

Raadscommissie Digitalisering & Informatiebeveiliging

Datum: 27-09-2022

In de raadscommissie van 27 september 2022 is er een presentatie gegeven met uitleg over de stand van zaken over de staat van de digitalisering en informatiebeveiliging. In de commissievergadering zijn aanvullende vragen gesteld die, vanwege tijdsgebrek, niet allemaal zijn beantwoord. Hieronder zijn de gestelde vragen opgenomen en voorzien van een antwoord. Indien de vraagstelling onverhoopt onjuist is geformuleerd dan ontvangt wethouder Kruis graag de juiste formulering (vraagstelling). Mochten de antwoorden aanleiding vormen voor vervolgvragen – dan ontvangt de wethouder deze graag schriftelijk.

1. Fractie: D66 – S. de Wilde

Vraag:

- 1.1 De vraag over inzicht in het IT-landschap is globaal beantwoord, verwachting was gedetailleerd inzicht in de applicaties, leveranciers – onpremise (in het eigen datacenter) en in de cloud.

Antwoord: het college heeft functioneel een schets gegeven over de ontwikkeling in het IT-landschap. In 2017 is een verschuiving van het eigen datacenter naar de cloud in gang gezet. In bijlage I is het functionele IT-landschap opgenomen van de belangrijkste taakvelden – waaronder burgerzaken, openbare ruimte, belastingen, sociaal domein, vergunningen, bedrijfsvoering etc.

- 1.2 Welke risico's worden door het college van dit IT-landschap onderkent voor o.a. inwoners, datagebruik en hoe waken we ervoor dat algoritmes niet op hol slaan.

Antwoord:

- 1) Op het moment dat deze kwetsbaarheden niet tijdig worden gedicht, of (nog) niet gedicht kunnen worden, neemt de kans op kwetsbaarheden als ransomware toe. De impact na een dergelijke succesvolle aanval kan groot zijn, niet alleen voor onze organisatie, maar zeker ook voor onze inwoners. De verantwoording voor het afdekken van risico is daarom een vast onderdeel van de risicoparagraaf in de jaarstukken. Zie ook de beantwoording bij 5.1 voor de onderkenning van risico's.
- 2) Het veranderende IT-landschap laat zien dat de gemeentelijke (gevoelige) data meer en meer geografisch verspreid wordt opgeslagen. Enerzijds draagt dit bij aan een hogere beschikbaarheid van de diensten, anderzijds vergroot dit de potentiële aanvalsoppervlakte. Waar de gemeente voorheen afhankelijk was van één virtuele dijk om de gegevens te beschermen, dient het nu alle dijken te monitoren, opdat de veiligheid van haar data optimaal beveiligd is. Voor het afdekken van risico's en de volwassenheidsgraad en weerbaarheid mee te laten groeien met de digitale ontwikkelingen is dit opgenomen in het uitvoeringsprogramma Lelystad Digitaal 2025 (LD2025) waarvoor in de programmabegroting budget is aangevraagd.
- 3) Algoritmes: een *algoritme* is een eindige reeks instructies in een vaststaande volgorde die de oplossing van een bepaald probleem beschrijft. Binnen de informatievoorzieningen worden instructies voor het toepassen van de wet, lokale verordeningen toegepast. Voor algoritmen die worden toegepast is het aantal gebruikte variabelen beperkt, er is altijd een menselijke kwalitatieve beoordeling van het resultaat.

Op de inrichting (het opzetten van een algoritme register is opgenomen in de uitvoering LD2025) en uitvoering hier wordt op het beheer en beheersen, voor o.a. het niet op hol slaan, door de CISO (chief information security officer) en FG (functionaris gegevensbescherming) toezicht gehouden. De Commissie van de Rekening is op 12 april 2021 over dit onderwerp geïnformeerd.

- 1.3 Welke monopolisten (leveranciers) leveren IT-systemen momenteel, komen we hier wel van af.

Antwoord: Nederland kent een groot areaal aan softwareleveranciers die specifiek informatievoorzieningen leveren voor de gemeentelijke dienstverlening. Voor Lelystad is er

geen sprake dat 1 leverancier alle applicaties levert – Europese aanbesteden hebben in de afgelopen jaren geleid tot; financieels systeem – Unit4, burgerzaken – PinkRoccade, belastingen – Tog Nederland, vergunningen – Centric, Sociaal Domein – Centric – zie ook losse bijlage. De inkoop van informatievoorzieningen is gebonden aan Europese wetgeving gericht op rechtmatigheid. Conform de geldende aanbestedingswetgeving wordt er in Lelystad uitvoering gegeven aan I-aanbestedingskalender 2025 – door de raad genomen besluit van 6 april 2021.

