Quickscan doorwerking onder-zoek RKE Informatiebeveiliging ‘Safe of Zeef’

Copyright © 2022 Eurofins Cyber Security

Inhoudsopgave

1 Inleiding 3

1.1 Aanleiding Quickscan "doorwerking" 3

1.2 Proces en aanpak Quickscan "doorwerking" 3

1.3 Leeswijzer 3

2 Uitkomsten Quickscan 4

2.1 Algemene uitkomsten 4

2.2 Status aanbevelingen RKE Rapport 2019 4

2.2.1 Aanbeveling 1 - aandacht voor informatiebeveiliging 5

2.2.2 Aanbeveling 2 - plan voor informatiebeveiliging 5

2.2.3 Aanbeveling 3 – cyber-BHV 6

2.2.4 Aanbeveling 4 - technische onderzoeken 6

2.2.5 Aanbeveling 5 - aandacht voor de menselijke factor 7

3 Evaluatie 8

Bijlage 1 Verklarende woordenlijst 9

heeft opmaak toegepast: Engels (Verenigde Staten)

1 Inleiding

1.1 Aanleiding quickscan “doorwerking”

Qbit Cyber Security (hierna: Qbit, sinds mei 2021 ‘Eurofins Cyber Security’) heeft in opdracht van de Rekenkamercommissie Emmen (hierna: de ‘RKE’) een onderzoek verricht in hoeverre de gegevens van burgers en bedrijven binnen de gemeente in voldoende mate zijn beveiligd. Dit heeft geresulteerd in het RKE-rapport *Informatiebeveiliging: “Informatie, safe of zeef?”* met daarin een vijftal aanbevelingen. De aanbevelingen zijn in een raadsbesluit van 30 april 2020 overgenomen.

In de afgelopen periode heeft informatiebeveiliging niets aan actualiteit ingeboet: recente incidenten in het bedrijfsleven en bij overheden bevestigen dit telkens opnieuw.

Reden te meer om na te gaan of de aanbevelingen uit het onderzoeksrapport zijn opgevolgd.

1.2 Proces en aanpak quickscan “doorwerking”

Na de presentatie van het RKE-rapport in de gemeenteraadscommissie van 16 januari 2020, heeft de wethouder op 27 januari 2020 schriftelijk aan de gemeenteraad laten weten dat een verbeterplan in concept is opgesteld en naar verwachting in februari zal worden opgeleverd. Vervolgens is in de raadscommissie van 12 maart 2020, bij behandeling van het raadsvoorstel, door de wethouder gezegd dat het verbetertraject goed op weg is en dat tussentijds de raad zal worden geïnformeerd over alle stappen. Daarna is het raadsvoorstel met het rapport als bijlage aan de orde geweest in raadsvergadering van 30 april 2020 en zijn de aanbevelingen overgenomen.

De RKE heeft samen met Eurofins Cyber Security middels deze quickscan de huidige status van de aanbevelingen willen vaststellen. Hiervoor is - geheel passend bij een corona-jaar - een digitale vragenlijst ontwikkeld. Deze vragenlijst is vervolgens voorgelegd aan raadsleden en aan de ambtelijke organisatie. Raadsleden hebben enkel de relevante vragen ter opvolging van de voor de raad bedoelde aanbevelingen ontvangen. De ambtelijke organisatie heeft daarnaast meer inhoudelijke vragen ontvangen.

Alle 11 fracties en medewerkers van de ambtelijke organisatie zijn uitgenodigd om deel te nemen. De RKE heeft zorggedragen voor het adresseren, zodat de onderzoekers geen toegang hebben gekregen tot de (privé)mailadressen van de raadsleden en ambtelijke organisatie.

De link naar de vragenlijst is verstuurd op 20 juni 2021. Op 28 juni 2021 is door de RKE een toelichting rondgestuurd n.a.v. vragen over de wijze van beantwoorden van de vragenlijst. Uiteindelijk is de vragenlijst afgesloten op 24 juli 2021. Per mail is door de ambtelijke organisatie op 21 juli nog een additionele toelichting gestuurd. Deze reactie is eveneens verwerkt in dit rapport, voor zover de antwoorden een aanvulling zijn op antwoorden die reeds waren ontvangen via de vragenlijst zelf.

De uitkomsten zijn geëxporteerd uit de gebruikte enquêtetool en door de onderzoekers verwerkt in hoofdstuk 2 van dit rapport.

Het rapport is voorgelegd aan het CMT voor een feitencheck.

