Gemeente Oegstgeest

Rekenkamercommissie WVOLV
info@rekenkamerwvolv.nl

Z025190144F

Verzenddatum	8 april 2021
Ons kenmerk	Z/21/143111/281082
Contactpersoon	Dhr. B.J.M. Kock
Telefoonnummer	14071

Onderwerp Bestuurlijke reactie onderzoek informatiebeveiliging

Geachte leden van de Rekenkamercommissie,

Hartelijk dank voor het toezenden van het conceptrapport en het ons in de gelegenheid stellen om een bestuurlijke reactie te geven. Wij hebben uw eerdere verzoek om een reactie te sturen over het hoofd gezien. Wij bieden u hiervoor onze excuses aan.

Allereerst willen wij u bedanken voor het onderzoek naar informatiebeveiliging. Dit is een onderwerp dat voor ons hoog op de agenda staat. De gemeente heeft een grote verantwoordelijkheid naar de burgers en ondernemers als het gaat om de beveiliging van gegevens en de continuïteit van dienstverlenging. Digitalisering brengt nieuwe dreigingen en risico's met zich mee. Die manifesteren zich in de ambtelijke organisatie, bij het dagelijks gebruik van informatie- en communicatiesystemen door ambtenaren, maar daarnaast krijgen bestuurders en politiek ambtsdragers veel gevoelige en vertrouwelijke informatie onder ogen en hebben ook toegang tot de gemeentelijke systemen.

De hack op de gemeente Hof van Twente in december 2020 heeft duidelijk gemaakt wat de impact is op de continuïteit van dienstverlening van een gemeente. We bevinden ons in een kat-en-muis spel wat betreft digitale- en cyberveiligheid. Onze detectiesystemen weren dagelijks duizenden aanvallen vanaf het internet af en behoeden ons voor toegang tot malafide websites wanneer een medewerker per ongeluk op een link heeft geklikt. Daarnaast ontvangen wij dagelijks informatie over updates die nodig zijn om kwetsbaarheden in systemen op te lossen. Deze moeten wij in veel gevallen direct oplossen met onze leveranciers, voordat hackers deze misbruiken. Preventief is het noodzakelijk te weten wat de staat van de techniek is en of, en zo ja waar, de systemen kwetsbaar zijn, maar nog veel belangrijker is het gedrag van de medewerkers. Het treffen van technische maatregelen is zinloos als medewerkers onzorgvuldig omgaan met wachtwoorden of zich niet bewust zijn wat de consequenties van hun handelen. Het is belangrijk om te weten hoe de schade zo beperkt mogelijk kan blijven en wat het handelingsperspectief is wanneer het onverhoopt toch fout gaat.

Het onderwerp krijgt steeds meer aandacht en gelukkig ook in de Leidse regio, Oegstgeest, is er geïnvesteerd. Binnen SP71 is er in 2019 een regionaal IB&P team (Informatiebeveiliging en Privacy) opgericht, zijn er een CISO en een FG benoemd en is het informatiebeveiligings- en privacybeleid geactualiseerd. De invoering van de AVG per 28 mei 2018 en de Baseline Informatiebeveiliging Overheid (BIO) per 1 januari 2020 hebben hieraan een extra impuls gegeven. Naar aanleiding van het onderzoek

door de Rekenkamercommissie Leiden/Leiderdorp in 2018 zijn er op de infrastructuur van de Leidse Regio, waar Oegstgeest onderdeel van uitmaakt, technische maatregelen getroffen. Zo worden de "buitengrenzen" van het ICT-domein bewaakt op verdachte verkeersstromen en is er een dienstverlening ingericht die periodiek scant op kwetsbaarheden of open deuren waar hackers actief misbruik van zouden kunnen maken. Daarnaast is er veel aandacht voor het vergroten van veilig gedrag en bewustzijn bij medewerkers.

Kortom, we achten informatiebeveiliging van groot belang en werken er samen met onze partners hard aan om de informatiebeveiliging op peil te houden en te versterken.

