Beantwoording vragen voorafgaand aan de raadscommissie

Nummer	DOC-22-585622
Zaaknummer	Z-21-180420
Naam commissielid	M. Hoogewerf
Fractie	Hart voor Medemblik
Onderwerp	Commissievragen HvM raadscie. 15-9 agendapunt 11.2 RKC-onderzoek informatieveiligheid
Datum waarop de vraag is gesteld	12 september 2022

Beantwoording uiterlijk woensdag 15:00 uur, voorafgaand aan de raadscommissie.
Portefeuillehouder
Afdeling

Inleiding
In het document wordt meerdere keren verwezen naar het document “22112073 – Rekenkamercommissie_Medemblik&Opmeer_techniek.pdf”. Hier zouden een aantal kritische aandachtpunten in staan en specifiek aanbevolen maatregelen. De pentesten zijn afgerond op 4 mei 2022. Ondertussen is het september 2022.

1.	Zijn alle aanbevelingen en maatregelen in dit document direct overgenomen en uitgevoerd?
antwoord	
2.	Zo nee, wat is de status van dit document en in hoeverre zijn de aanbevelingen overgenomen en uitgevoerd?
Antwoord	
3.	Zo nee, wat is de verwachte tijd die de organisatie nodig heeft om deze gaten in de dijk de dichten?
Antwoord	
4.	Kunt u een schatting geven van de kosten die het oplossen van deze problemen met zich meebrengt, ook al is dit opgenomen in het budget?
Antwoord	

In het rapport wordt het volgende aangegeven: “Bij de aanschaf van (IT) producten en diensten worden CISO en de privacy organisatie niet, of (te) laat betrokken, waardoor eisen m.b.t. informatiebeveiliging niet voldoende worden gewaarborgd.”

5.	Kunt u aangeven hoeveel producten, systemen of diensten aangeschaft zijn zonder een check bij de CISO of de privacy organisatie? (Zonder vertrouwelijke informatie weg te geven)
Antwoord	
6.	Kunt u aangeven, in uw eigen schatting, bij hoeveel van deze systemen de gemeente Medemblik een veiligheids- en/of privacy risico loopt? (Zonder vertrouwelijke informatie weg te geven)
Antwoord	

Vanuit de AVG is het verplicht om o.a. bij het op grote schaal verwerken van bijzondere persoonsgegevens een data protection impact assessment (DPIA) uit te voeren. In het rapport van de RKC staat, op pagina 15 bij punt 3.1.8, dat de gemeente weinig tot geen DPIA’s uitvoert en dat dit mogelijk onrechtmatig is.

7.	Bij welke processen is geconstateerd dat er geen DPIA aanwezig was?
Antwoord	
8.	Waarom is ervoor gekozen om geen DPIA uit te voeren, wetende dat dit tegen de AVG is?
Antwoord	
9.	Welke mitigerende maatregelen heeft de organisatie genomen om de gegevens van onze inwoners per direct beter te beschermen?
Antwoord	

In het RKC-rapport is geconstateerd dat de gemeente een beleidsdocument had wat “erg hoog over” was. De werkelijke situatie op de werkvloer verschilde aanzienlijk van de situatie zoals beschreven in de beleidsdocumenten. Zo is er geen sprake van een effectieve PDCA-cyclus en versiebeheer. Dit alles is verplicht vanuit de BIO en bijvoorbeeld basis ISO-normen zoals de ISO 9001 en ISO 27001.

10.	Is het mogelijk om, naast het wettelijke minimum van de BIO, als gemeente te kiezen om ISO 9001 gecertificeerd te worden?
Antwoord	
11.	Zo ja, bent u van mening dat bepaalde constateringen uit het RKC-rapport dan eerder opgevallen waren en opgelost konden worden?
Antwoord	
12.	Zo ja, bent u van mening dat er meer processen zijn binnen de organisatie die baat kunnen hebben van deze ISO-normering?
Antwoord	
13.	Zo nee, waarom niet?
Antwoord	

In het rapport is geconstateerd dat SSC DeSom niet gecertificeerd is volgens de ISO27001 en 27002 norm of zelfs een basis ISO9001 norm.

14.	Deelt u onze mening dat dit een minimumvereiste is voor elke organisatie die met privacygevoelige gegevens omgaat of die systemen levert aan een desbetreffende instantie?
Antwoord	
15.	Zo ja, op welke manier gaat u dit onder de aandacht brengen bij SSC DeSom en op wat voor termijn verwacht u dat deze organisatie zich gaat laten certificeren.
Antwoord	
16.	Zo nee, waarom niet?
Antwoord	

Op pagina 20 wordt aangegeven dat de gemeente Medemblik voornemend is om dit jaar nog een meerjarenplan te presenteren voor de bewustwording van de medewerkers op het gebied van informatieveiligheid te waarborgen.

17.	Welke stappen zijn gemaakt om dit meerjarenplan nog dit jaar kenbaar te maken aan de organisatie?
Antwoord	
18.	Gezien dat er in weinig tot geen gevallen gebruik wordt gemaakt van een PDCA-cyclus. Hoe gaat de organisatie waarborgen dat de menselijke factor in dit hele verhaal beheersbaar wordt?
Antwoord	