INFORMATIEVEILIGHEID VERDIENT MEER AANDACHT

RAPPORT
OVER INFORMATIEVEILIGHEID
IN
DONGEN, GOIRLE, HILVARENBEEK EN LOON OP ZAND

3 november 2023

rekenkamercommissie
in Midden-Brabant

Inhoud

Leeswijzer

In hoofdstuk 4 en 5 zijn enkele gekleurde tekstvlakken opgenomen. De groene vlakken hebben betrekking op gemeente Dongen. De blauwe tekstvlakken gaan in op de situatie bij de gemeenten Goirle, Hilvarenbeek en Loon op Zand. Dit onderscheid vloeit voort uit de wijze waarop de gemeenten hun IT-landschap hebben ingericht. In deze bestuurlijke nota wordt hier uitvoerig op ingegaan.

DEEL A RAPPORT RMB

1. Inleiding

1.1 Aanleiding onderzoek

Gemeenten maken bij de dienstverlening aan burgers en bedrijven steeds intensiever **gebruik** van geautomatiseerde informatiesystemen en daarin opgeslagen persoonsgegevens. De gemeenten gebruiken interne netwerken, externe IT-omgevingen en clouddiensten.

Externe onderzoeken van de Algemene Rekenkamer en de Zuidelijke Rekenkamer tonen aan dat er bij het openbaar bestuur veel te verbeteren valt. Zo stuitte het laatstgenoemde onderzoek op **kwetsbaarheden** in de uitvoering die werden veroorzaakt omdat kaders, richtlijnen, procedures en andere gemaakte afspraken niet altijd werden nageleefd en er onvoldoende werd gestuurd op de naleving daarvan.

Talloze **incidenten** van phisingaanvallen, ransomware incidenten, hacks en datalekken illustreren dit beeld over het openbaar bestuur. Dit roept vragen op, zoals: is de informatie van burgers voldoende veilig?

Verlies van gegevens(dragers), onzorgvuldigheid of oneigenlijk gebruik, het manipuleren van informatie en/of inbraak in informatiesystemen kan grote schade opleveren voor overheden, burgers en bedrijven. Dit betreft onder andere vertrouwelijke aanbestedingsinformatie of -beleidskeuzes, ICT-inrichting of privacygevoelige gegevens. Burgers, bedrijven en organisaties moeten erop kunnen vertrouwen dat hun persoonsgegevens in goede handen zijn bij de overheid.

Het is belangrijk dat de **gemeenteraad** goed bij informatieveiligheid betrokken is. Vandaar dat de RMB besloten heeft om onderzoek te doen naar de informatie-beveiliging van de gemeenten Dongen, Goirle, Hilvarenbeek en Loon op Zand.

1.2 De hoofdrolspelers in de informatiebeveiliging

Bij gemeenten ligt de verwerkingsverantwoordelijkheid bij **B&W**. In de ambtelijke organisatie is de Chief Information Security Officer (**CISO**) de centrale figuur. De CISO is interne toezichthouder op (het normenkader voor) de informatieveiligheid. Daarnaast is de Functionaris voor de Gegevensbescherming (FG) de interne toezichthouder op (het normenkader voor) de privacy.

De CISO en de FG hebben beiden een onafhankelijke rol en positie. Zij zijn verantwoordelijk voor het beleid van informatieveiligheid en privacy en voor het risico gebaseerd werken van de gemeentelijke organisatie. Zij rapporteren rechtstreeks aan de gemeentesecretaris; en vervolgens via de portefeuille-houder informatiebeveiliging aan het college van B&W.

De CISO en de FG zien toe en adviseren de organisatie bij het toepassen van alle maatregelen voor informatieveiligheid en privacy in alle processen. De ambtelijke proceseigenaren zijn verantwoordelijk voor de toepassing.