- 1.4 Is de functionaris ISO (information security officer) al een keer eerder aangevraagd, hier heeft D66 een amendement voor ingediend? Is de nu aangevraagde ISO een uitbreiding daarop?

Antwoord: Er is niet eerder een ISO functionaris bij de raad aangevraagd. In de begroting 2018-2021 is de functie CIO (chief information officer) aangevraagd waar D66 samen met CU een amendement voor hebben ingediend.

2. Fractie: CU – F. Volmer

Vraag:

- 2.1 Bij het zoeken op Gemeente IT-hack kwam naar voren dat er een wachtwoord 'welkom22' een enorme hack teweeg bracht. Was hier sprake van menselijk falen, kwetsbaarheid van een leverancier, is de gemeente Lelystad voorbereid op een dergelijk hack?

Antwoord: Het aangedragen voorbeeld is inderdaad ontstaan door menselijk falen.

Binnen de gemeente Lelystad zijn we er scherp op dat een tweede authenticatie wordt gebruikt (bijv. naam/wachtwoord gevolgd door sms). Nu zijn er ook andere methodes om op een netwerk binnen te dringen en kwaad te doen. Daarom is het noodzakelijk dat Gemeente Lelystad aanvullend investeert in Monitoring, Detectie en Response. Hiervoor is in de programmabegroting budget voor aangevraagd binnen het programma Lelystad Digital 2025, onderdeel Verhogen Digitale Weerbaarheid. Na implementatie kan de gemeente sneller ingrijpen waardoor de impact kleiner wordt.

- 2.2 Wie neemt beslissingen, menselijk oog of op basis van data.

Antwoord – Beslissingen worden genomen op basis van de analyse van een probleem. Eén van de instrumenten die daarvoor worden gebruikt is (informatie uit) data. Daarnaast worden bijvoorbeeld kennis van het beleidsveld en de context waarbinnen het probleem zich afspeelt ook meegenomen bij het maken van een beslissing. De beslissing wordt uiteindelijk door mensen genomen.

- 2.3 Wat zijn voor het college de top 3 van belangrijkste issues .

Antwoord – het college **ziet op dit moment de volgende issues:**

Digitalisering & Informatisering	Informatiebeveiliging
1.inclusie en digivaardigheden (iedereen doet mee)	1. Toenemende Cyberdreiging
2. rechtmatige inzet informatievoorzieningen	2. Verhogen Digitale Weerbaarheid
3. versterken van de informatievoorzieningen (fundament) voor de opgaven van de stad	3a. Personele uitbreiding op securitygebied 3b. *Hoog personeelsverloop

*door personeelsverloop verliest de gemeente kennis en inzichten op management en uitvoerend niveau. Bij aanneme van nieuw personeel wordt hier direct op geïnvesteerd om zo snel mogelijk weer op hetzelfde niveau te komen.

Voor de korte termijn worden risico's onderkend vanuit de krapte op de arbeidsmarkt en de torenhoge inflatie die de ICT-kosten sterk doen stijgen.

3. Fractie: Leefbaar Lelystad – W. Botter

Vraag:

3.1 Onlangs is er een agenda digitale grondrechten en ethiek opgesteld. Hiermee geven gemeenten richting aan de digitalisering van Nederland. Gaan, of werken wij inmiddels ook via deze agenda?

Antwoord – Het is zeer belangrijk dat de grondrechten van onze inwoners, ondernemers en maatschappelijke organisaties zijn geborgd. Om te voorkomen dat informatie op straat terecht komt of door niet bevoegde ambtenaren wordt gezien wordt er ingezet op informatiebeveiliging afgezet tegen de toenemende digitalisering. Op dit moment vindt er een ethische toetsing plaats bij het analyseren van data. Verder wordt het ethisch omgaan met informatie de komende jaren integraal ingebed in het uitvoeringsprogramma Lelystad Digitaal 2025. Hierbij gaat de gemeente de door de VNG afgegeven richtlijnen (handreiking).

3.2 In deze agenda staat wat voor soort Gemeente je wilt zijn en wat voor soort organisatie je wilt zijn in de relatie tussen overheid en burger. Volgen wij ook deze werkwijze?

