

Techniek

Gezien de overlap met een onlangs uitgevoerde pentest is er, in overleg met de rekenkamer, met de gemeente afgestemd dat de draadloze netwerken van de gemeente getest zouden worden, waarbij onder andere gekeken diende te worden of er voldoende segmentatie is tussen de verschillende netwerken.

Deze pentest heeft plaatsgevonden middels een test op locatie, waarbij heeft een medewerker van Hoffmann heeft geprobeerd toegang te verkrijgen tot de draadloze netwerken van de gemeente.

De onderzoekers zijn er in geslaagd om ongeautoriseerde toegang te verkrijgen tot het interne draadloze **'Lingewaard-Medewerkers' netwerk** van gemeente. Dit duidt op een potentiële kwetsbaarheid voor cyberaanvallen, echter viel verder pentest onderzoek op het interne medewerkers netwerk buiten scope.

Verder was daarnaast het interne **gasten netwerk** voldoende gesegmenteerd en voldoende beveiligd tegen hacken.

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

1. Inleiding

De Rekenkamercommissie gemeente Lingewaard (hierna genoemd: ‘de Rekenkamer’) heeft Hoffmann gevraagd een onderzoek uit te voeren naar de informatiebeveiliging bij de gemeente Lingewaard (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 Lingewaard voldoende 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? Voldoet dit beleid aan de BIO en zo ja, wordt dit door kwaliteitscertificaten (bijvoorbeeld BIO) ondersteund?
b. Welke risico’s en maatregelen heeft de gemeente benoemd? Past dit bij de antwoorden op a?
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?

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?

3. Techniek

a. Zijn de draadloze netwerken van de gemeente op dit moment voldoende beveiligd tegen hacken?
b. Is er sprake van voldoende segmentatie tussen deze netwerken?

De scope van het gehele IB-onderzoek betreft:

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

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

1.2 Contactinformatie

Naam	Functie	E-mail	Telefoon
Harald Langmar	Security Consultant	h.langmar@hoffmann.nl	06-46627115
Esther Kraan	Consultant Riskmanagement	e.kraan@hoffmann.nl	06-21330432
Mo Ballari	Sales Consultant	m.ballari@hoffmann.nl	06-47384377
Johan van Slooten	Director Riskmanagement	j.vanslooten@hoffmann.nl	06-11003083
Jeroen van Oort	Voorzitter RKC	info@jeroenvanoort.com	06-43586022
Astrid Boin	Secretaris-Onderzoek	a.boin@lingewaard.nl	06-21920733

1.3 Versies

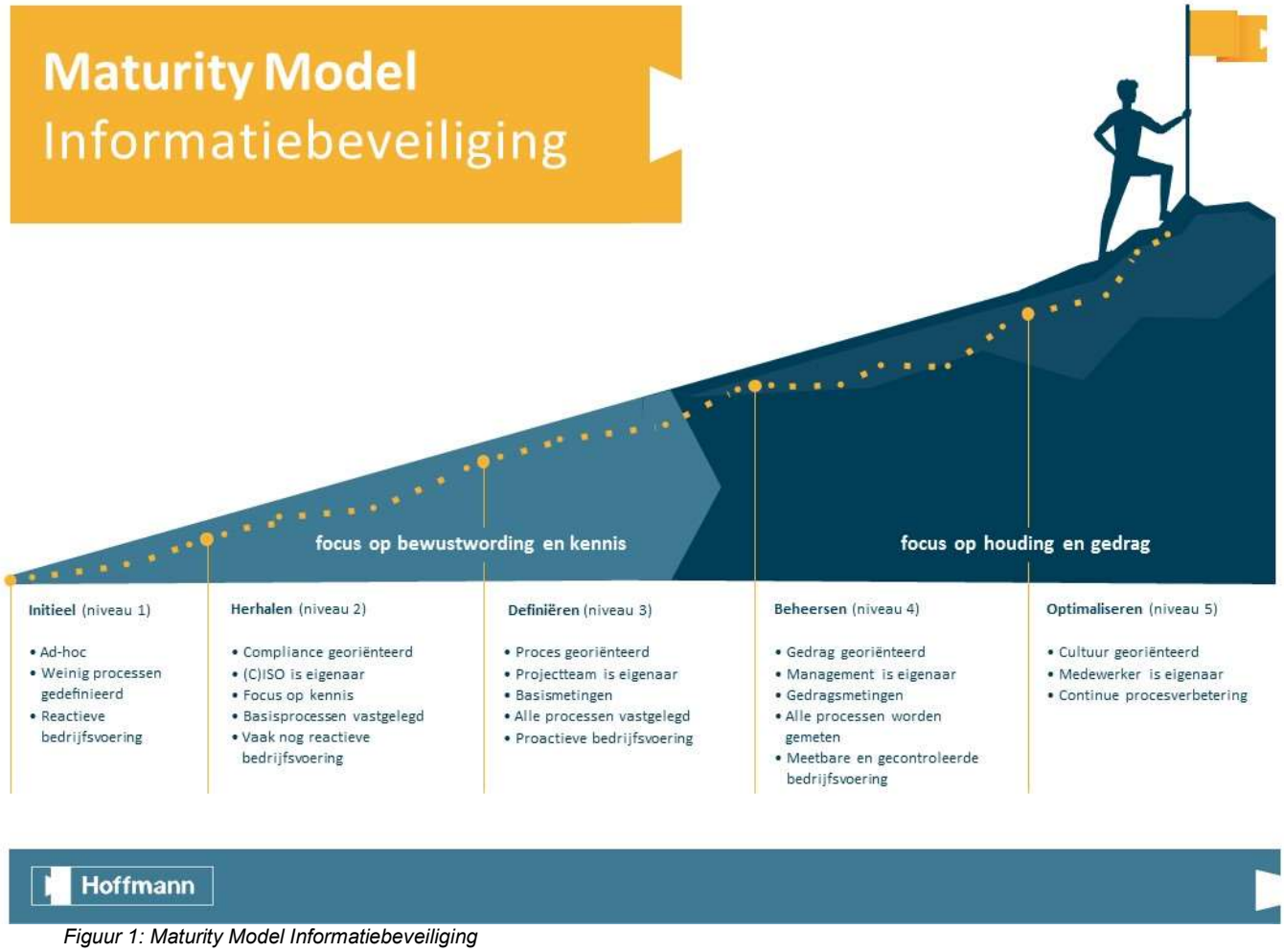
Versie	Datum	Status
1.1	09-05-2023	Conceptversie RKC
1.2	06-06-2023	Conceptversie 1.2 inclusief feedback RKC
1.3	27-07-2023	Versie 1.3 (inclusief ambtelijke reactie)

2. Conclusies

2.1 Conclusies

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 Lingewaard voldoende gewaarborgd?'*

Deze vraag laat zich het beste beantwoorden met behulp van onderstaand Maturity Model Informatiebeveiliging.



Figuur 1: Maturity Model Informatiebeveiliging

Het model geeft verschillende niveaus aan van de informatiebeveiligingscultuur binnen een organisatie. De eerste drie niveaus kenmerken zich door een focus op bewustwording en kennis, de laatste twee niveaus door een focus op houding en gedrag. Per niveau worden verschillende kenmerken genoemd.

Wanneer we de onderzoeksresultaten bekijken in het licht van dit model komt naar voren dat informatiebeveiliging binnen de gemeente Lingewaard voldoet aan verschillende kenmerken op niveaus 1, 2, 3 en 4, echter ontbreken er ook nog elementen op deze niveaus. Op het vlak van privacy constateren de

onderzoekers bijvoorbeeld dat het beleid is nog onvoldoende is uitgewerkt en dat processen beter gedefinieerd mogen worden. Daarbij is een groot deel van de werkzaamheden meer praktisch en ad-hoc dan gericht op de langere termijn. Dergelijke kenmerken bevinden zich tussen niveau 1 en 2. Anderzijds liggen er bijvoorbeeld verantwoordelijkheden op het vlak van informatiebeveiliging bij de teammanagers en worden er risicoanalyses uitgevoerd. Deze elementen bevinden zich op niveau 4.
Ook komt naar voren dat bepaalde kenmerken wel al op orde zijn voor bepaalde delen van de organisatie, waar andere delen nog niet zo ver zijn. Zo zijn er bijvoorbeeld nog niet voor alle teams risicoanalyses gemaakt, waardoor er op bepaalde vlakken nog geen zicht is op risico's en de nodige maatregelen. Onderzoekers concluderen dat de waarborging van informatieveiligheid stokt bij de inbedding van informatiebeveiliging in de praktijk. Dit heeft verschillende redenen; beleid is onvoldoende actueel of praktisch voorschrijvend, bij sommige afdelingen is er onvoldoende draagvlak c.q. urgentie, de bedrijfsvoering is veelal reactief en de bestuurlijke betrokkenheid en bereidheid straalt onvoldoende uit dat informatieveiligheid belangrijk is.