1.3 Leeswijzer

In hoofdstuk twee zijn de resultaten van het onderzoek beschreven. Allereerst is het algemene beeld weergegeven. Vervolgens is per aanbeveling uit het rapport van de RKE van 2019 aangegeven wat de huidige status is. In het laatste hoofdstuk (drie) geeft de RKE nog een samenvattende evaluatie van de bevindingen.

heeft opmaak toegepast: Engels (Verenigde Staten)

2 Uitkomsten quickscan “doorwerking”

2.1 Algemene uitkomsten

Respons

De vragenlijst is door 5 leden van de ambtelijke organisatie (gezamenlijk) beantwoord. Daarnaast hebben 7 fracties van de 11 aangeschreven fracties de lijst ingevuld. De uitkomsten zijn representatief op inhoud en responsaantal, gelet op de beperkte verspreidingskring.

Algemeen beeld

De hoofdvraag van het onderzoek in 2019 was:

“In hoeverre is de (digitale) informatiebeveiliging van (persoons)gegevens binnen de gemeente op orde en waaruit blijkt dat de privacy van de inwoners en bedrijven van gemeente Emmen jegens de gemeente en organisaties die de gemeentelijke taken uitvoeren voldoende gewaarborgd is?"

Uit deze quickscan komt naar voren dat geen van de aanbevelingen volledig is opgevolgd. Door de respondenten uit de ambtelijke organisatie is aangegeven dat de snelheid van het uitvoeren van verbeteringen laag ligt, omdat voorrang is gegeven aan het inrichten van de interne organisatie. Zo is er een (nieuwe) Chief Information Security Officer (CISO) aangesteld.

Een aantal fracties geeft aan dat opvolging onvoldoende is, er geen plan lijkt te zijn en het onderwerp (te) weinig is besproken.

De raad heeft in de raadscommissie van 12 maart 2021 aangegeven op de hoogte te willen blijven van de stand van zaken van de informatiebeveiliging via drie routes:

1) ENSIA-rapportage;
2) De managementletter of jaarverslag van de accountant; en
3) Middels het feitelijke verbeterplan.

Voor zover de onderzoekers dit na hebben kunnen gaan
(1) is de ENSIA-rapportage niet geagendeerd geweest in 2021 (tot en met oktober);
(2) beschrijft het jaarverslag van de accountant ook dat AVG en Informatiebeveiliging nog niet op een voldoende niveau zijn
(3) is er wel een verbeterplan opgesteld door de ambtelijke organisatie en is dit plan goedgekeurd door het CMT
(4) is dit verbeterplan nog niet gepresenteerd aan de raad, en
(5) geeft de begroting voor 2022 (p.76) aan dat er nog toegegroeid moet worden naar het “voldoen aan de normen van de BIO”.

Over het geheel gezien geeft de ambtelijke organisatie aan dat de gemeente nog niet volledig in control is op alle onderdelen van de aanbevelingen. De raad heeft onvoldoende zicht op en feitelijke informatie over de stand van zaken met betrekking tot de aanbevelingen.

Het is van groot belang om nu zorgvuldig en snel de feitelijke risico’s die de gemeente loopt te identificeren en mitigeren. Bijvoorbeeld een situatie zoals bij het Hof van Twente of recenter bij VDL-Nedcar, Mediamarkt of Ikea. Daar is implementatie van de BIO weer bij nodig.

2.2 Status aanbevelingen RKE Rapport 2019

In het onderzoek van de RKE in 2019 is gekeken naar diverse elementen van informatiebeveiliging, het proces daaromheen en de rol van de raad. Er zijn vervolgens 5 aanbevelingen gedaan. Hieronder zijn de hoofdpunten van deze 5 aanbevelingen opgenomen. Vervolgens is de oorspronkelijke, volledige, tekst van de aanbevelingen uitgewerkt met de huidige stand van zaken, zoals door de respondenten is aangegeven in de vragenlijst.

heeft opmaak toegepast: Engels (Verenigde Staten)

2.2.1 Aanbeveling 1 - aandacht voor informatiebeveiliging

'Wij bevelen aan dat de raad de BIO omarmt en het onderwerp "informatiebeveiliging en privacybescherming" minimaal eenmaal per jaar als agendapunt van de gemeenteraad opneemt. De raad dient zich daarbij te vergewissen dat de "hygiëne" op het gebied van informatiebeveiliging op orde is bij gemeente Emmen. Dit moet het geval zijn voor de domeinen waar al een "verantwoordingsplicht" voor geldt (Sociaal Domein en Burgerzaken), maar ook voor alle domeinen en afdelingen waar gegevens van burgers en organisaties worden gebruikt.'

Deze aanbeveling is niet opgevolgd.

