INFORMATIEMEMO RAAD

Kenmerk: 21INF00045

Datum advies: 16 juni 2021	**Onderwerp:** Raadsinformatiememo informatieveiligheid (n.a.v. rekenkamercommissierapport)
Kennis nemen van: Plan van aanpak naar aanleiding van rekenkamercommissierapport informatieveiligheid	
Status advies: openbaar	**Argument:** (indien niet openbaar)
Portefeuillehouder: B.E. Faber-de Lange	**Datum b&w-vergadering:** 22 juni 2021
Betrokkenen bij voorstel extern: -	**Betrokkenen bij voorstel intern:** M. Spierings, B. Jansen, L. van Ampting, A. Rombouts, K. van Lakwijk
Bijlagen: -	

Kennis nemen van:
Plan van aanpak naar aanleiding van rekenkamercommissierapport informatieveiligheid

Inleiding
Middels deze memo informeren wij u over de acties die gemeente Overbetuwe in haar bedrijfsvoering doorvoert om haar informatieveiligheid te versterken. Dit naar aanleiding van het rekenkamercommissierapport betreffende informatiebeveiliging (IB).

Uit dit rapport blijkt dat verbeteringen in onze informatiebeveiliging noodzakelijk zijn. Deze zaken nemen wij serieus, want informatieveiligheid is een cruciale randvoorwaarde voor een betrouwbare dienstverlening van gemeente Overbetuwe.

Daarom hebben we alle bevindingen en aanbevelingen uit dit rapport gebruikt bij de totstandkoming van een plan van aanpak. Dit plan richt zich op de verbetering van de centrale sturing en beheersing van de informatiebeveiliging (IB) van gemeente Overbetuwe. Hiermee groeien we naar een meer informatieveilige gemeente. Het plan bevat enkele tientallen acties/projecten die zijn opgenomen in een uitvoeringskalender..

Achtergrond
Als gemeente zijn we sterk afhankelijk van digitale processen. Het belang van adequate informatieveiligheid is daarbij groot, omdat de digitale dreiging op allerlei terreinen verder toeneemt. Informatieveiligheid moet dus ook bij gemeente Overbetuwe op orde zijn en blijven. Daarom zal gemeente Overbetuwe de komende jaren blijvend moeten investeren in de beveiliging van haar processen.

Belang van Informatiebeveiliging
Ook gemeenten zijn een potentieel doelwit voor cybercriminaliteit. Zie hiervoor onlangs de voorbeelden bij de gemeenten Lochem en Hof van Twente. Dit onderstreept dat het belangrijk is dat de interne informatiebeveiliging van gemeente Overbetuwe op orde is.

IB is essentieel voor de betrouwbaarheid en continuïteit van de gemeentelijke dienstverlening. Voor kwalitatief goede dienstverlening is het cruciaal dat informatie juist, volledig en tijdig beschikbaar is voor de gebruiker (medewerkers, maar ook inwoners, bedrijven en anderen die op ons rekenen). Daarnaast stellen we steeds hogere eisen aan de beveiliging van bedrijfs- en persoonsinformatie. Informatie is hiermee een belangrijke productiefactor geworden, waarvan de beschikbaarheid, exclusiviteit en integriteit moet worden gegarandeerd.

Huidige situatie
Zoals blijkt uit het rapport van de rekenkamer is de gemeten volwassenheid rondom IB om en nabij het volwassenheidsniveau ad hoc. Dit betekent dat gemeente Overbetuwe nog te ‘reactief’ handelt. Zo wordt er in geval van een incident weliswaar snel gehandeld (en een oplossing gevonden), maar nog niet op een voldoende gestructureerde manier. Dit willen we aanpakken.

Een niveau omhoog gaan in volwassenheid is ons streven, maar kost ook tijd. En hoe hoger het niveau van volwassenheid, des te hoger zijn ook de (jaarlijkse) kosten om dat niveau in stand te houden.

Gewenste situatie
Het verschil tussen het huidige niveau van volwassenheid en het gewenste niveau gebruiken we om zicht te krijgen op het groeitraject in de beheersing van informatiebeveiliging. Wij streven naar een optimaal niveau, rekening houdend met de risicobereidheid en karakteristieken van het betreffende aandachtsgebied. Het gewenste niveau is niet per definitie het maximale volwassenheidsniveau.

We willen de grootste groei realiseren in de aandachtsgebieden governance, risicomanagement en incidentmanagement. De mate van groei is afhankelijk van (beschikbare) mensen, middelen, technische en organisatorische haalbaarheid.