Hieronder volgen de conclusies voor ieder onderzocht onderdeel: organisatie, mens en techniek voor de gemeente Lingewaard.

2.1.1 Organisatie en proces

a. Welk beleid heeft de gemeente vastgesteld op het gebied van informatieveiligheid? Voldoet dit beleid aan de BIO en zo ja, wordt dit door kwaliteitscertificaten (bijvoorbeeld BIO) ondersteund?
Het 'Informatiebeveiligingsbeleid Gemeente Lingewaard' vormt de basis voor de informatiebeveiliging binnen de gemeente Lingewaard. Het beleid is uitgebreid en gericht op risico's en maatregelen, echter verwijst het naar zowel de BIO als naar een verouderd normenkader (BIG). Het beleid dient geactualiseerd te worden zodat het geheel in lijn is met de BIO. Daarnaast is er een 'Privacybeleid en regelement Lingewaard'. Het advies luidt om het privacybeleid beleid te actualiseren en uit te breiden met een praktische handleiding voor de praktijk.

b. Welke risico's en maatregelen heeft de gemeente benoemd?
Vanuit de interviews zijn er risico's benoemd op het vlak van dataclassificatie en logisch toegangsbeheer. Daarnaast geeft men aan nu voornamelijk reactief te acteren bij beveiligingsincidenten, de wens is om aanvallen van buitenaf te kunnen detecteren door middel van een SIEM/SOC[1].

c. Welke informatievelden van het hele gemeentelijke taakveld bestrijkt de risico-inventarisatie wel en welke niet?
Van de afdelingen ICT, Burgerzaken, Sociaal Domein, VTH (Vergunningen, toezicht en handhaving) en Facilitair zijn de risico's en nodige maatregelen (grotendeels) inzichtelijk gemaakt, overige afdelingen dienen dit nog te doen. Uit de interviews kwam de risicoanalyse van Personeel en organisatie (hierna genoemd P&O) als een prioriteit naar voren. Daarnaast is de risicoanalyse binnen het Sociaal Domein

[1] Zie hiervoor het Cybersecurity Woordenboek van Cyberveilig Nederland: www.cyberveilignederland.nl/woordenboek

nog niet volledig. Gezien de vertrouwelijkheid van de informatie binnen deze afdelingen, is het raadzaam om beiden aan te merken als prioriteit. De verantwoordelijkheid voor risicoanalyses ligt bij de teammanagers, onder begeleiding van de informatiebeveiligingsorganisatie.

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

De samenstelling en capaciteiten binnen de informatiebeveiligingsorganisatie zijn op orde. De functionarissen zijn formeel benoemd en verantwoordelijkheden zijn doorgaans duidelijk belegd. De informatiebeveiligingsorganisatie probeert, conform BIO en intern beleid, zoveel mogelijk verantwoordelijkheden te beleggen bij de organisatie zelf. Derhalve ligt bijvoorbeeld de verantwoordelijkheid voor het maken van de risicoanalyses bij de teammanagers. Daar waar risico's inzichtelijk gemaakt zijn werkt de informatiebeveiligingsorganisatie samen met de teams om de nodige maatregelen te implementeren. Er is echter een beperkt gealloceerd budget voor informatiebeveiliging (€25.000,-), waardoor managers vaak vanuit het eigen budget moeten financieren. Hierdoor wordt er in praktijk vaak voor andere prioriteiten gekozen. Daarnaast is er binnen de teams niet altijd voldoende capaciteit beschikbaar om de maatregelen door te voeren. De inbedding en bestendiging van informatiebeveiliging is mede vanwege deze factoren op bepaalde vlakken nog onvoldoende.

2. Mens

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

Gemeente Lingewaard maakt gebruik van een 'I-bewustzijnscampagne', een e-learning op het gebied van informatiebeveiliging en privacy. Elke (nieuwe) medewerker (langer dan 3 maanden in dienst) is verplicht om de e-learning te volgen. Dit geldt tevens voor medewerkers vanuit inhuur/uitvoeringsorganisaties. Daarnaast wordt intranet als medium gebruikt ten behoeve van bewustwording. Het advies is om, naast kennisdeling, tevens aandacht te besteden aan het daadwerkelijke informatieveilige gedrag van medewerkers in de praktijk (bijvoorbeeld door mail phishing tests of onderzoek naar het (praktisch) faciliteren van gewenste informatieveilige gedrag).

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

Tijdens de fysieke inlooptest is gekeken hoe het informatiebeveiligingsbeleid wordt nageleefd in de praktijk. Zo is geconstateerd dat medewerkers de computer vergrendelen wanneer zij de werkplek verlaten en werd door de meesten de personeelspas zichtbaar gedragen. Het clean desk beleid mag in praktijk beter worden opgevolgd, er was namelijk op verschillende plekken (bureaus en in archiefkasten) informatie in te zien. Het privacybeleid van de gemeente mag praktischer ingestoken worden om naleving in de praktijk te faciliteren.

3. Techniek

a. Zijn de draadloze netwerken van de gemeente op dit moment voldoende beveiligd tegen hacken?

De onderzoekers zijn er in geslaagd om ongeautoriseerde toegang te verkrijgen tot het interne draadloze '**Lingewaard-Medewerkers**' netwerk van gemeente. Dit betekend dat het interne netwerk potentieel kwetsbaar is voor cyberaanvallen. Hoffmann heeft dit risico niet verder onderzocht vanwege de vooraf afgestemde (beperkte) scope. Het interne **gasten** netwerk was wel voldoende beveiligd tegen hacken.

b. Is er sprake van voldoende segmentatie tussen deze netwerken?

Ja, er is sprake van voldoende segmentatie.

3. Organisatie

Voor het onderzoek naar de organisatie van informatiebeveiliging is een analyse uitgevoerd op de door de gemeente Lingewaard beschikbaar gestelde documentatie, rapporten en verklaringen. Daarnaast zijn er verschillende 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. 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
3.2.1.	Het IB beleid verwijst naar verouderde normenkader BIG	Het beleid is momenteel niet geheel in lijn met de BIO.	Evalueer en actualiseer het beleid (bij voorkeur jaarlijks) zodat deze in zijn geheel aansluit op de BIO en past bij de huidige situatie binnen de organisatie.
3.2.1.	Ten tijde van het onderzoek is er nog geen werking van het ISMS geconstateerd bij de gemeente Lingewaard, waarmee er structureel een PDCA aanpak op informatiebeveiliging (IB) wordt geborgd.	Doordat het ISMS nog niet volledig is ingericht, ontstaat het risico dat IB op ad-hoc basis wordt georganiseerd en dat er reactief op (nieuwe) dreigingen en risico's wordt geacteerd.	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.

3.2.2.	Er is door onderzoekers geen kennis genomen van een wachtwoordenbeleid welke de minimale eisen omtrent wachtwoorden beschrijft.	Het is in de praktijk onduidelijk of de wachtwoorden aan minimale veiligheidseisen dienen te voldoen (zoals beschreven in een wachtwoordenbeleid).	Stel het wachtwoordenbeleid (opnieuw) op en toets deze aan de technische maatregelen. Communiceer het beleid met medewerkers zodat duidelijk is wat van hen wordt verwacht.
3.2.4.	Er zijn geen recente rapportages beschikbaar vanuit de IB-organisatie.	Verminderde zichtbaarheid van de IB organisatie en bijbehorende ontwikkelingen komt niet ten goede aan de betrokkenheid en het bewustzijn.	Rapporteer periodiek aangaande de resultaten, doelen en ontwikkelingen op het vlak van IB.
3.2.5	Door het gebrek aan risicoanalyses hebben niet alle afdelingen even goed zicht op risico's en nodige maatregelen.	Het niet tijdig in kunnen spelen op (toekomstige) dreigingen maakt afdelingen, en daarmee ook de organisatie, kwetsbaar.	Voer de nog ontbrekende risicoanalyses uit zodat er een volledig beeld is van de risico's en nodige maatregelen gemeente breed.
3.2.6	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 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 elke aanschaf moet worden voldaan aan de eisen m.b.t. informatiebeveiliging[2]. Werkprocessen moeten ervoor zorgen dat de IB organisatie wordt betrokken.
3.2.6	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.	Het is raadzaam om periodiek (minimaal jaarlijks) een controle uit te voeren op de naleving van eisen m.b.t. informatiebeveiliging[3].