Antwoord: de gemeente volgt de VNG standaarden en handreikingen. Die zal ook voor deze uitwerking, binnen het uitvoeringsprogramma LD2025, ter hand worden genomen. Daar krijgt de agenda voor Lelystad richting en inhoud.

4. Fractie: InwonersPartij – J. Bergsma

Vraag:

4.1 Hoe gaan we om met ouderen?

Antwoord – 'Iedereen doet mee' is een belangrijk thema in de uitvoering van LD2025. Voor de diverse doelgroepen – waaronder ook de ouder - die het lastig en moeilijk vinden om de digitale veranderingen in onze samenleving te volgen worden momenteel begeleidingsprogramma's aangeboden. In relatie tot de verdere digitalisering zal samen met de ketenpartners een ondersteuningsprogramma in de vorm van trainingen, informatie, begeleiding etc. worden samengesteld.

5. Fractie: PvdA – J. Kortmann

Vraag:

5.1 Hoe gaan we om met de cloud act in relatie tot de recente berichtgeving van het NCSC.

Antwoord: De AVG en de BIO staan aan de basis van de beveiliging van de persoonsgegevens. De eisen uit de AVG en het BIO-normenkader maken deel uit van aanbestedingen bij nieuwe IT-producten/diensten. Verder is Gemeente Lelystad aangesloten bij de informatiebeveiligingsdienst (IBD). De IBD is onderdeel van de VNG en biedt op het gebied van privacy en informatiebeveiliging o.a. hulp, handreikingen en adviezen. Door hun korte lijnen met het NCSC deelt de IBD de relevante informatie met gemeenten. Dit houden wij vanzelfsprekend nauwlettend in de gaten.

Conclusion

EU Entities can be within the reach of the CLOUD Act, even if the EU Entities are located outside the U.S. In order for an EU Entity to completely avoid being subject to the CLOUD Act, it would need to process data using a non-U.S. entity, which either

- a) does not have a corporate relation to any company with a presence in the U.S. (such as a U.S. subsidiary) and that does not have sufficient contacts with the U.S. such that it is reasonable for the U.S. to assert jurisdiction over the EU Entity/non-US entity (which includes not selling products or services to customers in the US); or
- b) if it does have a corporate relationship with a company based in the U.S., the U.S. company must not have possession, custody, or control over the data that is stored in the EU.

5.2 Als alles in 1 cloud staat, en het gaat mis in de cloud, hoe dan verder?

Antwoord:

Definitie van een Cloud is: de cloud staat voor een netwerk dat met al de computers/diensten die erop aangesloten zijn een soort 'wolk van computers' vormt, waarbij de eindgebruiker niet weet op hoeveel of welke computer (s) de software draait of waar die computers precies staan.

Doordat elke leverancier zijn eigen cloudomgeving heeft, en Lelystad meerdere clouddiensten (lees applicaties bij meerdere leveranciers) afneemt, zijn de meeste clouddiensten geografisch van elkaar gescheiden. Dit spreidt het risico bij storingen. De eisen voor beschikbaarheid van de dienst komen voort uit de BIO, en maken onderdeel uit van de inkoop-/aanbestedingsbeleid van de gemeente.

6. Fractie: Groenlinks – I. Vink

Vraag:

6.1 Hoe ziet het tijdspad van de digitalisering ontwikkelingen (digitale diensten, overgang naar de cloud en bouwen van dashboards) voor de komende jaren.

Antwoord: op dit moment wordt de laatste hand gelegd aan het uitvoeringsprogramma Lelystad Digitaal 2025. Via de sporen Voorzieningen op Orde, Regie op Data en Inwoner Centraal wordt er een pallet van producten ontwikkelt. Het college biedt dit najaar het uitvoeringsprogrammaboekje ter informatie aan de raad.

6.2 De drie belangrijkste veiligheidsrisico's, kunt u die wellicht een cijfer geven, hoe weerbaar zijn we

Antwoord: In de kernboodschap van de ENSIA-rapportage [raadsinformatienota van 5 juli](#) jl. is het volgende verwoord: "De gemeente is in control". Met een blik op verdergaande digitalisering – o.a. opgelegd vanuit wetgeving – zal de gemeente de komende jaren te maken krijgen met (1) cyberrisico's dusdanig snel toenemen, dat er aanvullende (2) personele versterking nodig is om het volwassenheidsniveau en (3) de digitale weerbaarheid mee te laten groeien. Hierin is voorzien in de kaderbrief 2023-2026 en in de begroting 2023-2026 die aan de raad wordt aangeboden.