In uw rapport doet u een aantal bevindingen en geeft u aanbevelingen. Hierna gaan wij hierop in. Onder de betreffende bevinding of aanbeveling treft u steeds onze reactie aan.

Bevindingen
Het onderzoek leverde positieve en zorgwekkende bevindingen op. Het merendeel van de bevindingen vergt extra aandacht.

Positief:
Het informatiebeveiligingsbeleid en de organisatie rondom informatiebeveiliging bij de gemeenten zijn op orde. De meeste verbonden partijen hebben een informatiebeveiligingsbeleid opgesteld, dat periodiek wordt bijgesteld. Daarnaast werken de gemeenten aan bewustwording over informatiebeveiliging en privacy. Betrokkenen worden geïnformeerd bij een datalek. En het aantal datalekken wordt vermeld in de jaarrekeningen.

Zorgwekkend:
1. de gemeentelijke IT-netwerken zijn kwetsbaar door de aanwezigheid van verouderde software, cipher suites en protocollen voor encryptie, en door het gebruik van foute headers. Dit is aangetoond door de penetratietesten;

Reactie:
Er zijn volgens het rapport verouderde systemen aangetroffen. Deze systemen zijn in beeld bij Servicepunt71 omdat de ICT-infrastructuur periodiek wordt gescand. In sommige gevallen zijn kwetsbaarheden niet op te lossen. Bijvoorbeeld wanneer systemen dermate verouderd zijn dat de leverancier hier geen updates meer voor levert. Deze systemen zijn in beeld en gekoppeld aan projecten. Een groot deel van deze systemen verdwijnt wanneer de Leidse regio is gemigreerd naar de nieuwe digitale werkplek KNTR71, of wanneer grote vervangingstrajecten van bedrijfsapplicaties zijn afgerond. Daarnaast zijn er in Q42020 en Q12021 al veel verouderde systemen opgeruimd. De systemen die verouderd zijn en daardoor kwetsbaarheden bevatten hebben allemaal verhoogde dijkbewaking vanuit ons SOC en zijn geïsoleerd bij de ICT-leverancier om het risico op misbruik te voorkomen. De tekortkomingen die zijn geconstateerd op het digitaal fotoarchief, waren ernstig, maar hebben geen impact op de dienstverlening van de gemeente Oegstgeest. De website staat op zichzelf en heeft geen koppeling met achterliggende systemen. Alle geconstateerde tekortkomingen op de website van het digitaal fotoarchief zijn na bekend worden opgelost door de webmaster van Oegstgeest.

2. de gemeenten voeren te weinig penetratietesten en kwetsbaarhedenscans uit.

Reactie:
De leveranciers van zowel de websites van de Oegstgeest als van onze volledige ICT-infrastructuur voeren jaarlijks aantoonbaar penetratietesten uit, waar SP71 als ICT-organisatie verantwoording over krijgt en op steunt. De webservices van Oegstgeest die de primaire/publieke taken van de gemeente Oegstgeest ondersteunen zijn uitbesteed aan een externe partij. Deze partij wordt jaarlijks gepentest door Duijnborgh en is derhalve door de auditor/onderzoeker bewust buiten scope geplaatst omdat hij kon steunen op deze gegevens. De website die vervolgens gevonden en getest is (digitaal fotoarchief) was verouderd en bevatte de gerapporteerde tekortkomingen. Echter deze tekortkomingen zijn ernstig voor het digitaal fotoarchief maar hebben geen impact op de dienstverlening van de gemeente Oegstgeest. Er kunnen ook geen transacties uitgevoerd worden middels de pagina met impact op financiële systemen.

