Aan de fractie van Leefbaar 3B
T.a.v. de heer Duivesteijn en de heer Philippens

Van	College van B&W
Onderwerp	**Beantwoording raadsvragen Leefbaar 3B Maatregelen tegen ongemerkt zoeken in geheime gegevens in de ambtelijke organisatie**
Datum	**5 juli 2022**
Ons kenmerk	U22.03193
Uw brief van	20 mei 2022

Geachte heren Duivesteijn en Philippens,

Op 20 mei 2022 heeft u raadsvragen ingediend met betrekking tot maatregelen die worden genomen tegen ongemerkt zoeken in geheime gegevens in de ambtelijke organisatie. Met deze brief geven wij u antwoord op uw vragen.

Algemene toelichting
De afgelopen jaren maakte de gemeente forse stappen op het gebied van informatiebeveiliging. Het rekenkameronderzoek naar de stand van zaken van de informatiebeveiliging binnen de gemeente Lansingerland is daarbij één van de onderleggers geweest om verbeteringen te realiseren. Een grote stap in het verbeteren van de informatieveiligheid is het project TOP-werken geweest. Zowel op het niveau van het netwerk als de hardware zijn hierbij belangrijke verbeteringen doorgevoerd op informatie-veiligheid. Een aantal ‘veiligheidsprojecten’ zoals de implementatie van SIEM/SOC loopt nog. Met deze lopende projecten verhogen we het niveau van de informatieveiligheid de komende periode nog verder.

Via de paragraaf bedrijfsvoering bent u de afgelopen jaren apart geïnformeerd over de stand van zaken met betrekking tot ICT en informatiebeveiliging.

Vraag 1
Is het college op de hoogte van dit nieuwsartikel?

Antwoord vraag 1
Het college is op de hoogte van dit nieuwsartikel.

Vraag 2
Is er in de ambtelijke organisatie in Lansingerland sprake van vrije toegang tot alle systemen?

a. *Zo ja; acht het college dit wenselijk en noodzakelijk?*
b. *Zo nee; welke protocollen en checks en balances zijn er in de organisatie om te voorkomen dat er oneigenlijk gebruik gemaakt wordt van beschikbare informatie?*

Antwoord vraag 2
Nee. Er is geen sprake van vrije toegang tot de informatiesystemen van de gemeente Lansingerland. Er is een toegangsbeleid voor zowel de beveiliging van fysieke ruimten als voor de toegang tot informatie-systemen. Daarnaast zijn er verschillende procedures met betrekking tot het verlenen van toegang, die regelen hoe de toegang moet worden aangevraagd en welke eisen er zitten aan het verlenen van de toegang. Ook is er een wachtwoordbeleid, waarin eisen worden gesteld aan de wijze van toegang en de toegangsbeveiliging van de informatiesystemen zelf en waarin wordt afgedwongen het wachtwoord periodiek te wijzigen. Binnen de informatiesystemen wordt onderscheid gemaakt in de soorten toegang tot informatie. Door middel van autorisaties wordt ervoor gezorgd dat medewerkers alleen toegang hebben tot de informatie die ze ook echt nodig hebben voor hun werkzaamheden. De uitvoering van het beleid en de procedures wordt middels periodieke controles nagegaan.

Om een voorbeeld te geven; voor het verkrijgen van toegang tot het netwerk is altijd een tweede factor nodig.

Vraag 3
Wordt er vastgelegd (gelogd) wie welke informatie opvraagt?

a. *Zo ja; worden deze logfiles ook gecontroleerd, steekproefsgewijs en in welke frequentie en regelmaat?*
b. *Zo nee; wordt deze noodzakelijke beveiligingsmaatregel ingevoerd en wanneer?*