7. Fractie: Forum voor Democratie – J. Loijenga

Vraag:

7.1 Wordt data ook in Smartcity projecten ingezet?

Antwoord: Voor de uitvoering van het gemeentelijk beleid en dienstverlening wordt veel data ingezet. Met de nieuwste innovaties en technologie kunnen steeds meer zaken worden gemeten en omgezet naar data – bijvoorbeeld verkeersbewegingen, wateroverlast, gebruik van voorzieningen (bijv. parkeergarages). Vanuit Lelystad Digitaal 2020 zijn er voorbeelden van het slim inzetten van data (asbestdaken, barcode omgevingsvisie, scenario's bevolkingsprognose toepassen). Hier zal in het programma LD2025 een vervolg aan worden gegeven.

7.2 Steeds meer inwoners hebben t momenteel zwaar en geen geld voor computer, smartphone etc. – op welke wijze kan de gemeente deze groep ondersteunen?

Antwoord: de gemeente (op de begane grond) en diverse ketenpartners (Werkbedrijf, Welzijn en de bibliotheek) bieden op dit moment op diverse plaatsen ondersteuning waarbij, met of zonder begeleiding, gebruik gemaakt kan worden van een computer, kopieerapparaat.

8. Fractie: PVV - Mur

Vraag:

8.1 Is er een back-up in geval van een stroomstoring?

Antwoord: Van de informatie die wordt opgeslagen in het datacenter van het stadhuis en bij de leveranciers in de cloud worden back-ups gemaakt. De back-up voorzieningen worden periodiek getoetst.

Voor het spreiden van risico's van stroomonderbreking beschikt de gemeente zelf over drie geografische verspreide datacenters. Deze beschikken allen over noodstroom, waardoor de kans op stroomonderbreking zo klein mogelijk wordt gehouden.

Voor de back-up de cloud voorzieningen worden in aanbestedingen afspraken gemaakt over de beschikbaarheidseisen. Middels SLA-rapportage en een verklaring (bijv. ISO27001/ISAE3402 certificering) toont de leverancier aan of hij voldoet aan de gestelde afspraken/eisen.

8.2 Leggen we naast een digitale snelweg ook een provinciale weg aan voor Lelystad?

Antwoord:

De internetaansluiting van de gemeente Lelystad is op dit moment dubbel uitgevoerd. Bij uitval van de één zal de ander met een handmatige actie geactiveerd worden. Verder beschikt Lelystad over een Gemnet-aansluiting waar gemeente Lelystad clouddiensten afneemt, zoals Suwinet en de burgerzaken applicatie. Deze aansluiting is tevens dubbel uitgevoerd. Voor clouddiensten (meerdere datacenters op het internet) is het aan de dienstenleverancier van de cloudapplicatie om de beschikbaarheid te garanderen en is het een de proceseigenaar om daarop toe te zien.

9. Fractie: CDA - Graanoogst

Vraag:

9.1 Wat kunnen burgers doen als zorgen hebben over de informatiebeveiliging en wat doet de gemeenten nu al om deze zorgen weg te nemen?

Antwoord: Naast de landelijke initiatieven, waar tips te raadplegen zijn over informatiebeveiliging in je eigen omgeving, zoals veiliginternetten.nl is er ook op de gemeentelijke [website](#) aandacht voor digitale veiligheid. Hier staat wat burgers zelf kunnen doen. Verder is er een [week van de veiligheid](#) georganiseerd van 10 t/m 15 oktober op het stadhuisplein, hier maakt digitale veiligheid onderdeel van uit.

In de informatieverstrekking, trainingen en begeleiding – zie ook beantwoording 4.1 – zal aandacht worden besteed aan gevaren, risico's en het veilig opslaan van data en het omgaan met stevige (goede) wachtwoorden.

10. Fractie: JongLelystad – M. Aktan

Vraag:

10.1 In aansluiting van de vraag van D66 wil JongLelystad ook inzicht in het applicatielandschap van de gemeente - applicaties, endpoints, welk deel staat al in de cloud, welk deel is in beheer. Is het netwerk gesegmenteerd. Beantwoording mag in het geheim gedeeld worden.

