gemeente
Haarlemmermeer

Aan de Rekenkamercommissie van Haarlemmermeer
T.a.v. mevrouw M. Rosdorff
Postbus 250
2130 AG HOOFDDORP

Postbus 250
2130 AG Hoofddorp

Bezoekadres:
Raadhuisplein 1
Hoofddorp
Telefoon 0900 1852
Faxnummer 023 563 95 50

Cluster Info+
Contactpersoon de heer A.F.M. Witte
Telefoon 0900 1852
Uw brief
Ons kenmerk X.2020.01815
Bijlage(n) Geen
Onderwerp Rekenkamernotitie Resultaten vervolgonderzoek Informatiebeveiliging

Verzenddatum
- 2 JULI 2020

Geachte leden van de Rekenkamercommissie,

Dank voor uw vervolgonderzoek Informatiebeveiliging, in opvolging van uw uitgebreide onderzoek uit 2016 met de titel: 'Bewustwording als sleutel, de staat van de informatiebeveiliging in Haarlemmermeer'. Wij onderschrijven uw keuze om aandacht te besteden aan dit belangrijke onderwerp waarbij u toetst in hoeverre de aanbevelingen van toen door ons zijn opgepakt.
U heeft ons gevraagd om bestuurlijk wederhoor. Met deze brief geven wij u graag onze reactie. Daarbij kijken we eerst terug op de afgelopen vier jaar en hetgeen we hebben gedaan, vervolgens gaan we in op de stappen die nog gezet moeten worden en tenslotte staan we stil bij de conclusies en aanbevelingen in uw rapport.

Terugblik
In afgelopen jaren hebben wij het besluit, dat de raad heeft genomen na het debat over het rekenkamerrapport, omgezet in concrete actie. Zo hebben wij in 2016 de nota 'Informatiebeveiliging op orde' (2016.0022206) opgesteld met een bijbehorend plan van aanpak. Hierin staan zowel de eenmalige als de structurele technische, personele en organisatorische maatregelen en een bijbehorende begroting. In ons Personeelshandboek hebben we in 2017 de verplichting opgenomen dat alle medewerkers een training iBewustzijn volgen en daarvan certificaten behalen. Zonder certificaat kregen medewerkers geen laptop. In maart van dit jaar is een nieuwe versie van deze training verschenen, die voor 1 juli 2020 door medewerkers moet worden gevolgd. In week 26 was de training (met zes modules informatieveiligheid en drie modules privacywetgeving) al door meer driekwart van de organisatie met succes afgerond.

Ook hebben we in de afgelopen jaren veel werk verzet voor de invoering van nieuwe Europese en landelijke verplichtingen, zoals de Algemene Verordening Gegevensbescherming (AVG) en de Eenduidige Normatiek Single Information Audit (ENSIA). In november 2018 hebben we in de

nota 'Privacy, informatiebeveiliging en informatiebeheer' (2018.0076525) het beleid op deze gebieden geactualiseerd en voorgelegd aan de raad.

Sinds 2006 heeft onze gemeente een informatiebeveiligingsadviseur (information security officer, ISO) in dienst. In februari 2019 zagen wij de noodzaak om voor de uitvoering van het herziene beleid op interim-basis een externe Chief Informatie Security Officer (CISO) in de arm te nemen en hem te vragen om advies uit te brengen over hoe we risicogericht de informatiebeveiliging verder kunnen professionaliseren. Zijn bevindingen zijn uitgewerkt in een concreet plan van aanpak voor zowel privacy als voor informatiebeveiliging. In het najaar werden we getroffen door een hack. Dat was voor ons aanleiding tot een versnelling van de maatregelen zoals we hebben toegelicht in de nota 'Extra impuls voor informatiebeveiliging' (2019.0057821). De inzet van de CISO en deze maatregelen zijn uiterst effectief gebleken. Dit heeft er mede toe geleid dat we als één van de weinige overheden in Nederland de Citrix omgeving niet hoefden uit te schakelen toen in december 2019 als gevolg van een groot Citrix-lek wereldwijd tienduizenden bedrijven risico liepen om te worden gecompromitteerd. Bewustzijn creëren op ICT-gebied vinden we belangrijk. Maar ook het toelichten wat we doen en waarom we het doen. Daarom hebben we de raad op 12 december 2019 in een informatieve bijeenkomst geïnformeerd over de risico's op het gebied van informatiebeveiliging.