De CISO moet ervoor zorgen dat de gemeente voldoet aan **regelgeving**, te weten:

- Algemene Verordening Gegevensbescherming (AVG)
- Baseline Informatiebeveiliging Overheid (BIO)
- Eenduidige Normatiek Single Information Audit (ENSIA)

Gedetailleerde informatie over de AVG, de BIO en de ENSIA wordt gegeven in paragraaf 3.5. Hieronder wordt volstaan met korte omschrijvingen.

De **AVG** geldt vanaf 25 mei 2018 voor het beheer en gebruik van persoonsgegevens. De AVG geldt voor bedrijven en andere organisaties. Zeker na de decentralisaties in het sociaal domein (2015) is de hoeveelheid informatie die de gemeenten in beheer hebben in de vorm van (bijzondere) persoons-gegevens alleen maar toegenomen.

De **BIO** is sinds 1-1-2020 is van kracht. De BIO geeft het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen. Zo geeft de BIO aan dat een overheidsorganisatie bijvoorbeeld de toegang tot openbare netwerken zoals internet moet beveiligen, back-ups moet opslaan, een wachtwoordenbeleid moet hebben en de toegang door medewerkers tot computers en systemen moet regelen. De BIO is een gezamenlijke ontwikkeling van Rijk, provincies, gemeenten en waterschappen, die elk zijn vertegenwoordigd in de interbestuurlijke werkgroep die zorgdraagt voor het onderhoud van de BIO.

De **ENSIA** is een initiatief van gemeenten en de ministeries van BZK en SZW en 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. De ENSIA is een zelfevaluatie in de vorm van een checklist waarop de gemeente aangeeft in welke mate de organisatie aan de BIO voldoet. In de zelfevaluatie beantwoordt de gemeente zelf ‘op papier’ een aantal vragen met ‘ja’ of ‘nee’.

Dongen heeft de belangrijkste IT-diensten uitbesteed aan de gemeente Tilburg. Goirle, Hilvarenbeek en Loon op Zand hebben dat gedaan aan Equalit. Deze twee IT-leveranciers hebben op hun beurt ook hun eigen CISO.

2. Doel en aanpak van het onderzoek

2.1 Doel en afbakening

Met dit onderzoek krijgen raden antwoord op de vraag of de gemeenten kwetsbaar zijn voor cyberaanvallen gericht op persoonsgegevens en of de beschikbaarheid van de systemen gevaar loopt.

De RMB wil met dit onderzoek inzicht geven in de huidige staat van de technische beveiliging van de gegevens die de gemeente beheert. Daarbij gaat het er niet om de bedrijfsvoering in detail in de gemeenteraad te bespreken, maar wel om de gemeenteraad in positie te brengen om zijn controlerende rol ten aanzien van dit belangrijke onderwerp uit te voeren.

Informatiebeveiliging is meer dan ICT, computers en automatisering. Het gaat om alle uitingsvormen van informatie, alle mogelijke informatiedragers en alle informatie verwerkende systemen.

Dit onderzoek richt zich op de informatiebeveiliging en de organisatorische en technische maatregelen die gemeenten hebben getroffen om de gemeentelijke informatie te beschermen. Tezamen vormen deze maatregelen een Information Securitymanagement System (ISMS), waarbij de PDCA-cyclus (Plan, Do, Check, Act) wordt gevolgd.[1]

Uitgangspunten van de RMB zijn dat informatiebeveiliging de risico's van het werken met gevoelige informatie beoogt te beheersen (ondersteuning), dat de organisatie beschermd wordt tegen beveiligingsincidenten (verdediging) en dat het risicobewustzijn binnen de organisatie wordt vergroot (risicobewustzijn).

Hiertoe gelden de volgende hoofdprincipes voor informatiebeveiliging:

1. Vertrouwelijkheid: de data-eigenaar verschaft alleen geautoriseerde gebruikers toegang tot vertrouwelijke gegevens;
2. Integriteit: de dataverantwoordelijke waarborgt de integriteit (juistheid, volledigheid en tijdigheid) van gegevens;
3. Beschikbaarheid: de beschikbaarheid van informatie en IT voldoet aan de gemaakte continuïteitsafspraken.

