Rapport onderzoek Informatiebeveiligingscultuur Gemeente Almelo

Dossiernummer 22404067

Onderzoek in opdracht van

Rekenkamer gemeente Almelo

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

Samenvatting

De rekenkamer heeft laten onderzoeken hoe het staat met de informatiebeveiligingscultuur binnen de gemeente Almelo. De gemeente heeft veel informatie van inwoners, ondernemers en medewerkers. Vaak gaat het om gevoelige informatie, informatie waarvan je niet wilt dat iedereen deze kan bekijken of wijzigen, zoals bsn-nummers, adresgegevens, informatie over vergunningen of informatie over persoonlijke situaties en zorgverlening. Het is een belangrijke taak voor de gemeente om deze informatie veilig en vertrouwd te houden. Natuurlijk wordt er techniek gebruikt om dit te doen. Maar het is daarnaast ook belangrijk dat medewerkers van de gemeente veilig omgaan met deze informatie. Dit onderzoek gaat daarom over de informatiebeveiligingscultuur; hoe mensen binnen de gemeente denken, werken en besluiten nemen met als doel informatie te beschermen. Om dit te onderzoeken zijn er verschillende gesprekken gevoerd. Medewerkers die binnen de gemeente werken aan het veilig houden van informatie hebben verteld hoe zij dit doen. Daarnaast hebben ook medewerkers van verschillende andere afdelingen en leidinggevenden verteld hoe zij denken en werken aan het veilig houden van informatie. De onderzoekers hebben ook gekeken naar de verschillende plannen en het beleid over informatiebeveiliging. Als laatste is er ook gekeken naar hoe medewerkers zich gedragen in de praktijk. De toetsen in de praktijk en interviews laten zien dat medewerkers vaak niet precies weten wat er van hen verwacht wordt om informatie veilig te houden. Veel medewerkers hebben bijvoorbeeld een inlognaam en wachtwoord op een website ingevuld nadat zij een phishing e-mail hebben ontvangen. Dit was onderdeel van de test, maar het laat zien dat veel medewerkers een phishing e-mail niet kunnen herkennen. Uit het onderzoek blijkt dat er lange tijd te weinig aandacht voor bewustzijn en training over het veilig werken met informatie is geweest. Medewerkers krijgen geen cursus of voorlichting over het onderwerp. Ook bij de leidinggevenden en bestuurders mag er meer aandacht komen voor het onderwerp. Leidinggevenden en bestuurders nemen beslissingen over hoe er met informatie gewerkt wordt. Het is daarom belangrijk dat zij goed weten wat er nodig is om informatie veilig en vertrouwelijk te houden. Daarnaast zijn leidinggevenden en bestuurders vaak een belangrijk voorbeeld voor medewerkers. Als zij laten zien dat het belangrijk is om bewust met informatie om te gaan, dan zullen medewerkers dit voorbeeld volgen. Om informatie goed te beschermen mag de gemeente meer doen aan bewustwording en aandacht voor het denken, werken en besluiten nemen met als doel de informatie te beschermen.

INHOUDSOPGAVE

1. Inleiding 4
1.1 Doelstellingen en scope 4
1.1.1 Doelstelling en onderzoeksvragen 4
1.1.2 Maturity Model Informatiebeveiliging 6
1.1.3 Aanpak en scope 6
1.2 Versiebeheer 7
2. Conclusies en advies 8
2.1 Conclusies 8
2.1.1 Hoofdvraag 8
2.1.2 Opzet 8
2.1.3 Bestaan 10
2.1.4 Werking 11
2.1.5 Rol van de raad 13
2.2 Advies 14
3. Bevindingen en aanbevelingen 16
3.1 Overzicht bevindingen en aanbevelingen 16
3.2 Toelichtingen bevindingen en aanbevelingen 18
3.2.1 Beleid 18
3.2.2 Informatiebeveiligingsorganisatie 18
3.2.3 Mensen, middelen, budget 19
3.2.4 Leiderschap & betrokkenheid Raad/College 20
3.2.5 Bewustwording 21
3.2.6 Incidentmeldingen 22
3.2.7 Wisselwerking met processen 23
3.2.8 Gedrag in de praktijk 24
3.2.8.1 Mail-phishingtest 24
3.2.8.2 Fysieke inlooptest 25
3.2.8.3 Aanbevelingen over gedrag in de praktijk 25
Disclaimer 27
4. Bijlagen 28
4.1 Maturity modelinformatiebeveiliging 28
4.2 Verloop mail-phishing test 29
4.3 Verloop fysieke inlooptest 31
4.4 Verklarende woordenlijst 32
4.5 Overzicht geïnterviewden 35
4.6 Overzicht bestudeerde documenten 36

1. Inleiding

De Rekenkamer van de gemeente Almelo (hierna genoemd: ‘de Rekenkamer’) heeft Hoffmann gevraagd een onderzoek uit te voeren naar de informatiebeveiligingscultuur bij de gemeente Almelo (hierna genoemd: ‘de gemeente’). Informatiebeveiliging beschermt de informatie binnen de gemeente tegen een breed scala aan bedreigingen door middel van organisatorische, technische en beleidsmatige maatregelen. Deze maatregelen vallen of staan echter bij het gebruik en opvolging van de gebruiker (de mens). Daarmee wordt de kwetsbaarheid voor bedreigingen voor een groot deel bepaald door het gedrag van de medewerkers van de gemeente. 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. Dit onderzoek richt zich daarom op de informatiebeveiligingscultuur binnen de gemeente Almelo, vanuit een menselijk, proces én systeemperspectief. Op basis van de bevindingen zijn de aanbevelingen in kaart gebracht welke gebruikt kunnen worden om het bewustzijnsniveau naar een hoger niveau te tillen. Dit onderzoek heeft plaatsgevonden in de periode juni t/m augustus 2024.

1.1 Doelstellingen en scope

1.1.1 Doelstelling en onderzoeksvragen

De volgende doelstelling staat in het onderzoek centraal:

Middels een nulmeting het huidige kennis- en bewustzijnsniveau van de medewerkers (inclusief college en raad) van de gemeente Almelo en de wisselwerking van menselijk gedrag met de systemen in kaart brengen en hierbij verbeteractiviteiten te benoemen die aansluiten bij de huidige bedrijfscultuur van de gemeente, om het kennis- en bewustzijnsniveau optimaal naar een hoger volwassenheidsniveau te tillen.

De hoofdvraag van dit onderzoek luidt:

- *Hoe is de staat van de informatiebeveiligingscultuur en de wisselwerking met de systemen en processen?*

De beantwoording van de hoofdvraag wordt ondersteund door deelvragen. Per deelgebied zijn de volgende deelvragen geformuleerd waar in hoofdstuk 2 antwoord op wordt gegeven:

1. Opzet

- *Welke plaats kregen cultuur en bewustwording in het beleid én de praktijk rond informatiebeveiliging?*
- *Zijn hier specifieke uitgangspunten over vastgelegd?*
- *Zijn beleid en praktijk voldoende om het hoofd te bieden aan (externe) ontwikkelingen? Heeft de gemeentelijke organisatie voldoende zicht hierop?*

- *Hoe worden de uitgangspunten van het beleid bijgesteld naar aanleiding van de praktijk? Is hier een terugkerend proces voor?*

2. Bestaan

- *Is het beleid rond bewustwording en informatiebeveiligingscultuur geoperationaliseerd?*
    - *In welke vorm en welke concrete acties zijn genomen (voorlichting, opleiding, training, instructie, voorbeeldgedrag etc)?*
    - *Is daarbij onderscheid gemaakt in doelgroepen en zo ja welke (in de organisatie, college, raad)?*
    - *Wordt periodiek geëvalueerd en op basis daarvan doorontwikkeld? Hoe gaat die evaluatie, bijvoorbeeld op basis van eventuele incidenten, in zijn werk en omvat dit contact met medewerkers?*
    - *Zijn specifieke middelen toegekend?*

3. Werking

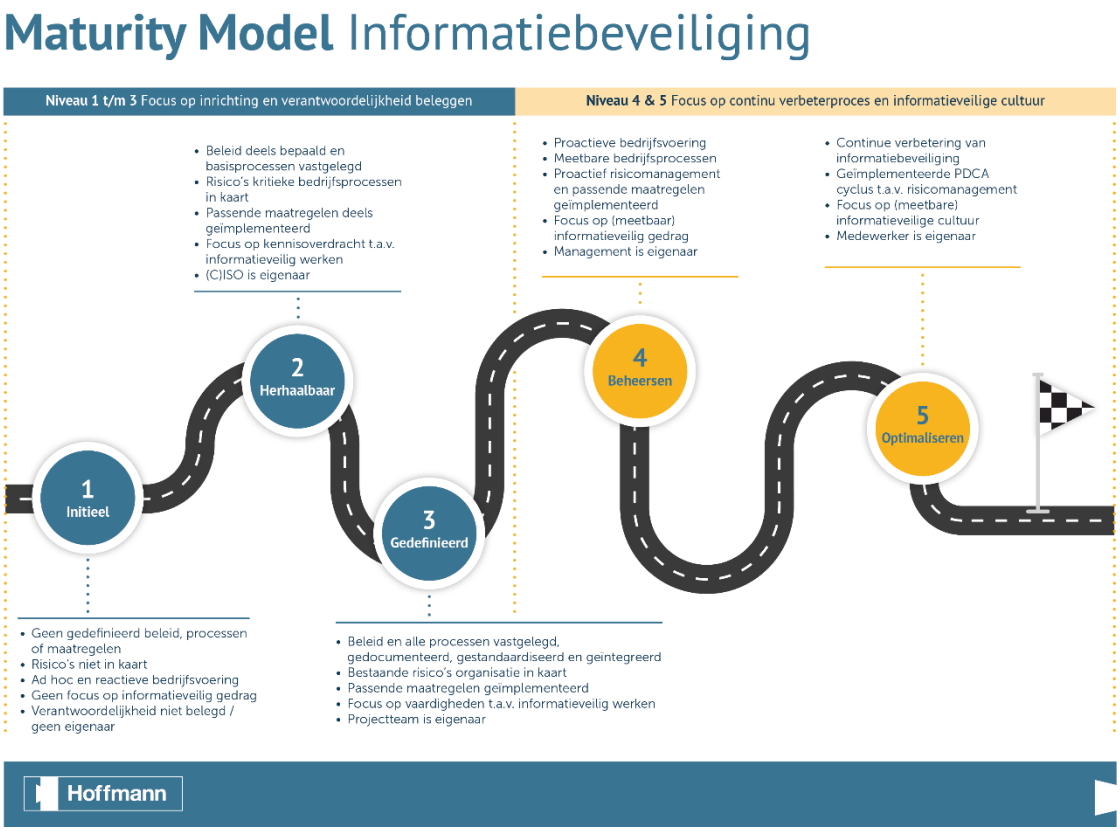
- *Wat zegt de uitkomst van de (eventuele) evaluaties over het gedrag, kennis- en bewustzijnsniveau van de medewerkers en hun wisselwerking met de systemen en processen?*
- *Wat voor bedrijfscultuur heerst binnen de gemeente rondom informatiebeveiliging? Toelichting: Het is niet het doel van dit onderzoek om de totale bedrijfscultuur te onderzoeken, de nadruk ligt op de informatiebeveiligingscultuur. Maar we willen wel oog hebben voor verband(en) van de informatiebeveiligingscultuur met de totale bedrijfscultuur.*
- *Hoe kijken raad, college en organisatie zelf naar de informatiebeveiligingscultuur en de vragen in dit onderzoek?*
- *Wat kan hier objectief over gezegd worden en aan toegevoegd worden met dit rekenkameronderzoek? Zelf denken we hierbij aan: test van bewustzijn door bijv. penetratietest, phishing mails, een audit of juist een totaal andere test van het informatieveiligheidsbewustzijn van medewerkers en hun wisselwerking met de systemen en processen.*

