1E TERMIJN AGENDAPUNT 5.05 BRIEF REKENKAMERCOMMISSIE OSS OVER HET ONDERZOEK NAAR INFORMATIEVEILIGHEID

1e TERMIJN SP

Op 8 januari jongstleden hebben verschillende fracties van de organisatie een introductie gehad over het IT landschap en organisatie van de gemeente Oss.
Hierbij is kort het onderwerp informatiebeveiliging aan de orde geweest; alles was onder controle zo was in het kort de conclusie toen.
Het is dan ook verontrustend dat de rekenkamer met het extern onderzoek heeft geconcludeerd dat de informatieveiligheid juist onvoldoende is.
De SP fractie is blij met de conclusie dat de aanbevelingen van de rekenkamercommissie integraal worden overgenomen.

Daarnaast adviseert de SP fractie om bij het in çontrol komen van de organisatie rondom informatiebeveiliging verder te gaan dan voorschriften en protocollen.
Om informatiebeveiliging structureel in de cultuur van de organisatie te verankeren is bijvoorbeeld het instellen van een informatieveiligheid werkgroep denkbaar.
In zo'n werkgroep zitten naast de voor informatieveiligheid verantwoordelijke functies vooral ook vertegenwoordigers van alle afdelingen in de organisatie.
Binnen de werkgroep wordt advies gegeven en worden trainingen georganiseerd.
De afdelingsvertegenwoordigers worden daarmee ambassadeurs in hun eigen afdeling voor informatieveiligheid en dragen zo bij tot een cultuurverandering rondom dit onderwerp in alle afdelingen en blijft het geen tot 'IT' beperkt onderwerp.
Vraag aan de portefeuillehouder:
- Hoe denkt de portefeuillehouder vorm te geven aan duurzame aandacht voor informatieveiligheid binnen de gehele organisatie van de gemeente Oss?

1E TERMIJN VDG

Wij kunnen achter het raadsbesluit ten aanzien van informatieveiligheid staan.

Gezien de kwetsbaarheden die aangetoond zijn, zien wij graag een pro-actieve houding van de organisatie om bij het vervolgonderzoek beter uit de bus te komen. Eerder zijn wij vanuit de organisatie als gemeenteraad bijgepraat op het gebied van ICT en alle ontwikkelingen. Dat was een goede sessie. Graag zouden wij weer zo'n sessie hebben voor de zomervakantie 2020 om te bespreken waar we staan op het gebied van ICT en informatieveiligheid.

1E TERMIJN CDA

Het CDA is geschrokken van de uitkomsten van het onderzoek. Wij vinden het goed dat de aanbevelingen vanuit de rekenkamercommissie worden nageleefd en uitgevoerd. In de bestuurlijke reactie van het college wordt gesproken over de maatregelen die direct zijn genomen na de

aanbevelingen. Daarin wordt gesproken over ´het gedrag van medewerkers, beleid en uitvoering met elkaar in samenhang brengen´ Zijn er concrete voorbeelden te geven van deze veranderingen?

1E TERMIJN BETER OSS

Eens met voorstel

1E TERMIJN VVD

De VVD-fractie heeft hier een opmerking bij: Het onderzoek is alleen gericht op de ambtelijke organisatie. Dit geldt voor de meeste onderzoeken naar de informatieveiligheid. In het onderzoek is geen aandacht besteed aan de informatieveiligheid bij raadsleden, terwijl hier naar onze mening een (groot) risico zit. Ibabs is namelijk heel makkelijk toegankelijk en hiermee dus ook alle informatie. Als raadslid ben je namelijk niet verplicht om iedere keer in te loggen met een wachtwoord en/of code via bijv. telefoon. Je kunt Ibabs op je Ipad gewoon open laten staan. De VVD-fractie vraagt hier aandacht voor en zou graag zien dat er stappen worden gezet om de informatieveiligheid bij raadsleden te verbeteren.

1E TERMIJN D66

We hebben tijdens de podiumbijeenkomst geconstateerd dat er flinke hiaten in de beveiliging van de gemeente Oss zitten. D66 maakt zich zorgen. Het herstel heeft inmiddels wel plaatsgevonden. Er komt nl een vervolgonderzoek. Echter op dit moment is de effectiviteit van de getroffen maatregelen nog niet getoetst. Gaat dit nog gebeuren? Is gedrag, beleid en uitvoering genoeg om een en ander 'dekkend' te herstellen? Worden medewerkers hierin goed getraind?
Op welke manier wil de portefeuillehouder in de toekomst borgen dat de er geen hiaten blijven of komen in de informatieveiligheid van de gemeente Oss?