Antwoord vraag 3
Op vele vlakken binnen de organisatie wordt er gelogd. Deze logfiles worden nog niet altijd gestructureerd geanalyseerd en gecontroleerd. Voor Suwinet (bevat van alle inwoners van Nederland onder andere gegevens over uitkeringen, werk, re-integratie, voertuiggegevens en opleidingen) is dit wel het geval. Suwinet rapportages worden ieder kwartaal gecontroleerd en intern besproken en er wordt gewerkt met een zogenoemde ‘white-list’ (alleen voor personen op de ‘white-list’ zijn, op basis van doelbinding van de raadpleging, raadplegingen mogelijk, dus niet voor iedere inwoner van Nederland). Daarnaast wordt per applicatie kritisch gekeken wie welke toegang nodig heeft en hebben medewerkers dus enkel toegang tot de gegevens die nodig zijn voor de uitvoering van hun werkzaamheden.

Controle op de logging zou voor meer applicaties moeten gebeuren, dit vergt ambtelijke inzet. Teammanagers dienen dit te organiseren voor de applicaties waar zij verantwoordelijk voor zijn. Het uitbreiden van controles op logging (op basis van een risicoanalyse) binnen de organisatie is ook onderdeel van de verdere doorontwikkeling van privacy en informatiebeveiliging waarvoor extra capaciteit aangevraagd is. Als verbeteractiviteit staat dit ook in het door de directie vastgestelde (jaar)plan informatiebeveiliging 2022-2023.

Het nalopen van logging vereist veel capaciteit van applicatiebeheerders en vereist ook iets van een systeem; er moet bijvoorbeeld gefilterd kunnen worden op bepaalde informatie. Het is zeer tijdrovend om handmatig door alle bestaande logging heen te gaan.

Momenteel loopt er daarom binnen de organisatie een aanbesteding betreffende een SIEM & SOC. Marktoriëntatie heeft inmiddels plaatsgevonden en momenteel wordt er gewerkt aan het programma van eisen. SIEM staat voor Security Incident and Event Monitoring. Middels een SIEM kun je gestructureerd en geautomatiseerd servers, applicaties en databases monitoren. Hierdoor kan onder andere in een vroeg stadium misbruik van systemen gedetecteerd worden. De SOC (het Security Operations Center) zal de omgeving monitoren op afwijkingen, logs analyseren en rapporteren aan de gemeente. Incidenten/ bevindingen worden conform prioritering die het SOC aanbrengt vervolgens intern opgepakt.

Risicogebaseerd zal per systeem bekeken worden of logging mogelijk is en of het te koppelen is aan een SIEM. Daarnaast wordt er komende tijd (gekoppeld aan de SIEM & SOC aanbesteding) een loggingsbeleid en procedure opgesteld voor de organisatie. Nadat dit beleid en procedure formeel zijn zal de controle op logging binnen applicaties verder worden uitgebreid.

Vraag 4
Welke aanbevelingen uit het Rekenkamer Rapport "wat niet weet, maar wel deert" (2017; p. 16, p. 17) zijn inmiddels opgevolgd en op welke wijze? Als ze niet zijn opgevolgd, waarom niet?

Gezien de conclusies uit het onderzoek doet de rekenkamer de volgende aanbevelingen aan het college van B en W.

