Postadres:
Gemeente Almelo
Postbus 5100
7600 GC Almelo

Bezoekadres:
Haven Zuidzijde 30
7607 EW Almelo

telefoon: **(0546) 54 11 11**
e-mail: **gemeente@almelo.nl**
internet: **www.almelo.nl**

Rekenkamer Almelo
Postbus 5100
7600 GC ALMELO

Uw brief	Uw kenmerk	Ons kenmerk	Datum
18 december 2024		UIT - 24118711	21 januari 2025

Bijlage(n)	Doorkiesnummer	Behandeld door	Zaaknummer
	0546-541111	M.I. Legtenberg	DCS - 2486879

Onderwerp
Bestuurlijke reactie rekenkameronderzoek informatiebeveiligingscultuur

Geachte heer Mastwijk,

Op 18 december 2024 heeft u ons het rekenkamerrapport van het onderzoek 'Informatiebeveiligingscultuur gemeente Almelo' aangeboden inclusief een concept raadsvoorstel (Raad – 2408465). Met belangstelling hebben wij deze stukken gelezen. De rekenkamer Almelo heeft ons uitgenodigd om een zienswijze te formuleren op het rapport en het raadsvoorstel.

Hierbij geven wij onze reactie op het rekenkameronderzoek.
We kunnen ons vinden in de conclusies zoals die in hoofdstuk 2 weergegeven zijn. Hierna geven wij aan op welke wijze wij invulling willen gaan geven aan de aanbevelingen die in hoofdstuk 3 opgenomen zijn. Daar maken we wel het volgende voorbehoud bij. Wanneer tijdens de uitvoering blijkt dat de invulling onverhoopt vraagt om aanvullende inzet, middelen of financiën, kan dit leiden tot een bestuurlijke heroverweging van de invulling. Volgens de lijn die daarover afgesproken is zullen we in dat geval de raad daarover rapporteren via de P&C cyclus.
Wij hebben de aanbevelingen indien mogelijk geclusterd en geven per cluster van aanbevelingen onze zienswijze.

Aanbeveling 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 organisatiebrede visie.

Aanbeveling 2: 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.

Bank: BNG Bank, Den Haag
NL56 BNGH 028 50 00 187
BIC Code: BNGHNL2G

BTWnr.
NL 0015 84 108 B 01

Aanbeveling 3: Faciliteer medewerkers door het gewenste informatieveilige gedrag concreet te beschrijven en te communiceren. Denk aan bijvoorbeeld operationele richtlijnen of gedragsregels.

Aanbeveling 8: 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.
Aanbeveling 9: 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.

Aanbeveling 11: 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.

In uw aanbevelingen 1, 2, 3, 8, 9 en 11 geeft u concreet aan hoe de informatiebeveiliging, de cultuur en de bewustwording kan worden verbeterd.

De gemeente heeft strategisch en tactisch informatiebeveiligingsbeleid. Het strategische beleid vormt de basis voor de ontwikkeling en implementatie van doeltreffende beveiligingsmaatregelen, terwijl het tactische beleid aanvullende richtlijnen biedt om de informatiebeveiliging te versterken en te waarborgen.

Op het gemeentelijk kennisplatform staan talrijke documenten die medewerkers ondersteunen bij het bewustzijn. Voorbeelden zijn: Informatiebeveiliging voor nieuwe medewerkers, 10 vuistregels voor veilig internetten, het herkennen van phishingsmail en de juiste acties nemen en praktische tips en richtlijnen voor informatiebeveiliging. Door middel van intranetberichten en actieve communicatie binnen teamoverleggen door onder meer privacy officers, is dit onder de aandacht gebracht.

Hoffmann constateert dat de beschikbare informatie niet leidt tot de gewenste bewustwording. We zijn daarom voornemens om de reeds beschikbare informatie voor medewerkers te evalueren en op een andere wijze aan te bieden, zodat de effectiviteit van de informatie wordt verhoogd. Mocht dit leiden tot noodzakelijke aanpassingen, dan zal het dit bij de eerstvolgende actualisatie in het strategisch- of tactisch informatiebeveiligingsbeleid aangepast worden.

Aanbeveling 4: Finaliseer de inrichting van de ISMS-tool en zet deze in voor doeleinden als integraal risicomanagement en PDCA-cycli.

Aanbeveling 10: Zet integraal risicomanagement op en beleg verantwoordelijkheden bij de daarvoor aangewezen (proces)eigenaren. De inrichting van de ISMS-tool kan de organisatie hierin faciliteren.