Scope
Dit plan van aanpak richt zich op de verbetering van de centrale sturing en beheersing van de informatiebeveiliging van gemeente Overbetuwe en haar bedrijfsvoering. De uitvoering van de verschillende activiteiten is altijd een verantwoordelijkheid van de betreffende proces- of risico-eigenaar, aangewezen binnen de organisatie. De acties en projecten hebben betrekking op de gehele organisatie en zijn gericht op zowel de mens, techniek en proces.

Wat gaan we doen?
Het plan van aanpak IB beslaat een periode van 2021 tot 2023 en omvat de volgende drie speerpunten:

1. Het verbeteren van de governance van IB;
2. Het versterken van het risicomanagement;
3. Het verbeteren van incidentmanagement.

1. Het verbeteren van de governance van IB
De verantwoordelijkheid voor beheersing van de IB is formeel belegd in de lijn, zoals ook beschreven in het gemeentebrede informatiebeveiligingsbeleid. De directie is verantwoordelijk voor de kaderstelling, stuurt op concernrisico’s, controleert of de getroffen maatregelen in overeenstemming zijn met de betrouwbaarheidseisen en bepaalt of deze voldoende bescherming bieden. Ook evalueert zij periodiek de beleidskaders en stelt deze waar nodig bij.

IB moet op het hoogste managementniveau vertegenwoordigd zijn, zodat het bewaken en ondersteunen van de bedrijfsdoelstellingen adequaat kan gebeuren. Daarom is om meer grip te krijgen op dit proces een stuurgroep opgericht, onder voorzitterschap van de gemeentesecretaris. De stuurgroep houdt zicht

op de voortgang van de roadmap. De uitvoering vindt plaats in de bedrijfsorganisatie middels een projectgroep.

2. **Versterken van risicomanagement**

Op basis van een integrale en collectieve aanpak van risicomanagement wordt vanuit concern control een beter inzicht verkregen in de risico's en worden acties geformuleerd om de risico's te verkleinen of weg te nemen. IB is een belangrijk onderdeel van deze integrale risicomanagement aanpak.

Ook het risicobewustzijn van de medewerkers zelf wordt verhoogd. Bij beveiligingsincidenten is het onbewust handelen van de mens een belangrijke oorzaak. Om die reden wordt in kennis en kunde van medewerkers met betrekking tot informatiebewust handelen geïnvesteerd.

Uit voorgaande volgt verder dat medewerkers hierover in gesprek gaan met hun leidinggevende om de weerbaarheid in de het omgaan met waardevolle data te verhogen.

Daarnaast wordt de technische maatregel SIEM/SOC (Security Information & Event Management / Security Operations Center) geïmplementeerd in onze gemeente, in samenwerking met gemeente Lingewaard. Dit stelt ons organisatorisch en instrumenteel beter in staat om kwetsbaarheden en risico's te detecteren. Primaire processen van onze worden aangesloten op de monitoringsfunctie van het SIEM/SOC.

3. **Verbeteren van incidentmanagement**

De incident- en escalatieprocedures worden periodiek geëvalueerd. Zo heeft onze gemeente centraal zicht op de verschillende incidenten en datalekken, ook in samenwerking met ICT van gemeente Lingewaard. Op basis van nieuwe inzichten wordt het beleid continu aangescherpt en geëvalueerd. De tijdige en effectieve afhandeling van beveiligingsincidenten wordt bewaakt en zo nodig bijgestuurd.

Aanpak

De genoemde speerpunten zijn vertaald in 41 acties/projecten (allen ook weer direct te relateren aan het rekenkamercommissierapport). Voldoende tijd en capaciteit van deskundig personeel vormt daarbij een kritische succesfactor.

Een projectgroep is inhoudelijk verantwoordelijk voor de uitvoering. Deze werkt de noodzakelijke verbeteringen uit in actie- en projectplannen. De stuurgroep wordt hierover geïnformeerd en is verantwoordelijk voor het bepalen van prioriteiten en het monitoren van de voortgang.

Uitvoeringskalender

Hieronder vindt u onze voorgenomen acties/projecten voor de komende 2 jaar in relatie tot onze drie speerpunten. De stuurgroep verfijnt de prioritering en zorgt voor een realistische uitvoeringskalender, rekening houdend met de aanbevelingen uit het rekenkamerrapport. Met de punten 1, 2, 6, 7, 13, 14, 16, 33, 37 en 41 zijn wij reeds gestart, al dan niet in samenwerking met ICT Lingewaard.