4. Rol van de raad

- *Hoe is de raad bij de verschillende onderdelen betrokken geweest (kaderstelling, geïnformeerd, in staat om te controleren)?*
- *Is de raad op de hoogte waar informatiebeveiliging voor staat en welke beveiligingsaspecten cruciaal zijn om in te regelen?*
- *Hoe zou de raad graag geïnformeerd willen worden als het gaat om wat informatiebeveiliging allemaal omvat?*
- *Wat mist de raad nu als het gaat om de inrichting en de borging van informatiebeveiliging?*
- *Hoe zou de raad de inrichting en borging van informatiebeveiliging binnen de gemeente graag terug willen zien (ideaal)?*
- *Waar liggen de grootste uitdagingen als het gaat om de inrichting van informatiebeveiliging?*

1.1.2 Maturity Model Informatiebeveiliging

Het 'Maturity Model Informatiebeveiliging' (zie figuur 1 en bijlage 4.1) wordt als normenkader gebruikt en helpt de informatiebeveiligingscultuur te duiden. Dit model geeft verschillende niveaus aan waarbij het uitgaat van fasen van ontwikkeling. Per niveau worden verschillende kenmerken genoemd. Op basis van de kenmerken schatten de onderzoekers het huidige niveau van informatiebeveiligingscultuur van de gemeente Almelo in. Dit model is uiteraard een richtlijn en kent haar beperkingen. Het is meer gericht op het 'hoe' en minder op het 'wat' en 'wie' in de ontwikkeling binnen de niveaus.



Figuur 1: Maturity Model informatiebeveiliging, zie bijlage 4.1 voor een grotere versie

1.1.3 Aanpak en scope

De aanpak van dit onderzoek bestaat uit vier fasen:

- Informatie-uitvraag bij de organisatie en documentanalyse; een analyse uitgevoerd op de door de gemeente Almelo beschikbaar gestelde documentatie. Toetsing aan het normenkader van de Baseline Informatiebeveiliging Overheid (hierna: BIO) is bekeken binnen het kader van de hoofdvraag (cultuur en bewustwording).
- Toetsing; door middel van praktijktoetsen is gekeken naar hoe het gedrag van medewerkers zich uit in de praktijk.
- Interviews en raadsessie; interviews met verschillende medewerkers van de gemeente, zowel uit de informatiebeveiligingsorganisatie als daarbuiten en een sessie met vertegenwoordigers vanuit de raad.

- Rapportage; rapportage met bevindingen, aanbevelingen en beantwoording van de onderzoeksvragen. De rapportage is ter wederhoor neergelegd bij de ambtelijke organisatie en het college.

Dit onderzoek heeft plaatsgevonden in de periode juni t/m augustus 2024. Het onderzoek is een kwalitatief onderzoek en is een momentopname van de situatie zoals deze ten tijde van het onderzoek wordt gezien en ervaren. In bijlage 4.5 is een opgave van de geïnterviewden opgenomen, evenals een overzicht van de documenten die zijn meegenomen in de beoordeling.

De scope van het gehele onderzoek betreft:

- afhankelijk van het ingezette middel alle medewerkers, dan wel een gericht aantal medewerkers van de gemeente Almelo;
- het stadhuis van de gemeente Almelo.

In bijlage 4.4 is een verklarende woordenlijst opgenomen met informatiebeveiligingstermen ter bevordering van de leesbaarheid van het rapport.

1.2 Versiebeheer

Versie	Datum	Status
1.0	28-08-2024	Concept rapport Rekenkamer
1.1	13-09-2024	Aangepast concept rapport Rekenkamer
1.2	31-10-2024	Aangepast concept rapport (feedback Rekenkamer en ambtelijk wederhoor verwerkt)
1.3	26-11-2024	Definitief rapport

2. Conclusies en advies

2.1 Conclusies

2.1.1 Hoofdvraag

Het onderzoek dat Hoffmann in opdracht van de Rekenkamer heeft uitgevoerd, heeft de beantwoording van de volgende hoofdvraag als resultaat:

- Hoe is de staat van de informatiebeveiligingscultuur en de wisselwerking met de systemen en processen?

Informatiebeveiligingscultuur verwijst naar de set van ideeën, gewoonten en gedragingen binnen een organisatie die gericht zijn op de bescherming van informatie. De staat van deze informatiebeveiligingscultuur kunnen we duiden door deze te plotten op het Maturity Model Informatiebeveiliging (zie bijlage 4.1). Dit model geeft verschillende niveaus aan van de informatiebeveiligingscultuur binnen een organisatie. Er wordt in het model uitgegaan van fasen van ontwikkeling. Per niveau worden verschillende kenmerken genoemd. Op basis van de kenmerken schatten de onderzoekers het huidige niveau van informatiebeveiligingscultuur van de gemeente Almelo tussen niveau één en twee. Met de komst van de nieuwe Chief Information Security Officer (hierna: CISO) is de verantwoordelijkheid voor de informatiebeveiligingscultuur daar belegd, behorende bij het tweede niveau. Er zijn echter nog geen beleid of processen aangaande de informatiebeveiligingscultuur en bewustzijn, passend bij niveau één. Het gebrek aan concrete acties gericht op informatieveilig gedrag en bewustwording heeft zijn weerslag op de wisselwerking met de systemen en processen, processen worden bijvoorbeeld nog onvoldoende aangepast naar aanleiding van incidenten of risico's in de praktijk. De resultaten van de toetsing van het gedrag in de praktijk bevestigen dat medewerkers onvoldoende bewust zijn en onvoldoende kennis hebben van wat van hen wordt verwacht. Het geeft het belang en de urgentie aan van structurele aandacht voor de informatiebeveiligingscultuur. De gemeente Almelo zet middels een nieuwe bewustwordingscampagne (start najaar 2024) in op verbetering.

Hieronder volgt de beantwoording van de deelvragen voor ieder onderzocht onderdeel: opzet, bestaan, werking en rol van de raad.

2.1.2 Opzet

- *Welke plaats kregen cultuur en bewustwording in het beleid én de praktijk rond informatiebeveiliging?*

Het 'Strategisch Gemeentelijk Informatiebeveiligingsbeleid gemeente Almelo 2021 tot 2026' is opgesteld volgens het format van de Vereniging van Nederlandse Gemeenten (hierna: VNG) / Informatiebeveiligingsdienst (hierna: IBD). Buiten een aantal standaard principes en uitgangspunten wordt verder geen aandacht besteed aan cultuur of bewustwording. Het tactisch beleid beschrijft enkel het bevorderen van het informatiebeveiligingsbewustzijn als één van de verantwoordelijkheden van zowel de CISO, de Information Security Officer (hierna: ISO) als het lijnmanagement. De gemeente beschikt momenteel

niet over een concreet plan waarin beschreven staat hoe men structureel aandacht besteedt aan de informatiebeveiligingscultuur en het verhogen van het bewustzijn onder zijn medewerkers.

Het gebrek aan beleid of een programma rondom informatiebeveiligingscultuur en bewustwording heeft zijn weerslag op de praktijk. Het thema heeft lange tijd weinig tot geen aandacht gekregen, waarmee de organisatie niet voldoet aan de richtlijnen beschreven in de BIO.[1] Met de komst van de huidige CISO wordt opnieuw ingezet op de cultuur en bewustwording rondom informatiebeveiliging. In het najaar van 2024 wordt gestart met een nieuwe bewustwordingscampagne voor alle medewerkers en is onlangs een presentatie over informatiebeveiliging en privacy toegevoegd aan het onboardingprogramma voor nieuwe medewerkers.

- *Zijn er specifieke uitgangspunten over cultuur en bewustwording vastgelegd?*

Het strategische informatiebeveiligingsbeleid benoemt een aantal uitgangspunten zoals:

- "Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken."

Met als praktische invulling:

- "Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures."

De genoemde training in het gebruik van beveiligingsprocedures vindt momenteel niet plaats. Daarnaast laten de uitgangspunten veel ruimte voor een tactische/operationele uitwerking, welke niet aanwezig is. De hierboven genoemde uitgangspunten zijn afkomstig uit het format van de VNG/IBD en zouden nog meer geformuleerd kunnen worden vanuit een 'eigen' visie en huidige stand van zaken binnen de gemeente Almelo.

- *Zijn beleid en praktijk voldoende om het hoofd te bieden aan (externe) ontwikkelingen? Heeft de gemeentelijke organisatie voldoende zicht hierop?*

In zowel het Strategisch als het Tactisch Informatiebeveiligingsbeleid wordt verwezen naar het dreigingsbeeld van de IBD.[2] Daarin wordt een overzicht gegeven van trends en verwachtingen wat betreft externe dreigingen. De gemeente is tevens aangesloten bij de IBD welke door middel van meldingen helpt zich te houden op kwetsbaarheden. De risico's op het vlak van informatiebeveiliging veranderen snel en de menselijke factor speelt een steeds groter wordende rol. Aandacht voor deze menselijke factor, bijvoorbeeld in de vorm van investering in bewustzijn, krijgt al langere tijd onvoldoende aandacht. Het gebrek aan structurele aandacht voor informatiebeveiligingsbewustzijn en de huidige inrichting van de praktijk maakt dat informatiebeveiliging voornamelijk ad-hoc en incidentgedreven wordt opgepakt. Van een meer toekomstgerichte en strategische aanpak op ontwikkelingen is minder sprake. Omdat de

[1] Zie hiervoor BIO 'Veilig personeel' Hoofdstuk 7.2

[2] https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2023-2024/

huidige uitvoering zich voornamelijk richt op de actuele gang van zaken is de vraag of de gemeente het hoofd weet te bieden aan (externe) ontwikkelingen moeilijk te beantwoorden. Het zal afhangen van de situatie en de ontwikkeling waarmee de gemeente op dat moment wordt geconfronteerd.