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

3.2.7	De gemeente beschikt niet over continuïteit/crisismanagement plannen. Het is voor onderzoekers onduidelijk of het gemeentelijk beleidsteam geformaliseerd is. Bij een cybercrisis wordt er ad hoc een gelegenheidsteam opgericht.	Wanneer een crisisteam niet geformaliseerd is het risico dat er tijdens een calamiteit/crises niet de juiste medewerkers geïnformeerd worden, verantwoordelijkheden onduidelijk zijn en/of er niet voldoende mandaat is om beslissingen te nemen.	Stel informatiebeveiligingscontinuïteit/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.
3.2.8	Het privacy-beleid sluit onvoldoende aan bij de behoeften van de organisatie. Er worden wettelijke kaders en uitgangspunten uiteengezet, echter mist het kaders en richtlijnen voor opvolging in de praktijk.	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 privacy-beleid zodat het een vertaalslag maakt van de wettelijke opdracht en bijdraagt aan de praktische uitvoering hiervan.
3.2.8	Het verwerkingsregister van de gemeente is bijna up to date, echter nog niet volledig bijgewerkt.	De gemeente voldoet hiermee nog niet geheel aan de verantwoordingsverplichting zoals gesteld in de AVG.	Werk het verwerkingenregister bij en richt de organisatie zo in dat dit een continu doorlopend proces wordt.
3.2.9	De bestaande classificatierichtlijnen zijn onvoldoende werkzaam in de praktijk. Het is daardoor onduidelijk welke vertrouwelijkheid een document heeft.	De gemeente heeft onvoldoende zicht op welke informatie zich waar bevindt. Hiermee bestaat het risico dat er onvoldoende beveiligingsmaatregelen worden genomen voor gevoelige informatie.	Besteed aandacht aan inbedding van het classificatiebeleid in de praktijk. Doe dit door bewustwording en voorbeeldgedrag.
3.2.9	Autorisaties worden soms nog geselecteerd op basis van bestaande rechten van collega's in plaats van op autorisatieprofielen.	Het risico bestaat dat er te veel of onjuiste autorisaties worden verleend aan (nieuwe) collega's. Hierdoor wordt er mogelijk onterecht toegang verleend aan gevoelige informatie.	Stel autorisatieprofielen op per functie, gebaseerd op risicoanalyses.
3.2.11	Er is weinig wisselwerking tussen bestuur en organisatie op het vlak van informatiebeveiliging en privacy. Geen duidelijke betrokkenheid en bereidheid aangaande informatiebeveiliging.	Het gebrek aan betrokkenheid en bereidheid draagt negatief bij aan de bewustwording van medewerkers en de naleving van beleid in de praktijk.	Er mag meer urgentie en betrokkenheid getoond worden in de vorm van bijvoorbeeld bestuurlijke vragen, het vrijmaken van budget en gelegenheid voor overleg en presentaties.

3.2 Overzicht van de bevindingen

3.2.1 Beleid

Het 'Informatiebeveiligingsbeleid gemeente Lingewaard (versie 2, 14-06-2021)' vormt de basis voor informatiebeveiliging bij de gemeente. Het beleid is vastgesteld en getekend, tevens is er sprake van versiebeheer als verantwoordelijkheid van de CISO. Het beleid is volledig en neemt de lezer mee in zowel de nut en noodzaak van informatiebeveiliging, als de verschillende risico's en genomen maatregelen binnen de gemeente. Per risico c.q. onderdeel is goed aangegeven waar de verantwoordelijkheid binnen de organisatie behoort.

Wat opvalt is dat er in enkele gevallen wordt verwezen naar verouderde normenkader; de Baseline Informatiebeveiliging Gemeenten (BIG) en dat ook de opzet van het beleid in grote lijnen overeenkomt met die van de BIG. In de gesprekken kwam naar voren dat het beleid is opgesteld in de tijd van de overgang van de BIG naar BIO (gepubliceerd in 2019), en dat er daarom overlap merkbaar is. Volgens de BIO is het vereist om het beleid periodiek te evalueren en waar nodig te actualiseren om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is[4]. Het advies luidt dan ook om het beleid aan te passen zodat deze in zijn geheel aansluit op de BIO en in het beleid op te nemen met welke frequentie het beleid wordt geëvalueerd[5].

Het beleid omschrijft een Plan, Do, Check, Act cyclus (PDCA) en ook het Information Security Management System[6] (ISMS) wordt genoemd. Hiermee geeft de gemeente aan informatiebeveiliging te zien binnen een continu verbeterproces. In praktijk beschikt de gemeente over een ISMS tool, echter wordt deze nu nog voornamelijk gebruikt als een documentenbibliotheek met bijvoorbeeld 'best practices' van toezichthouders (bijv. van de Informatiebeveiligingsdienst) en oudere documenten van de gemeente zelf. Ten tijden van het onderzoek is de tool overgedragen aan een nieuwe leverancier welke werkt aan een nieuwe inrichting. Hierdoor zou de tool meer als ondersteuning voor de ISMS organisatie moeten gaan dienen. Het streven is om het beleggen van de verantwoordelijkheden rondom dit proces, aanwijzen van actiehouders en in gang zetten van de cyclus tegen de zomer van 2023 af te ronden.

3.2.2 Wachtwoordenbeleid

In het informatiebeveiligingsbeleid wordt verwezen naar een wachtwoordenbeleid van de gemeente. Onderzoekers hebben dit betreffende document niet ter analyse ontvangen, in de plaats daarvoor werd het document '*Regeling tijd- en plaatsonafhankelijk werken'* ontvangen. Hierin wordt vermeld dat de medewerker zorgvuldig moet omgaan met de wachtwoorden die nodig zijn om contact te maken met het netwerk van de gemeente. Daarnaast is het document '*Aanvaardbaar gebruik bedrijfsmiddelen*' aangeleverd, welke gedragsregels beschrijft rondom wachtwoorden. Bij navraag tijdens het interview

[4] Zie BIO: informatiebeveiligingsbeleid 5.1.2
[5] Zie BIO: informatiebeveiligingsbeleid 5.1.1.1
[6] Zie hiervoor het Cybersecurity Woordenboek van Cyberveilig Nederland: www.cyberveilignederland.nl/woordenboek

worden enkele eisen genoemd waar wachtwoorden aan dienen te voldoen, echter hebben onderzoekers geen kennis genomen van een beleid dat deze eisen beschrijft. In de gesprekken komt naar voren dat wachtwoorden steeds minder belangrijk worden omdat de gemeente graag over wil naar biometrisch inloggen (met bijvoorbeeld vingerafdruk of irisscan). In het kader van de AVG kan men echter de medewerkers hier niet toe verplichten en zal er sprake blijven van wachtwoordgebruik. Het advies is daarom om een wachtwoordenbeleid (opnieuw) op te stellen/te herijken en de technische maatregelen hierop af te stellen zodat de beschreven wachtwoordvereisten afgedwongen worden door het systeem. Daarnaast kan het beleid bijdragen aan informatieveilig wanneer het voorschrijft wat de gemeente van medewerkers verwacht op het vlak van wachtwoorden.

3.2.3 Informatiebeveiligingsorganisatie

De informatiebeveiligingsorganisatie van de gemeente Lingewaard bestaat uit de chief information security officer (hierna genoemd: CISO), de functionaris gegevensbescherming (hierna genoemd: FG), een privacy officer (hierna genoemd: PO), drie information security officers (ISO's). Waar nodig worden zij ondersteund door twee beveiligingsmedewerkers en een communicatiemedewerker. De CISO rapporteert aan de wethouder (portefeuillehouder) en de gemeentesecretaris (leidinggevende). De FG rapporteert op het vlak van privacy rechtstreeks aan het directieteam. De functies van FG is parttime ingevuld, de functionaris is tevens parttime juridisch adviseur. Zowel de FG als de PO rapporteren aan de teammanager Juridische zaken.