Extra aandacht:
3. de gemeenten beoordelen niet-systematisch de operationele procedures, voeren niet-systematisch risicoanalyses uit, inventariseren niet-systematisch de risico's met verbonden partijen, en passen het informatiebeveiligingsbeleid niet aan;

Reactie:
Vanuit de VNG/IBD is het dreigingsbeeld Nederlandse Gemeenten 2021-2022 opgesteld. Hierin staan generieke risico's beschreven gericht op de ambtelijke organisatie, het openbaar bestuur en de politiek en de burgers en bedrijven. Waar de organisatie in 2021 nog een verantwoording aflegt op de generieke risico's zoals benoemd in het dreigingsbeeld, dienen de risico's toekomstig meer toegespitst op specifieke processen en ketens gericht te zijn om eventuele cascade-effecten in beeld te krijgen. Daartoe worden in 2021 risicoanalyses uitgevoerd. De operationele procedures conform de rijksbrede normen van BIO worden door ons geïmplementeerd. Gedurende 2020 (en tijdens het onderzoek) was dit gedeeltelijk onderhanden werk, was een groot deel afgerond en geïmplementeerd in onze processen. Een aantal documenten wordt nog nader uitgewerkt of is behandeling bij de OR voor instemming. De opgave hierop is in beeld.

4. de gemeenten hebben een onvolledig en/of gedateerd verwerkingsregister;

Reactie:
Zie de reactie op aanbeveling 4, die verderop in deze brief volgt.

5. de gemeenten hebben de informatiebeveiligingsrisico's en beheersingsmaatregelen niet opgenomen in de paragraaf Weerstandsvermogen van de programmabegroting (= aangenomen aanbeveling in 2016);

Reactie:
Door beter aan te sluiten bij de P&C-cyclus en afstemming met concerncontrollers moet bewerkstelligd worden dat de beheersingsmaatregelen een plek krijgen in de paragraaf weerstandsvermogen. Overigens worden niet alle risico's die geïnventariseerd worden zichtbaar in de paragraaf weerstandsvermogen, omdat alleen de grootste risico's daarin vermeld worden.

6. de gemeenten geven geen sturing aan de verbonden partijen op het gebied van informatiebeveiliging (= aangenomen aanbeveling in 2016).

Reactie:
Digitale weerbaarheid vraagt met nadruk om een ketenbenadering, waar naast de veiligheidsregio bijvoorbeeld ook Holland Rijnland, de sociale jeugdteams, de omgevingsdienst en bijv. belastingsamenwerking onderdeel van uitmaken. We voelen ons als eigenaar van de gegevens die ketenpartners verwerken nadrukkelijk (mede)verantwoordelijk voor informatiebeveiliging bij de ketenpartners. De risico-gerichte aanpak zoals genoemd onder 3 start met het inzichtelijk maken van wat verantwoordelijkheid voor informatiebeveiliging betekent voor de keten, de keten is immers zo sterk als de zwakste schakel. De gemeente moet kritisch zijn richting de zwakste schakels en eisen stellen aan de ketenpartners. Dat betekent ook het stellen van maatregelen m.b.t. informatieveiligheid als randvoorwaarde binnen ketensamenwerkingen. We hebben hierin samen met onze partners nog een slag te slaan, maar zijn inmiddels op weg. Het geven van sturing is alleen mogelijk in goede samenwerking met de verbonden partijen zelf en de participerende gemeenten.

Reactie op aanbevelingen uit het Algemene openbare rapport

Aanbeveling 1: de IT-netwerken te versterken door de geconstateerde kwetsbaarheden op te heffen;

Reactie:
Als reactie op de resultaten van de penetratietest zijn direct maatregelen getroffen op de pagina van het digitaal fotoarchief, Deze moesten voorzien in het wegnemen van de geconstateerde risico's en kwetsbaarheden. Het interne netwerkverkeer wordt continu gemonitord en gecontroleerd om tijdig te in te grijpen bij hack pogingen.

Aanbeveling 2: minimaal jaarlijks penetratietesten en kwetsbaarhedenscans uit te voeren;

Reactie:
Naar aanleiding van het onderzoek door de Rekenkamercommissie Leiden/Leiderdorp in 2018 zijn er technische maatregelen getroffen. Zo worden de "buitengrenzen" van het ICT-domein bewaakt op verdachte verkeersstromen en is er een dienstverlening ingericht die periodiek scant op kwetsbaarheden of open deuren waar hackers actief misbruik van zouden kunnen maken. De leveranciers van zowel de websites van de Oegstgeest als van onze volledige ICT-infrastructuur voeren jaarlijks aantoonbaar penetratietesten uit, waar SP71 als organisatie verantwoording over krijgt en op steunt.