> **Onderdeel 4.1.a rekenkamer rapport**
> *Stel veiligheidsrisico's, in plaats van beveiligingsnormen, centraal bij de inrichting van informatiebeveiliging:*
> *a. Voer voor de informatiesystemen, die volgens de risicoclassificatie een hoog risico kennen, een diepgaande risicoanalyse uit, waarbij een inschatting wordt gemaakt van de kans dat een risico zich voordoet en de impact als een risico zich voordoet; hierbij gaat het niet alleen om gevolgen voor de gemeentelijke organisatie, maar met name ook voor de burgers.*
>
> **Beantwoording 4.1.a**
> Vanuit informatiebeveiliging worden bij grote wijzigingen en nieuwe aanbestedingen baseline-toetsen uitgevoerd. Uit deze toetsen komt een beveiligingsniveau conform de BIO. Afhankelijk van het beveiligingsniveau dienen (aanvullende) maatregelen genomen te worden voor de beveiliging in processen/applicaties en systemen.
>
> In 2018 is voor het laatst een gemeentebrede risicoanalyse uitgevoerd. De bevindingen hieruit zijn opgepakt of onderdeel van jaarplannen. De gemeentebrede risicoanalyse staat voor dit jaar opnieuw gepland (in het jaarplan).
>
> Dit jaarplan is risicogebaseerd opgesteld op basis van onder andere de BIO. Hiervoor heeft een GAP-analyse plaatsgevonden waarbij is gekeken welke onderdelen van de Baseline Informatie-veiligheid Overheid (BIO) nog niet (voldoende) zijn geïmplementeerd. Deze onderdelen zijn ingeschaald op basis van kans en impact en de uitkomsten hiervan hebben de prioritering in het jaarplan bepaald. Hierbij wordt (impliciet) een afweging gemaakt waar de grootste risico's voor de organisatie, bestuurders en/of betrokken/burgers zitten.
>
> Daarnaast zijn in het jaarplan onder andere de uitkomsten van de jaarlijkse ENSIA-verantwoording (ENSIA wordt door gemeenten, provincies, waterschappen en enkele onderdelen binnen de rijksoverheid gebruikt om zich te verantwoorden over de staat van informatiebeveiliging op basis

van de BIO en het gebruik van de Geo-basisregistraties), informatie vanuit de informatie-beveiligingsdienst (IBD) en het Nationaal Cyber Security Center (NCSC), lessen uit grootschalige incidenten en lessen uit interne incidenten meegenomen.

In het jaarplan informatieveiligheid 2022/2023 zijn diepgaande risicoanalyses op informatie-systemen opgenomen. De prioritering van de uitvoering van deze risicoanalyses is bepaald aan de hand van een risico inschatting die is gedaan op alle gemeentelijke applicaties en systemen in het kader van beschikbaarheid, integriteit en vertrouwelijkheid van de informatie hierin. Momenteel zijn de diepgaande risicoanalyses in uitvoering.

Onderdeel 4.1.b rekenkamer rapport
Neem passende maatregelen om de specifieke risico's die uit deze analyses naar voren komen te mitigeren (of accepteer de risico's).

Beantwoording 4.1.b
Dit is een logisch vervolg op a. De specifieke maatregelen zijn opgenomen in het jaarplan informatieveiligheid, in behandelplannen of zijn reeds uitgevoerd.

Onderdeel 4.1.c rekenkamer rapport
Maak een planning voor de implementatie van de maatregelen.

Beantwoording 4.1.c
Dit is een continu proces. Daarnaast is dit onderdeel van het jaarplan. Het laatste jaarplan gaat over 2022-2023.

Onderdeel 4.2 rekenkamer rapport
Stel voor de uit te voeren beveiligingsmaatregelen de benodigde middelen ter beschikking, voer de maatregelen daadwerkelijk onverkort uit en laat per kwartaal door de Chief Information Security Officer (CISO) rapporteren over de voortgang en de resultaten daarvan. Grijp in als de resultaten afwijken van de verwachting

Beantwoording 4.2
De CISO rapporteert ieder kwartaal over voortgang en resultaten van het jaarplan aan de directie. Uit de voortgang van de afgelopen 1-1,5 jaar blijkt dat een deel van de beveiligingsmaatregelen pas effectief geïmplementeerd kan worden als er ook voldoende 'ambtelijke' capaciteit is om dit te doen en te kunnen monitoren. Via de P&C cyclus zijn en worden hier dan ook middelen voor aangevraagd, o.a. via de begroting 2022 (voorstel eerste begrotingswijziging 2022).

Onderdeel 4.3 rekenkamer rapport
Pak systematisch en gericht de diverse kwetsbaarheden aan die uit de interne penetratietest naar voren zijn gekomen en monitor dit door middel van een kwartaalrapportage. Beoordeel uiterlijk na een jaar aan de hand van een nieuwe interne penetratietest of de kwetsbaarheden naar behoren zijn aangepakt.