- *Hoe worden de uitgangspunten van het beleid bijgesteld naar aanleiding van de praktijk? Is hier een terugkerend proces voor?*

Momenteel worden de uitgangspunten in het beleid nog niet aangepast naar aanleiding van de praktijk. Er wordt gewerkt aan de inrichting van een Information Security Management Tool (hierna: ISMS-tool) zodat een dergelijke kwaliteitscyclus (Plan Do Check Act-cyclus, hierna PDCA-cyclus) opgezet kan worden.[3]

2.1.3 Bestaan

- *Is het beleid rond bewustwording en informatiebeveiligingscultuur geoperationaliseerd?*

Er is momenteel weinig tot niets beleidsmatig vastgelegd op het vlak van bewustwording en informatiebeveiligingscultuur. Het thema krijgt al langere tijd weinig tot geen aandacht in de praktijk.

  - *In welke vorm en welke concrete acties zijn genomen (voorlichting, opleiding, training, instructie, voorbeeldgedrag etc)?*

    Sinds kort wordt een presentatie gegeven over informatiebeveiliging en privacy bij de onboarding van nieuwe medewerkers. Verder lopen geen concrete acties om het informatiebeveiligingsbewustzijn van de medewerkers te verhogen of de informatiebeveiligingscultuur te versterken. In het najaar van 2024 gaat de nieuwe bewustwordingscampagne van de gemeente Almelo van start. Middels verschillende media zal het thema onder de aandacht gebracht worden en alle medewerkers krijgen toegang tot een e-learning.

  - *Is daarbij onderscheid gemaakt in doelgroepen en zo ja welke (in de organisatie, college, raad)?*

    Er wordt qua bewustwording momenteel geen onderscheid gemaakt in doelgroepen, de ambitie is uitgesproken om de e-learning in de toekomst wel functie/rolspecifiek in te richten. Ook is de CISO voornemens om aparte kennissessies voor de griffie, het college, management en directie te organiseren.

  - *Wordt periodiek geëvalueerd en op basis daarvan doorontwikkeld? Hoe gaat die evaluatie, bijvoorbeeld op basis van eventuele incidenten, in zijn werk en omvat dit contact met medewerkers?*

    Op dit moment is nog geen sprake van een kwaliteitscyclus zoals in de vraag beschreven. De gemeente Almelo beschikt over een ISMS-tool, een programma dat onder andere een PDCA-cyclus kan faciliteren, echter is het programma nog niet ingericht om dit te doen.

[3] Zie verklarende woordenlijst in bijlage 4.4

Momenteel is men bezig met deze inrichting, met de ambitie om begin 2025 het management hierbij te betrekken. Het management zal als proceseigenaar de input moeten geven voor deze PDCA-cyclus. Met deze input wordt het mogelijk om de praktijk als feedback te gebruiken om zowel het beleid als de processen aan te passen. Ook de incidentenregistratie en de uitkomsten van de e-learning wil men op termijn onderdeel maken van een PDCA-cylcus.

Het gebruik van een ISMS-tool faciliteert de uitvoering van een PDCA-cyclus, echter hoeft geen voorwaarde te zijn om hier inhoudelijk al een start mee te maken. Het betrekken van het management, juist in de fase vooraf, kan van meerwaarde zijn van de adaptie van dit proces en het gebruik van de tool.

- *Zijn specifieke middelen toegekend?*
  De CISO acht het huidige budget als voldoende voor de beoogde ambities en doelstellingen van 2024. De wethouder, tevens portefeuillehouder, geeft aan niet meer budget vrij te maken voor informatiebeveiliging. Het budget is gedeeltelijk gealloceerd onder IT security (binnen het ICT budget), het gedeelte voor bewustwording is apart gealloceerd en staat los van het ICT budget. Wel heeft de informatiebeveiligingsorganisatie de wens om uit te breiden in capaciteit en vraagt de snel veranderende wereld van cybersecurity en aankomende nieuwe wetgeving (zoals de NIS2) een nieuwe kijk op het thema.[4] Ook zullen de aanbevelingen uit dit rapport vragen om extra investering. De verwachting is daarmee dat het huidige budget in de komende jaren niet meer toereikend zal zijn.[5]

2.1.4 Werking

- *Wat zegt de uitkomst van de (eventuele) evaluaties over het gedrag, kennis- en bewustzijnsniveau van de medewerkers en hun wisselwerking met de systemen en processen?*

Vanuit de gemeente vinden geen toetsen of evaluaties plaats op het vlak van het gedrag, kennis- en bewustzijnsniveau en de wisselwerking met de systemen en processen.

- *Wat voor bedrijfscultuur heerst binnen de gemeente rondom informatiebeveiliging? Toelichting: Het is niet het doel van dit onderzoek om de totale bedrijfscultuur te onderzoeken, de nadruk ligt op de informatiebeveiligingscultuur. Maar we willen wel oog hebben voor verband(en) van de informatiebeveiligingscultuur met de totale bedrijfscultuur.*

Informatiebeveiliging is nauwelijks onderdeel van de bedrijfscultuur binnen de gemeente Almelo. Zowel in beleid als in praktische zin is er weinig aandacht voor de rol van de mens en zijn gedrag, kennis, gewoonten en ideeën rond dit thema. Het wordt veelal gezien als een operationele verantwoordelijkheid

[4] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn/

[5] De Cyber Security Raad** hanteerde in 2017 10% van het ICT-budget als ondergrens. De dreiging is sinds 2017 alleen maar toegenomen. IBD_dreigingsbeeld_2023-2024_DEF-versie.pdf (informatiebeveiligingsdienst.nl)

van de CISO en de ICT-afdeling, waar het eigenlijk meer als een verantwoordelijkheid van iedereen beschouwd zou moeten worden.

Kijkende naar de organisatiecultuur, blijkt uit de gesprekken met functionarissen en medewerkers dat binnen de gemeente een redelijke aanspreekcultuur heerst, men voelt zich doorgaans op zijn of haar gemak om anderen aan te spreken. Wanneer medewerkers over meer kennis en bewustzijn beschikken aangaande informatiebeveiliging, zou dit onderdeel van de organisatiecultuur een positieve bijdrage kunnen leveren aan het verstevigen van de informatiebeveiligingscultuur.

- *Hoe kijken raad, college en organisatie zelf naar de informatiebeveiligingscultuur en de vragen in dit onderzoek?*

Over het geheel genomen lijken alle partijen het thema informatiebeveiliging te zien als een belangrijk onderwerp. Gaat het over informatiebeveiligingscultuur, dan zien wij dit voornamelijk terugkomen in de gesprekken met de informatiebeveiligingsorganisatie zelf en de interviews met medewerkers. De informatiebeveiligingsorganisatie zegt hier de komende tijd aandacht aan te willen besteden, mede door de nieuwe bewustwordingscampagne. Medewerkers geven het belang aan van zaken als elkaar helpen, elkaar aanspreken en het goede voorbeeld geven. Er is daarbij nog sprake van bewuste onbekwaamheid, wat logisch is gezien de minimale aandacht in de afgelopen jaren. In de gesprekken komt naar voren dat zij wel bewust zijn van hun verantwoordelijkheden en daarnaast ook erg gemotiveerd zijn om ‘het goed te doen’. Echter, wordt men daar dermate weinig in gestuurd en gefaciliteerd dat het vaak een blinde vlek is in hoeverre zij voldoen aan wat van hen verwacht mag worden.

Hoe verder de afstand van de organisatie, hoe meer het thema als een ‘operationele ICT-kwestie’ wordt gezien. De aandacht van het college gaat voornamelijk uit naar vaststelling van beleid en dat zaken operationeel goed worden aangestuurd door de gemeentesecretaris. Daar ligt nog een kans om informatiebeveiliging meer vanuit een visie en een cultuurperspectief te benaderen en te benadrukken. Binnen de raad wordt informatiebeveiliging gezien als een ICT-verantwoordelijkheid en men heeft geen zicht op het cultuur-aspect hieromtrent.

- *Wat kan hier objectief over gezegd worden en aan toegevoegd worden met dit rekenkameronderzoek?*

In het kader van het onderzoek hebben twee toetsen plaatsgevonden om de wisselwerking tussen het kennis, gedrag- en bewustzijnsniveau van de medewerkers en de systemen en processen te kunnen duiden. De mail-phishing test laat een hoog percentage (31%) zien van medewerkers die geklikt hebben op een link én inloggegevens hebben ingevuld. Hieruit valt te concluderen dat zij onvoldoende in staat zijn om een dergelijke mail-phishing te herkennen. Dit toont de nut en noodzaak voor meer bewustwording rondom informatiebeveiliging. Als tweede hebben onderzoekers een fysieke inlooptest uitgevoerd. Hieruit blijkt dat de fysieke toegangsbeveiliging in het stadhuis vrij goed op orde is, waarbij enkele verbeterpunten zijn opgemerkt. Ook hierbij werd het belang van het beveiligingsbewustzijn duidelijk, on-

derzoekers kregen (onbedoelde) hulp van medewerkers van de gemeente om binnen te komen en werden, eenmaal in het stadhuis, niet meer aangesproken op hun aanwezigheid. Medewerkers mogen meer bewust gemaakt worden van hun rol binnen de (informatie)beveiliging en geïnformeerd worden over welk gedrag van hen verwacht wordt op dit vlak.

2.1.5 Rol van de raad

- *Hoe is de raad bij de verschillende onderdelen betrokken geweest (kaderstelling, geïnformeerd, in staat om te controleren)?*

De raad is weinig betrokken op het thema informatiebeveiliging, cultuur en bewustwording. De raad wordt incidenteel geïnformeerd, bijvoorbeeld aangaande grotere incidenten zoals 'Hof van Twente'. De kaderstellende en controlerende rol worden op dit thema niet tot nauwelijks in praktijk gebracht.

- *Is de raad op de hoogte waar informatiebeveiliging voor staat en welke beveiligingsaspecten cruciaal zijn om in te regelen?*

De raad ziet informatiebeveiliging als een belangrijke 'hygiënefactor' waarvan de verantwoordelijkheid ligt bij de ICT-afdeling. De raad beschikt over onvoldoende kennis en informatie om kritisch mee te denken over de inrichting van informatiebeveiliging.

- *Hoe zou de raad graag geïnformeerd willen worden als het gaat om wat informatiebeveiliging allemaal omvat?*

De raad geeft aan voornamelijk geïnteresseerd te zijn in (grotere) incidenten, incidenten welke in de media of politiek tot vragen zouden kunnen leiden.