Uit de vragenlijst komt naar voren dat de raad informatiebeveiliging van belang vindt. Echter, de raad heeft niet het initiatief genomen om het in 2021 te agenderen. De raad is van mening dat het college het initiatief dient te nemen om de raad te informeren omdat dit immers is toegezegd door de wethouder.

Sinds 2020 heeft de gemeenteraad geen verantwoording ontvangen over hygiëne van niet verplichte verantwoordingsdomeinen. Voor Burgerzaken en het Sociaal Domein zal de raad op korte termijn worden geïnformeerd via het ENSIA-instrument. Dit is aangegeven door de ambtelijke organisatie in hun gezamenlijke reactie op de vragenlijst. De onderzoekers constateren dat de ENSIA verantwoording nog niet plaats heeft gevonden op dit moment (oktober 2021). In de rapportage van de accountant, het jaarverslag 2020, komt naar voren dat zowel op het gebied van de informatieveiligheid als de AVG/privacy beheersing nog aandacht nodig is.

Zoals in de oorspronkelijke rapportage ook is aangegeven, zijn het ENSIA-instrument en het jaarverslag van de accountant geen volledige rapportage over de gehele beheersing. De ENSIA werkt grotendeels op basis van zelfonderzoek en kent slechts verplichte verantwoording op DigiD en op SUWI. Het is wel zo dat een globaal beeld over de implementatie van de BIO kan worden verkregen via deze rapportage, omdat de BIO het geldende toetsingskader is voor het Sociaal Domein.

Over het geheel gezien is de conclusie dat de gemeente “er nog niet is”. Het is voor de gemeenteraad onvoldoende duidelijk waar het echt knelt en tegen welke “aanvallen” de gemeente nu wel en niet bestand is.

2.2.2 Aanbeveling 2 - plan voor informatiebeveiliging

'Wij bevelen de raad aan het college te verzoeken om te komen met een plan van aanpak om de BIO "te implementeren". Dit plan dient in ieder geval te beschrijven:
a. De huidige situatie, gekoppeld aan de eisen van de BIO.
b. De gewenste situatie, met maatregelen op centraal niveau en per domein gespecifieerd (input: risicoanalyses bij de teams/afdelingen zelf).
c. Specifieke risicoanalyse uitkomsten binnen de domeinen "Burgerzaken, Sociaal Domein en Belastingen".
d. De verantwoordelijkheid van iedere medewerker rondom informatiebeveiliging.
e. De specifieke rollen en verantwoordelijkheden om de BIO op korte termijn in te kunnen voeren.
f. De doelstellingen en indicatoren over het wel of niet voldoen aan de doelstellingen (kritieke prestatie-indicatoren) die zullen worden gesteld.
g. Planning voor de implementatie.
h. Benodigde (extra) middelen.'

Deze aanbeveling is deels opgevolgd. De BIO is nog niet volledig geïmplementeerd, maar er is wel een verbeterplan opgesteld en dit is verder geconcretiseerd in het [jaarplan informatiebeveiliging 2022].

Het verbeterplan is door de ambtelijke organisatie opgesteld en goedgekeurd door het CMT. De noodzakelijke onderwerpen van de BIO komen hierin aan de orde, maar ook ontwikkelingen die

heeft opmaak toegepast: Engels (Verenigde Staten)

meer recent zijn zoals de resolutie 'Digitale Veiligheid: kerntaak voor gemeenten'. De hoofdlijnen[1] van het jaarplan zijn voor zover bekend nog niet gepresenteerd aan de raad.

Met name het jaarplan 2022 bevat stevige ambities en dat is ook nodig, volgens de onderzoekers. De respondenten uit de ambtelijke organisatie geven aan dat de CISO de acties en daarmee de te treffen maatregelen bewaakt. Actiehouders zijn verantwoordelijk voor de uitvoering van hun eigen acties. Samen met de CISO wordt dit besproken. Een aandachtspunt betreft, volgens de ambtelijke organisatie, het integreren van de voortgang met de reguliere planing- & controlcyclus.

De aanbeveling noemt ook het beschikbaar stellen van middelen. Er zijn middelen ter beschikking gesteld en in de begroting van 2022 is een post van €170.000 opgenomen om de informatiebeveiliging en privacybescherming verder te verbeteren. De onderzoekers stellen dat dit niet voldoende zal zijn om alle aandachtspunten op te lossen. De ambtelijke organisatie geeft dit ook aan. Deze geeft vervolgens aan dat de focus komt te liggen op:

1) Mens (zie aanbeveling 5)
2) Techniek d.m.v. het inrichten van technische monitoring en
3) Bewuste aandacht voor continuïteitsmanagement, voor als het een keer 'echt' misgaat.