1E TERMIJN GROENLINKS

Tijdens de afgelopen rekeningcommissie werden o.a. vragen gesteld aan de afdeling ICT over hoe gebruik en uitwisseling van informatie binnen onze gemeente binnen veilige kaders geschiedt. Na accountance-controle werden er namelijk vragen gesteld over of de informatieveiligheid binnen het ambtelijk apparaat wel voldoende was. De reactie van de verantwoordelijke ambtenaren was toen dat die informatieveiligheid op orde was, hoewel er natuurlijk wel eens dingen misgaan, maar alles was onder controle.
De vaagheid van deze reactie blijkt een voorspelling te zijn geweest van de uitkomst van het onderzoek dat de rekenkamercommissie heeft ingesteld. Inzet van een ethisch hacker heeft volgens GroenLinks aangetoond dat die informatieveiligheid meer dan onvoldoende was. Dank aan de rekenkamercommissie voor de opzet van dit onderzoek dat in een korte tijd veel aan het licht heeft gebracht.

GroenLinks complimenteert ook de voortvarendheid waarmee ambtelijk Oss met de resultaten van het onderzoek aan de slag is gegaan waardoor de onveiligheid van de Osse informatievoorziening weer hersteld is.
GroenLinks ziet ook een reactie van burgemeester en gemeentesecretaris op het onderzoek. GroenLinks vindt het terecht dat in die reactie wordt gesteld dat "externe ogen" van essentieel belang zijn om ook in de toekomst voortdurend alert te kunnen zijn op het optimaliseren van informatieveiligheid. GroenLinks adviseert om explicieter vast te leggen hoe die externe ogen vanaf nu structureel en planmatig worden ingezet bij het op peil houden van die informatieveiligheid. In de reactie die wij lezen wordt de controle voor de toekomst vooral gezocht binnen de interne processen.
Neemt de portefeuillehouder het advies van GroenLinks over om de inzet van externe ogen voor het vervolg structureel en planmatig te organiseren? En als dat zo is, laat ze de Raad dan weten hoe dat wordt gedaan?
Tot zover onze 1e termijn**.**

1E TERMIJN PVDA

De PvdA is op zijn zachts gezegd geschrokken van de resultaten van het onderzoek dat de rekenkamer heeft laten verrichten m.b.t. het niet in control zijn als het gaat om informatieveiligheid en privacy. De conclusie is van het onderzoek is glashelder: de veiligheid van de systemen waar de gemeente mee werkt is onvoldoende.
Het college heeft in de ogen van de PvdA adequaat gereageerd op de hiaten in het systeem. Daarmee zou je opgelicht adem kunnen halen en kunnen zeggen dat we de hiaten in de informatieveiligheid gelukkig op tijd hebben ontdekt en blij mogen zijn dat er verder geen ongelukken zijn gebeurd.
Toch bevreemd het de PvdA dat in de bedrijfsvoering zelf dat niet eerder is opgemerkt.
De fractie van de PvdA heeft naar aanleiding van de bevindingen van dit onderzoek wel de nodige vragen:
· Heeft het te maken met het piepen en kraken van de organisatie zoals het college dat in de programmabegroting 2020 omschreef? Zo ja, wat gaat het college daar dan aan doen?
· Of heeft het te maken dat er na het mislukken van de samenwerking ict met de omliggende gemeenten in BLOU en is er dus te weinig aandacht is geweest voor de informatieveiligheid? Of is er te weinig geïnvesteerd in nieuwe technieken?
Waarom heeft de accountant de hiaten in de bedrijfsvoering ten aanzien van de informatieveiligheid niet eerder opgemerkt?
En tot slot, vinden we de onder 2 genoemde beslispunt erg cryptisch: 'De Analyse van de overige kwetsbaarheden en het herstel daarvan in te zetten'
Kan de portefeuille houder toelichten wat hier precies mee wordt bedoeld?
En tenslotte de onder vijf genoemde beslispunt vinden we als PvdA wat mager geformuleerd. Wij zouden graag het komende jaar wat vaker en periodiek geïnformeerd willen worden

1E TERMIJN LOF