- *Wat mist de raad nu als het gaat om de inrichting en de borging van informatiebeveiliging?*

Tijdens de sessie met de raad werd door enkele raadsleden uitgesproken dat zij een stuk kennisdeling missen, zij zouden meegenomen willen worden in een bewustwordingscampagne zoals die voor de medewerkers wordt ingericht.

- *Hoe zou de raad de inrichting en borging van informatiebeveiliging binnen de gemeente graag terug willen zien (ideaal)?*

De raad ziet informatiebeveiliging voornamelijk als een verantwoordelijkheid van de ICT-afdeling. Idealiter zien zij dat de ICT-afdeling technisch alles goed beveiligd en dat zij in uitvoering van de rol als raadslid soepel kunnen werken met de ICT-middelen.

- *Waar liggen de grootste uitdagingen als het gaat om de inrichting van informatiebeveiliging?*

De raad ziet informatiebeveiliging hoofdzakelijk als een uitdaging op overhead c.q. financieel gebied. Zaken bekend uit de media, zoals ransomware en hacks worden genoemd als grote risico's voor de gemeente. Tijdens de sessie met de raad is niet duidelijk geworden wat de grootste uitdaging is aangaande de inrichting van informatiebeveiliging. Er is binnen de raad weinig zicht op wat de inrichting

van informatiebeveiliging vraagt, en daarmee ook onvoldoende zicht op de daarbij behorende uitdagingen.

2.2 Advies

Informatiebeveiliging gaat uit van drie basisprincipes; beschikbaarheid, integriteit en vertrouwelijkheid. Informatie moet op het juiste moment en voor de juiste mensen beschikbaar zijn, de correctheid en zuiverheid van informatie moet gewaarborgd worden en de informatie moet beschermd zijn voor ongeoorloofde toegang. Informatiebeveiligingscultuur draagt bij aan de waarborging van deze principes. Het zegt iets over het belang dat wordt gehecht aan informatiebeveiliging, welke normen en waarden men heeft rondom het thema, welke besluiten er worden genomen en welk gedrag men vertoont. Een sterke informatiebeveiligingscultuur is cruciaal om de doelen op het vlak van beschikbaarheid, integriteit en vertrouwelijkheid te behalen. Het Maturity Model informatiebeveiliging (bijlage 4.1) geeft de verschillende niveaus weer van informatiebeveiligingscultuur. Uit dit onderzoek blijkt dat de gemeente hier nog stappen in te zetten heeft. Dit vraagt een structurele inzet van de gehele organisatie, van raad en bestuur tot aan de medewerkers van de gemeente, elk met eigen rol.

De gemeente Almelo start in het najaar van 2024 met een nieuwe bewustwordingscampagne voor alle medewerkers. Hiermee wordt een belangrijke eerste stap gezet richting het verhogen van het kennisniveau en het informatiebeveiligingsbewustzijn van de medewerkers. Kijkende naar gedrag vanuit de psychologie is de totstandkoming van gedrag afhankelijk van drie factoren; motivatie (willen), capaciteit (weten en kunnen), gelegenheid (gefaciliteerd worden en de kans krijgen). De eerste stap naar het gewenst gedrag is in lijn met de acties die gemeente Almelo in het najaar van 2024 uitzet, het creëren van basiskennis en begrip. Onderzoekers adviseren om deze inspanningen op kennis vervolgens te toetsen met het gedrag in de praktijk door bijvoorbeeld mail-phishing simulaties. Het is raadzaam om te analyseren of de nieuwe kennis resulteert in het gewenste gedrag in de praktijk. Het is namelijk bekend dat ‘weten wat je moet doen’ niet altijd resulteert in datzelfde gedrag. Indien het gedrag uitblijft, zou de organisatie kunnen onderzoeken of andere interventies (gericht op het creëren van gelegenheid of het stimuleren van de motivatie) nodig zijn.

Om te groeien qua informatiebeveiligingscultuur is nog een aantal andere factoren belangrijk om in ogenschouw te nemen, zoals ook leiderschap. Om het thema gewicht en prioriteit te geven is het van belang dat er betrokkenheid is vanuit het gehele bestuur van de gemeente. Zij kunnen het belang uitdragen, voorbeeldgedrag vertonen en het thema verweven met strategische besluitvorming en de visie van de gemeente. Het belang van betrokkenheid in leiderschap vertaalt zich ook door naar de leden van het lijnmanagement. Zij hebben enerzijds een belangrijke rol in het overbrengen van kennis en het sturen op het gewenste gedrag. Anderzijds speelt rondom cultuur nog een andere belangrijke (vaak onzichtbare) factor, namelijk ‘socialisatie’. Socialisatie beschrijft het proces waarbij (nieuwe) medewerkers leren over de organisatiecultuur door te kijken naar het gedrag van anderen, zoals collega’s en leidinggevenden. Hoe het leiderschap zich hierbij opstelt is vaak van grote invloed op hoe medewerkers

zich deze cultuur eigen maken. Onderzoekers adviseren daarom ook specifiek in te zetten op het verhogen van de kennis en het bewustzijn bij het lijnmanagement. Daarnaast is het van belang dat zij ook in praktische zin voldoende worden gefaciliteerd om de verantwoordelijkheid rondom informatiebeveiliging op zich te nemen.

Onbekend maakt onbemind, daarom is zichtbaarheid van de informatiebeveiligingsorganisatie alsook van het thema informatiebeveiliging belangrijk bij het versterken van de informatiebeveiligingscultuur. Recent is het Serviceplein opnieuw ingericht als centraal meldpunt. Wat betreft zichtbaarheid zou men kunnen overwegen om daarnaast ook mogelijkheid te bieden om persoonlijk vragen te stellen of twijfels te delen, bijvoorbeeld door aan te sluiten bij teamsessies of het organiseren van inloopspreekuren. Het geven van periodieke updates van ontwikkelingen aangaande informatiebeveiliging binnen de gemeente Almelo of het aanstellen van ambassadeurs zijn andere vormen waar men aan zou kunnen denken. Daarbij is het belangrijk om rekening te houden met de verschillen in doelgroepen en andere locaties dan het stadhuis, zoals de Turfkade, ook regelmatig te bezoeken. Qua capaciteit is het de vraag of dit realistisch te verwachten is van de huidige informatiebeveiligingsorganisatie. Een uitbreiding van het aantal Information Security Officers (hierna: ISO) valt hierbij te overwegen.

Cultuur laat zich niet snel veranderen, het vraagt een geïntegreerde en consequente aanpak waarbij voortdurende aandacht is voor de gewenste verandering. Het is dan ook van belang dat de hierboven genoemde adviezen worden geïntegreerd in beleid en processen en worden belegd in duidelijke rollen en verantwoordelijkheden. Om de kwaliteit te waarborgen is het wenselijk om een kwaliteitscyclus op te zetten waarbij de verschillende processen rondom informatiebeveiligingen periodiek worden geëvalueerd en waar nodig worden aangepast. Het is een thema dat gedragen moet worden door de gehele organisatie. Informatiebeveiliging is niet enkel de verantwoordelijk van de CISO of de informatiebeveiligingsorganisatie. Informatiebeveiliging is van alle medewerkers van de gemeente.

3. Bevindingen en aanbevelingen

Voor het onderzoek naar de informatiebeveiligingscultuur is een analyse uitgevoerd op de door de gemeente Almelo beschikbaar gestelde documentatie. Daarnaast zijn verschillende interviews uitgevoerd met medewerkers binnen de informatiebeveiligingsorganisatie binnen de gemeente voor toelichting op het gevraagde materiaal. Daarnaast hebben gesprekken plaatsgevonden met medewerkers, de portefeuillehouder en vertegenwoordigers vanuit de raad om een breed beeld te kunnen schetsen van de huidige cultuur rondom informatiebeveiliging. Het onderzoek is een kwalitatief onderzoek en is een momentopname van de situatie zoals deze nu wordt gezien en ervaren. In paragraaf 3.1 is een overzicht opgenomen van de belangrijkste bevindingen en aanbevelingen. In paragraaf 3.2 wordt op thema toelichting gegeven op deze bevindingen en aanbevelingen. In bijlage 4.5 is een overzicht van de geïnterviewden opgenomen, evenals een overzicht van de documenten die zijn meegenomen in de beoordeling.

3.1 Overzicht bevindingen en aanbevelingen

Nr.	Paragraaf	Bevinding	Aanbeveling
1	3.2.1	Het strategisch informatiebeveiligingsbeleid van de gemeente Almelo is opgesteld op basis van een standaard format waarbij geen expliciete aandacht besteed is aan de informatiebeveiligingscultuur.	Maak het een meer gemeente ‘eigen’ document wat een duidelijke ‘toon aan de top’ aangaande informatiebeveiliging communiceert. Positioneer hierin informatiebeveiliging, cultuur en bewustwording als een fundamentele pijler, met nadruk op de lange termijn en een organisatiebrede visie.
2	3.2.1	De gemeente beschikt momenteel niet over een tactisch beleidsstuk waarin beschreven staat hoe men structureel aandacht besteedt aan het verhogen van het informatiebeveiligingsbewustzijn onder haar medewerkers.	Stel een concreet plan op waarin de aandacht voor het informatiebeveiligingsbewustzijn uitgewerkt is en borg deze in processen. Maak deze processen onderdeel van een PDCA-cyclus.
3	3.2.1	Op het vlak van informatiebeveiliging zijn er weinig operationele beschrijvingen of handleidingen ter ondersteuning van de praktijk.	Faciliteer medewerkers door het gewenste informatieveilige gedrag concreet te beschrijven en te communiceren. Denk aan bijvoorbeeld operationele richtlijnen of gedragsregels.
4	3.2.1, 3.2.5, 3.2.7	De ISMS-tool van de gemeente Almelo is nog onvoldoende ingericht om in te zetten in de praktijk.	Finaliseer de inrichting van de ISMS-tool en zet deze in voor doeleinden als integraal risicomanagement en PDCA-cycli.
5	3.2.3	Het aantal processen en te faciliteren lijnmanagers is een zeer grote scope voor een enkele ISO.	De praktische uitvoering en het oppakken van verantwoordelijkheden door het lijnmanagement dient voldoende gefaciliteerd te worden. Het is raadzaam om een uitbreiding van deze ondersteuning, in de vorm van ISO’s, te overwegen.