Er is een periodiek informatiebeveiligingsoverleg, geleid door de CISO, waar de gehele informatiebeveiligingsorganisatie bij aansluit. De FG, PO en de CISO hebben daarnaast wekelijks overleg. Rollen en functies binnen de informatiebeveiligingsorganisatie zijn geformaliseerd en het is duidelijk waar verantwoordelijkheden liggen.

De verantwoordelijkheid voor de uitvoer van het informatiebeveiligingsbeleid ligt, conform BIO, bij de teammanagers en directie, waarbij zij ondersteund worden door de ISO's. Daar waar nodig, wordt er geëscaleerd naar de CISO. De CISO is zich bewust van de nodige functiescheiding en probeert dit in praktijk zo goed mogelijk vorm te geven door de verantwoordelijkheid zoveel mogelijk binnen de organisatie te beleggen.

Naast de interne informatiebeveiligingsorganisatie is er een nauwe samenwerking met gemeente Overbetuwe. Gemeente Lingewaard is verantwoordelijk voor de ICT van gemeente Overbetuwe. Gemeente Overbetuwe is verantwoordelijk voor de belastingen van de gemeente Lingewaard. De CISO's van beide gemeentes hebben periodiek overleg en nemen tevens voor elkaar waar in het geval van afwezigheid.

3.2.4 Verantwoording

Jaarlijks legt de gemeente verantwoording af op het vlak van informatieveiligheid door het uitvoeren van de ENSIA audit. Binnen de gemeente Lingewaard is de CISO belegd met deze taak. Vervolgens wordt de ENSIA door een externe auditor gecontroleerd, de uitkomsten worden opgenomen in de collegeverklaring.

Intern rapporteert de CISO vanuit het IB overleg twee keer per jaar aan de directie en één keer per jaar aan het college over ontwikkelingen, trends en behoeften vanuit informatiebeveiliging. Vanwege een samenloop van omstandigheden, zoals COVID-19 en een tijdelijke afwezigheid van de CISO, is er een periode geen IB-overleg geweest, waardoor er geen recente rapportages beschikbaar zijn (onderzoekers hebben rapportages ontvangen uit 2021). Ten tijden van het onderzoek vindt het IB-overleg wel weer plaats[7]. Recent is besloten om, in plaats van eens per kwartaal, twee keer per jaar, gezamenlijk met de privacy organisatie, te rapporteren naar management en directie.

3.2.5 Risicoanalyse

Waar de BIG meer gericht was op het treffen van maatregelen, legt de BIO meer de nadruk op risicomanagement. Sinds de overgang naar de BIO ligt er binnen de gemeente dan ook meer de nadruk op risicoanalyses. De verantwoordelijkheid voor deze risicoanalyses ligt bij de teammanagers, de CISO heeft hierbij een adviserende en ondersteunende rol, maar voert de analyses niet uit. Hierdoor is de functiescheiding in theorie goed gewaarborgd. In de praktijk komt echter naar voren dat de teams deze verantwoordelijkheid nog niet in alle gevallen op zich nemen. Uit de interviews blijkt dat de analyses voor de onderdelen als ICT, Burgerzaken, Sociaal domein, VTH (Vergunningen, toezicht en handhaving) en facilitair (grotendeels) gemaakt zijn. Het voltooien van de overige risicoanalyses is een lopend proces en betekend vooralsnog minder zicht op risico's en eventuele nodige maatregelen. Gebrek aan bewustzijn c.q. urgentie, onvoldoende capaciteit, gebrek aan budget of een combinatie van deze factoren zorgen ervoor dat er verschillen zijn in hoe de verantwoordelijkheden rondom informatiebeveiliging binnen de teams worden opgepakt.

3.2.6 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 Lingewaard hanteert de GIBIT inkoopvoorwaarden (Vereniging Nederlandse Gemeenten), waarin onder meer geheimhouding, privacybescherming en aansprakelijkheid zijn geregeld bij de aankoop van IT producten/diensten. Binnen de gemeente zijn er twee inkoopadviseurs welke adviseren en begeleiden t.a.v. het verloop van aanbestedingen. Het proces binnen het zaaksysteem is zo ingericht dat zij betrokken worden bij investeringen boven €50.000,-. Investeringen onder €20.000,- hoeven niet te worden geregistreerd in het zaaksysteem. Het eventuele gebruik van software binnen de gemeente, die niet bekend is bij de informatiebeveiligingsorganisatie en die mogelijk niet voldoen aan de veiligheidseisen (Schaduw IT), is hiermee een reëel risico.

[7] Uit de ambtelijke afstemming blijkt dat tevens het overleg tussen de IB-organisatie (CISO, FG en PO) en de portefeuillehouder op het vlak van informatiebeveiliging en privacy recentelijk weer is opgepakt.

Net als bij de eerder genoemde risicoanalyses, ligt ook bij inkoop en leveranciersselectie een grote verantwoordelijkheid bij de teams zelf. De inkoopadviseurs geven advies over het inkoopproces, echter zijn niet verantwoordelijk voor de inhoudelijke beoordeling van de informatiebeveiliging van het product/dienst. Het inkoopproces is zodanig ingericht dat teams zelf met een adviesvraag dienen uit te reiken naar de CISO of de FG/PO. Binnen de organisatie is er echter geen proces waarin wordt geborgd dat de CISO en/of FG/PO meekijkt met deze inhoudelijk beoordeling. Uit de interviews blijkt dat de informatiebeveiligingsorganisatie niet altijd óf soms te laat wordt betrokken bij inkooptrajecten en leveranciersselecties. 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 te voldoen aan de minimale gestelde kwaliteit op het vlak van informatiebeveiliging.

Om te borgen dat tijdens de looptijd van een contract de leverancier blijft voldoen aan de overeengekomen informatiebeveiligingseisen, is het raadzaam om deze in praktijk (periodiek) te toetsen. Het informatiebeveiligingsbeleid vermeld een “right to audit”, waarmee de gemeente het recht heeft om dit (eventueel via een externe auditor) te doen. In praktijk wordt hier echter geen gebruik van gemaakt en uit interviews blijkt dat het binnen de organisatie niet duidelijk is wie hiervoor verantwoordelijk is. Het advies is om de verantwoordelijkheid te beleggen en deze controle op te nemen in het leveranciersmanagementproces.

3.2.7 Incidentmanagement

De BIO heeft een focus op risicomanagement en stelt daarom ook eisen aan het continuïteitsbeheer van een gemeente[8]. Het informatiebeveiligingsbeleid van de gemeente Lingewaard verwijst, conform deze eisen, naar een eigen Business Continuity Management (BCM) plan[9]. Onderzoekers hebben deze echter niet ter beoordeling ontvangen. Uit gesprekken blijkt dat er momenteel geen (actuele) continuïteitsplannen zijn, en dat deze ten tijden van het onderzoek worden opgesteld c.q. herzien. Onderzoekers hebben wel verschillende documenten ontvangen met de te nemen stappen in het geval van een informatiebeveiligingsincident/datalek.

Tot voor kort was de burgemeester portefeuillehouder aangaande informatiebeveiliging, echter omdat zij in het geval van calamiteiten ook de voorzitter is van het crisisteam, is onlangs de wethouder als nieuwe portefeuillehouder benoemd. Buiten deze voorzittersrol is de verdere samenstelling van een crisisteam, bij gebrek aan een BCM plan, niet geformaliseerd[10]. Indien zich een cybercrisis aandient wordt er ad-hoc een gelegenheidsteam opgericht. De (jaarlijkse) oefening (zoals beschreven in het informatiebeveiligingsbeleid) vindt in de praktijk niet plaats.

---

[8] Zie BIO: Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer 17.1

[9] Zie hoofdstuk 10 van het informatiebeveiligingsbeleid van de Gemeente Lingewaard

[10] Nav ambtelijke afstemming hebben onderzoekers een presentatie ontvangen (Presentatie wethouders crisisbeheersing piket.ppt) waarin het Gemeentelijk Beleidsteam wordt beschreven. Het is uit het document niet op te maken of dit ook daadwerkelijk geformaliseerd is.

