INFORMATIENOTA VOOR DE RAAD

Nummer: 198

Portefeuillehouder:	J. Schoone
Portefeuille:	Personeel en organisatie, Informatisering en automatisering, bedrijfsvoering, digitalisering/ICT
Programma:	0 Bestuur en ondersteuning
Taakveld:	0.1 Bestuur

Datum: 24-5-2022

Onderwerp: Informatienota ENSIA 2021

DE RAAD NEEMT KENNIS VAN:

1. De uitkomsten van de ENSIA zelfevaluatie op het gebied van informatiebeveiliging

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[1] 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 2021 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), BRO (Basisregistratie Ondergrond), WOZ (Waardering Onroerende Zaken), BRP (Basisregistratie Persoonsgegevens) en Reisdocumenten. In het voorjaar van 2022 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.

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

[1] Horizontale verantwoording: verantwoording vanuit het college aan de gemeenteraad

KERNBOODSCHAP

De gemeente is in control. Wel moet opgemerkt worden dat cyberrisico's dusdanig snel toenemen, dat er aanvullende personele versterking nodig is om het volwassenheidsniveau en de digitale weerbaarheid mee te laten groeien. Hierin is voorzien in de kaderbrief 2023-2026. Op het gebied van investering in proces en techniek volgt een voorstel in 'Lelystad Digitaal 2025', die ook aan de raad aangeboden gaat worden.

De onderbouwing van de kernboodschap is onderverdeeld in twee delen, te weten:

1. Informatiebeveiliging 2021
2. Resultaten uit de ENSIA en opvolging
2.1. Baseline Informatiebeveiliging Overheid (BIO)
2.2. DigiD en Suwinet
2.3. Basisregistraties BAG, BGT, BRO en WOZ
2.4. Basisregistraties BRP en Reisdocumenten

1. Informatiebeveiliging 2021

2021 was het jaar met de meeste ransomware aanvallen. Dit is zorgwekkend omdat deze trend toe blijft nemen. Met cybercriminaliteit wordt veel geld 'verdiend' en zijn de daders nagenoeg onaantastbaar. Hierdoor schieten ze als paddenstoelen uit de grond en zijn de aanvallen over het internet al winstgevender dan de drugshandel. Het risico wat de cybercriminelen veroorzaken is hiermee in korte tijd sterk toegenomen.

Wereldwijde gebeurtenissen vonden ook hun weerslag bij gemeenten. Een in het oog springend voorbeeld uit 2021 was bijvoorbeeld de ernstige kwetsbaarheid in Log4j. Door nauwe samenwerking met de Informatiebeveiligings-dienst (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 hoog-risico-kwetsbaarheids-meldingen vanuit de IBD waar te nemen. Deze vereisten directe inzet, wat de druk op ICT vergroot. Dergelijke kwetsbaarheden zijn vooraf noch te voorspellen, noch te voorkomen.

Op het moment dat deze kwetsbaarheden niet tijdig worden gedicht, of (nog) niet gedicht kunnen worden, neemt de kans op ransomware toe. Niet alleen vanwege deze alsmaar toenemende dreiging, maar ook m.b.t. Lelystad Next Level en Lelystad Digitaal 2025 dient Lelystad mee te groeien in de digitale weerbaarheid en volwassenheid. Hiervoor is in de kaderbief 2023-2026 is (bij onderwerp 6) noodzakelijk budget opgenomen voor het aanstellen van drie beveiligingsspecialisten. Op het gebied van investering in proces en techniek volgt een voorstel in 'Lelystad Digitaal 2025', die ook aan de raad aangeboden gaat worden.

2. Resultaten uit de ENSIA zelfevaluatie en opvolging

De zelfevaluatie heeft over de volledige breedte van de BIO plaatsgevonden. Om de informatiebeveiliging verder te verstevigen zijn er voor 2022 actiepunten aangeduid en ondertussen belegd bij het desbetreffende team / functionaris.