6	3.2.4	Informatiebeveiliging wordt door het college gezien als een voornamelijk operationeel thema.	Wanneer het gaat om het neerzetten van een stevige informatiebeveiligingscultuur zou het college hier nadrukkelijker een rol kunnen innemen. Een duidelijke visie en de 'toon aan de top' doet veel met het belang dat door de rest van de organisatie wordt gehecht aan het thema.
7	3.2.4	De raad is weinig betrokken bij het thema informatiebeveiliging. De kaderstellende en controlerende rol wordt in de praktijk niet uitgevoerd.	De raad mag de kaderstellende en controlerende rol explicieter innemen. Raadsleden mogen daartoe meer gefaciliteerd worden door het college. Denk aan het bijbrengen van de nodige kennis en bewustwording door bijvoorbeeld training of informatiesessies van de CISO. Daarnaast mag de raad actiever openstaan om meegenomen te worden in het onderwerp, door bijvoorbeeld vragen en verzoeken te doen, te gaan kijken bij andere gemeenten of een werkgroep op te richten.
8	3.2.5	Binnen de gemeente Almelo is geen structurele aanpak voor bewustwording op het vlak van informatiebeveiliging. Hiermee voldoet de gemeente niet aan de richtlijnen beschreven in de BIO.	In het najaar van 2024 start de gemeente met een nieuwe campagne om het informatiebeveiligingsbewustzijn en kennis rond dat thema te verhogen. Het is van belang dat dit wordt geborgd in processen en dat de campagne wordt gecombineerd met toetsing en analyse op het gedrag in de praktijk.
9	3.2.6	Er worden relatief weinig incidentmeldingen gedaan door medewerkers.	Communiceer duidelijk wat het proces is rondom het melden van incidenten. Informeer de medewerkers over wat verstaan wordt onder een incident. Verlaag de gevoelsmatige drempel om te melden door een veilige omgeving te creëren, bijvoorbeeld door het delen van voorbeelden en positieve communicatie in reactie op meldingen.
10	3.2.7	De verantwoordelijkheden voor de informatiebeveiligingsrisico's binnen de processen liggen voornamelijk bij de CISO en de ICT-afdeling in plaats van het daarvoor verantwoordelijke leiderschap. Informatiebeveiliging mag hierbij als een meer integraal risico beschouwd worden.	Zet integraal risicomanagement op en beleg verantwoordelijkheden bij de daarvoor aangewezen (proces)eigenaren. De inrichting van de ISMS-tool kan de organisatie hierin faciliteren.
11	3.2.8	Het gedrag van medewerkers in de praktijk resulteert in (informatie)beveiligingsrisico's op zowel fysiek als digitaal vlak.	Besteed consequente en voortdurende aandacht aan bewustwording, kennisdeling en de rol van de medewerkers binnen (informatie)beveiliging. Faciliteer de medewerker door het gewenste informatieveilige gedrag te beschrijven (in bijvoorbeeld gedragsregels). Periodieke toetsing en analyse van het gedrag in de praktijk draagt bij aan de inzet van effectieve interventies.

3.2 Toelichtingen bevindingen en aanbevelingen

3.2.1 Beleid

Het ‘Strategisch Gemeentelijk Informatiebeveiligingsbeleid gemeente Almelo 2021 tot 2026’ is op het moment van onderzoek vigerend binnen de gemeente. Het beleid beschrijft kort de gemeentelijke visie, ontwikkelingen op het vlak van informatiebeveiliging, uitgangspunten, verantwoording en taken en verantwoordelijkheden. Het volgt hiermee het format van de VNG en IBD, waarmee het voldoet aan de BIO. Buiten een aantal standaardprincipes en uitgangspunten wordt verder geen aandacht besteed aan cultuur of bewustwording. Het beleid zou meer ingezet kunnen worden om bewustwording en informatiebeveiliging te positioneren als een fundamentele pijler van de organisatiecultuur, met de nadruk op langetermijndoelen en een organisatiebrede visie. Op deze manier wordt het een meer richtinggevend en ‘eigen’ document wat een duidelijke ‘toon aan de top’ communiceert.

Onderzoekers hebben tevens het ‘Tactisch Informatiebeveiligingsbeleid 2023-2026’ ontvangen. Het tactisch beleid zou een beschrijving moeten geven van de uitwerking van de strategisch geformuleerde doelen. Het bevorderen van het informatiebeveiligingsbewustzijn wordt in dit document meerdere keren aangehaald, bijvoorbeeld als verantwoordelijkheid van zowel de CISO, ISO als het lijnmanagement. Het beschrijft echter niet de praktische uitwerking hiervan. De gemeente beschikt momenteel niet over een tactisch beleidsstuk waarin beschreven staat hoe men structureel aandacht besteedt aan het verhogen van het informatiebeveiligingsbewustzijn onder haar medewerkers.

De ontvangen documentatie en de informatie uit de interviews toont aan dat tevens op operationeel niveau weinig beschreven is op het thema informatiebeveiliging. Onderzoekers hebben een ‘Procedure gevonden bedrijfsmiddelen’ ontvangen, welke omschrijft wat medewerkers kunnen doen indien zij zaken als een telefoon, laptop, dossiers, toegangspas of gegevensdrager hebben gevonden. Onderzoekers adviseren om ook de rest van het gewenste ‘informatieveilige gedrag’ te beschrijven en te communiceren zodat alle medewerkers weten wat van hen op dit vlak verwacht wordt.

Momenteel worden de uitgangspunten in het beleid nog niet aangepast naar aanleiding van de praktijk. Momenteel wordt gewerkt aan de inrichting van een ISMS-tool zodat een dergelijke kwaliteitscyclus opgezet kan worden.

3.2.2 Informatiebeveiligingsorganisatie

De informatiebeveiligingsorganisatie van de gemeente Almelo bestaat ten tijde van het onderzoek uit een CISO, TISO, ISO, Functionaris Gegevensbescherming (hierna: FG) en vier Privacy Officers (hierna: PO) waarvan twee externen. De CISO is sinds januari 2024 werkzaam voor de gemeente Almelo. Met deze aanstelling is de rol van CISO anders gepositioneerd dan voorheen, namelijk direct onder de gemeentesecretaris in plaats van onder ICT. Dit maakt dat de CISO meer onafhankelijke bewegingsruimte heeft en zich dichter bij het bestuur bevindt, waardoor zij met meer mandaat haar functie in kan richten.

De hierboven genoemde herpositionering is een mooi signaal van de gemeente, waarmee de organisatie laat blijken het belang in te zien van informatiebeveiliging. Uit de interviews blijkt dat dit lange tijd anders is geweest. Informatiebeveiliging werd soms ook wel het 'ondergeschoven kindje' genoemd, een thema dat eigenlijk door alle lagen van de organisatie onvoldoende begrepen en opgepakt werd. In de waan van de dag kwam men vaak niet toe aan een structurele aanpak op het vlak van informatiebeveiliging. Tegenwoordig is het team uitgebreid en verstevigd, zowel inhoudelijk als qua positionering.

Een mooi signaal is tevens het gekozen profiel van de huidige CISO. Bij de selectie is specifiek gekeken naar de behoeften vanuit de organisatie. De CISO heeft een achtergrond in, en een opdracht gekregen op het vlak van 'de mens' en bewustwording.

Deze veranderingen binnen het team hebben positief bijgedragen aan de huidige ingezette tendens. De CISO is bekend bij het management, het directieteam en het college. Te merken is dat de bereidwilligheid en interesse positief is beïnvloed door haar komst.

3.2.3 Mensen, middelen, budget

Op termijn zou het team graag nog willen groeien in capaciteit. De grootte van de organisatie en het totaal aantal processen is een zeer grote scope om door een enkele ISO te overzien, beamen ook de onderzoekers. Een uitbreiding van de capaciteit biedt meer gelegenheid tot (praktische) ondersteuning van het management, welke verantwoordelijkheid dragen voor de informatiebeveiliging van de processen en systemen binnen hun organisatieonderdeel. Daarnaast geeft extra capaciteit de CISO de gelegenheid om haar toezichthoudende en adviserende rol zuiverder in te richten. Nu is de beoogde functiescheiding vanwege de capaciteit vaak nog lastig te realiseren, zo schrijft én beoordeelt zij bijvoorbeeld haar eigen beleidsstukken.

Naast de wens voor uitbreiding van de ISO's geeft het team tevens aan behoefte te hebben aan extra security collega's. Uit de gesprekken blijkt dat zaken momenteel nog veel ad-hoc opgepakt, waar een uitbreiding de mogelijkheid geeft om het technische beveiligingsvraagstuk meer strategisch en toekomstgericht in te vullen. Extra capaciteit in de vorm van security medewerkers helpt tevens de gewenste 'security by design' in praktijk te brengen, doordat men meer capaciteit heeft om aan te sluiten bij inkoop en innovatie.[6] Te merken is dat de informatiebeveiligingsorganisatie nu vaak te laat wordt betrokken bij nieuwe ontwikkelingen, waardoor beveiligingseisen niet altijd (op tijd) worden toegepast.

De CISO beschikt momenteel over voldoende budget om de beoogde ambities en doelstellingen van 2024 in te vullen. Het budget is gedeeltelijk gealloceerd onder IT-security (binnen het ICT-budget), het gedeelte voor bewustwording is apart gealloceerd en staat los van het ICT-budget. Met de bovenstaande ambities voor het team, de snel veranderende wereld van cybersecurity en aankomende

[6] Zie verklarende woordenlijst in bijlage 4.4

nieuwe wetgeving als de NIS2 is de verwachting dat het huidige budget in de komende jaren niet meer toereikend zal zijn.[7]

Vanuit het gesprek met de wethouder blijkt dat gezien de verwachte financiële tekorten de komende jaren (financiële) investeringen vaak een discussiepunt zijn en zwaar drukken op besluitvorming. Meer budget voor informatieveiligheid concurreert met andere uitgaven binnen de gemeente. Vaak met uitgaven dichter bij de inwoners en ondernemers staan en daarmee ook politiek meer voor het voetlicht komen. Het belang van informatiebeveiliging zal daarom extra moeten worden belicht om in de toekomst te komen tot een evenwichtige verdeling van de schaarse financiële middelen.

3.2.4 Leiderschap & betrokkenheid Raad/College

De wethouder/portefeuillehouder geeft aan dat het college informatiebeveiliging meer als een operationeel dan een beleidsmatig thema benadert. Zij geeft aan dat er weinig tot geen betrokkenheid is bij de operatie. De rol van het college komt explicieter naar voren op het moment dat nieuw beleid vastgesteld moet worden. Wanneer het gaat om het neerzetten van een stevige informatiebeveiligingscultuur zou het college hier nadrukkelijker een rol kunnen innemen. Een duidelijke visie en de ‘toon aan de top’ doen veel met het belang dat door de rest van de organisatie wordt gehecht aan het thema.

