Raadsvergadering: 15 april 2025
Registratienummer: R 2408465

De Raad van de Gemeente Almelo:

Gezien het voorstel van de rekenkamer Almelo;

Besluit:

1. De conclusies van de rekenkamer over het onderzoeksrapport Informatiebeveiligingscultuur over te nemen.
2. De praktische aanbevelingen uit het rapport (nummers 1, 2, 3, 4, 5, 8, 9, 10 en 11) vast te stellen en het college op te dragen deze ten uitvoering te brengen.
3. Het college op te dragen een plan van aanpak te formuleren voor de uitvoering van de praktische aanbevelingen en hierover de raad infomeren per separate raadsbrief.
4. De kaderstellende aanbevelingen (nummers 6 en 7) uit het rapport vast te stellen en het college op te dragen deze ten uitvoering te brengen door:
    - bijeenkomsten te organiseren voor raad en college om kennis te verwerven, te werken aan de eigen bewustwording en de raad mee te nemen in de keuzes waar Almelo voor staat (bijvoorbeeld keuzes die i.h.k.v. de praktische aanbevelingen moeten worden gemaakt), en vervolgens
    - het gesprek tussen raad en college te voeren over de benodigde kaderstelling door de raad, zoals bijvoorbeeld over ambities en risico's en de mogelijk daaruit voortvloeiende benodigde bijstelling van budgetten en de gewenste visie die het college naar de organisatie uit zal dragen.
5. Het college te verzoeken om een geactualiseerd beeld, over maximaal 3 jaar, van het bewustzijnsniveau van de informatiebeveiliging op basis van een door/namens het college uitgevoerd onderzoek gelijkwaardig aan dit rekenkameronderzoek (bijvoorbeeld door een 2.13a onderzoek).

Gedaan in de openbare vergadering van 15 april 2025,

de griffier, **de burgemeester,**

drs. J.W. Scherpenzeel **R.T.A. Korteland**

Raadsvergadering: 15 april 2025
Registratienummer: R 2408465

Naam: E Alp
Datum: 11 februari 2025
Team: Raadsgriffie

Voorstel aan de raad

Onderwerp	**Rekenkameronderzoek Informatiebeveiligingscultuur**
Portefeuillehouder	**Rekenkamer Almelo**

Samenvatting raadsvoorstel

De rekenkamer helpt de gemeenteraad bij het controleren van het college van burgemeester en wethouders door het doen van onderzoek. De RKA onderzocht in 2024 de informatiebeveiligings-cultuur van de gemeente Almelo. Bureau Hoffmann voerde het onderzoek uit, vanuit een menselijk-, proces- en systeemperspectief. Op basis van het onderzoeksrapport formuleerde de RKA-conclusies en aanbevelingen voor het college van B&W om het bewustzijnsniveau naar een hoger niveau te tillen. De RKA stelt de gemeenteraad voor om de conclusies over te nemen en de aanbevelingen vast te stellen zodat het college deze tot uitvoering kan brengen.

Voorgesteld raadsbesluit

1. De conclusies van de rekenkamer over het onderzoeksrapport Informatiebeveiligingscultuur over te nemen.
2. De praktische aanbevelingen uit het rapport (nummers 1, 2, 3, 4, 5, 8, 9, 10 en 11) vast te stellen en het college op te dragen deze ten uitvoering te brengen.
3. Het college op te dragen een plan van aanpak te formuleren voor de uitvoering van de praktische aanbevelingen en hierover de raad infomeren per separate raadsbrief.
4. De kaderstellende aanbevelingen (nummers 6 en 7) uit het rapport vast te stellen en het college op te dragen deze ten uitvoering te brengen door:
    - bijeenkomsten te organiseren voor raad en college om kennis te verwerven, te werken aan de eigen bewustwording en de raad mee te nemen in de keuzes waar Almelo voor staat (bijvoorbeeld keuzes die i.h.k.v. de praktische aanbevelingen moeten worden gemaakt), en vervolgens
    - het gesprek tussen raad en college te voeren over de benodigde kaderstelling door de raad, zoals bijvoorbeeld over ambities en risico's en de mogelijk daaruit voortvloeiende benodigde bijstelling van budgetten en de gewenste visie die het college naar de organisatie uit zal dragen.
5. Het college te verzoeken om een geactualiseerd beeld, over maximaal 3 jaar, van het bewustzijnsniveau van de informatiebeveiliging op basis van een door/namens het college uitgevoerd onderzoek gelijkwaardig aan dit rekenkameronderzoek (bijvoorbeeld door een 2.13a onderzoek).