Beantwoording 4.3
Met de inrichting van de nieuwe werkplek (TOP-werken) zijn de bevindingen uit de interne penetratietest meegenomen en opgelost. Uit de interne penetratietest van eind 2021 blijkt dat alle constateringen van het rekenkameronderzoek zijn opgepakt. Daarnaast is intern een kwetsbaarheden scan tool aangeschaft. Hiermee kan ad hoc inzicht worden verkregen in eventuele kwetsbaarheden. Deze kwetsbaarheden worden risico gebaseerd opgepakt. Tevens zijn er wekelijks (en indien nodig meer) gesprekken tussen ICT

en informatiebeveiliging om kwetsbaarheden te bespreken en afhankelijk van prioritering op te pakken. In deze gesprekken wordt tevens de voortgang bewaakt.

Onderdeel 4.4 rekenkamer rapport
Verbeter de toegangsbeveiliging op kantoorlocaties, daarbij gebruikmakend van de uitkomsten van de inlooptest van de rekenkamer. Beoordeel uiterlijk na een jaar met nieuwe inlooptesten of de zwakke plekken zijn verholpen.

Beantwoording 4.4
Naar aanleiding van het rekenkameronderzoek is de toegangsbeveiliging aangescherpt en is extra aandacht gegaan naar de bewustwording van medewerkers. Concrete voorbeelden van verbeteringen die zijn aangebracht zijn:

- Het verstrekken van pashouders en keycords, zodat medewerkers van Lansingerland en ingehuurde medewerkers zichtbaar te herkennen zijn.
- Er zijn paslezers aangebracht in de liften
- Er zijn procedures en controles ingericht op het gebied van clean desk/clear screen
- Een jaarlijkse gebouwcheck om te kijken hoe de fysieke veiligheid ervoor staat.
- In 2019 heeft er een hertest plaatsgevonden.
- De raadszaal is voorzien van sloten en zit op slot als deze niet gebruikt wordt.

Aandachtspunten die er zijn met betrekking tot de fysieke toegang zijn onderdeel van het jaarplan informatiebeveiliging. Er vinden periodiek gesprekken plaats met de teammanager exploitatie. Uitvoering van de verbeterpunten is binnen de organisatie in de lijn belegd en hiermee dus verantwoordelijkheid van de teammanager exploitatie. Gezien de huidige bouwkundige inrichting van het gemeentehuis blijft het gemeentehuis kwetsbaar. Dit is ook een gevolg van de destijds bij de bouw van het gemeentehuis gewenste open en multifunctionele karakter van het gemeentehuis.

Conform jaarplan zal er dit jaar opnieuw een inlooptest plaatsvinden.

Daarnaast is met TOPwerken geregeld dat toegang tot het netwerk binnen het gemeentehuis alleen mogelijk is met een laptop of een device van de gemeente zelf. Indien een kwaadwillende zich toch toegang heeft verschaft tot het netwerk, dan komt deze terecht op het gastennetwerk. Het gasten-netwerk is gescheiden van het gemeentelijk netwerk.

Onderdeel 4.5 rekenkamer rapport
Versterk het bewustzijn van medewerkers ten aanzien van informatiebeveiliging door een awareness programma. Beoordeel met testen in welke mate dit awareness programma effectief is geweest.

Beantwoording 4.5
Bewustwording is een terugkerend en belangrijk onderdeel van de jaarplannen informatiebeveiliging. Bewustwording bestaat onder andere uit:
Sessies voor nieuwe medewerkers, kwartaalrapportages, uitvoeren dPIA's en baselinetoetsen, uitvoeren van controles, aansluiten bij teamoverleggen, uitnodigen spreker, berichtgeving via intranet.
In 2019 hebben telefonische en online phishingtesten plaatsgevonden om de effectiviteit van de awareness te testen.
Dit zal in 2022 opnieuw plaatsvinden. Ondanks de continue aandacht en berichten hierover zal naar aanleiding van de bevindingen uit deze testen specifieke aandacht worden besteed aan de aandachts-punten die naar voren zullen komen in de testen.