Doel van deze hoofdprincipes is een goed gepositioneerde informatiebeveiliging binnen de gemeenten, waarbij het beleid helder is, de inrichting en techniek op orde zijn en waarbij ook sprake is van een goede control, ingebed in het primaire proces als onderdeel van het concern risicomanagement.

[1] ISMS is een managementsysteem voor informatiebeveiliging en gaat uit van de zogenaamde PDCA-cyclus (Plan, Do, Check, Act). Generieke stappen daarin zijn vast te stellen wat bedrijfskritiek is en het uitvoeren van een risicoanalyse (Plan), vaststellen wat moet je verbeteren (Do), verifiëren of er voldoende maatregelen zijn (Check) en hoe acteer je op eerdere stappen, verbeter je de organisatie, het proces, de techniek en het handelen van medewerkers (Act)? Continu anticiperen en verbeteren is het uitgangspunt om goed te kunnen acteren op steeds veranderende dreigingen.

2.2 Vraagstelling

De centrale onderzoeksvraag van de RMB is: *Kunnen de gemeenteraad en de burgers ervan op aan dat de persoonsgegevens zijn beschermd?*

De deelvragen zijn:

- Is de informatiebeveiliging in organisatorische zin zodanig dat deze op orde is en op niveau blijft?
- Is de informatiebeveiliging in technische zin zodanig dat deze op orde is en op niveau blijft?

Uit een landelijk overzicht van de Nederlandse Vereniging van Rekenkamers en Rekenkamercommissies (NVRR) van onderzoeksrapporten over informatie-veiligheid NVRR blijkt dat normen vaak betrekking hebben op het beleid ten aanzien van informatiebeveiliging en privacybescherming, en of dat *op orde* is.

2.3 Aanpak onderzoek

Organisatorisch: De RMB heeft een extern bureau gevraagd om de organisatorische beheermaatregelen van de gemeenten te onderzoeken, die de gemeente inzet om de persoonsgegevens van haar burgers te beschermen.

Technisch: De RMB heeft een ethisch hacker ingeschakeld om de IT-beveiliging van de infrastructuur (externe en interne netwerk) te onderzoeken, via het toepassen van penetratietesten. In het onderzoek is gezocht naar kwetsbaarheden bij het verkrijgen van toegang tot vertrouwelijke informatie.

2.4 Terugkoppeling door de RMB aan de CISO's

De RMB heeft in maart 2023 de bevindingen van de ingeschakelde bureaus besproken met de betrokken CISO's van 'onze' vier gemeenten (Dongen, Goirle, Hilvarenbeek en Loon op Zand) en met de CISO's van de IT-leveranciers (Tilburg en Equalit). Hierdoor heeft de RMB van dichtbij kunnen zien op welke wijze de – tijdens het onderzoek - geconstateerde kwetsbaarheden door de CISO's werden aangepakt.

2.5 Verantwoording onderzoek

De RMB is alle interne en externe partijen erkentelijk voor de bijdrage die zij – vanuit hun verschillende posities en verantwoordelijkheden – hebben geleverd aan dit onderzoek bij dit gevoelige onderwerp.

Het onderzoek is gestart in februari 2022 en afgerond in juli 2023. De doorlooptijd was 1,5 jaar, terwijl de opzet was om het onderzoek – met de inschakeling van een gerenommeerd ethisch hacker - in korte tijd uit te voeren en snel aan de gemeenteraden te rapporteren.

De RMB heeft in het onderzoek een zorgvuldig proces met de betrokken vier gemeenten en de twee externe IT-leveranciers (Equalit en Tilburg) uitgevoerd, waarbij alle betrokkenen steeds in de gelegenheid zijn gesteld om hun inbreng te leveren en steeds hun terugkoppeling te geven op verslagen van interviews en tussenrapportages.