De gemeentesecretaris speelt een belangrijke rol in hoe informatiebeveiliging in de praktijk wordt vormgegeven. De informatiebeveiligingsorganisatie ervaart dat de huidige gemeentesecretaris het thema informatiebeveiliging serieus neemt en dat er een merkbaar gevoel voor urgentie heerst. De gemeentesecretaris is vrij recent begonnen bij de gemeente Almelo (september 2023), het zal in de toekomst moeten blijken of de ervaren betrokkenheid wordt omgezet in de juiste prioriteitstelling, visie en besluitvaardigheid. In de gesprekken komt naar voren dat hier bij het college soms nog onvoldoende inzicht is. Weten dat ‘iets’ moet gebeuren is nog niet hetzelfde als doorzien wat daar allemaal voor nodig is. Hier ligt een belangrijke taak voor de CISO (en de FG) door het in kaart brengen van de risico’s en duidelijk te communiceren wat dit vraagt van de organisatie.

Vanuit zowel interviews met functionarissen en de wethouder alsmede de raadsessie in het kader van het onderzoek mag geconcludeerd worden dat de betrokkenheid van de raad minder sterk is. Enerzijds is dat logisch, aangezien de raad op een grotere afstand staat van de informatiebeveiligingsorganisatie. Anderzijds zijn wel zaken te noemen waaruit betrokkenheid afgeleid kan worden. Zo komen bijvoorbeeld weinig tot geen vragen of verzoeken vanuit de raad. Tijdens een presentatie aan de raad over informatiebeveiligingsbewustzijn kwamen er voornamelijk ICT-gerelateerde vragen, waardoor het beeld heerst dat de raad het thema voornamelijk ziet als een ICT-vraagstuk. Daarnaast werd tijdens interviews benoemd dat raadsleden soms ongenoegen uiten over beveiligingsmaatregelen, waarbij maatregelen worden gezien als belemmerend en soms opgevat worden als een vorm van wantrouwen. De raad en het college hebben onderling enkel overleg op het vlak van informatiebeveiliging als het aankomt op de

[7] De Cyber Security Raad** hanteerde in 2017 10% van het ICT-budget als ondergrens. De dreiging is sinds 2017 alleen maar toegenomen. IBD_dreigingsbeeld_2023-2024_DEF-versie.pdf (informatiebeveiligingsdienst.nl)

vaststelling van nieuw beleid. Er is verder geen gesprek op het vlak van ambities, risico's of werking van het beleid.
Onderzoekers herkennen de nadruk op ICT vanuit de raadsessie in het kader van dit onderzoek. Wanneer het gesprek gaat over informatiebeveiliging, wordt voornamelijk verwezen naar gebruikersproblematiek die de raadsleden ervaren tijdens het uitvoeren van hun rol. De raad mag hierin zijn kaderstellende en controlerende rol meer innemen door kritisch en constructief mee te denken. Dit vraagt echter wel om kennis en bewustwording, waarin de raadsleden aangeven onvoldoende gefaciliteerd te worden. Anderzijds wordt tijdens de sessie ook aangegeven dat het thema wordt gezien als 'overhead' en dat het politiek geen aantrekkelijk onderwerp is, waardoor de raad niet geheel open lijkt te staan om meegenomen te worden in het onderwerp. Er is zowel aan de vraag- als aanbodkant ruimte voor verbetering.

3.2.5 Bewustwording

Binnen de gemeente Almelo is geen structurele aanpak voor bewustwording op het vlak van informatiebeveiliging. Hiermee voldoet de gemeente niet aan de daarvoor beschreven richtlijnen beschreven in de BIO.[8] In het verleden is er een eenmalige quiz/vragenlijst geweest welke handmatig, per e-mail, door de toenmalige CISO werd verstuurd. Omdat dit niet geborgd was in een systeem of proces, is dit met het vertrek van deze CISO gestopt. Daarnaast was er discussie over de kwaliteit van de vragenlijst, vragen waren veelal te technisch, niet relevant of onjuist. Er werd gemonitord of men de vragenlijst invulde, er werd echter niet op deelname gestuurd.

De CISO heeft sinds haar start in het begin van dit jaar zich eerst vooral gericht op een aantal technische projecten welke stil waren komen te liggen. Daarnaast is een start gemaakt met de opzet voor een nieuwe bewustwordingscampagne, deze gaat dit najaar (2024) van start.

Binnen deze campagne worden meerdere communicatievormen gebruikt om het thema informatiebeveiliging onder de aandacht te brengen. Tevens krijgt elke medewerker (tevens inhuur) toegang tot een e-learning module. In de toekomst is het de bedoeling om deze e-learning functie- c.q. rolspecifiek te maken. Het deelnamepercentage wordt geregistreerd en gedeeld met het management als verantwoordelijke voor de sturing op de deelname. Ook is het de ambitie om de e-learning als meet- en stuurmiddel in te zetten door middel van de inhoudelijke scores. Zo kan er bijvoorbeeld gekeken worden of er bij bepaalde afdelingen specifieke behoeftes zijn waar de afdeling op in kan spelen. Idealiter wordt deze feedback onderdeel van de PDCA-cyclus waarbij het management bijvoorbeeld de informatie kan gebruiken om processen aan te passen ten behoeve van de informatieveiligheid.

De e-learning wordt tevens aangekondigd bij de onboarding van nieuwe medewerkers. Sinds kort wordt in het onboardingprogramma van nieuwe medewerkers al een korte presentatie gehouden op het vlak van informatiebeveiliging en privacy.

[8] Zie hiervoor BIO 'Veilig personeel' Hoofdstuk 7.2

Het management heeft een belangrijke rol als het gaat om informatiebeveiliging en de cultuur. Zij hebben een voorbeeldrol, zijn risico-eigenaar binnen de eigen processen én zijn verantwoordelijk voor het bevorderen van het bewustzijn onder de eigen medewerkers. Om deze verantwoordelijkheid goed in praktijk te kunnen brengen, mag het management meer gefaciliteerd worden. Naast inhoudelijke ondersteuning op processen en risico's is er behoefte aan handvatten en kennis ten behoeve van de eigen bewustwording én om het thema over te dragen richting medewerkers. Vanuit de interviews blijkt dat er veel wisselingen zijn op managementniveau. Doordat aangaande bewustwording geen vast programma of cyclus bestaat, is de aandacht voor informatiebeveiliging in veel opzichten afhankelijk van het gevoel van urgentie en de aanwezige kennis bij de manager. De CISO heeft zich daarom in het begin van haar aanstelling als eerste gericht op de bewustwording en zichtbaarheid bij het management.

De beoogde interventies op het vlak van bewustwording spelen allen in op het verhogen van het kennisniveau. Het bewerkstelligen van een basisniveau aan kennis is een goede eerste stap richting het gewenste informatieveilige gedrag. Vanuit de psychologie is echter bekend dat 'naast weten wat je moet doen' (weten en kunnen) ook motivatie (willen) en gelegenheid (gefaciliteerd worden en de kans krijgen) een rol spelen in het tot stand komen van gedrag. Het is daarom raadzaam om, na verloop van tijd te toetsen en te analyseren hoe het gedrag zich in de praktijk ontwikkelt. Wanneer blijkt dat men wel op de hoogte is van een bepaalde gewenste gedraging (weten en kunnen), maar dit niet laat zien, zou een interventie welke inspeelt op motivatie (willen) of faciliteert in gelegenheid (gefaciliteerd worden en de kans krijgen) nuttig kunnen zijn. Zo zou de organisatie bijvoorbeeld kunnen voorschrijven dat medewerkers geen vertrouwelijke gesprekken voeren in het bijzijn van anderen/onbevoegden. Medewerkers kunnen hier kennis van hebben genomen én gemotiveerd zijn om het gedrag te vertonen, echter zal het gewenste gedrag niet in praktijk zichtbaar worden wanneer er onvoldoende ruimtes beschikbaar zijn waar medewerkers dergelijke gesprekken kunnen houden. Het ontbreekt dan aan de gelegenheid. Het is daarom belangrijk om elk van deze drie facetten in ogenschouw te nemen bij gedragsverandering.

3.2.6 Incidentmeldingen

Gekeken naar de omvang van de organisatie worden volgens de CISO relatief weinig incidenten gemeld, een beeld dat wordt bevestigd door het aantal meldingen van de praktijktoets in het kader van dit onderzoek (zie paragraaf 3.2.8.1). Het merendeel van de meldingen komen vanuit de systemen zelf (middels logging).[9] Vanuit de interviews met medewerkers lijken hier meerdere zaken aan ten grondslag te liggen. Enerzijds blijkt het soms nog onduidelijk te zijn wat het juiste proces is; hoe en waar incidenten gemeld moeten worden. Recent is dit proces beschreven en zijn stappen ondernomen om het Serviceplein als verzamelpunt te maken voor meldingen van incidenten. Anderzijds blijkt het vaak nog niet duidelijk te zijn wat er onder een 'incident' wordt verstaan. Wanneer men niet weet wat onder een incident verstaan wordt, is de kans kleiner dat een melding wordt gedaan. De gemeente hoopt hier met een focus op bewustwording een verschil in te maken en de meldbereidheid te verhogen. Andere manieren

[9] Zie verklarende woordenlijst in bijlage 4.4

om deze meldbereidheid te verhogen is het creëren van een veilige cultuur om te melden. In het verleden zou wel eens heftig gereageerd zijn op fouten en incidenten. Dit komt in meerdere gesprekken naar voren, echter hebben geen van de gesprekspartners dit zelf ervaren. Het geeft aan hoe hardnekkig dit soort geluiden kunnen zijn en hoe lang deze binnen de organisatie blijven rondzingen. De huidige CISO heeft zich als doel gesteld om toegankelijk en benaderbaar te zijn in de hoop dat iedereen zich vrij voelt om zaken te melden. Het openlijk communiceren over fouten en incidenten kan tevens bijdragen aan een cultuur waarin men zich veilig voelt om te melden. 'Het' kan immers iedereen overkomen.

Ook de reactie op een melding van een incident kan positief bijdragen aan de meldbereidheid. Een positieve reactie waarbij duidelijk wordt uitgelegd wat met de melding gedaan gaat worden werkt uitnodigend om een volgende keer weer te melden. In bijlage 4.2 is een reactie opgenomen vanuit de Servicedesk aan een (externe) medewerker op de door de onderzoekers verstuurde mail-phishing. De reactie geeft instructies, maar biedt ook nog ruimte voor verbetering. Zo zou de mail nog kunnen bedanken voor de melding en aan kunnen geven waarom het goed is dat de melding gedaan is. Relatief kleine aanpassingen die een positief verschil in beleving kunnen maken.