Het advies is om crisismanagement/continuïteitsplannen op te stellen waarin de crisisteams met taken en bevoegdheden worden omschrijven. Het is daarnaast aan te raden duidelijke crisis scenario's met bijbehorende actieplannen te omschrijven, welke periodiek (jaarlijks) worden geëvalueerd. Om tot een optimale situatie te komen, dienen deze plannen en het managen van calamiteiten ook periodiek te worden geoefend.

3.2.8 Privacy

De privacyorganisatie bij de gemeente Lingewaard bestaat uit een (parttime) FG en een (parttime) PO. De FG heeft een toezichthoudende rol, de PO is adviserend richting de organisatie. Uit de gesprekken blijkt dat strikte functiescheiding in praktijk soms niet haalbaar is, gezien de praktische prioriteiten en hulpvragen vanuit de organisatie. De organisatie worstelt soms nog met de verantwoordelijkheden op het vlak van privacy, zowel inhoudelijk als op het vlak van capaciteit. Veel van de verantwoordelijkheden komen daarom nog bij de PO en FG terecht, waar deze eigenlijk behoren bij de teams. Door deze praktische omstandigheden ligt de focus vooral op ad-hoc en reactieve werkzaamheden, waardoor er minder ruimte is voor meer overstijgende of strategische thema's zoals beleid, bewustwording en het uitvoeren van risicoanalyses.

Onderzoekers hebben het 'Privacybeleid Gemeente Lingewaard' ter analyse ontvangen. Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente en richt zich op zowel persoonsgegevens van inwoners en andere burgers als medewerkers en (keten)partners. Het beleid omschrijft voornamelijk de (wettelijke) kaders, uitgangspunten en definities. Hiermee is het document meer (abstract) beschrijvend dan (praktisch) voorschrijvend, waardoor het voor de medewerkers in praktijk minder bruikbaar is. Het advies luidt dan ook om een praktische vertaalslag van de wettelijke opdracht te maken, zodat deze faciliterend is aan de uitvoering hiervan. Daarnaast is er geen sprake van versiebeheer en is het document niet aantoonbaar vastgesteld/getekend[11]. De naam van de FG en contactgegevens zijn niet genoemd en ook de rol van privacy officer wordt niet vermeld in het stuk. Hieruit maken de onderzoekers op dat het document niet up to date is, wat wordt bevestigd in de interviews. Het advies is om het beleid te actualiseren naar de huidige situatie en uit te breiden met een praktische kaders en richtlijnen voor de praktijk.

Op het vlak van privacy kan de organisatie nog groeien aan 'volwassenheid'. Er mogen stappen gezet worden qua eigen verantwoordelijkheid en bewustwording binnen de teams en het beleid dient geactualiseerd en aangevuld te worden. Daarnaast moeten processen meer in kaart worden gebracht en beter ingebed worden in de praktijk. Voorbeelden hiervan zijn het bijwerken van het verwerkingenregister en de uitvoer van dpia's[12].

[11] Uit ambtelijke afstemming blijkt dat het beleid is vastgesteld en getekend door college (https://lokaleregelgeving.overheid.nl/CVDR485347). Neemt niet weg dat, wanneer dit niet in het interne document vermeld is, het onduidelijk is voor de organisatie.

[12] Zie hiervoor het Cybersecurity Woordenboek van Cyberveilig Nederland: www.cyberveilignederland.nl/woordenboek

3.2.9 Logisch toegangsbeleid

Om te kunnen waarborgen dat informatie een passend beschermingsniveau krijgt, dienen beveiligingsmaatregelen te zijn afgestemd met van het type data en het belang ervan voor de organisatie[13]. Onderzoekers hebben kennis genomen van de 'Richtlijnen dataclassificatie 2022' van de gemeente. Een volledig document dat duidelijke richtlijnen geeft. De werking in de praktijk mag echter nog beter ingebed worden. Zo is bijvoorbeeld de door onderzoekers ontvangen documentatie in geen geval voorzien van een classificatieniveau.

Naast dat dataclassificatie belangrijk is bij de selectie van juiste beveiligingsmaatregelen, draagt het tevens bij aan correct beheer van toegangsrechten binnen de gemeente. Om te voorkomen dat onbevoegden toegang krijgen tot informatie, is het wenselijk om de toegang te baseren op verantwoordelijkheden en/of functie[14]. Binnen het sociaal domein zijn de autorisatieprofielen al in kaart gebracht en worden deze tevens tussentijds gecontroleerd. Op andere plekken in de organisatie worden autorisaties bijvoorbeeld geselecteerd op basis van bestaande rechten bij collega's. Om de autorisatieprofielen te kunnen maken zullen er risicoanalyses gemaakt moeten worden per team. De verantwoordelijkheid hiervoor ligt bij het management, met ondersteuning van P&O. De verantwoordelijkheid voor het maken van de uiteindelijke autorisatieprofielen mag in de praktijk duidelijker worden belegd.

Uit de interviews komt naar voren dat de gemeente soms nog minder goed zicht heeft op welke informatie zich waar bevindt. In het kader van bovenstaande processen van classificatie en beheer van toegangsrechten is het van belang om hier zicht op te krijgen.

3.2.10 Bewustwording medewerkers

De BIO stelt dat de organisatie een verantwoordelijkheid heeft voor het bewustzijn, opleiding en training van medewerkers ten aanzien van informatiebeveiliging[15]. De gemeente Lingewaard heeft dit vormgegeven in een 'I-bewustzijnscampagne', een e-learning op het gebied van informatiebeveiliging en privacy. Elke (nieuwe) medewerker (langer dan 3 maanden in dienst) is verplicht om de e-learning te volgen. Dit geldt tevens voor medewerkers vanuit inhuur/uitvoeringsorganisaties. De privacy officer rapporteert de deelname aan het management, het management is verantwoordelijk voor de opvolging bij medewerkers. Intranet wordt tevens als medium ingezet om medewerkers te informeren over relevante thema's. De gemeente is voornemend om in de bewustwordingscampagne meer te gaan inzetten op social engineering, aangezien men voorbeelden hiervan steeds vaker ziet terugkomen in de praktijk. E-learnings zijn een efficiënte manier van kennisdeling en bewustwording. Het einddoel is echter informatieveilig gedrag terug te zien bij de medewerkers. Kennis en bewustzijn zijn geen garantie voor het daadwerkelijke gedrag in de praktijk. Om het leereffect te versterken kan de gemeente de e-learnings nog combineren met oefening in de praktijk, bijvoorbeeld in de vorm van periodieke mail-phishing tests.

[13] Zie BIO: Informatieclassificatie 8.2
[14] Zie BIO: Toegangsbeveiliging van systeem en toepassing 9.4.1.2
[15] Zie BIO: Veilig personeel 7.2.2

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.

3.2.11 Organisatiecultuur

De omgang met informatiebeveiliging kan men zien als onderdeel van een organisatiecultuur. De organisatiecultuur is het geheel aan gedeelde waarden, overtuigingen, aannames en patronen van gedrag binnen een organisatie. (Nieuwe) Medewerkers kijken voornamelijk naar het gedrag van leidinggevenden om te bepalen wat de gedeelde waarden, overtuigingen, aannames en patronen van gedrag binnen de organisatie zijn. Het bestuur en leidinggevenden hebben daarmee een belangrijke voorbeeldfunctie. Tijdens de interviews komt naar voren dat er gedurende de laatste jaren minder wisselwerking is tussen bestuur en organisatie op het vlak van informatiebeveiliging en privacy. Verzoeken om presentaties te houden binnen college en raad worden afgehouden, overleggen met de portefeuillehouder vinden geen doorgang en er worden nauwelijks tot geen bestuurlijke vragen gesteld[16]. Een andere graadmeter voor het bewustzijn is de bereidheid voor het vrijmaken van budget. Het voor informatiebeveiliging gealloceerde budget (€25.000,-) is slechts toereikend voor de ENSIA en een aantal technische tests[17]. Voor overige maatregelen dient het budget vanuit de teams te komen. De bewustwording en het managen van risico's gebeurt nu voornamelijk 'bottum up'. Duidelijke betrokkenheid en bereidheid vanuit bestuur en leidinggevenden zal helpen om de bewustwording en informatiebeveiliging te bestendigen binnen de organisatiecultuur.

4. Mens

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 is getest door middel van 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.

