INFORMATIENOTA VOOR DE RAAD

Nummer: 183

Portefeuille: : WMO, Jeugdzorg en Beheer Openbare Ruimte
Programma: : Bestuur en ondersteuning
Taakveld: : Bestuur

Datum : 25 mei 2021

Onderwerp: informatienota voor de raad over informatiebeveiliging

DE RAAD NEEMT KENNIS VAN:
1. De uitkomsten van de ENSIA zelfevaluatie op het gebied van informatiebeveiliging.
2. De uitkomsten van de pentest.

INLEIDING

ENSIA is het sinds 2017 jaarlijks verplichte verantwoordingsproces op informatiebeveiliging bij gemeenten. ENSIA (Eenduidige Normatiek Single Information Audit) heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus.
Het college van B&W is verantwoordelijk voor de uitvoering van dit proces en wordt onder regie van de CISO (Chief Information Security Officer) uitgevoerd. De uit de ENSIA geprioriteerde aanbevelingen worden d.m.v. deze informatienota met de raad gedeeld. Hiermee voldoet de gemeente Lelystad aan haar horizontale verantwoordings-verplichting en heeft de raad inzichtelijk waar de aandachtspunten liggen en dat deze punten in de organisatie zijn uitgezet.

Eén van de onderdelen binnen de ENSIA is de jaarlijkse zelfevaluatie op de informatiebeveiliging. Deze heeft in 2020 plaatsgevonden en omvatte de totale breedte van de BIO (Baseline Informatiebeveiliging Overheid), met inbegrip van DigiD, Suwinet en de basisregistraties BAG (Basisregistratie Adressen en Gebouwen), BGT (Basisregistratie Grootschalige Topografie) en BRO (Basisregistratie Ondergrond), BRP (Basisregistratie Persoonsgegevens) en Reisdocumenten. In het voorjaar van 2021 is bovendien een verplichte externe onafhankelijke audit gedaan op DigiD en Suwinet, waar de getekende Collegeverklaring voor is opgeleverd. In hoofdstuk 2 van deze notitie zijn de uitkomsten per onderdeel beschreven.

Daarnaast is in 2020 via de kadernota budget aangevraagd voor het structureel uitvoeren van pentesten. Een pentest is een controle waarbij ethische hackers systemen onderzoeken op kwetsbaarheden. De pentest is recentelijk uitgevoerd. U heeft bij het toekennen van het budget verzocht om het resultaat van de eerste pentest in 2021. Zoals in “de beantwoording van de door raadsleden gestelde vragen over de kadernota 2021-2024” is toegezegd, treft u in het laatste onderdeel van deze notitie de uitkomst en opvolging n.a.v. deze pentest op hoofdlijnen aan.

Inherent aan de materie, komen in deze nota de benodigde hoeveelheid begrippen en afkortingen aan bod. Daarom treft u als bijlage van deze nota een begrippenlijst aan, waarin deze begrippen in één helder overzicht zijn weergegeven, met daarbij een korte toelichting.

Kernboodschap
De kernboodschap is onderverdeeld in drie delen, te weten:

1. Informatiebeveiliging 2020
2. Resultaten uit de ENSIA en opvolging
   2.1. BIO
   2.2. DigiD en Suwinet
   2.3. BAG, BGT en BRO
   2.4. BRP en Reisdocumenten
   2.5. Conclusie
3. Resultaten uit eerste pentest 2021

1. Informatiebeveiliging 2020

1.1 Wereldwijde gebeurtenissen vonden ook hun weerslag bij gemeenten. In het oog springende voorbeelden uit 2020 waren bijvoorbeeld de ernstige kwetsbaarheden in Citrix, Oracle en Exchange. Zo heeft het lek in Citrix er begin 2020 voor gezorgd dat werknemers van de gemeente Lelystad, net als de meeste andere Citrixafnemers, een paar dagen niet op afstand konden werken. Door nauwe samenwerking met de Informatiebeveiligingsdienst (IBD) zijn gemeenten direct geïnformeerd en geadviseerd op het moment dat dergelijke kwetsbaarheden aan het licht kwamen. De meldingen vanuit de IBD zijn binnen de gemeente Lelystad kordaat en accuraat opgepakt, waardoor risico's tijdig zijn gemitigeerd en schade is voorkomen
Ten opzichte van vorige jaren, is er een toename in het aantal kwetsbaarheids-meldingen vanuit de IBD waar te nemen. Meldingen over hoge risico's vereisen directe inzet, wat de druk op ICT vergroot. Dergelijke kwetsbaarheden zijn vooraf noch te voorspellen, noch te voorkomen.

