Retouradres: Postbus 8 3300 AA DORDRECHT

Aan

de heer W.K.B. de Feijter
van fractie ChristenUnie/SGP

p/a raadsgriffie@dordrecht.nl

Gemeente Dordrecht
Spuiboulevard 300
3311 GR DORDRECHT

T 14078
www.dordrecht.nl

Contactpersoon
J.D.H. Verschoor
T +31787707296
E jdh.verschoor@dordrecht.nl

Datum 19 november 2024
Ons kenmerk 2024-0115948
Betreft Beantwoorden artikel 40-vragen inzake Cyberveiligheid

DOSSIER
Afschrift:
- raadsgriffier t.b.v. raads(commissie)leden

Geachte heer De Feijter,

Bij brief van 12 oktober 2024, bij ons ingekomen op 18 oktober 2024, heeft u op grond van artikel 40 van het Reglement van Orde van de gemeenteraad namens fractie ChristenUnie/SGP vragen gesteld inzake cyberveiligheid.
Wij beantwoorden uw vragen als volgt.

Vraag 1. *Heeft het college onderzocht hoeveel cyberaanvallen er zijn uitgevoerd op de gemeente?*

Antwoord Nee, dit is niet onderzocht. Cyberaanvallen vinden continu – op geautomatiseerde wijze – plaats bij vrijwel iedere met het internet verbonden organisatie. Het totaal aantal cyberaanvallen zegt weinig over hun ernst en impact. Bovendien verandert de aard van cyberrisico's voortdurend. Dit bemoeilijkt metingen en maakt ze al snel achterhaald.

Wel vindt er real-time monitoring plaats op onze systemen, wat ons direct waarschuwt bij significante ontwikkelingen. Dit is echter slechts één onderdeel van een groot pakket aan beveiligingsmaatregelen dat niet los van elkaar gezien kan worden.

Vraag 2. *Welk percentage van het ICT-budget is ingeruimd voor de beveiliging van ICT-systemen?*

Antwoord Wij nemen de beveiliging van onze ICT-systemen serieus en kiezen daarom voor een integrale aanpak voor de beveiliging van ICT-systemen. Zo staan onze ICT-infrastructuur en werkplekken tegenwoordig in de beveiligde omgeving van KPN. Hiermee borgen we de veiligheid van onze systemen nu én in de toekomst.

Deze integrale aanpak bemoeilijkt het deze vraag te beantwoorden. Dit heeft twee redenen:

1. Ons ICT-budget is niet verder gespecificeerd naar dit soort kosten. Want de kosten voor het beveiligen van systemen is namelijk vervlochten met andere ICT-kosten. Bijvoorbeeld: Over het algemeen worden de beveiligingskosten bij het aanschaffen van een nieuwe applicatie niet gespecificeerd in de offerte.

2. Beveiliging van ICT-systemen is niet enkel van technische aard en wordt ook niet enkel betaald vanuit het ICT-budget. Onze ICT-systemen worden niet alleen 'beveiligd' door maatregelen in de ICT zelf, maar ook door fysieke en organisatorische maatregelen. Denk hierbij bijvoorbeeld aan toegangsbeveiliging van specifieke ruimten en aan functiescheiding binnen onze processen en aan beleidsafspraken zoals bijvoorbeeld dat medewerkers hun scherm vergrendelen als ze niet achter hun pc zitten.

Vraag 3. *Heeft het college vooruitlopend op de Cyberbeveiligingswet al één of meerdere van de tien maatregelen genomen die voortvloeien uit de wettelijke zorgplicht? Zo ja, welke? Zo nee, hoe draagt het college er zorg voor dat deze maatregelen zo snel mogelijk worden genomen?*

Antwoord Wij hebben alle tien de maatregelen die voortvloeien uit de Cyberbeveiligingswet geïmplementeerd middels maatregelen die gemeentes al verplicht zijn te nemen vanuit de Baseline Informatiebeveiliging Overheid.

Vraag 4. *Wordt er gekeken hoe gevoelige informatie wordt beschermd als een externe partij bijvoorbeeld het ICT-systeem inricht van een overheidsinstelling, zoals een GMR?*

Antwoord Het is voor ons onduidelijk wat u precies bedoelt met "GMR".
Als externe partijen gevoelige gegevens voor ons beheren, dan wordt contractueel vastgelegd welke beveiligingseisen zij moeten hanteren voor het beschermen van deze gegevens. Dit wordt risicogebaseerd bepaald. Dat wil zeggen: hoe gevoeliger de gegevens (en dus hoe hoger het risico), hoe hoger de eisen die wij stellen aan de leverancier.

Vraag 5. *Welke stappen worden ondernomen om gemeentemedewerkers bewust te maken van cyberdreigingen en hun digitale weerbaarheid te vergroten?*

Antwoord Het vergroten van de digitale weerbaarheid van medewerkers wordt bereikt door in te zetten op een aantal onderdelen: bewustwording van gevaren en dreigingen (welke dreigingen zijn er), kennis van procedures en meldingprocessen (hoe en waar meldt men een verdachte situatie) en competenties voor veilig gedrag (hoe herkent en gaat men om met onveilige situaties).

Hierom hebben wij verschillende doorlopende bewustwordings-campagnes en trainingen. Bijvoorbeeld; wekelijkse mailberichten aan medewerkers met een verplichtend karakter om hen bewuster te maken over een bepaald informatiebeveiligingsthema, een poster- en informatiecampagne rondom het herkennen en melden van datalekken en een training voor nieuwe medewerkers.

Vraag 6. *Stelt het college cyberveiligheidseisen aan ketenpartners?*

Antwoord Vanuit onze rol als verwerkingsverantwoordelijke stellen wij dit soort eisen aan onze ketenpartners.

Vraag 7. *Worden de veiligheid van digitale systemen en het personeel jaarlijks ge(pen)test?*

Antwoord Ja, wij voeren jaarlijks pentesten uit op bedrijfskritische systemen. Tevens voeren we minimaal jaarlijks phishing mail campagnes uit.

Vraag 8. *Ligt er een plan klaar in het geval dat de gemeente gehackt zou worden? Omvat dit plan communicatie richting burgers?*

Antwoord Ja, er is een crisismanagement plan en een business-continuïteitsplan voor het geval de gemeente gehackt wordt. Onderdeel van het crisismanagement plan is ook hoe zorg te dragen voor een adequate communicatie richting burgers bij een dergelijke situatie.

Vraag 9. *Is te allen tijde bekend waar gevoelige informatie, zoals persoonsgegevens van burgers, zich bevindt? Staat deze informatie op één plek of is deze verspreid over meerdere plekken?*

Antwoord Privacygevoelige gegevens worden in meerdere applicaties vastgelegd. Middels één register houden we nauwkeurig bij in welke applicatie welke (privacygevoelige) gegevens worden opgeslagen. Bovendien worden back-ups gemaakt van deze gegevens. Ook de locatie daarvan is exact bekend.

Vraag 10. *Zijn de verantwoordelijkheden m.b.t. cyberveiligheid binnen de gemeentelijke organisatie duidelijk verdeeld? Is voor iedereen helder wie de aanspreekpunten zijn binnen de organisatie?*

Antwoord Ja, verantwoordelijkheden zijn duidelijk belegd in ons strategisch informatiebeveiligingsbeleid.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,

Het college van Burgemeester en Wethouders

C.H.W.M. Post
secretaris

P.A.C.M. van der Velden
burgemeester