Onderdeel 4.6 rekenkamer rapport
Neem alle mogelijke organisatorische en technische maatregelen om (onbewust) slordig omgaan met vertrouwelijke informatie door medewerkers te voorkomen.

Beantwoording 4.6
Deze aanbeveling is ontzettend ruim. Er worden diverse maatregelen genomen om slordig omgaan met vertrouwelijke informatie door medewerkers te voorkomen. Onder andere bewustwording bij medewerkers, oppakken van verbeteracties n.a.v. incidenten en datalekken, oppakken en meenemen van bevindingen uit DPIA's en baselinetoetsen en het automatisch locken van het beeldscherm na een periode inactiviteit. Ook is printen alleen mogelijk met gebruik van een persoonlijke toegangspas. Maatregelen worden genomen op basis van een bepaald risico. De afweging wordt hierbij gemaakt of het zinvol is om bepaalde maatregelen in te voeren.

Onderdeel 4.7 rekenkamer rapport
Neem maatregelen tegen de kwetsbaarheden die uit de externe penetratietest van de rekenkamer naar voren zijn gekomen.

Beantwoording 4.7
4.1.1 Sophos onnodig benaderbaar vanaf het internet
Is destijds direct opgepakt en opgelost. Inmiddels is Sophos overigens niet meer in productie.

4.1.2 Verouderde Javascript bibliotheken op de website van Lansingerland.nl
Is destijds direct opgepakt en opgelost. Inmiddels is de website vernieuwd. De website wordt tevens meegenomen in pentesten die periodiek worden uitgevoerd. Daarnaast toetst het Rijk per kwartaal de veiligheid van gemeentelijke websites en e-mail. De website(s) van Lansingerland is in de laatste test als 'goed' bestempeld. Informatie hierover is te vinden op: https://www.forumstandaardisatie.nl/

4.1.3 Cross-Site Scripting (Reflected)
Is destijds direct opgepakt en opgelost. Inmiddels is de website vernieuwd. De website wordt tevens meegenomen in pentesten die periodiek worden uitgevoerd.

4.1.4 Metadata
Is destijds direct opgepakt en opgelost. Inmiddels is de website vernieuwd. De website wordt tevens meegenomen in pentesten die periodiek worden uitgevoerd.

Onderdeel 4.8 rekenkamer rapport
Beoordeel uiterlijk na een jaar met een nieuwe externe penetratietest of er nog kwetsbaarheden in de beveiliging tegen cyberaanvallen zitten en neem eventuele passende maatregelen.

Beantwoording 4.8
Vanwege beperkte ICT-capaciteit en het TOP-werken project waarin veel van de aanbevelingen uit het rekenkamer onderzoek zijn meegenomen heeft herhaling van de pentesten later plaatsgevonden dan uiterlijk een jaar na het rapport van de Rekenkamer. Uit de laatst uitgevoerde pentest (december 2021) zijn enkel laag en midden risico bevindingen gedetecteerd. Deels zijn deze opgepakt (op basis van prioritering), deels onderdeel van het jaarplan informatieveiligheid 2022-2023.

Onderdeel 4.9.a rekenkamer rapport
Richt volwassen contractmanagement in, inclusief een Service Level Agreement met de leverancier en een periodieke verantwoording over de afspraken die daarin zijn vastgelegd.

Beantwoording 4.9.a
Contractmanagement is ingericht binnen de organisatie. Dit is nog niet overal binnen de organisatie even ver ontwikkeld en heeft aandacht nodig. Bij nieuwe inkooptrajecten is informatiebeveiliging voor de gehele organisatie een standaard onderdeel van de inkoop-procedure. Voorafgaand aan de aanbesteding wordt risico gebaseerd bepaald welke beveiligings-eisen meegenomen dienen te worden in contracten.
Vanuit het Haagse Beek traject waarin functies opnieuw zijn beoordeeld, is extra formatie op het vlak van ICT beschikbaar gesteld. Vanuit deze extra formatie komt er een ICT regisseur die de rol van contractmanagement op zich gaat nemen.