De bevindingen van de RMB staan in hoofdstuk 4 (organisatie) en hoofdstuk 5 (techniek) van de voorliggende nota. Deze hoofstukken zijn aangepast naar aanleiding van het ambtelijk wederhoor, dat plaats vond tussen 8 mei en 1 juni 2023. De verwerkingswijze hiervan heeft de RMB gerapporteerd aan de gemeentesecretaris om volledig transparant te zijn over de wijze waarop de ambtelijke reacties zijn verwerkt in de uiteindelijke nota van bevindingen.

2.6 Rapportages

De onderliggende technische informatie staat in niet-openbare technische rapportages. Met behulp van deze (geheime) rapporten heeft de RMB tijdens het onderzoek de gemeenten op ambtelijk niveau aangegeven welke onderwerpen aandacht nodig hebben.

Openbaarmaking van deze informatie is schadelijk voor de informatieveiligheid van de gemeente(n). Om deze reden zijn deze rapporten geheim. Alle bestuurlijk relevante informatie staat in voorliggende bestuurlijke nota, die geanonimiseerd is. De bestuurlijke nota schetst de uitkomsten op hoofdlijnen en geeft hierdoor een derde geen herleidbare informatie over gevonden kwetsbaarheden. Hiermee wordt invulling gegeven aan de gemaakte afspraken met alle betrokkenen voorafgaand aan dit onderzoek.

3. Beleidskader informatieveiligheid[2]

3.1 Verantwoordelijkheid gemeenten

De verwerkingsverantwoordelijken zijn de colleges van burgemeester en wethouders. In de ambtelijke organisatie is de eerdergenoemde Chief Information Security Officer (CISO) de centrale functionaris, die zorgt voor de uitvoering en het interne toezicht.

3.2 Extern toezicht

De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de AVG en daarmee verbonden regelgeving. De AP kan sancties opleggen.

3.3 Landelijke ondersteuning door VNG

Binnen het verband van de Vereniging Nederlandse Gemeenten VNG zijn bestuurlijke principes vastgelegd voor informatieveiligheid. De VNG heeft in 2019 tien bestuurlijke principes voor informatieveiligheid opgesteld:

1. *Bestuurders bevorderen een veilige cultuur*
2. *Informatiebeveiliging is van iedereen*
3. *Informatiebeveiliging is risicomanagement*
4. *Risicomanagement is onderdeel van de besluitvorming*
5. *Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking*
6. *Informatiebeveiliging is een proces*
7. *Informatiebeveiliging kost geld*
8. *Onzekerheid dient te worden ingecalculeerd*
9. *Verbetering komt voort uit leren en ervaring*
10. *Het bestuur controleert en evalueert*

De RMB onderkent het belang van ieder van deze bestuurlijke principes en geeft in het onderzoek dan ook aandacht aan ambities, risicomanagement, beschikbare middelen, onzekerheid, leerprocessen en verantwoording.

3.4 Informatiebeveiligingsdienst (IBD)

Als onderdeel van de VNG draagt de IBD (informatiebeveiligingsdienst) namens gemeenten bij aan de deskundigheid over informatiebeveiliging en brengt het kennisproducten hierover uit.

---

[2] Bronnen:

- Vng_agenda_digitale_veiligheid_2020-2024_def.pdf;
- Rekenkamerrapport: Weten wat je moet weten Regionaal rekenkameronderzoek naar informatiebeveiliging en privacybescherming — NVRR;
- https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/01/De-10-bestuurlijke-principes-voor Informatiebeveiliging_20190109.pdf
- Update: CISO, Privacy Officer en FG; wie doet en mag wat? - Informatiebeveiliging & Privacy (ib-p.nl)

De IBD van de VNG is een landelijk opererend team dat in actie komt bij beveiligingsincidenten voor alle Nederlandse gemeenten en is onderdeel van de Vereniging Nederlandse Gemeenten (VNG). De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC).