3.2.7 Wisselwerking met processen

De gemeente Almelo beschikt over een ISMS-tool, een programma dat onder andere een PDCA-cyclus kan faciliteren, echter is het programma nog niet ingericht om dit te doen. Momenteel is men bezig met deze inrichting, met de ambitie om begin 2025 het management hierbij te betrekken. Het management zal als proceseigenaar de input moeten geven voor deze PDCA-cyclus. Met deze input wordt het mogelijk om de praktijk als feedback te gebruiken om zowel het beleid als de processen aan te passen. Het gebruik van een ISMS-tool faciliteert de uitvoering van een PDCA-cyclus, echter hoeft geen voorwaarde te zijn om hier inhoudelijk al een start mee te maken. Het betrekken van het management, juist in de fase vooraf, kan van meerwaarde zijn van de adaptie van dit proces.

De afhandeling van security-incidenten is recent op papier gezet. De bedoeling is om uiteindelijk de incidentenregistratie als input te gebruiken om de algehele kwaliteit te verbeteren (onderdeel te maken van een PDCA-cyclus). Vooralsnog worden deze niet gebruikt als onderbouwing voor aanpassingen of verbeteringen.

Kijkende naar het proces van inkoop en innovatie, wordt de informatiebeveiligingsorganisatie vaak nog te laat en soms pas achteraf betrokken. Hierdoor is het lastig om de gewenste 'security by design' te voeren. Vanuit de afdeling zijn acties ondernomen om de zichtbaarheid te vergroten, zo is bijvoorbeeld het contact met adviseurs is geïntensiveerd. In het afgelopen jaar is de situatie hierdoor verbeterd en wordt de afdeling naar eigen zeggen al vaker aangehaakt. Het geeft aan dat informatiebeveiliging nog niet 'top of mind' is bij medewerkers en daarom beter geborgd mag worden binnen (nieuwe) processen.

Informatiebeveiliging gaat voor een groot deel over risicomanagement. Op het vlak van integraal risicomanagement mag de gemeente Almelo nog stappen zetten. Wanneer onvoldoende zicht is op risico's

binnen de verschillende processen is het tevens lastig om hier prioritering aan te brengen en besluitvorming op toe te passen. De CISO heeft een belangrijke rol in het communiceren van risico's op bestuurlijk niveau, niet alleen incidentgedreven maar ook op de langere termijn. Verder is dit echter een thema wat de gehele organisatie zal moeten gaan omarmen. Volgens het beleid is het management als proceseigenaar verantwoordelijk voor de informatiebeveiligingsrisico's binnen de eigen processen, waar de informatiebeveiligingsorganisatie behoort te ondersteunen en faciliteren. In praktijk mag deze verantwoordelijkheid duidelijker belegd en opgepakt worden.

3.2.8 Gedrag in de praktijk

De toetsing van het gedrag van medewerkers is momenteel geen periodiek terugkerende gebeurtenis binnen de gemeente Almelo. Vanuit de ICT-afdeling geeft men aan graag vaker te willen testen met bijvoorbeeld mail-phishings, de tooling is er tevens voor aanwezig, men krijgt hier echter geen goedkeuring voor.

Om een beeld te krijgen van het bewustzijn en het gedrag in de praktijk, en daarmee antwoord te kunnen geven op de deelvragen rondom werking, zijn in het kader van dit onderzoek een tweetal testen uitgevoerd:

1. Mail-phishingtest, waarbij een e-mail naar alle medewerkers van de gemeente Almelo is verstuurd die uitnodigde op een link te klikken en de gebruiker te verleiden om persoonlijke inloggegevens af te geven;
2. Fysieke inlooptest, waarbij twee medewerkers van Hoffmann hebben geprobeerd om zonder toestemming toegang te krijgen tot de gemeentelijke werkplekken.

3.2.8.1 Mail-phishingtest

Bij de mail-phishingtest is in 40% van het totaal aantal verstuurde e-mails geklikt op de link in de e-mail. Vervolgens zijn bij 31% van het totaal aantal verstuurde e-mails inloggegevens achtergelaten.
Dit percentage is relatief hoog vergeleken met andere gemeenten waar een soortgelijk scenario is toegepast. Gemiddeld zien de onderzoekers dat ongeveer 15% van de gebruikers hun gebruikersnaam en wachtwoord achterlaat.

Binnen de gemeentelijke organisatie zijn 22 meldingen geregistreerd. Vergeleken met het totaal aantal verzonden mail-phishings is dit relatief laag (1,8%). Hieruit kunnen twee mogelijke, elkaar niet uitsluitende, conclusies getrokken worden; medewerkers zijn niet in staat geweest om de mail-phishing te herkennen als zodanig (bevestigd door het grote aantal dat reacties in kliks en inloggegevens) én c.q. óf het meldproces is onvoldoende duidelijk en bekend (zoals tevens blijkt uit de interviews, besproken in paragraaf 3.2.6).

Een beschrijving van de opzet en het verloop van de test en de resultaten is opgenomen in bijlage 3.2. Vanwege de gevoeligheid van bepaalde details is ervoor gekozen om deze in bijlage 4.7 (vertrouwelijk) op te nemen.

3.2.8.2 Fysieke inlooptest

Gedurende de test is het de Mystery Guests (MG's) gelukt toegang te verkrijgen tot het stadhuis en de kantoorruimtes. Hierbij konden ze onopgemerkt binnen het pand verblijven. Binnen in het pand en bij de hoofdingang viel op dat de beveiliging alert was op hun aanwezigheid. Uiteindelijk kregen de MG's wel toegang tot het stadhuis door (onbedoelde) hulp van andere medewerkers. Hoewel ze door de gangen konden lopen, hadden ze geen toegang tot de lift of trap zonder een pas. Dit toont aan dat interne toegangscontroles effectief zijn, maar dat de beveiliging aan de buitenste ringen nog verbeterd kan worden en het gedrag van medewerkers hier tot een beveiligingsrisico leidt. Op een aantal verdiepingen zagen de MG's onbeheerde werkplekken met (gevoelige) documenten, zoals een formulier voor bijzondere bijstand. Het was opvallend dat de MG's niet werden aangesproken door medewerkers terwijl zij herhaaldelijk, zonder zichtbare toegangspas, over dezelfde verdiepingen hebben gelopen en zich op een aantal plekken hebben opgehouden. Het was voor de MG's niet mogelijk om de beveiligde zones (zoals SER ruimte of de bestuursvleugel) te betreden zonder toegangspas.

In bijlage 4.3 zijn in het kort de opzet en doelstellingen van de inlooptest opgenomen. In bijlage 4.7 (vertrouwelijk) is een uitgebreide beschrijving van het verloop van de fysieke inlooptest opgenomen.

3.2.8.3 Aanbevelingen over gedrag in de praktijk

De hierboven beschreven resultaten onderschrijven het belang van een consequente en voortdurende aandacht voor bewustwording, kennisdeling en de rol van de medewerker binnen (informatie)beveiliging. Het is belangrijk om medewerkers mee te nemen in de verschillende technieken, vormen en consequenties van phishing en social engineering te beginnen door de aankomende bewustwordingscampagne, maar ook door praktijktoetsen en het delen van actuele voorbeelden. Daarnaast is het belangrijk dat zij meegenomen worden in wat van hen verwacht wordt aangaande informatieveilig gedrag en hoe te handelen in een geval van phishing c.q. social engineering. Op dit moment vormt het hulpvaardige, onbewust onbekwame gedrag van de medewerker een beveiligingsrisico.

Naast aanbevelingen op de factor 'mens' zijn ook bevindingen gedaan aangaande fysieke beveiliging, hieronder worden een aantal relevante maatregelen beschreven;

- *Striktere toegangscontrole alle in- en uitgangen van het stadhuis:* Zorg ervoor dat toegang tot alle ingangen strikt gecontroleerd wordt en dat medewerkers alert zijn op personen die proberen mee te lopen. Mogelijk zouden sommige ingangen vervangen kunnen worden door een tourniquet, omdat constante monitoring niet altijd haalbaar is.
- *Compartimentering:* Indien men door de eerste beveiligingsschil is gekomen, is het relatief eenvoudig om zich door het pand voort te bewegen. Hoffmann adviseert om ook binnen het pand

een effectievere vorm van compartimentering te realiseren. Bijvoorbeeld door op elke verdieping in het trappenhuis een paslezer te plaatsen of in ieder geval op de verdiepingen waar kritieke ruimten aanwezig zijn (zoals de postkamer, SER, bestuursvleugel).

- *Regelmatig beoordelen van beveiligingsprocedures:* Periodieke herzieningen en oefeningen zoals deze fysieke inlooptest helpen om de effectiviteit van de huidige procedures te beoordelen en te verbeteren.
- *Beheer van gevoelige documenten*: Zorg ervoor dat gevoelige documenten altijd veilig worden opgeborgen, zelfs op onbeheerde werkplekken. Het onder de aandacht (blijven) brengen van de clean desk policy kan hierbij helpen, evenals het beschikbaar stellen van kasten of kluisjes voorzien van een slot.
- *Prompt aanspreken van onbekenden:* Medewerkers moeten worden aangemoedigd om onbekende personen direct aan te spreken en hun aanwezigheid te verifiëren. Gezien de grootte van de organisatie en de doorloop van personeel zou het aanmoedigen van het zichtbaar dragen van de personeelspas een bijdrage kunnen leveren in het identificeren van (ongewenste) personen.