Inleiding

<u>Aanleiding onderzoek en onderzoeksaanpak</u>
Bureau Hoffmann heeft namens de RKA de informatiebeveiligingscultuur in de gemeente Almelo onderzocht. Informatiebeveiliging beschermt de informatie binnen de gemeente tegen een breed scala aan bedreigingen d.m.v. organisatorische, technische en beleidsmatige maatregelen. Die vallen of staan bij het gebruik en opvolging van de gebruiker. Bureau Hoffmann richtte zich daarom in dit onderzoek op de informatiebeveiligingscultuur, vanuit een menselijk, proces én systeemperspectief.

Daarbij stond de volgende doelstelling 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 luidde: *"Hoe is de staat van de informatiebeveiligingscultuur en de wisselwerking met de systemen en processen?"*

In het onderzoek is het Maturity Model Informatiebeveiliging gebruikt als normenkader om de cultuur te duiden. Dit model geeft verschillende niveaus aan (van 1: initieel tot 5: optimaliseren), uitgaande van fasen van ontwikkeling. Voor het onderzoek zijn de belangrijkste documenten geanalyseerd, er vonden 2 praktijktoetsen plaats en er vonden interviews plaats met raadsleden, de portefeuillehouder, functionarissen en medewerkers van de gemeente Almelo.

Samenvatting beantwoording hoofdvraag

Op basis van het onderzoek wordt het huidige niveau van de informatiebeveiligingscultuur van de gemeente Almelo ingeschat tussen niveau 1 en 2 van het Maturity Model (zie bijlage X). Er zijn nog geen beleid of processen aangaande de informatiebeveiligingscultuur en bewustzijn. Het gebrek aan concrete acties gericht hierop heeft zijn weerslag op de wisselwerking met de systemen en processen. Deze conclusie geeft het belang en urgentie aan van structurele aandacht voor de informatiebeveiligingscultuur.

Samenvatting beantwoording deelvragen

Opzet

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. Dit heeft zijn weerslag op de praktijk. Met de komst van de huidige CISO wordt opnieuw ingezet op cultuur en bewustwording met een bewustwordings-campagne in het najaar van 2024.
Het strategische informatiebeveiligingsbeleid benoemt een aantal uitgangspunten over cultuur en bewustwording maar nog meer uitgangspunten kunnen geformuleerd worden vanuit een 'eigen' visie en huidige stand van zaken in de gemeente.
Omdat de 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 gebrek aan beleid en de huidige inrichting van de praktijk maken dat informatiebeveiliging voornamelijk ad-hoc en incident gedreven wordt opgepakt.
Momenteel worden de uitgangspunten in het beleid nog niet aangepast naar aanleiding van de praktijk, maar hier wordt wel aan gewerkt.

Bestaan

Momenteel is 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. Vooralsnog wordt geen onderscheid gemaakt in doelgroepen, wel is de ambitie uitgesproken om in de toekomst de (nog komende) e-learning functie/rol specifiek in te richten en aparte kennissessies te organiseren.
Er is op dit moment nog geen sprake van een kwaliteitscyclus waarbij periodiek wordt geëvalueerd en op basis daarvan wordt doorontwikkeld.
De verwachting is dat het overnemen van de aanbevelingen, maar ook aankomende nieuwe wetgeving, vragen om een extra investering en dat daarmee het huidige budget in de komende jaren niet meer toereikend zal zijn.

Werking

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 van de CISO en de ICT-afdeling, waar het eigenlijk meer als een verantwoordelijkheid van iedereen beschouwd zou moeten worden. Er is wel sprake van een redelijke aanspreekcultuur.
Over het geheel genomen lijken alle partijen het thema informatiebeveiliging te zien als een belangrijk onderwerp. Gaat het over de informatiebeveiligingscultuur, dan komt dit voornamelijk

terug in de gesprekken met de informatiebeveiligingsorganisatie zelf en bij medewerkers. 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. Het college vindt 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.
De toetsen die plaatsvonden om de wisselwerking tussen kennis, gedrag- en bewustzijnsniveau te duiden laten de nut en noodzaak zien voor meer bewustwording rondom informatiebeveiliging.

Rol van de raad
De raad is weinig betrokken op het thema informatiebeveiliging, cultuur en bewustwording en wordt incidenteel geïnformeerd. De kaderstellende en controlerende rol worden op dit thema niet tot nauwelijks in praktijk gebracht.
De raad ziet daarnaast 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.
Idealiter ziet de raad 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. Een deel van de raad heeft aangegeven meegenomen te willen worden in een bewustwordingscampagne maar geeft ook aan voornamelijk geïnteresseerd te zijn in (grotere) incidenten.
Tot slot ziet de raad informatiebeveiliging hoofdzakelijk als een uitdaging op overhead c.q. financieel gebied.