Alle Nederlandse gemeenten kunnen hiervan gebruik maken. Bovendien vervult de IBD de functie van CERT/CSIRT. (Computer Emergency Response Team/Computer Security Incident Response Team), die wordt ingeschakeld bij incidenten.

De IBD stelt iedere twee jaar een dreigingsbeeld op voor gemeenten. In het rapport Dreigingsbeeld Informatiebeveiliging 2023-2024 constateert de IBD dat de risico's voor gemeenten groeien. Gemeenten doen – volgens de IBD - al veel om hun informatie goed te beveiligen, maar er is meer nodig om gelijke tred te houden met de dreiging. De IBD constateert dat het aantal ransomware-aanvallen groeit en dat deze ook steeds professioneler worden uitgevoerd. Bij zo'n aanval versleutelen criminelen bestanden om vervolgens losgeld te eisen om ze weer beschikbaar te stellen. Ook ziet de IBD steeds meer en ernstigere fouten in software. Het lukt criminelen zo om toegang te krijgen tot gemeentelijke systemen. Het rapport van de IBD benadrukt het belang van investeringen in informatieveiligheid.

De IBD zegt over de positionering van de CISO in het Dreigingsbeeld 2023-2024 (blz. 14): *"De Chief Information Security Officer (CISO) en Privacy Officer (PO)[3] kunnen de gemeentesecretaris binnen een structurele en cyclische aanpak adviseren over de verdeling van budget, vanuit inzicht in de risico's en oplossingsrichtingen. En daarmee een belangrijke rol spelen bij het plannen, uitvoeren, controleren en bijstellen van activiteiten gericht op informatiebeveiliging en privacy. Het is nuttig om informatiebeveiliging te integreren in reguliere gemeentelijke plannen. Denk hierbij aan afdelingsplannen, het Integraal Veiligheidsplan (IVP), en de risicoparagraaf in de gemeentelijke begroting."*

En in het Dreigingsbeeld 2023-2024 (blz. 19): *"De CISO en de FG[4] zijn strategisch adviseurs voor de gemeentesecretaris, directie en bestuur. Dit komt tot uitdrukking in hun plek binnen de organisatie en in hun functiewaardering. Gelet op het concernbrede werkgebied is een plek binnen een concernstaf (of soortgelijke omgeving) de meest logische."*

[3] CISO en FG zijn beide toezichthouder en elkaar equivalent voor informatieveiligheid en privacy. Onder de FG kan een PO worden aangesteld, die de business ondersteunt met praktische hulp en advies. Privacy Officer (PO): Waar de CISO verantwoordelijk is voor het informatiebeveiligingsbeleid is de PO verantwoordelijk voor het actualiseren en bewaken van het privacy beleid binnen de gemeente.

[4] Functionaris Gegevensbescherming (FG): De FG is een door de AVG verplicht gestelde functie die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG. De positie, taken en verantwoordelijkheden van de FG zijn vastgelegd in de AVG. De adviezen en aanwijzingen die de FG geeft zijn niet geheel vrijblijvend. Daarom geniet deze functionaris een bepaalde mate van bescherming. Dit betekent dat de dienstverleningsovereenkomst niet op oneigenlijke gronden mag worden beëindigd (externe FG), of dat de FG-ontslagbescherming heeft (interne FG). De FG adviseert en rapporteert aan het hoogste niveau van de organisatie.