1.2 Op 1 januari 2020 is de Baseline Informatiebeveiliging voor Overheid (BIO) ingegaan en vervangt de voorloper Baseline Informatiebeveiliging Gemeente (BIG). De BIO is verplicht voor alle overheidsinstanties en zorgt ervoor dat zij hetzelfde normenkader hanteren en dezelfde taal spreken. Hierdoor wordt de overheid weerbaarder en zijn samenwerkingsverbanden efficiënter te realiseren. Omdat bij zowel de BIG als de BIO de wereldwijde standaard ISO27001/2 ten grondslag ligt, was de impact van het actualiseren van dit beveiligingsbeleid en bijbehorende procedures klein.

1.3 Het coronavirus heeft ervoor gezorgd dat de meeste werknemers van de gemeente Lelystad digitaal vanuit huis zijn gaan werken. Bewustwording in het veilig omgaan met informatie is hier uitermate belangrijk. Om de professionaliteit van het bewustwordingsprogramma en de bewustwording te verhogen (en te borgen) is hiervoor in de kadernota van 2020 budget aangevraagd en toegekend. Dit heeft ertoe geleid dat in Q1 2021 het meerjarig bewustwordingsprogramma voor elke medewerker van start is gegaan.

2. Resultaten uit de ENSIA en opvolging

2.1 ENSIA-onderdeel BIO: De zelfevaluatie heeft over de volledige breedte van de BIO plaatsgevonden. De gemeente is in control. Om de informatiebeveiliging verder te verstevigen, zijn er voor 2021 actiepunten aangeduid en ondertussen belegd bij het desbetreffende team / functionaris. Deze punten zijn hieronder weergegeven en het gros is relatief eenvoudig op te volgen.

Generieke actiepunten	Tijdpad gereed	Belegd bij teamleider / functionaris
Bewustwording: Nulmeting uitvoeren binnen de organisatie t.b.v informatiebeveiligingsbewustzijn	Q1 2021	IMA
Bewustwording: Alle medewerkers toegang geven tot trainingsmateriaal t.b.v informatiebeveiligingsbewustzijn	Q1 2021	IMA
Kwartaalcontrole op naleving van het beleid in de MDM/MAM[1] - omgeving. Doel hiervan is om aan te tonen dat gemeentelijke mobiele devices/telefoons/surfaces compliant zijn aan de gemeentelijke policy. Hiervoor dient ook het proces beschreven te zijn.	Q2 2021	IMA
Bij de migratie van gegevens naar de Office-365-Cloud dient deze vooraf geclassificeerd te worden. Dit dient in het O365-project geborgd te zijn.	Q1 2021	CIO
Procedure opstellen om uniform om te gaan met verhoogde toegangsrechten binnen de top 10-systemen uit het bedrijfscontinuïteitsplan (BCP).	Q2 2021	CIO
Kwartaal-controle op de verhoogde gebruikersrechten binnen de top 10 BCP-systemen uitvoeren. Verslag van de beoordeling is dan vereist.	Q2 2021	CIO
Leveranciersautorisatie tot het gemeentelijke netwerk beschrijven (condities en procedures) en implementeren	Q1 2021	IMA
De (minimaal jaarlijkse) restore (van de backup) controleren op integriteit en dit vastleggen in een verslag	Q1 2021	IMA
Centraal inzichtelijk maken waar BCP top 10 systemen en applicaties loggegevens opslaan en welke gegevens in deze log worden opgeslagen (indien bekend aangevuld met bewaartermijn).	Q2 2021	IMA
Opnemen in bouwstenen voor aanbestedingen: Leverancier geeft aan welke maatregelen zij hebben genomen om de aan hun opgelegde eisen ook door te vertalen naar hun toeleveranciers. Doel is om dit in het contract terug te zien komen.	Q1 2021	IMA/CIO

2.2 ENSIA-onderdeel DigiD en Suwinet: Vanwege hun specifieke normenkader, zijn drie applicaties verplicht diepgaand onderzocht op informatiebeveiligingsaspecten. Alle applicaties voldoen aan alle eisen binnen de norm.

Onderdeel	Voldoet aan alle normen
DigiD Burgerzaken	Ja
DigiD Formulieren	Ja
Suwinet Participatie	Ja

Een externe onafhankelijke auditor heeft voor DigiD en Suwinet een assurancerapport op de collegeverklaring afgegeven. Deze zijn gedeeld met de verticale toezichthouder.

[1] MDM/MAM: Mobile Device Management / Mobile Application Management is het beheer op de mobiele telefoons, laptops en applicaties

2.3 ENSIA-onderdeel BAG, BGT en BRO:

In de onderstaande tabel zijn de behaalde totaalscores van BAG, BGT en BRO weergegeven. Alle drie de basisregistraties voldoen aan de norm. Het college legt jaarlijks verantwoording af aan de landelijke toezichthouder, zo heeft dat ook dit jaar plaatsgevonden.