#	Actie / Project
1	Stuurgroep en projectgroep informatiebeveiliging oprichten en inrichten rapportagecyclus
2	Inregelen periodiek evalueren en sturen op gemaakte dienstverleningsafspraken aan de hand van managementinformatie van ICT Lingewaard.
3	Aanstellen ICT security officer
4	Opstellen toegangsbeleid
5	Actief (uit)dragen van IB
6	Aanbesteden en laten uitvoeren penetratietest (nulmeting) op ICT infrastructuur en daarover begrijpelijk rapporteren en adviseren tot verbeteringen.
7	Kwetsbaarhedensscan op ICT infrastructuur uitvoeren en daarover begrijpelijk rapporteren en adviseren tot verbeteren kwetsbaarhedenmanagement.
8	Invoeren leermanagementsysteem (LMS) voor ten minste informatiebeveiliging.

9	Vastlegging van het onderwerp ‘geheimhouding bij uitdiensttreding’ bij exitgesprek in het personeelsdossier
10	Controles op informatiebeveiliging plannen en uitvoeren
11	Onderwerp IB opnemen in agenda van team- en afdelingsoverleggen.
12	IB opnemen in Werk- en Ontwikkelplan.
13	Bedrijfscontinuiteitsmanagement opstellen en uitvoeren.
14	Integraal risicomanagement uitvoeren.
15	Koppelen van bedrijfsmiddelen en informatie(systemen) aan eigenaren.
16	Verbeteren (proces) registratie en afhandeling IB incidenten.
17	CAB proces documenteren
18	Intakeboard proces documenteren
19	Informatie rondom IB wat relevant is voor iedereen, vaker delen op startpagina van Intranet
20	Registratie van deelname basistraining IB voor nieuwe medewerkers.
21	Lijnmanager stuurt actief op deelname IB training en succesvol doorlopen e-learnings.
22	Wijzigingsmanagementbeleid opstellen en uitvoeren
23	Patchmanagementbeleid opstellen en uitvoeren
24	Basisprocessen IB op orde brengen.
25	IAM beleid opstellen en implementeren
26	Decentraal binnen de teams formele aanspreekpunten voor IBenP (informatiebeveiliging en privacybescherming) creëren en hen als vraagbaak en uitdrager laten fungeren
27	Opnemen van IB (risico-) eigenaarschap in taakomschrijving lijnmanager.
28	GAP en impactanalyse uitvoeren
29	Onderhoud ISMS verbeteren
30	Loggingbeleid opstellen en implementeren
31	Aansluiten op IBD netwerkinventarisatie (NWI)
32	Expliciet risico-afweging maken en vastleggen welke kritische applicaties een test-omgeving behoeven.
33	CMBD juist en volledig maken en houden.
34	Loggingbeleid opstellen en implementeren.
35	Inrichten basismaatregelen CIS controls
36	Opstellen en implementeren hardeningbeleid.
37	2FA implementeren voor systemen en toepassingen indien toegang tot informatie, systeemfuncties en toepassingen wordt verleend vanuit een onvertrouwde zone naar een vertrouwde zone.
38	MDM beleid opstellen en implementeren.
39	Logische toegangsbeveiligingsbeleid opstellen en implementeren
40	Realiseren SIEM/SOC
41	Gezamenlijke ICT omgeving creëren

Aanbevelingen rekenkamerrapport

Bovenstaande acties en projecten zijn allen te herleiden tot de bevindingen en aanbevelingen uit het rekenkamerrapport. Hieronder is weergegeven welke acties/projecten welke aanbeveling tegemoet komen.