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

2.2 ENSIA onderdeel: DigiD en Suwinet

Vanwege hun specifieke normenkader, zijn deze twee applicaties verplicht diepgaand onderzocht op informatiebeveiligingsaspecten. Alle applicaties voldoen aan alle eisen binnen de norm. Een externe onafhankelijke auditor heeft voor DigiD en Suwinet een assurancerapport op de collegeverklaring afgegeven. Deze zijn gedeeld met de verticale toezichthouder.

Onderdeel	Voldoet
DigiD burgerzaken	Ja
Suwinet Participatie	Ja

2.3. ENSIA Onderdeel: Basisregistraties BAG, BGT, BRO en WOZ

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

Onderdeel	Voldoet
BAG	Ja, 82% op de totaalscore. (Norm toezichthouder = 75%) NB: één categorie (actualiteit) scoort met 72% onder de norm van 75%
BGT	Ja, 100%
BRO	Ja, 100%
WOZ	WOZ debuteert dit jaar in de ENSIA-verantwoording, er is (nog) geen norm door toezichthouder opgelegd.

Om dit niveau vast te houden, hebben de medewerkers van BAG, BGT, BRO en WOZ samen met de CISO actiepunten voor 2022 benoemd en in gang gezet. Deze punten zijn hieronder weergegeven.

Onderdeel	Actiepunten
BAG	Om de actualiteit te verbeteren, wordt het gebruik van het kwaliteitsdashboard maandelijks ingezet om fouten in de BAG op te sporen en eventueel op te lossen. Er gaan meerdere vergelijkingen toegepast worden o.a. BAG/WOZ en BAG/BGT om verschillen uit te sluiten. Hiermee is per 1-11-2021 aangevangen en wordt in mei 2022 geëvalueerd. Maandelijks wordt dit besproken in team overleg.
BAG	Aanpassing procedure van vergunningsvrije objecten zodat ook deze objecten de BAG bereiken
BGT	De verbetermaatregelen voor de BGT, zijn ervoor om de 100-score te borgen en te continueren. Hiervoor wordt elke landmeter naast de algemene werkzaamheden, specialist op een werkterrein. Hierdoor wordt kennis vergroot (niet iedereen hoeft alle ontwikkelingen te volgen). Door korte lijnen is kennis overdracht geborgd. Deze afspraken worden in 2022 geïmplementeerd.
BRO	De verbetermaatregel voor de BRO, is ervoor om de 100-score te borgen en te continueren. De BRO-beheerder zal zich ook in 2022 inspannen om kennis en informatie intern en extern te delen.
WOZ	Met de aanschaf van de nieuwe belastingapplicatie is het beveiligingsniveau en de architectuurplaat bij oplevering op orde. Om dit niveau te handhaven is het nodig om de volgende controles cyclisch uit te voeren: - controle op actualiteit van de architectuurplaat - compliance check op BIO-maatregelen/beleid - controle op de uitval
WOZ	Stel in samenspraak met de ICT-leverancier voor de WOZ-uitvoering een meerjarenplan voor de ICT-ontwikkelingen on waarin de elementen BRK Levering 2.0, SOR en Common Ground worden opgenomen.

2.4. ENSIA onderdeel: Basisregistraties BRP en Reisdocumenten

Dit onderdeel bevat de resultaten van de antwoorden op de vragen in de ENSIA-tool.

Onderdeel ENSIA BRP	Waarde Lelystad	Maximale Score	Percentages
BRP-organisatie	400	400	100%
BRP-toegang	380	400	95%
BRP-naleving	360	400	90%
Puntentotaal BRP ENSIA	1.140	1.200	95%

Onderdeel Reisdocumenten	Waarde Lelystad	Maximale Score	Percentages
Reisdocumenten-organisatie	400	400	100%
Reisdocumenten -toegang	380	400	95%
Reisdocumenten -naleving	400	400	100%
Puntentotaal Reisdocumenten	1.180	1.200	98%

De behaalde scores zijn goed te noemen.

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.

VERVOLG

De follow-up op daadwerkelijke naleving van de actiepunten vindt gedurende 2022 plaats.
De ENSIA-cyclus voor 2022-2023 start op 1 juli 2022.

Bijlagen

1. “Begrippenlijst behorende bij de raadsinformatienota”