Onderdeel 4.9.b rekenkamer rapport
Zorg voor actieve betrokkenheid van het management als (gemandateerde) eigenaars van de gegevens bij het toezicht op de beveiliging en het beheer van de gegevens.

Beantwoording 4.9.b
Dit is een continu proces. Teammanagers hebben grote verantwoordelijkheden, waaronder informatiebeveiliging en privacy zover het hun processen, mensen en systemen betreft. Dit is ook vastgelegd in ons informatiebeveiligingsbeleid en privacy beleid. Teammanagers worden hierbij geadviseerd vanuit het team informatiebeveiliging en privacy. Eigenaarschap m.b.t. security ervaren is een proces waarmee we gestart zijn. Dit gebeurt onder andere door presentaties, het aansluiten bij overleggen, het agenderen van beveiligingsvraagstukken bij directie en het uitzetten van metingen bij eigenaren.

Onderdeel 4.9.c rekenkamer rapport
Laat regelmatig onafhankelijke audits uitvoeren op de kwaliteit van de dienstverlening rond het technisch beheer van de applicaties.

Beantwoording 4.9.c
Dit is onderdeel van contractmanagement. Dit is een van de onderwerpen die als actiepunt is opgenomen in het jaarplan informatieveiligheid en tevens een van de redenen voor uitbreiding van de formatie binnen team ICT. Met de komst van een ICT-regisseur zal dit onderwerp de passende aandacht krijgen.

Onderdeel 4.9.d rekenkamer rapport
Maak bij testwerkzaamheden gebruik van geanonimiseerde data.

Beantwoording 4.9.d
Zover dit mogelijk is wordt er gewerkt met geanonimiseerde data. Voor ketentesten e.d. blijkt dit lastig te zijn. Hierom wordt niet bij alle testwerkzaamheden met geanonimiseerde data gewerkt.

Vraag 5
Met amendement A2018-005 heeft de raad het college opgedragen een actieplan op te stellen. Is dit actieplan opgesteld en wanneer is het naar de raad gestuurd?

Antwoord vraag 5
Na het rekenkameronderzoek zijn er diverse actieplannen (deelplannen) opgesteld en uitgevoerd. Zo is er bijvoorbeeld binnen het Sociaal Domein een project gestart om de informatieveiligheid te verbeteren (zie hiervoor T18.00336). Een ander voorbeeld hiervan is het project TOPwerken. Tijdens dit project zijn grote verbeteringen op het gebied van informatieveiligheid doorgevoerd in de organisatie. Tussentijds is

er gecommuniceerd met betrekking tot de stand van zaken van informatieveiligheid. Zie hiervoor bijvoorbeeld U18.02292. Tot slot wordt er vanuit informatiebeveiliging jaarlijks een actieplan opgesteld voor het komende jaar. De Raad wordt geïnformeerd via de begroting en de jaarstukken (in de paragraaf bedrijfsvoering wordt op hoofdlijn informatie gegeven over informatieveiligheid en privacy).

Vraag 6
Welke andere toegangsbeperkende maatregelen zijn genomen om informatie in ambtelijke systemen te beveiligen?

Antwoord vraag 6

a. *Wordt een sterk wachtwoord geforceerd afgedwongen*?
Sterke wachtwoorden worden geforceerd afgedwongen conform de eisen die de BIO aan wachtwoorden stelt.

b. *Moeten wachtwoorden periodiek worden aangepast?*
Wachtwoorden dienen periodiek te worden gewijzigd conform de eisen die de BIO hieraan stelt.

c. *Wordt actief gecontroleerd op uitgelekte wachtwoorden (hashes)?*
Er wordt momenteel niet actief gecontroleerd op uitgelekte wachtwoorden. Voor toegang tot de werkomgeving is een tweede en periodiek een derde factor vereist. Hierom heeft actieve controle op uitgelekte wachtwoorden momenteel niet de hoogste prioriteit.