Aanbeveling 3: Systematisch operationele procedures te beoordelen, systematisch risicoanalyses uit te voeren, systematisch de risico's met verbonden partijen te inventariseren, en het informatiebeveiligingsbeleid zo nodig aan te passen;

Reactie:
Wij verwijzen u hiervoor naar onze reactie bij bevinding 3.

Aanbeveling 4: het verwerkingsregister volledig en/of geactualiseerd te maken;

Reactie:
De onderzoekers hebben eind juni 2020 kennisgenomen van een register in ontwikkeling waarin overigens de relevante processen zijn opgenomen en verantwoord. Dit register is in het najaar van 2020 generiek gecontroleerd door contactpersonen binnen de afdelingen van de gemeente. De laatste toevoeging dateert van maart 2021 (proces bij Burgerzaken). Het register is via intranet raadpleegbaar en er is zoals door de

onderzoekers ook is vastgesteld een procedure beschikbaar voor het aanmelden van wijzigingen en updates. Het register is een dynamisch overzicht. We herkennen in die zin het beeld niet dat het register niet volledig is en/of geactualiseerd wordt. Wij hebben de ambitie om de verwerkingen periodiek en risicogericht te reviewen. Dat maakt onderdeel uit van het 'privacy programma' waarin dergelijke procedures van 'ad hoc'-maatregel door ontwikkelingen naar 'control' maatregelen.

Aanbeveling 5: de informatiebeveiligingsrisico's en beheersingsmaatregelen op te nemen in de paragraaf Weerstandsvermogen en in een speciale paragraaf informatiebeveiliging in de gemeentelijke programmabegroting;

Reactie:
Wij zullen overwegen of wij een aparte paragraaf informatiebeveiliging zullen opnemen in de programmabegroting. Dit hangt samen met onze insteek om de programmabegroting met name te richten op nieuwe ontwikkelingen. Overigens hebben wij zowel en de programmabegroting van 2019 als 2020 aandacht besteed aan dit onderwerp.

Aanbeveling 6: sturing te geven aan de verbonden partijen op het gebied van informatiebeveiliging;

Reactie:
Wij verwijzen hier naar bevinding nummer 6.

Aanbeveling 7: kennisuitwisseling over informatiebeveiliging te stimuleren tussen FG's, CISO's en verbonden partijen;

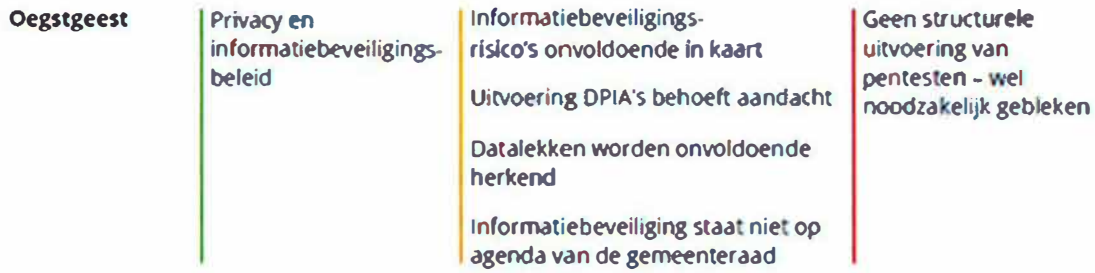
Reactie:
Oegstgeest werkt naast Leiden, Leiderdorp en Zoeterwoude ook nauw samen met de Holland Rijnland – gemeenten ook vanuit het perspectief van de veiligheidsregio Hollands Midden. Daarnaast onderhouden de FG en CISO goede contacten met hun collega functionarissen in de Bollenstreek en de gemeente Den Haag. Er vindt collegiaal overleg plaats, ook met betrekking tot vraagstukken ten aanzien verbonden partijen waarin onze gemeenten participeren. De contacten met de functionarissen van de verbonden partijen – behoudens Holland Rijnland - zijn tot dusver vooral functioneel en incident gedreven geweest. We streven ernaar om deze contacten verder aan te halen en tot meer onderlinge kennisuitwisseling te komen.