We zien een gedegen risico- en impactanalyse als een cruciale stap binnen de borging van informatiebeveiliging. Hierbij wordt een overzicht gemaakt van alle gegevensverzamelingen en applicaties binnen onze organisatie. Deze gegevensverzamelingen en applicaties worden geanalyseerd op risico's en de impact op de beschikbaarheid, integriteit en betrouwbaarheid van informatie.

Na het uitvoeren van de risico- en impactanalyse is het van groot belang om passende beveiligingsmaatregelen te implementeren. Het is tevens van essentieel belang om de naleving van deze maatregelen te waarborgen door middel van bewustwording, training en periodieke interne controles.

Om te zorgen dat informatiebeveiliging(sbeleid) effectief wordt verankerd, is in het beleid vastgelegd dat een PDCA-cyclus moet worden ingeregeld en dat een Information Security Management Tool (ISMS-tool) moet worden ontwikkeld en geïmplementeerd. De ISMS-tool ondersteunt de planning, uitvoering, borging en controle van processen binnen de PDCA-cyclus.

Vanwege beperkte capaciteit is de ISMS-tool nog niet in gebruik genomen.

In het tactisch beleid zijn de taken, bevoegdheden en verantwoordelijkheden van de proceseigenaren beschreven. Met het opstellen van processen, zoals benoemd in de vorige aanbevelingen, zal hier ook aandacht aan worden besteed. Maar ook hier zullen keuzes moeten worden gemaakt. Niet alles kan en niet alles kan tegelijk.

Aanbeveling 5: 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.

De afgelopen 2 jaar heeft de ambtelijke organisatie budgettair neutraal geïnvesteerd in het informatiebeveiligingsteam. De positie van CISO is geformaliseerd en verstevigd. Daarnaast zijn de ISO en Technical ISO in het functieboek opgenomen en de beveiligingsfunctionarissen voor rijbewijzen en reisdocumenten aangesteld. Desondanks constateren wij met de toenemende dreiging, regelgeving (NIS-2, AI-act) en complexiteit dat de ondersteuning niet op het benodigde en gewenste niveau is. Uitbreiding van de ondersteuning is wellicht gewenst, maar dit hangt echter samen met de grotere financiële opgave waar Almelo voor staat en zal in dit licht afgewogen moeten worden.

Aanbeveling 6: 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.

Het college ziet in dat de 'toon aan de top' belangrijk is. Daarom zijn in het strategisch beleid 10 principes voor informatiebeveiliging vastgesteld die vooral gaan over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen het bestuur bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk onderwerp van gesprek op de bestuurstafel.
Bovenstaande onderstrepen we met de ingezette bewustwordingscampagne, die ook specifiek is gericht op het college.

Aanbeveling 7: 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.

Het college legt jaarlijks verantwoording af aan de gemeenteraad over de stand van zaken van informatiebeveiliging, in lijn met de P&C-cyclus. Er zijn inmiddels informatiebeveiligings-awareness activiteiten gepland (Q1 2025), waaronder een informatiesessie voor de raad. Indien de raad meer behoefte heeft aan training en informatiesessies over informatiebeveiliging en bewustwording hiervan, kunnen meer van dergelijke sessies georganiseerd worden.

Aanbeveling 12: 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.

In het tactisch beleid wordt ingegaan op de monitoring, evaluatie en verbetering.
Het beleid stelt dat een effectieve borging van informatiebeveiliging een continu proces van monitoring, evaluatie en verbetering vereist. Door regelmatige controles en audits (opzet, bestaan en werking) kunnen we de implementatie en effectiviteit van beveiligingsmaatregelen beoordelen. Incidenten en afwijkingen worden geregistreerd, geanalyseerd en periodiek gerapporteerd aan relevante functionarissen en het management. Deze bevindingen bieden waardevolle inzichten om verbeteringen door te voeren en risico's te verminderen.
Bovendien moeten we een cultuur van voortdurende verbetering stimuleren door middel van feedbackmechanismen, regelmatige evaluaties en herzieningen van het informatiebeveiligingsbeleid en de maatregelen. Over een paar jaar zal er een vergelijkbaar onderzoek uitgevoerd worden om te bepalen of de informatiebeveiligingscultuur is verbeterd.

Wij vertrouwen erop dat onze zienswijze duidelijk maakt welke stappen we al hebben ondernomen en welke we nog gaan nemen om de informatiebeveiligingscultuur te verbeteren. We kijken uit naar de verdere behandeling van het rapport in de raad.

Hoogachtend,
Burgemeester en wethouders van Almelo,
de secretaris, de burgemeester,

J.H. Dijkstra R.T.A. Korteland