<u>Advies</u>
De aanbevelingen hieronder vloeien uit het volgende voort. Om te komen tot een hoger bewustzijnsniveau is een structurele inzet nodig van de gehele organisatie, raad en college tot aan de medewerkers van de gemeente, elk met eigen rol. De eerste stap naar het gewenste gedrag is in lijn met de acties die de gemeente in het najaar van 2024 uitzet, het creëren van basiskennis en begrip. Er zou geanalyseerd moeten worden of de nieuwe kennis resulteert in het gewenste gedrag in de praktijk.
Daarnaast is leiderschap een belangrijke factor. Om het thema gewicht en prioriteit te geven is het van belang dat er betrokkenheid is vanuit het gehele bestuur van de gemeente. Dit vertaalt zich door naar de leden van het lijnmanagement. Hoe het leiderschap zich opstelt is van invloed op hoe (nieuwe) medewerkers zich de cultuur eigen maken (socialisatie).
Verder is het van belang dat zowel de informatiebeveiligingsorganisatie als het thema informatiebeveiliging zichtbaar is.

<u>Aanbevelingen</u>
De rekenkamer heeft de aanbevelingen onderverdeeld in 'praktische' aanbevelingen en 'kaderstellende' aanbevelingen. De praktische aanbevelingen liggen vooral bij het college waarmee zij dan ook direct en op eigen wijze mee aan de slag kan. De kaderstellende aanbevelingen (nummer 6 en 7) vragen om een goed ingericht proces waar zowel raad als college bij betrokken zijn. De rekenkamer doet een voorstel aan de raad op het inrichten van dit proces in het dictum van dit raadsvoorstel.
Tot slot doet de rekenkamer nog een aanvullende, eigen, aanbeveling.

Praktische aanbevelingen (1,2,3,4,5, 8, 9, 10, 11)

Nr.	Paragraaf rapport	aanbeveling
1	3.2.1	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 organisatie brede visie.
2	3.2.1	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	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	Finaliseer de inrichting van de ISMS-tool en zet deze in voor doeleinden als integraal risicomanagement en PDCA-cycli.
5	3.2.3	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.
8	3.2.5	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	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	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	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.

Kaderstellende aanbevelingen (6,7)

Nr.	**Paragraaf rapport**	**aanbeveling**
6	3.2.4	Wanneer het gaat om het neerzetten van een stevige informatie-beveiligingscultuur 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 mag de kader stellende 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.

Op termijn vergelijkbaar onderzoek
De rekenkamer adviseert de Raad om het college van B&W te verzoeken een vergelijkbaar onderzoek uit te voeren over een nader te bepalen periode (van in elk geval enkele jaren) om te bepalen of het informatiebeveiligingsbewustzijn is toegenomen, gedrag is veranderd en daarmee de informatiebeveiligingscultuur is verbeterd.

Beoogd effect
De aanbevelingen aan de raad over te nemen en het college te verzoeken uitvoering te geven aan de aanbevelingen. Zodoende de informatiebeveiligingscultuur te versterken en daarmee de informatieveiligheid.

Argumenten voor
Met het overnemen van de genoemde aanbevelingen uit het onderzoeksrapport kunnen het college van B&W en de ambtelijke organisatie alle inspanningen met betrekking tot de informatieveiligheid, en specifiek de informatiebeveiligingscultuur, nader te versterken in de reeds ingeslagen weg.

Kosten, opbrengsten en dekking
Het onderzoek is gefinancierd uit het onderzoeksbudget van de rekenkamer Almelo.

Vervolg
Het college van B&W dient over de opvolging van de aanbevelingen jaarlijks te rapporteren aan de gemeenteraad, conform invoering van de Wet versterking decentrale rekenkamers sinds 1 januari 2024. Het college van B&W heeft aangegeven dit te (gaan) doen via de Jaarverantwoording.

Bijlagen
- Onderzoeksrapport Hoffmann – Informatiebeveiligingscultuur (INT -2494365)
- Bijlage 4.7 (vertrouwelijk) (INT- 2494367)
- Bestuurlijke reactie college van B&W (volgt)

De rekenkamer Almelo, _____

de secretaris,	**de voorzitter,**
E. Alp	J.J. Mastwijk