Basisregistratie	Totaalscore Lelystad	Norm Landelijk
BAG	88%	75%
BGT	100%	75%
BRO	100%	60% (ivm proefjaar)

Om dit goede niveau vast te houden, hebben de medewerkers van BAG, BGT en BRO, samen met de CISO actiepunten voor 2021 benoemd en in gang gezet. Deze punten zijn hieronder weergegeven.

Basisregistraties BAG / BGT / BRO	Basis-registratie
De inspanningen t.o.v. de vorige zelfevaluatie laten stappen vooruit zien qua actualiteit. Het percentage verwerkingstermijn definitieve pandgeometrie is aanzienlijk verbeterd, maar nog niet voldoende. De applicatiebeheerder heeft dit punt besproken met de landmeters en zijn tot het volgende verbeterpunt gekomen: Wat: Er wordt een script ontwikkeld door de beheerder waarbij de nog in te meten panden in kaart worden gebracht. Hierdoor is het voor de landmeters inzichtelijk welke panden er ingemeten moeten worden. Wie: Applicatiebeheerder ontwikkelt het script, deze wordt maandelijks gedraaid. De output wordt aan de landmeters aangeleverd. Evaluatiemoment: in mei 2021 wordt deze maatregel geëvalueerd om na te gaan of er bijsturing nodig is.	BAG
Elke landmeter wordt naast de algemene werkzaamheden, specialist op een werkterrein. Hierdoor wordt kennis vergroot (niet iedereen hoeft alle ontwikkelingen te volgen). Door korte lijnen is kennisoverdracht geborgd.	BGT
Het verbetervoorstel uit 2019 krijgt al behoorlijk vorm. Het beheerpakket Geovisia wordt al gebruikt voor de Groenbestekken. Het gevolg is dat meer mutaties gemeld worden, waardoor de actualiteit van de BGT beter wordt. Maar er is nog meer potentie, ook team Wegen gaat beheer middels Geovisia inregelen, we verwachten van dit team ook goede feedback.	BGT
De koppeling is gereed. We onderzoeken nu of een ander BGT verwerkingspakket (GISkit) tools biedt voor verdere verbetering.	BGT
Het gebruik van luchtfoto's levert (te) grote bestanden, met de huidige tools is dit niet inzetbaar. Het wachten is op de nieuwste AHN (Actueel Hoogtebestand Nederland), verwachting is dat deze eind 2020 begin 2021 beschikbaar komt	BGT
De BRO-coördinator maakt een werkbeschrijving voor de achtervang, zodat bij afwezigheid van de BRO-Coördinator er geen onduidelijkheden zijn	BRO
De betrokken medewerkers nog enthousiaster maken, door ze te wijzen op de landelijke initiatieven zoals webinars en bijeenkomsten van het ministerie. Het doel is om zo de BRO zo nog beter op de kaart te zetten.	BRO
Bij de meeste BRO-gebruikers wordt het BRO proces inmiddels intrinsiek uitgevoerd, echter bij een select aantal medewerkers zit het nog niet in hun automatische werkwijze, maar worden er door collega's op aangesproken om de BRO-processen te volgen. Het is geen onwil, maar in sommige gevallen wordt er gewoonweg niet aan gedacht. Verbeterpunt is dan ook om deze personen individueel te benaderen en te wijzen op de processen, waardoor uiteindelijke de BRO-werkwijze hun systeem komt.	BRO

2.4 ENSIA-onderdeel BRP & Reisdocumenten:
Dit onderdeel bevat de resultaten van de antwoorden op de vragen in de ENSIA-tool.

Onderdeel BRP	Waarde Lelystad	Maximale score	Percentages
Organisatie van de beveiliging	370	400	93
Toegangsbeveiliging	320	400	80
Naleving	335	400	84
Puntentotaal BRP ENSIA	**1.025**	**1.200**	**85**

Onderdeel Reisdocumenten	Waarde Lelystad	Maximale score	Percentages
Organisatie van de beveiliging	190	200	95
Toegangsbeveiliging	200	250	80
Naleving	200	200	100
Puntentotaal Reisdocumenten	**590**	**650**	**91**

De behaalde scores zijn goed te noemen. Omdat continue verbetering wordt nagestreefd, zijn de volgende actiepunten binnen het team belegd:

BRP en Reisdocumenten (RD)	Basis-registratie
Continuïteitsplannen jaarlijks testen op geldigheid en bruikbaarheid.	BRP
Medewerkers binnen drie maanden na indiensttreding een training I-bewustzijn laten volgen.	BRP + RD
Het sleutelbeheer inrichten op basis van een sleutelplan.	BRP + RD
Een onbemensde werkplek altijd vergrendelen.	BRP + RD
Informatie automatisch ontoegankelijk maken na inactiviteit van maximaal 15 minuten.	BRP + RD
Media met vertrouwelijke informatie opslaan op een plek die niet toegankelijk is voor onbevoegden.	RD

De door de B&W ondertekende uittreksels met de resultaten van de zelfevaluatie reisdocumenten en de BRP zijn aangeboden aan het Ministerie van BZK. De resultaten van de BRP zijn eveneens aangeboden aan de Autoriteit Persoonsgegevens.