De onderzoekers herkennen deze punten ook als meest kritische aandachtsgebieden, maar willen de gemeente meegeven dat een goede en feitelijke technische meting (pentest - zie aanbeveling 4) hiervan ook minimaal onderdeel moet zijn.

2.2.3 Aanbeveling 3 – cyber-BHV

'De RKE beveelt de raad aan het college te verzoeken inzicht te geven hoe het college stuurt op adequate afhandeling van informatiebeveiligingsincidenten en of, waar nodig, additionele maatregelen worden getroffen.'

Deze aanbeveling is niet opgevolgd.

De gemeente heeft nog geen grote incidenten gehad zoals bij collega gemeenten wel het geval is (denk aan Hof van Twente). Dat is positief. Dit kan echter wel gebeuren; dan is het van groot belang dat iedereen voorbereid is. De onderzoekers stellen vast dat binnen de ambtelijke organisatie het proces bekend is. Bij mogelijke ernstige incidenten zal het CMT en het college worden betrokken.

Het is van groot belang dat de 'cyber-BHV' op orde is. Daarvoor blijft het wenselijk dat de hele organisatie, ook de gemeenteraad, geïnformeerd is over het proces van het afhandelen van informatiebeveiligingsincidenten en dat bijvoorbeeld bekend en getraind is hoe de voorlichting naar burgers en de raad verloopt bij een (groot) incident of datalek.

2.2.4 Aanbeveling 4 - technische onderzoeken

'Tevens beveelt de RKE aan vanuit de raad het college op te roepen voldoende middelen beschikbaar te stellen om de continu veranderende dreigingen op het gebied van informatiebeveiliging te kunnen monitoren en, vervolgens en waar nodig, aanvullende maatregelen te treffen. Zonder een adequate scanner, zal de gemeente niet in staat zijn voldoende technische dreigingen uit te sluiten. Het is van belang dat hiervoor voldoende middelen beschikbaar zijn en blijven, zeker nu waarschijnlijk gaat blijken dat de BIO überhaupt meer middelen vereist. Het plan vormt hiervoor de input.'

Deze aanbeveling is gedeeltelijk opgevolgd.

Er zijn wel technische onderzoeken uitgevoerd, maar alleen voor zover dit verplicht is gesteld door externe kaders zoals DigiD. Er is nog geen gestructureerde aanpak opgesteld, waarin periodiek en risicogericht onderzoeken op technisch gebied worden gepland, uitgevoerd en opgevolgd. De huidige stand van zaken kan op technisch gebied dus kwetsbaar zijn.

[1] Hoofdlijnen zijn nodig omdat details uit het jaarplan mogelijk de gemeente kwetsbaar maken vanwege het openbare karakter.

heeft opmaak toegepast: Engels (Verenigde Staten)

Er zijn sinds 16 januari 2020 geen periodieke (technische) kwetsbaarhedenscans uitgevoerd (i.c. pentesten) op de IT-omgeving van de gemeente. Om SIEM/SOC[2] verder uit te rollen, is er een passsage opgenomen in de kadernota en zijn de voorbereidingen gestart. Er is nog geen duidelijkheid of er in de tussentijd een feitelijke meting (pentest) gepland staat en of de juiste omvang is gekozen.

De scans worden uitgevoerd op een zodanige wijze dat ze geen invloed hebben op de beschikbaarheid en integriteit van de IT-omgeving.

Er is een security assessment uitgevoerd door Microsoft. De daaruit afkomstige bevindingen moeten nog worden besproken (status oktober 2021). Ook de inrichting van een SIEM/SOC, als belangrijk instrument om incidenten en kwetsbaarheden snel te signaleren, moet in 2022 nog worden ingericht.

2.2.5 Aanbeveling 5 - aandacht voor de menselijke factor

'Wij bevelen de raad aan het college te informeren dat het van groot belang is, en een verplichting in de BIO, om door te gaan met de bevordering van bewustzijn, houding en gedrag. Daarnaast zorgt een actieve rol van de raad voor meer draagvlak en structurele aandacht op het gebied van bewustwording. Door goed de dialoog te blijven voeren en de voortgang te monitoren, kan de gemeente Emmen beter sturen op aspecten zoals gedrag en cultuur.'

Deze aanbeveling is gedeeltelijk opgevolgd.

Er is een bewustwordingsprogramma opgesteld en in uitvoering. Het college is hierover ook geïnformeerd, maar volgens de respondenten is de raad hierin niet meegenomen. De onderzoekers hebben hier ook geen agendapunt voor kunnen vinden. De raad heeft in de vergadering van 30 april 2020 de aanbevelingen onderschreven, maar de terugkoppeling vanuit het college richting de raad (dat er een programma is gestart en de doelen hiervan) moet nog plaats vinden.