Categorie & Prio	Aanbeveling	Actie/project
MENS	Duidelijk maken welke verwachtingen het college heeft van de lijnmanagers ten aanzien van informatiebeveiliging en zorgen dat zij met behulp van kennisoverdracht ook in staat zijn om hun taken, verantwoordelijkheden en bevoegdheden ten aanzien van informatiebeveiliging uit te voeren.	Zie 1, 5, 21, 26, 27
MENS	Structureel verbeteren van awareness. Het implementeren van een Leermanagementsysteem (LMS)	Zie 8, 10, 12, 14, 20 en 21
MENS	Informatiebeveiliging nadrukkelijker in het indiensttredingsproces opnemen zodat nieuwe medewerkers ‘secure-by-design’ worden ingewerkt.	Zie 8, 20 en 21
PROCES	Kritische bedrijfsmiddelen identificeren, deze van betrouwbaarheidseisen voorzien en deze koppelen aan eigenaren. Vervolgens risicoanalyses uitvoeren op de bedrijfskritische processen en bedrijfsmiddelen zodat deze adequaat beheerst kunnen worden.	Zie 15, 16, 18, 27, 31, 32 en 33
PROCES	Beleid opstellen voor de onderwerpen die verplicht zijn vanuit de BIO. Deze formeel vast laten stellen, waarmee op een gedetailleerder niveau invulling gegeven wordt aan de strategische doelstellingen van Overbetuwe.	Zie 4, 22, 23, 24, 25, 30, 38 en 39
PROCES	Integraal risicomanagement integreren zodat alle risico’s, dus niet alleen in het kader van informatiebeveiliging, op dezelfde manier worden geïdentificeerd, geclassificeerd en behandeld.	Zie 14, 15 en 16
PROCES	Opstellen van een uitgebreid plan (roadmap) waarin wordt beschreven hoe de naleving van de BIO en daarmee ook de volwassenheid ten aanzien van informatiebeveiliging op korte termijn aantoonbaar wordt verbeterd.	Zie 1, 2, 12, 28 en 29
PROCES	Zorg dragen voor een planning met betrekking tot informatiebeveiliging welke alle verplichte activiteiten bevat voor het continu verbeteren daarvan.	Zie 1, 2, 28 en 29
PROCES	Het college en de raad meer en vaker bij het onderwerp informatiebeveiliging betrekken.	Zie 1 en 2

PROCES	Zorgen dat bewijslast (‘evidence’), waarmee aangetoond kan worden dat wordt voldaan aan BIO-eisen, wordt vastgelegd op een centrale locatie, zodat een helder overzicht ontstaat van de tekortkomingen ten opzichte van de BIO.	Zie 24 en 29
PROCES	Een strategisch programma voor informatiebeveiliging binnen Overbetuwe starten zodat informatiebeveiliging structureel wordt verbeterd en geborgd.	Zie 1, 2, 12 en 13
TECHNIEK	Een (penetratie)test uitvoeren op de ICT-infrastructuur om inzicht te verkrijgen in (mogelijke) kwetsbaarheden (nulmeting). Geautomatiseerde kwetsbaarhedenscans uitvoeren waarmee periodiek gemonitord wordt op kwetsbaarheden.	Zie 6 en 7
TECHNIEK	Zorgen dat de basisprocessen van ICT op orde worden gebracht en deze monitoren om ongewenste situaties te voorkomen.	Zie 15, 16, 20, 21, 22, 23, 24, 25, 26, 34, 35 en 36
TECHNIEK	Zorgen dat ICT over de benodigde middelen beschikt om documentatie op orde te brengen en te houden en er periodiek hersteltesten uitgevoerd kunnen worden zodat vastgesteld kan worden of backups succesvol teruggeplaatst kunnen worden of dat de overeengekomen afspraken ook daadwerkelijk gerealiseerd kunnen worden.	Zie 15, 24, 40 en 41
FYSIEK	Zorgen dat duidelijk is op welke locaties zich bedrijfsmiddelen van Overbetuwe bevinden, zodat daar adequate beveiliging op kan worden toegepast.	Zie 13, 15, 16, 17 en 29
FYSIEK	Overweeg om de Crime Prevention Through Environmental Design (CPTED) principes toe te passen om gewenst gedrag te stimuleren en om ongewenst gedrag te beperken.	Zie 8, 14, 20 en 21

Samenvatting

Om haar informatieveiligheid te versterken, worden de komende periode binnen de bedrijfsvoering van gemeente Overbetuwe enkele tientallen acties/projecten uitgevoerd. Het plan van aanpak IB beslaat een periode van 2021 tot 2023 en omvat drie speerpunten:

1. Het verbeteren van de governance van IB;
2. Het versterken van het risicomanagement;
3. Het verbeteren van incidentmanagement.

Communicatie

De raad wordt via het reguliere proces geïnformeerd over de voortgang, namelijk via de paragraaf bedrijfsvoering in de Jaarstukken.

Behandelend adviseur voor technische vragen: B. Jansen, tel.: 14 0481, email: bernard.jansen@overbetuwe.nl

HET COLLEGE VAN BURGEMEESTER EN WETHOUDERS,

de gemeentesecretaris,	de burgemeester,
P.J.E. Breukers	R.P. Hoytink-Roubos