2.5 Conclusie:
Concluderend kan gesteld worden dat de actiepunten vanuit de ENSIA in beeld en belegd zijn. Door het opvolgen op basis van bovenstaande bevindingen, blijft de gemeente Lelystad in control wat de beveiligingsinspanning betreft, worden verantwoordelijken geinformeerd en wordt het volwassenheidsniveau elk jaar weer verhoogd.

VERVOLG
De follow-up op daadwerkelijke naleving van de actiepunten vindt gedurende 2021 plaats.
De ENSIA-cyclus voor 2021-2022 start op 1 juli 2021.

3. Resultaten uit eerste pentest in 2021

Hoe is de hacker-selectie tot stand gekomen?
Gemeente Lelystad is deelnemer van het VNG onderdeel GGI-Veilig. GGI-veilig helpt gemeenten hun digitale weerbaarheid te verhogen en hun ICT-infrastructuur veiliger te maken. GGI-Veilig bestaat uit een portfolio van producten en diensten voor operationele informatiebeveiliging. Eén van deze diensten zijn pentesten. Na het doorlopen van een minicompetitie via de VNG, is de dienstenleverancier gekozen die op basis van een abonnement ethische hackers inzet voor ongeveer vier pentesten per jaar. De ethische hacker past methodologien toe die zijn gebaseerd op internationale standaarden, aanbevelingen en richtlijnen.

Wat is de scope van de Pentest?
Gekozen is om de beveiliging van kaart.lelystad.nl te onderzoeken. Kaart.lelystad.nl is een server die geo-informatie op een kaart weergeeft, waarbij de bezoeker zelf meerdere kaartlagen in en uit kan schakelen. Het besturingssysteem van deze server in beheer is bij ICT en de webapplicatie wordt onderhouden door de leverancier. Daarbij is nagegaan of de etische hacker bij de achterliggende database kan komen.

Wat zijn de bevindingen uit de pentest?
De ethische hackers hebben op 24 en 25 maart 2021 van 9:00 tot 17:00 geprobeerd om kwetsbaarheden te ontdekken. Er is een beperkt aantal van drie kwetsbaarheden ontdekt, waarvan nul kritische en één belangrijke.
Bevinding 1: Geconstateerd is dat de webapplicatie de ingevoerde tekst in de adresbalk van de bezoeker onvolledig valideert. Een hacker kan op deze manier code naar de webserver sturen. Hier heeft de ethische hacker een technische oplossing aangeraden: “vervang ingevoerde metakarakters, < > “ ‘ en =, door de gelijkwaardige HTML-entiteiten (< > etc).“
Er zijn geen signalen dat de ontdekte kwetsbaarheid door hackers misbruikt is.
Bevinding 2: Het zichtbaar zijn van sessie-informatie in de adressenbalk van de browser. Omdat de website kaart.lelystad.nl alleen openbare informatie toont aan de burger, kent de aangetoonde kwetsbaarheid een laag risico.
Bevinding 3: De naam en versie van de webapplicatie is op te vragen vanuit de adresbalk van de browser. Als een kwaadwillende hacker kennis heeft van deze webapplicatie en de kwetsbaarheden in deze versie kent, dan kan hij hiervan misbruik maken. De aanbeveling n.a.v. deze pentest is om deze versie-informatie niet prijs te geven.

Hoe is er opvolging gegeven aan de drie bevindingen ?
Omdat de kwetsbaarheden zich in de webapplicatie bevonden, zijn deze bij de leverancier gemeld. Vervolgens zijn er tijdelijke mitigerende maatregelen getroffen waardoor misbruik van de kwetsbaarheden niet meer mogelijk was. Een structurele oplossing voor het verwijderen van de kwetsbaarheden vereist een upgrade van de webapplicatie. Op het moment van dit schrijven is de upgrade ingepland op 17 mei 2021.

Vervolg:
Positief is dat de ethische hacker door het aantoonbaar maken van drie kwetsbaarheden zijn meerwaarde heeft aangetoond. Jaarlijks worden vier omgevingen getest, wat inhoudt dat in 2021 nog drie andere pentesten op de planning staan. Vanzelfsprekend zal ook hier opvolging worden gegeven aan de eventuele bevindingen.

BIJLAGEN

1. “Begrippenlijst behorende bij de raadsinformatienota”