Het programma is gestart met een analyse van de huidige en gewenste cultuur binnen de gemeente, op het gebied van informatiebeveiliging.

De respondenten uit de ambtelijke organisatie geven aan dat een programma is opgesteld op basis van 10 ‘Gouden Regels voor informatiebeveiliging en privacy’ en dat het lopende programma op hoofdlijnen achtereenvolgens de volgende onderdelen bevat: Cultuurscan; workshop; kennis-nulmeting; e-learning en een phishing campagne”.

De organisatie geeft aan dat het einddoel het aantoonbaar voldoen aan de BIO is. Het is volgens de onderzoekers niet mogelijk om ineens de BIO te implementeren, onder andere vanwege het verandermanagement aspect.

De door de gemeente gekozen aanpak om eerst de cultuur te bepalen en pas daarna ‘strepen te gaan trekken’ is logisch. De respondenten uit de ambtelijke organisatie geven aan dat het ‘beleggen van verantwoordelijkheid en eigenaarschap’ prioriteit krijgt. De onderzoekers lezen hieruit dat de gemeente een structurele inbedding verlangt en niet zomaar ‘een trucje’ wil uitvoeren. Dat is verstandig, voor zover de feitelijke gaten bekend zijn (aanbeveling 4). Toch is enige haast wel degelijk geboden. De wereld van de informatiebeveiliging staat immers niet stil.

[2] SIEM/SOC staat voor Security Incident & Event Monitoring/Security Operations Center. Dit betreft een samenwerking tussen een applicatie en een team om continu opvallende zaken in het netwerk van de gemeente te kunnen monitoren en opvolgen.

heeft opmaak toegepast: Engels (Verenigde Staten)

3 Evaluatie

De RKE constateert aan de hand van de quick-scan dat de aanbevelingen uit het raadsbesluit niet of slechts gedeeltelijk zijn geëffectueerd. De monitoring over de voortgang/opvolging van de aanbevelingen vanuit de gemeenteraad schiet inhoudelijk te kort, al is door de raad wel conform de afspraken met het college gehandeld: de raad toetst de verantwoording via ENSIA-instrument en via jaarverslag van de accountant.

Weliswaar heeft de gemeente niet stilgestaan en de aandacht voor het op orde krijgen van de interne organisatie is een goede zaak, maar de voortgang op de diverse onderdelen van informatiebeveiliging verloopt traag. Het gevoel van urgentie is bij ambtelijk beleidsverantwoordelijken in voldoende mate aanwezig; de RKE betwijfelt of dit ook bij de raad het geval is:~~lijkt (ook bij de raad) onvoldoende aanwezig.~~ dDe raad is niet tot niet volledig geïnformeerd, maar brengt zichzelf daarbij ook onvoldoende in stelling.

heeft opmaak toegepast: Engels (Verenigde Staten)

Bijlage 1 Verklarende woordenlijst

Afkorting	Definitie
~~BIO~~	~~Basinline Informatiebeveiliging Overheid.~~
BIO	Baseline Informatiebeveiliging Overheid. Beschrijft het basisniveau van informatiebeveiliging dat gehanteerd wordt binnen de Nederlandse overheid, waaronder ook de gemeente.
BRP	Basisregistratie Personen.
CISO	Chief Information Security Officer: Kaderstelling informatieveiligheid en toetst naleving, signaleert, adviseert, maakt (beleid)instrumentarium en communiceert (voorlichting).
CMT/CMB	Concern Management Team geeft de kaders voor informatieveiligheid, privacy en informatiebeheer. CMB is opdrachtnemer vanuit CMT.
DigiD	DigiD is de veilige manier om in te kunnen loggen op websites van de gemeente Emmen. Online dienstverlening is hiermee mogelijk. Beheerder is “Logius” en de gemeente moet jaarlijks over beheersing verantwoorden.
ENSIA	Eenduidige Normatiek Single Information Audit.
FG	Functionaris voor de Gegevens bescherming. Ziet toe op en geeft advies over privacybescherming. Verplicht voor overheden vanuit de AVG.
SIEM	Security Information & Event Management dat als doel heeft informatie te “filteren” of signalen te creëren waardoor potentiële gevaren op het netwerk opgevolgd kunnen worden.
SOC	Security Operations Center is de dienst die op basis van signaleren (vanuit het SIEM) actief aan de slag gaat.
SUWI	Wet Structuur Uitvoeringsorganisatie Werk en Inkomen.

heeft opmaak toegepast: Engels (Verenigde Staten)