Aanbeveling 8: het onderwerp informatiebeveiliging en privacybeleid jaarlijks afzonderlijk te agenderen en de betrokkenheid van de gemeenteraad hierbij te vergroten (bijvoorbeeld door training).

Reactie:
De gemeenteraad heeft sinds de inwerkingtreding van de AVG interesse getoond in de voortgang van de implementatie. De commissie is in het voorjaar van 2020 bijgepraat middels een informatieve sessie. We zijn uiteraard bereid om daar een vervolg aan de geven. We adviseren om dit raadsbreed aan te bieden omdat gegevensbescherming en – breder – cybersecurity voor eenieder relevant is. Niet alleen vanuit kaderstellend en controlerend perspectief, maar ook voor de werkzaamheden van de raadsleden zelf en de maatschappelijk impact.

Conclusies per gemeente
Ook op de conclusies voor Oegstgeest hebben wij een reactie.

groen: op orde | oranje: aandacht nodig | rood: zorgwekkend



DPIA's "gegevensbeschermingeffectbeoordelingen" – behoeft aandacht
Tijdens de besprekingen met de onderzoekers hebben wij reeds toegelicht dat de DPIA's regionaal worden uitgevoerd omdat dit veelal regionale (i.c. de SP71-gemeenten) projecten betreft. We noemen als voorbeeld de invoering van een regionale toegangspas en de software suite voor applicaties binnen het sociaal domein. Projecten starten met het uitvoeren van een zogenaamde 'baselinetoets'. Als hieruit blijkt dat er persoonsgegevens of andere vertrouwelijke en/of gevoelige gegevens worden verwerkt, waarbij waarschijnlijk sprake is van een hoog risico, dan is het uitvoeren en van een DPIA en een aanvullende risicoanalyse op de beveiligingsaspecten verplicht. Binnen Oegstgeest zijn er weinig nieuwe verwerkingen geweest die aan dit criterium voldoen.

Wel merken we op dat het de ambitie is om ook bestaande verwerkingen risicogericht periodiek te 'reviewen' ongeacht of er zich wijzigingen in het proces hebben voorgedaan. Daarmee krijgen ook reeds langer bestaande processen een kritische blik en worden daar waar nodig aanpassingen doorgevoerd. De maatregel krijgt aandacht vanuit het 'privacy-programma'.

Datalekken worden onvoldoende herkend
Er worden in Oegstgeest relatief weinig datalekken gemeld. Het is de vraag of daarmee kan worden geconcludeerd dat datalekken onvoldoende worden herkend. Zeker na het datalek in 2016 is het bewustzijn sterk gestegen. Wij hebben het datalek geëvalueerd en hiervan geleerd. Wij blijven werken aan de bewustwording rondom het herkennen en melden van datalekken. We zijn nu in onze contracten veel strakker op informatieveiligheid bij onze leveranciers.

Informatiebeveiliging op de agenda van de gemeenteraad
Hier verwijzen wij naar de aanbeveling nummer 8.

Tot slot

U heeft een aantal stevige bevindingen gedaan en aanbevelingen gedaan. Deze zouden het beeld kunnen geven dat wij onvoldoende of ondermaats presteren als het om informatiebeveiliging gaat. Wat ons betreft zou een dergelijk beeld geen recht doen aan de staat van en inspanningen op het de onderwerpen informatiebeveiliging en privacy. Zoals u ook in onze reactie kunt lezen voldoen wij aan veel van uw aanbevelingen en bevindingen. Dit belet ons niet om onze verdere stappen te nemen om de informatiebeveiliging op een hoger plan te brengen, samen met onze partners.

Hoogachtend,
burgemeester en wethouders van Oegstgeest,

Jeffrey Versluis
secretaris

Emile Jaensch
burgemeester