d. *Is er sprake van 2FA (2-factor authenticatie) of het gebruik van een externe authenticatiesleutel?*
Er is sprake van 2FA voor toegang tot de werkomgeving en voor de meeste SaaS-applicaties (bijvoorbeeld iBabs). Ook wordt periodiek een derde factor gevraagd via bijvoorbeeld een sms.

e. *Wordt regelmatig gecontroleerd of inloggegevens nog gekoppeld zijn aan actieve medewerkers?*
    i. *Zo ja, door wie en is hier ook sprake van een vierogenprincipe?*
    ii. *Zo nee; waarom niet en acht het college het wenselijk dat dit gebeurt?*
Ja, er vindt regelmatig een controle plaats op de gebruikersdatabase. Deze controle wordt uitgevoerd door de CISO en wordt gecontroleerd door de teammanagers.

f. *Wordt toegang vanaf externe systemen/ IP-adressen geblokkeerd of via een whitelist toegelaten?*
    i. *Zo nee; waarom niet en acht het college het wenselijk dat dit gebeurt?*
Toegang tot het bedrijfsnetwerk is enkel middels een tweede factor mogelijk. Dit is een vorm van whitelisten. Enkel medewerkers in het bezit van de tweede factor kunnen op het bedrijfsnetwerk komen. Ook kun je enkel op het gemeentelijk netwerk inloggen met door de gemeente uitgegeven apparatuur.
Whitelisting vindt ook plaats middels firewall rules. De firewall staat aan de grens van je netwerken, de rules bepalen welke informatie wel en niet wordt doorgelaten.

We passen een geofilter toe op diverse diensten. Dit geofilter zorgt ervoor dat onder andere de werkomgeving enkel benaderbaar is vanuit specifieke locaties. Door het toepassen van dit filter verklein je de kans op cyberaanvallen omdat diverse diensten voor een groot aantal landen, zonder aanvullende acties, niet benaderbaar zijn.

g. *Wordt toegang vanaf externe systemen/ IP-adressen gemonitord en steekproefsgewijs uitgelezen?*
    i. *Zo ja; op welke wijze, hoe vaak wordt dit gedaan en door wie of wat?*
    ii. *Zo nee; waarom niet en acht het college het wenselijk dat dit gebeurt?*

Toegang vanaf externe systemen/IP-adressen wordt momenteel deels gemonitord. Dit wordt gedaan met de bedoeling om verdachte structuren te detecteren. Bij het signaleren van verdachte structuren/toegangspogingen doen we vervolgonderzoek. Dit vindt nog niet gestructureerd plaats door het ontbreken van middelen en capaciteit. Met de inrichting van SIEM&SOC krijgt de organisatie hier meer grip op.

Vraag 7
Is er een informatiebeveiligingsfunctionaris (CISO) actief in de organisatie?
Zo ja; voor hoeveel uur en is dit voldoende om in control te zijn?

Antwoord vraag 7
Er is momenteel een CISO actief binnen de organisatie. Dit is voor 28 uur. Daarnaast is er een adviseur informatiebeveiliging voor 18 uur.

Dit is voldoende om de toezichthoudende functie uit te voeren en om te reageren op incidenten en vraagstukken vanuit de organisatie. Hierbij is er een spanning op operationeel niveau (binnen de teams) en binnen ICT. Veel verantwoordelijkheden horen bij de teams belegd te zijn, echter binnen de teams is er een gebrek aan capaciteit voor uitvoering van de werkzaamheden. Dit is onder aanleiding geweest voor het voorstel bij de begroting van 2022 om capaciteit toe te voegen voor ICT/informatiebeveiliging.