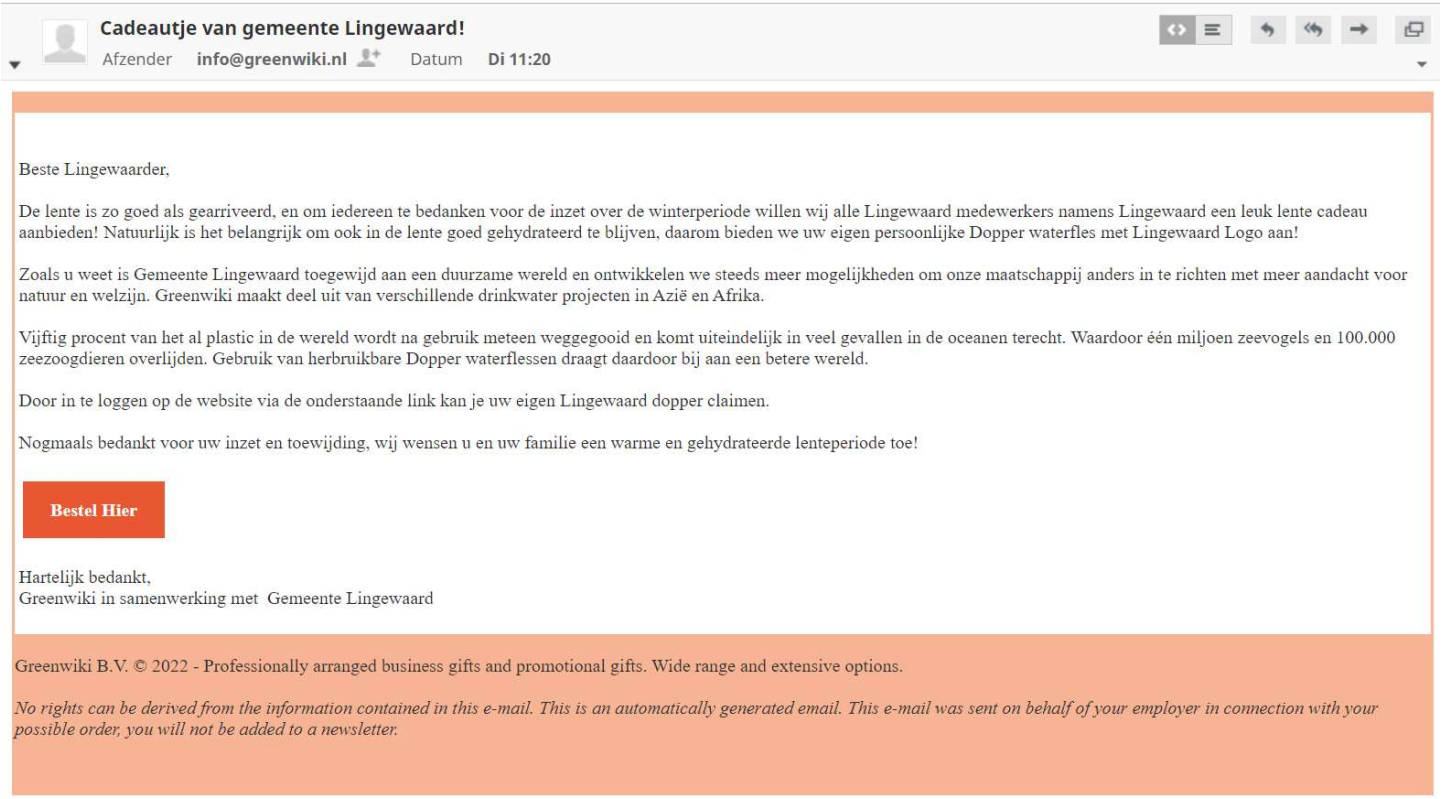
In dit hoofdstuk worden de bevindingen in detail beschreven en zijn schermafdrukken en foto's opgenomen ter illustratie.

[16] Uit ambtelijke afstemming blijkt dat met de verschuiving van de portefeuilles (januari 2023) er beter contact is tussen college en de informatiebeveiligingsorganisatie en dat het overleg met de portefeuillehouder weer doorgang vindt. Men ervaart dat de nieuwe portefeuillehouder betrokken en geïnteresseerd is in informatiebeveiliging en privacy.

[17] Uit de ambtelijke afstemming blijkt dat er in 2022 ruim €600.000,- is geïnvesteerd in nieuwe ICT. Onderzoekers hebben deze investering niet onderzocht, te verwachten is dat dit tevens ten goede is gekomen aan de informatiebeveiliging binnen de gemeente. Dit neemt echter niet weg dat er weinig gealloceerd budget is voor informatiebeveiliging, waardoor investeringen op dit vlak afhankelijk zijn van andere prioriteiten binnen de organisatie en teambudgetten.

4.1 Mail-phishing test

Gedurende het onderzoek traject hebben Onderzoekers van Hoffmann in overleg met gemeente Lingewaard een mail-phishing verstuurd naar alle medewerkers. De e-mail is op 20 maart 2023 om 09:08 uur verstuurd en bevatte de volgende inhoud:



Cadeautje van gemeente Lingewaard!

Afzender **info@greenwiki.nl** Datum **Di 11:20**

Beste Lingewaarder,

De lente is zo goed als gearriveerd, en om iedereen te bedanken voor de inzet over de winterperiode willen wij alle Lingewaard medewerkers namens Lingewaard een leuk lente cadeau aanbieden! Natuurlijk is het belangrijk om ook in de lente goed gehydrateerd te blijven, daarom bieden we uw eigen persoonlijke Dopper waterfles met Lingewaard Logo aan!

Zoals u weet is Gemeente Lingewaard toegewijd aan een duurzame wereld en ontwikkelen we steeds meer mogelijkheden om onze maatschappij anders in te richten met meer aandacht voor natuur en welzijn. Greenwiki maakt deel uit van verschillende drinkwater projecten in Azië en Afrika.

Vijftig procent van het al plastic in de wereld wordt na gebruik meteen weggegooid en komt uiteindelijk in veel gevallen in de oceanen terecht. Waardoor één miljoen zeevogels en 100.000 zeezoogdieren overlijden. Gebruik van herbruikbare Dopper waterflessen draagt daardoor bij aan een betere wereld.

Door in te loggen op de website via de onderstaande link kan je uw eigen Lingewaard dopper claimen.

Nogmaals bedankt voor uw inzet en toewijding, wij wensen u en uw familie een warme en gehydrateerde lenteperiode toe!

Bestel Hier

Hartelijk bedankt,
Greenwiki in samenwerking met Gemeente Lingewaard

Greenwiki B.V. © 2022 - Professionally arranged business gifts and promotional gifts. Wide range and extensive options.

No rights can be derived from the information contained in this e-mail. This is an automatically generated email. This e-mail was sent on behalf of your employer in connection with your possible order, you will not be added to a newsletter.

Figuur 1: Mail phishing met als onderwerp: 'Cadeautje van gemeente Lingewaard!'

Figuur 2: Phishing website gemeente Lingewaard

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.

De eerste gebruikersnaam met bijbehorend wachtwoord is diezelfde dag ontvangen om 18:35 uur. De laatste persoonlijke inloggegevens zijn ontvangen op 22 maart om 09:01 uur.

Door zowel zelflerende technische veiligheidsmaatregelen als door verschillende meldingen van medewerkers bij de servicedesk, is de mail snel opgevallen, ondervangen en op een ‘black-list’ gezet. Hierdoor is de e-mail niet bij iedereen binnengekomen. Helaas is het niet duidelijk door hoeveel medewerkers de mail wel is ontvangen. Op 22 maart, aan het einde van de dag, is er een bericht van de servicedesk uitgegaan naar de rest van de organisatie om te informeren over de mail-phishing. Door bovenstaande alertheid en acties is het aantal gebruikers dat op de link heeft geklikt en de gebruikersnaam en wachtwoord hebben ingevuld, relatief beperkt gebleven.

Er zijn in totaal 14 unieke bezoekers geregistreerd waarvan 5 gebruikers hun gebruikersnaam en wachtwoord hebben ingevuld. Het wachtwoord is niet opgeslagen, ook zijn de inloggegevens niet getest op geldigheid. De mail-phishing actie is gestopt op 23 maart 2023 omstreeks 15:00.