Vervolgstappen
We beseffen dat we er hiermee nog niet zijn. We zijn bijvoorbeeld nog bezig met de uitvoering van de maatregelen die we hebben beschreven in de nota 'Extra impuls voor informatiebeveiliging'. Daarbij streven wij ernaar om nog dit jaar grotendeels te voldoen aan de Baseline Informatiebeveiliging Overheid (BIO). De BIO omvat echter 18 hoofdstukken met 114 risicobeperkende maatregelen. Dit is dus veelomvattend en vraagt tijd én aandacht. Door het coronavirus moesten bijna alle ambtenaren thuiswerken. Om veilig thuis te kunnen werken, waren maatregelen nodig. Die gaan dan voor. Onderwerpen met hoge beveiligingsrisico's pakken wij altijd als eerste aan. Zo hebben we dit ook afgesproken in onze risicogestuurde aanpak die we hebben vastgesteld in de nota 'Privacy, informatiebeveiliging en informatiebeheer'. Het coronavirus laat zien dat we flexibel moeten zijn en privacy en veiligheid vooropstellen.

De conclusies en aanbevelingen van de Rekenkamercommissie
Wij herkennen veel van de opmerkingen en de conclusies die u maakt in uw notitie. In lijn met uw advies is besloten de CISO én de Functionaris Gegevensbescherming onafhankelijk te positioneren binnen het cluster Corporate Control. Nu de raad het financiële voorstel in de Voorjaarsrapportage 2020 voor de financiële dekking heeft geaccordeerd, zetten wij het proces in gang om een CISO in vaste dienst aan te nemen.

Zoals gezegd onder 'vervolgstappen', ligt de rest van dit jaar de nadruk op het uitvoeren van de aangekondigde maatregelen in de nota 'Extra Impuls voor informatiebeveiliging'. Daarnaast werken wij aan een nieuwe visie op het gebied van verdere digitalisering. Het is ook vanuit de ENSIA én de BIO voorgeschreven om periodiek het informatiebeveiligingsbeleid te actualiseren. Het geactualiseerde beleidsdocument willen we begin 2021 aanbieden aan de raad. Daarin zullen we – in lijn met uw voorstel – onze ambities nader concretiseren. De financiële situatie van de gemeente vormt echter wel een uitdaging bij het nemen van de benodigde aanvullende maatregelen.

In lijn met uw advies hebben wij er nu al voor gekozen om voortaan een jaarlijkse 'pentest' te laten uitvoeren. Het ene jaar wordt van binnen de organisatie getest en het andere jaar vanuit de buitenkant, tenzij er aanleiding bestaat (risicogedreven) om dit eerder te doen. Wat we ook

direct ter harte nemen is de noodzaak voor een structureel en doelmatig bewustzijnsprogramma. We zetten het ingeslagen pad om naar een doorlopende activiteit en zullen dit vastleggen in het geactualiseerde beleidsdocument dat u begin volgend jaar mag verwachten.

In uw notitie heeft u een aantal stellingen opgenomen voor het debat in de gemeenteraad. Met betrekking tot de vierde stelling over samenwerking met andere gemeenten noemen wij twee voorbeelden waaruit blijkt dat wij – waar dat kan – graag samenwerken met andere gemeenten. Zo hebben we er in het afgelopen jaar bewust voor gekozen om voor 'security incident and event monitoring' (SIEM) deel te nemen aan de Europese aanbesteding GGI Veilig van de Vereniging Nederlandse Gemeenten. Ook heeft onze gemeente afgelopen jaar het initiatief genomen om de CISO's van de provincie Noord-Holland periodiek kennis te laten uitwisselen. Daarnaast hebben we veelvuldig contact met de informatiebeveiligingsdienst (IBD) van de VNG en met CISO's van tientallen andere gemeenten.

Er zitten echter ook grenzen aan de mogelijkheden tot samenwerking. De risicoprofielen van gemeenten wijken dusdanig af, dat we op onderdelen ook specifieke eigen maatregelen moeten nemen en eigen kennis en kunde in huis halen.

Slotwoord

Samenvattend nemen wij uw aanbevelingen dus ter harte en zij sterken ons in de uitvoering van de lijn die we met de 'Extra impuls voor informatiebeveiliging' eind 2019 hebben ingezet. Ook is uw rapport een extra aanmoediging om alert te blijven op de continu veranderende dreigingen (zoals hacks en phishing) van buitenaf.

Wij verwachten u hiermee voldoende te hebben geïnformeerd,

Hoogachtend,
burgemeester en wethouders van de gemeente Haarlemmermeer,

de secretaris,	de burgemeester,
drs. Carel Brugman	Marianne Schuurmans-Wijdeven