Vraag 8
Is Lansingerland aangesloten bij de IBD (informatiebeveiligingsdienst) van de VNG?
a. Zo ja; op welke wijze wordt er momenteel gebruik gemaakt van de kennis en expertise van de IBD?
    i. Is de Baseline Informatiebeveiliging Overheid (BIO) volledig geïmplementeerd? Zo niet, waarom niet?
b. Zo niet; wordt er gebruik gemaakt, en op welke wijze, van een andere externe, onafhankelijke, organisatie of consultant om de interne beveiliging op orde te houden en waarom die partij?

Antwoord vraag 8
De gemeente Lansingerland is aangesloten bij de IBD. Vanuit de IBD ontvangen wij algemene en specifieke kwetsbaarheidswaarschuwingen en algemene adviezen. Kwetsbaarheidswaarschuwingen worden direct na ontvangst geanalyseerd, geprioriteerd en geregistreerd in het incidentenregistratie systeem. Op basis hiervan vindt verdere opvolging plaats.

Een goed voorbeeld van de samenwerking met de IBD is de recente wereldwijde kwetsbaarheid in Log4J. Gedurende deze tijd hebben we als gemeente intensief contact gehad met de IBD, andere gemeenten en leveranciers om de impact en risico's van de kwetsbaarheid in kaart te brengen en de veiligheid van onze informatie en systemen zo goed mogelijk te waarborgen.

De BIO is grotendeels geïmplementeerd. Periodiek voeren we analyses uit op de maatregelen uit de BIO om te bepalen waar we staan en waar we naartoe moeten. De vertaalslag naar de praktijk is vastgelegd in het jaarplan 2022-2023. Het is van groot belang om te beseffen dat 100% veiligheid niet bestaat. Er is altijd sprake van nieuwe ontwikkelingen waardoor nieuwe kwetsbaarheden kunnen ontstaan. Daarnaast

hebben we te maken met de menselijke factor; mensen zullen altijd in staat zijn om maatregelen bewust of onbewust te omzeilen. Het is onmogelijk om de risico's op gebied van informatieveiligheid tot nul terug te brengen. Op basis van risicoafweging worden maatregelen getroffen. Hierbij wordt continu de afweging gemaakt of het beoogde doel de inzet van middelen rechtvaardigt.

Vraag 9

Zijn of worden medewerkers getraind in "awareness"?

a. *Zo ja, door welke partij en hoe vaak?*
b. *Zo nee, waarom niet en acht het college dit wenselijk?*
c. *Zijn of worden er periodieke (onaangekondigde) testen gedaan onder werknemers om 'awareness' te vergroten, zoals (spear) phishing?*
    i. *Zo ja; wie organiseert deze testen en wat zijn de bevindingen?*
    ii. *Zo niet; waarom niet en acht het college het wenselijk dat dit gebeurt?*

Antwoord vraag 9

a. Ja. Medewerkers worden intern getraind in awareness. Dit wordt niet structureel door een andere partij gedaan, maar grotendeels door de CISO en/of adviseur informatiebeveiliging zelf. Iedere nieuwe medewerker volgt binnen drie maanden na indiensttreding een presentatie/ training op het vlak van informatiebeveiliging en privacy, er wordt geregeld aangesloten bij team overleggen en doorlopend vindt bewustwording plaats via het intranet of via de mail wanneer daar aanleiding toe is.
b. N.v.t.
c. Ja. Periodiek worden er onaangekondigde testen gedaan, geïnitieerd door de CISO en uitgevoerd door een onafhankelijke externe partij. Inzicht in de uitkomsten kunnen in deze beantwoording niet in detail worden gegeven, aangezien dit de kwetsbaarheden van de organisatie toont. Wel kan worden gezegd dat de bevindingen risico gestuurd worden opgepakt door het team van informatiebeveiliging, privacy en ICT.

Wij verwachten dat wij met deze brief antwoord hebben gegeven op uw raadsvragen.

Met een vriendelijke groet,
burgemeester en wethouders van Lansingerland

Mickel Beckers
Gemeentesecretaris

drs. Pieter van de Stadt
Burgemeester