Antwoord: zie beantwoording van 2.1. Circa 40% van de gemeentelijke applicaties staan in de cloud. Dit percentage zal de komende jaren vanuit diverse aanbestedingen toenemen. Het college is bereid om dit antwoord en de meegeleverde softwarecatalogus in een informele bijeenkomst toe te lichten.

10.2 Welke lopende uitdagingen op het gebied van informatiebeveiliging ziet het college op dit moment. Gericht op de BIO - hoe staan we ervoor, welke onderdelen verdienen verbetering en wat is daar voor nodig.

Antwoord: zie antwoord 6.2

In de nota zijn onderstaande actiepunten opgenomen:

2.1 ENSIA Onderdeel: Baseline Informatiebeveiliging Overheid (BIO)

De belangrijkste actiepunten uit de BIO zijn hieronder weergegeven.

Onderdeel	Actiepunten	Team
BIO	Inzet Privileged Access Management (PAM) voor interne beheerders en leveranciers die verhoogde rechten nodig hebben	IMA
BIO	Kwetsbaarheden nog beter inzichtelijk krijgen door inzet van nieuwe technieken in de kwetsbaarheidsscanner (Vulnerability scans)	IMA
BIO	Het minimaal elk half jaar beoordelen van speciale toegangsrechten	IMA
BIO	Verder doorvoeren hardening in de IT omgeving - Servers - Werkplekken - Backupomgeving	IMA
BIO	Verder doorvoeren van de netwerksegmentering in de IT-omgeving	IMA
BIO	Backupomgeving aanvullend beveiligen met immutable backup	IMA
BIO	Implementatie Role Based Access Control (RBAC)	IMA / P&O
BIO	Actualiseren screeningsbeleid	P&O
BIO	Inzichtelijk krijgen welke (informatie)systemen er horen bij de BCP-processen incl. benodigde hersteltijden	CS / Teamleiders / IMA

10.3 Beschikt de gemeente over een draaiboek in geval van een calamiteit?

Antwoord: Eén van de ENSIA aanbevelingen uit 2019 is het opstellen van een bedrijfscontinuïteitsplan (BCP) – de bedrijfskritische processen/applicaties zijn in kaart gebracht en worden uitgewerkt. Bij een cybercalamiteit wordt een crisisteam samengesteld die vanuit een BOB-methode opereert. Het team is inmiddels getraind. ICT heeft vorig jaar het incident response plan beschreven en zijn er scenariokaarten uitgewerkt.

11. Fractie: VVD – Eelco Schrijver

Vraag:

11.1 Er is sprake van krapte op de arbeidsmarkt, worden er onderdelen uitbesteed en/of samengewerkt. “Het wiel niet opnieuw uitvinden”, wat doen we landelijk of met buurgemeenten.

Antwoord: Om het wiel niet opnieuw uit te vinden is de gemeente aangesloten bij de Informatiebeveiligingsdienst en zijn er tweewekelijkse overlegmomenten waarop de CISO's van Noord-Holland en Lelystad elkaar informeren over lopende zaken. Verder is het firewall-beheer en de monitoring daarvan belegd bij de leverancier, onder regie van ICT. Daarnaast werkt de gemeente, vanuit VNG/GBI-verband, binnen de ontwikkelingen van het sociaal domein op diverse onderdelen met elkaar samen.

11.2 Uitbesteden van diensten naar andere entiteiten, gebeurt dat nationaal/internationaal

Antwoord: het uitbesteden van cloud-/saas diensten gebeurt op nationaal niveau.

11.3 Op welke wijze vindt de opslag van clouddata plaats - nationaal of internationaal?

Antwoord: Internationaal. Maar dan wel binnen de EER (EU plus IJsland, Noorwegen en Liechtenstein) waar de AVG van toepassing is. De AVG is een Europese verordening die de bescherming van persoonsgegevens standaardiseert.

Dit wordt standaard als eis bij aanbestedingen opgenomen:

EL18	De opslag van de applicatie en gegevens en overige onderdelen van de Oplossing vindt fysiek plaats binnen de Europese Economische Ruimte en bij een hosting partij/datacenter die geen vestiging heeft in de Verenigde Staten, dit in verband met de USA Freedom Act. Dan wel dat de Opdrachtnemer kan garanderen dat de data niet onder USA Freedom Act kan worden opgevraagd.	
------	---	--

[Reflexivität.com](#) centerisodochan | elistat