De resultaten laten zien dat de organisatie in combinatie met de technische maatregelen, relatief goed in staat is om mail-phishing te herkennen en onderscheppen. Om een goed beeld te krijgen hoe het is gesteld met het bewustzijn van medewerkers (technische maatregelen uitgesloten), raden wij de organisatie aan om een dergelijke mail-phishing test nogmaals uit te voeren, echter deze van tevoren te ‘white-listen’ zodat de mail bij iedereen aankomt.

Aanbevelingen

- Blijf medewerkers voortdurend bewust maken van mail-phishing-technieken door praktijktoetsen, bewustwordingsprogramma’s en het delen van actuele voorbeelden;
- Communiceer duidelijk wat er van medewerkers wordt verwacht aangaande informatieveilig gedrag;
- Zorg ervoor dat medewerkers weten welke domeinnamen van de gemeente zijn en dat men geen gebruik moet maken van andere domeinen.

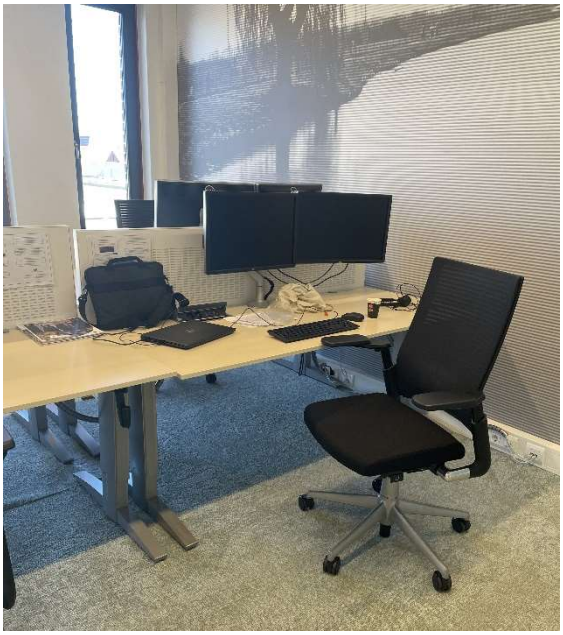
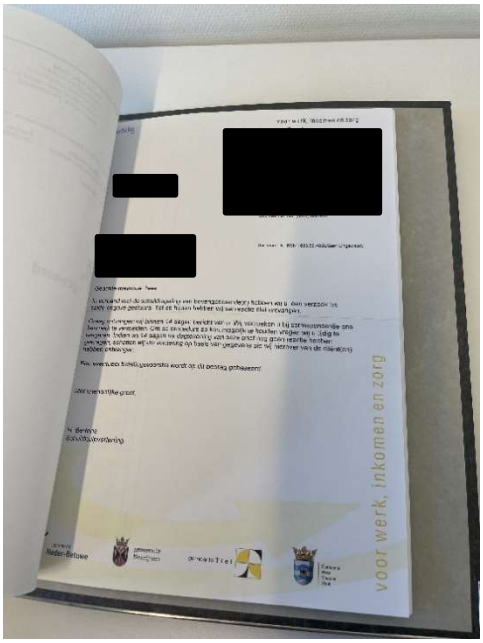
4.2 Mystery guest bezoek

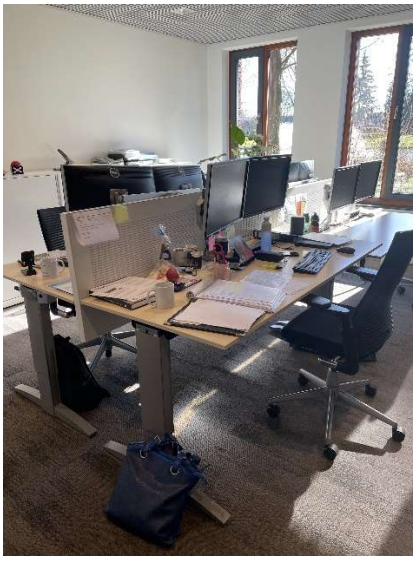
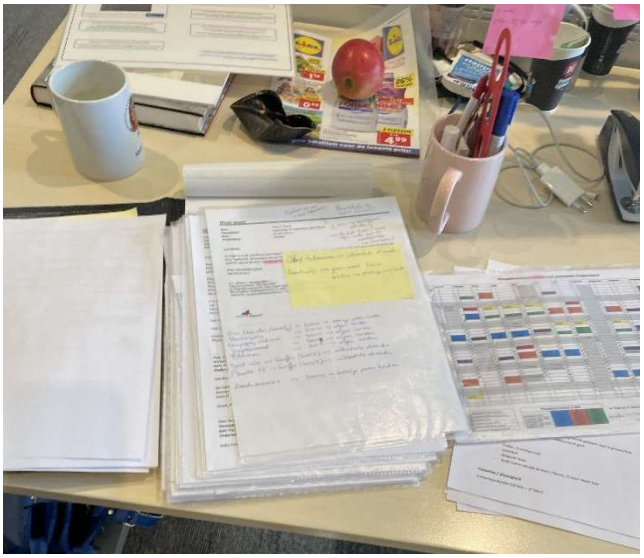
Op dinsdag 28 februari 2023 heeft een Mystery Guest van Hoffmann, hierna te noemen ‘MG’, een fysieke inlooptest verricht bij het gemeentehuis van de gemeente Lingewaard (Kinkelenburglaan 6, 6681 BJ Bemmel). Hieronder een overzicht van de gebeurtenissen.

Tijd	Omschrijving activiteit
12:32	MG parkeert haar auto op het parkeerterrein op het buitenterrein van het gemeentehuis. MG kijkt vanuit de auto waar de ingangen van het gebouw zijn. MG ziet een ingang met een tourniquet waar mensen naar binnen- en buiten gaan. MG ziet dat de tourniquet voor één persoon is en dat men een pas aanbiedt.
12:37	MG stapt uit en ziet een persoon van het kantoor richting een auto lopen. MG spreekt de persoon aan, zegt een afspraak te hebben en vraagt waar de ingang is. De persoon blijkt een medewerker te zijn en geeft aan dat de hoofdingang om de hoek is en dat de ingang met de tourniquet de personeelsingang is. MG bedankt de medewerker en loopt richting de hoofdingang.  *Foto 1: Foto vanaf parkeerplaats met zicht op de personeelsingang.*
12:41	MG ziet een mogelijke medewerker richting de hoofdingang lopen. MG loopt achter deze persoon aan en loopt langs de beveiliging (aan rechterzijde). MG wordt niet aangesproken en blijft de medewerker volgen. De medewerker slaat rechtsaf en opent de eerste deur zonder pas. MG volgt en belandt in de algemene vergaderruimten. Tegenover deze deur zit een andere deur met een paslezer. De medewerker opent deze deur met een pas en MG volgt wederom. MG bevindt zich op dit moment in de beveiligde zone. MG heeft de indruk dat zij door één of enkele personen wordt gezien, maar wordt niet aangesproken.

Tijd	Omschrijving activiteit
12:48	MG loopt naar de eerste etage, slaat linksaf en daarna rechts en komt in een algemene ruimte. Aan haar linkerkant ziet ze een afdeling met 'Service desk' en ziet zij een aantal kluizen met cijfercodes. MG loopt rechtdoor, hangt haar jas op en besluit plaats te nemen op een van de, naar haar vermoeden, algemene werkplekken. Hier opent MG haar laptop om de indruk te wekken dat zij aan het werk is. MG heeft de indruk dat zij door één of enkele personen wordt gezien, maar wordt niet aangesproken.  *Foto 2 & 3: Kluisjes eerste etage en zitplaats algemene werkplek.*
12:55	MG besluit om de eerste etage verder te verkennen en loopt wederom langs de service desk en slaat linksaf. Hier staat een printer, waarin geen (vertrouwelijke) documentatie wordt aangetroffen. Tevens staat een vertrouwelijke papierbak welke afgesloten is. MG ziet ook de inkomende post liggen, welke vrij toegankelijk is. MG komt diverse medewerkers tegen. Het valt MG op dat vrijwel alle medewerkers hun pas zichtbaar dragen. MG wordt niet aangesproken op het feit dat zij geen pas draagt.