Disclaimer

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

Esther Kraan,
Psycholoog - Consultant Cybersecurity & Security Riskmanagement

Laurens Kolfschoten - Security Consultant

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

Johan van Slooten

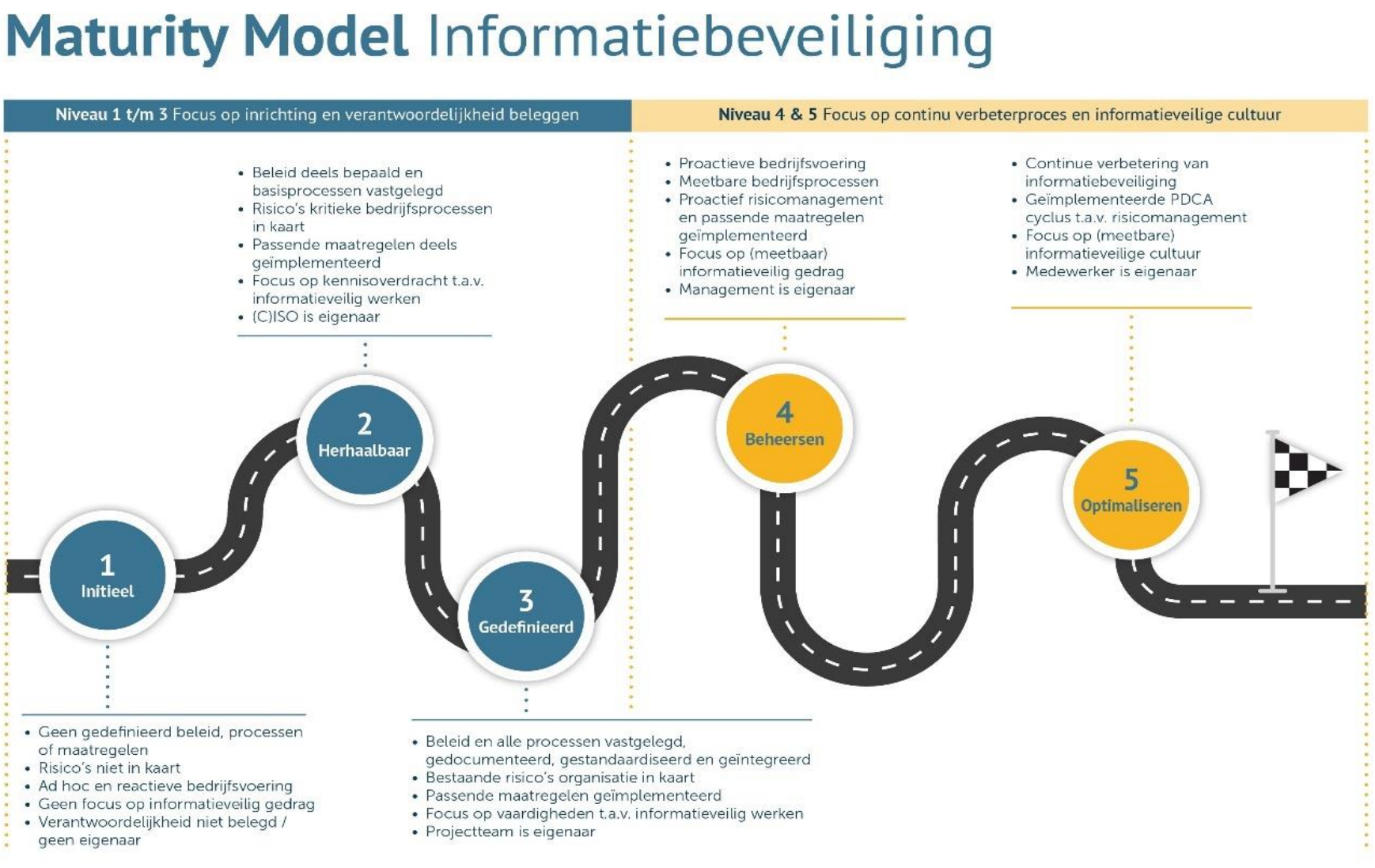
Directeur Cybersecurity & Security Risk management

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, 26 november 2024

4. Bijlagen

4.1 Maturity modelinformatiebeveiliging



4.2 Verloop mail-phishing test

Gedurende de onderzoeksperiode hebben onderzoekers van Hoffmann in overleg met gemeente Almelo een mail-phishing verstuurd naar alle medewerkers. De e-mail werd verstuurd van een e-mailadres met een ander domein dan @almelo.nl. Op donderdag 4 juli 2024 rond 11:00 uur werd de mail naar 1208 unieke e-mailadressen verstuurd. In de e-mail werd een drinkfles aangeboden, zogenaamd vanuit de gemeente. De e-mail was ondertekend op een manier die gebruikelijk is in de gemeentelijke organisatie. Men kon de drinkfles bestellen door te klikken op een link en op de website de inloggegevens in te vullen.

Figuur 2: inhoud mail-phishing (zie vertrouwelijke bijlage 4.7)
Figuur 3: website mail-phishing (zie vertrouwelijke bijlage 4.7)

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

Er zijn in totaal 487 unieke bezoekers geregistreerd (40%) waarvan 373 gebruikers (31% van totaal verstuurde mail-phishings, 77% van de websitebezoekers) hun gebruikersnaam en wachtwoord hebben ingevuld. De test is gestopt op dinsdag 9 juli rond 12:40 uur door de website te vervangen door een boodschap dat het een test betrof en dat deze inmiddels is afgerond.

Vanuit de gemeentelijke informatiebeveiligingsorganisatie is gecommuniceerd dat het om een ‘spambericht’ gaat. De medewerkers werden geïnformeerd over de mail, tips om dergelijke berichten te herkennen en er werd aangegeven hoe zij het beste konden handelen.

Een aantal van de medewerkers hebben gereageerd op de mail-phishing door deze te beantwoorden, een voorbeeld van de reacties:

- *“Hoe zit voor mijn overige collega’s die geen mail hebben gekregen over een doper? Kan ik dit voor bestellen of ?”*
- *“Wat een ontzettend leuk initiatief! Dank je wel!”*
- *“Nog duurzamer is om geen Dopper’s te laten fabriceren 😉 ”*

Vanuit een andere reactie klonk meer reserve:

- *“Beste collega, leuke actie! maar ik vind heel raar en heb er moeite mee om mijn wachtwoord op een externe website (bestel.bedrijfsvouchers.nl) in te voeren. Dit voelt niet goed en lijkt mij in strijd met de introductiecursus dataveiligheid.”*

Onderzoekers adviseren niet op phishingmails te reageren, ook niet om wantrouwen te uiten. Het geeft kwaadwillende de bevestiging dat het e-mailadres geldig en actief is én het contact biedt een directe opening om de ontvanger toch te overtuigen en aan te zetten tot actie.

Een (externe) medewerker heeft melding gedaan van de mail-phishing en de volgende reactie ontvangen van de servicedesk:

Beste [redacted]

Meldingsnummer: INC-62947
Omschrijving: FW: Een duurzame zomerattentie
Prioriteit: 3

Jouw melding, bij ons bekend onder **INC-62947**, is door ons opgelost.

De oplossing is:

> Beste collega,
> De mail die hebt ontvangen is inderdaad een phishing mail. Gelieve de mail te verwijderen, en als jij de link hebt aangeklikt, dan moet je meteen je wachtwoord wijzigen via start.almelo.nl. En als dat niet lukt graag langskomen bij het Serviceplein op de 4e etage.
>
> Met vriendelijke groet,
> [redacted]

Ben je van mening dat dit niet het geval is dan kun je via het Self Service Portal je melding bewerken.

Reageer je niet binnen twee weken na ontvangst van deze mail, dan wordt de melding definitief gesloten.

Figuur 4: reactie servicedesk op melding mail-phishing

4.3 Opzet fysieke inlooptest

Aan medewerkers van Hoffmann is ten behoeve van de opdracht toestemming verleend om dinsdag 2 juli 2024 tussen 06:00 en 23:00 uur, als onderzoekers / Mystery Guests (hierna te noemen MG's) het pand aan de Haven Zuidzijde 30, 7607 EW te betreden en om foto's te maken.

De doelstellingen van de fysieke inlooptest luiden:

- Testen of het mogelijk is om als mystery guest de panden fysiek te betreden;
- Testen of het mogelijk is om vertrouwelijke informatie (digitale en fysieke informatie) te bereiken;
- Testen van de awareness van de medewerkers en beveiliging en of/hoe zij de beveiligings-maatregelen toepassen.

Een gedetailleerd verslag van de inlooptest is op vertrouwelijke basis verstrekt aan de gemeente (bijlage 4.7).

4.4 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 Evan cybersecuritytermen die voorkomen in deze rapportage.

BEGRIP	BETEKENIS
BIO	Baseline Informatiebeveiliging Overheid, het basis normenkader voor informatiebeveiliging binnen de overheid.
CISO	De medewerker die aangewezen verantwoordelijk is voor informatiebeveiliging. Rol op strategisch niveau. Bestuur blijft altijd eindverantwoordelijke.
FG	Functionaris Gegevensbescherming. Verantwoordelijk voor toezicht op toepassing en naleving van de AVG.
Gebruikersnaam	Naam waarmee een gebruiker in een computersysteem kan inloggen.
Informatiebeveiligingsorgansiatie	Het team wat zich binnen een bedrijf bezig houdt met het beschermen van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie.
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.
Inloggegevens	Gebruikersnaam en wachtwoord waarmee in een computersysteem kan inloggen.

BEGRIP	BETEKENIS
Incident	Gebeurtenis of actie waarbij de beveiliging van hardware, software, informatie, een proces of organisatie mogelijk is gevaar is gebracht of geheel of gedeeltelijk is doorbroken.
Logging	Het automatisch bijhouden van veranderingen en gebeurtenissen binnen een systeem.
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.
Mitigerende maatregel	Een activiteit met als doel om de oorzaak of het gevolg van een ongewenste gebeurtenis weg te nemen, of te verkleinen.
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. In dat geval gaat de mystery guest een beveiligde ruimte in. Daar probeert hij in te breken op het lokale computernetwerk.
PDCA	Plan-Do-Check-Act (cyclus). Stappen ter verbetering van bijvoorbeeld een proces of beleid.
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.
Ransomware	Ransomware is malware die de databestanden van gebruikers versleutelt, met als doel om deze later te ontsleutelen in ruil voor losgeld.
Security by design	Een product, dienst of systeem ontwerpen en vanaf het begin ook de beveiliging mee ontwikkelen en testen.

BEGRIP	BETEKENIS
SER	Satellite Equipment Room, een satelliet van het technische hart van een bedrijf. Ruimte waarin serverapparatuur, netwerkapparatuur en IT-infrastructuur aanwezig zijn.
Toon aan de top	De houding en gedrag van het hogere management en de invloed hiervan op de cultuur en normen binnen de gehele organisatie.
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

4.5 Overzicht geïnterviewden

Functie	Datum interview
CISO	2 juli 2024 + 4 juli 2024
TISO	2 juli 2024
Functionaris gegevensbescherming	2 juli 2024
ISO	2 juli 2024
Interviews medewerkers (5)	4 juli 2024 + 16 juli 2024
Wethouder / portefeuillehouder	16 juli 2024
Sessie raadsleden	16 juli 2024

4.6 Overzicht bestudeerde documenten

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

Document	Versie	Datum
Strategisch Gemeentelijk Informatieveiligheidsbeleid gemeente Almelo 2021-2026	1.2	05-08-2021
Procedure datalekken Gemeente Almelo	2.0	07-05-2024
Jaarverslag 2023 van de Functionaris Gegevensbescherming	-	-
Update privacy & informatiebeveiliging	-	Dec. 2023
Procedure gevonden bedrijfsmiddelen-documenten	-	-
Projecten Informatiebeveiliging – Jaarplan 2024	-	-
Quick reference chart melden datalek	-	-
Rapportage informatiebeveiliging Gemeente Almelo Q3 en Q4 2023	-	12-12-2023
Tactisch informatiebeveiligingsbeleid 2023-2026 Gemeente Almelo	1.0	-
Verbeterplan informatiebeveiliging-v1.2	1.2 definitief	-


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