Tijd	Omschrijving activiteit
	  *Foto 4 en 5: Printer en postvakken.*  *Foto 6: Vertrouwelijk papierbak (afgesloten).*
12:59	MG verkent de eerste etage. Veel van de werkplekken zijn bezet waardoor MG niet ongezien de documentatie op werkplekken kan inzien. Op de onbemande werkplekken valt het op dat de laptops allemaal vergrendeld zijn. MG ziet wel onbemande werkplekken waar documentatie op tafel ligt. Zij heeft de indruk dat zij door één of enkele personen wordt gezien, maar wordt niet aangesproken.

Tijd	Omschrijving activiteit
13:10	MG besluit naar de tweede etage te bewegen. Zij neemt de lift naar boven en heeft geen pas nodig. Hier zijn minder medewerkers aanwezig dan op de eerste verdieping. Veel van de werkplekken zijn onbemand.  *Foto 7: Onbemande werkplek tweede etage.*
13:11	MG loopt door tot het einde van de gang en betreedt een werkruimte waar geen medewerkers aanwezig zijn. Aan haar rechterkant staat een archiefkast welke niet afgesloten is. MG treft in deze kast mappen aan, met daarin verschillende documenten.   *Foto 8 & 9: Documenten in open archiefkast.*

Tijd	Omschrijving activiteit
13:14	MG loopt de kamer uit richting de liften en verplaatst zich naar de begane grond. Ze loopt door de kantoorruimte en treft een printer aan, zonder documentatie. MG ziet onbemande werkplekken waar de laptops wederom zijn vergrendeld, maar waar wel documentatie op het bureau ligt. MG verplaatst zich over de gang met als doel om de linkervleugel van het gebouw te verkennen. MG komt diverse medewerkers tegen en krijgt zelf een broodje aangeboden. MG wordt niet aangesproken door de medewerkers met de vraag wie zij is of waarom zij geen pas draagt.
13:18	MG bevindt zich buiten de beveiligde zone en wacht zo onopvallend mogelijk bij een koffiehoek tot zij iemand ziet die de linkerkant van het gebouw betreedt. Een medewerker loopt langs, richting de deur, biedt zijn pas aan en loopt naar binnen. De deur staat lang genoeg open voor MG om mee naar binnen te lopen. MG slaat rechtsaf en betreedt een grote vergaderzaal. Het valt MG op dat de deur, waar zij doorheen kwam, nog steeds niet dicht is. De medewerker, welke zij gevolgd was, had zijn pas aangeboden bij de volgende deur aan de rechterkant. MG verplaatst zich richting deze deur, omdat zij vermoed dat deze ook nog openstaat. MG kan haar voet nog tussen de deur plaatsen en betreedt zo de beveiligde ruimte. MG loopt door de ruimte heen en loopt naar achteren. Zij leest op het naambordje van een vergaderruimte het woord ‘burgemeester’, in de ruimte is een vergadering bezig. MG heeft de indruk dat zij door één of enkele personen wordt gezien, maar wordt niet aangesproken.
13:30	MG besluit terug te lopen om de andere kant van de linkervleugel te verkennen. Zij ziet onderweg nog een aantal werkplekken die onbemand zijn, maar waar wel documenten liggen.   *Foto 10 & 11: Onbemande werkplekken met documenten.*

Tijd	Omschrijving activiteit
13:34	De deur naar de andere kant van de linkervleugel is beveiligd, om toegang te krijgen is een pas nodig. Het valt MG op dat de deur niet goed dichtzit. MG duwt tegen de deur en krijgt zo toegang tot de beveiligde zone. MG ziet dat het slot waarschijnlijk onbruikbaar is.   *Foto 13 & 14: deur naar beveiligde zone & slot dat waarschijnlijk onbruikbaar is.*
13:35	MG loopt op de begane grond, slaat linksaf gaat vervolgens rechtdoor en komt aan bij de entree. MG besluit daarom terug te lopen. MG een ruimte waar men aan het werk is en waar een pasje voor nodig is om binnen te komen. MG besluit door te lopen naar de eerste etage.
13:40	Op de eerste etage komt MG aan bij de eerder beschreven ruimtes. Kort daarop wordt de inlooptest beëindigd.

5. Techniek

Initieel was er afgestemd dat er een technisch onderzoek (pentest) zou plaatsvinden waarbij getoetst zou worden middels een interne en externe pentest, of de informatiesystemen van de gemeente voldoende beveiligd zijn tegen het risico van hacken. Gezien het feit dat er recentelijk door een andere derde partij een pentest is uitgevoerd op het netwerk van de gemeente, is er in overleg met de gemeente en de rekenkamer en mede gezien deze overlap, afgestemd dat het draadloze netwerk van de gemeente getest zou worden, waarbij onder andere gekeken diende te worden of er voldoende segmentatie is tussen deze netwerken.

Deze pentest heeft plaatsgevonden middels een test op locatie, waarbij heeft een medewerker van Hoffmann zowel met als zonder voorinformatie de volgende penetratietesten heeft uitgevoerd:

- Wifi penetratietest van het medewerkers Wifi-netwerk;
- Wifi penetratietest van het gasten Wifi-netwerk.

De onderzoekers zijn er in geslaagd om ongeautoriseerde toegang te verkrijgen tot het interne draadloze **'Lingewaard-Medewerkers'** netwerk van de gemeente. Het was voor onze onderzoeker mogelijk om met een onderschept account in te loggen op het interne draadloze **'Lingewaard-Medewerkers'**. Dit vormt een mogelijkheid om het domein/netwerk over te nemen.

Gezien de beperkte scope (vanwege de eerder uitgevoerde pentest), is dit risico verder niet door Hoffmann getoetst en heeft onze onderzoeker de mogelijkheden die hij potentieel had met dit onderschepte account, verder niet onderzocht. Echter indien een account met geldige rechten kan worden onderschept, zoals onze onderzoeker heeft kunnen doen, wordt de kans vergroot op een verdere succesvolle aanval op het netwerk van de gemeente.

Verder was het onderzochte interne **gasten** netwerk voldoende gesegmenteerd en voldoende beveiligd tegen hacken.

Tijdens het onderzoek is één kritieke kwetsbaarheden geconstateerd die hierop direct telefonisch is besproken met de CISO.

De penetratietesten hebben plaatsgevonden op maandag 6 maart 2023.

5.1 Rapportage penetratietesten

De detailbevindingen en specifieke aanbevolen maatregelen van de penetratietest zijn beschreven in het document: "Pentestrapport Lingewaard.docx. Om te voorkomen dat kwaadwillenden de geconstateerde kwetsbaarheden kunnen misbruiken, is dit document als geheim geclassificeerd.

Disclaimer

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

Harald Langmar,
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, 27 juli 2023

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

6.2 Overzicht geïnterviewden

Functie	Datum interview
CISO	24 januari 2023
Privacy adviseur	24 januari 2023
Inkoopadviseur	26 januari 2023
Functionaris gegevensbescherming	27 januari 2023
ISO IV	6 maart 2023
Wethouder	13 maart 2023

6.3 Overzicht bestudeerde documenten

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

Document	Versie	Datum
Kwartaalrapportage IB en Privacy Q1-2021	-	-
Datalekproces	-	-
Kwartaalrapportage IB en P Q2-2021	-	-
309520 Informatiebeveiligingsbeleid gemeente Lingewaard – Getekend	2.0	14-06-2021
Proces informatiebeveiligingsincidenten	-	-
Kwartaalrapportage IB en P Q3-2021	-	-
Privacybeleid en reglement Lingewaard	-	-
270435 Kaders op gemeentelijke informatie	-	-
Risico Heatmap Cluster IV – Automatisering – DT	-	-

Document	Versie	Datum
Voortgangsrapportage invoeringsplan IV 20221104	-	-
8.1.3 Aanvaardbaar gebruik bedrijfsmiddelen 2020-04-08	-	08-04-2020
Regeling tijd- en plaatsonafhankelijk werken 21102014	-	18-09-2014
Richtlijnen dataclassificatie 2022	1.0	10-11-2022
071221 def EHRM systeem	4.0	07-12-2021
164088 notitie Governance Bijlage voor college	-	-
301121 def DPIA Peutermonitor	4.0	01-11-2021
DPIA getekend door FG en PBB	1.4	04-10-2021
Proces Incident Management	1.0	25-11-2022
Proces melden beveiligingsincidenten en datalekken	-	-
Printscreen datalekmelding	-	-


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