En in het Dreigingsbeeld 2023-2024 (blz. 20): *"Mede als gevolg van een gebrek aan aandacht en eigenaarschap bij de ambtelijke top zijn veel CISO's, PO's en FG's onvoldoende 'in positie'. De afstand tot het management is te groot en belangrijke informatie, bijvoorbeeld over risico's, bereikt het management niet. Ook spreken deze functionarissen en het management vaak niet 'dezelfde taal'. Omdat informatiebeveiliging ten onrechte wordt gezien als een ICT-kwestie, zitten deze belangrijke functionarissen 'verstopt' binnen ICT/I&A afdelingen."*

3.5 Regelgeving

Landelijke norm 1: privacywetgeving

De Algemene Verordening Gegevensbescherming (AVG) geldt voor bedrijven en andere organisaties. De AVG geldt vanaf 25 mei 2018 voor het beheer en gebruik van persoonsgegevens (er ging een transitieperiode van twee jaar aan vooraf). Het is een Europese verordening die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert. De AVG is ook bekend onder de Engelse naam General Data Protection Regulation (GDRP).

In Nederland vervangt de AVG de Wet bescherming persoonsgegevens (Wbp). Ten opzichte van die Wbp zijn de privacyrechten van mensen versterkt en uitgebreid. Voor organisaties gelden er meer verplichtingen bij het verwerken van persoonsgegevens. En er is een verantwoordingsplicht, die inhoudt dat met documenten moet kunnen worden aangetoond dat de juiste organisatorische en technische maatregelen zijn genomen om aan de AVG te voldoen.

Zo moeten overheden zo min mogelijk gegevens verwerken en dat binnen een passend beveiligingsregime doen. De AVG is de belangrijkste basiswet voor de bescherming van persoonsgegevens. Daarnaast gelden er in het sociaal domein specifieke wetten zoals de Jeugdwet, de Wet maatschappelijke ondersteuning (Wmo), de Participatiewet, de Wet gemeentelijke schuldhulpverlening, etc. Deze wetten bevatten op sommige onderdelen specifieke regels die voorgaan op de AVG.

Persoonsgegevens mogen alleen worden verwerkt in overeenstemming met de wet en met een gerechtvaardigd doel. Bij het verwerken van persoonsgegevens moet een aantal uitgangspunten in acht genomen worden.

Landelijke norm 2: Interbestuurlijke afspraak met Baseline Informatiebeveiliging Overheid (BIO)

De BIO geeft het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen. Het is dan ook een gezamenlijke ontwikkeling van Rijk, provincies, gemeenten en waterschappen, die elk zijn vertegenwoordigd in de interbestuurlijke werkgroep die zorgdraagt voor het onderhoud van de BIO.

Eerder hadden de overheidslagen ieder hun eigen baseline. Bij gemeenten was dit de BIG, waarbij de G staat voor gemeenten. Na een voorbereidingstraject zijn deze baselines per 1-1-2019 vervangen door de gezamenlijke BIO. De BIO ondersteunt overheidsorganisaties in de wijze waarop zij hun informatie-beveiliging organiseren en uitvoeren.

Zo worden de aandachtsgebieden voor de beveiliging benoemd en de rollen en verantwoordelijkheden van degenen die hierbij betrokken zijn.

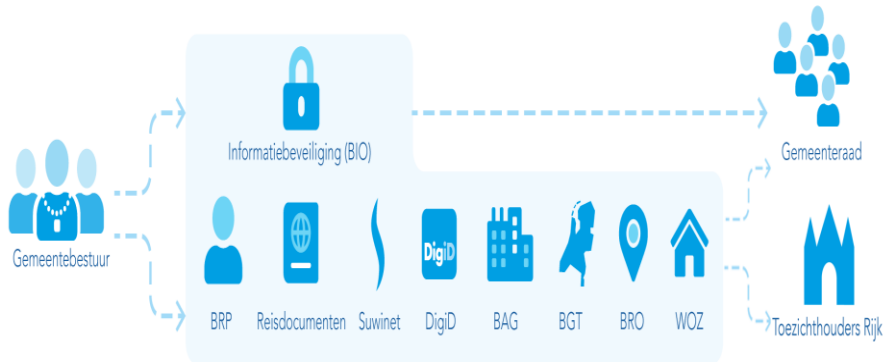
Heel in het kort ziet de toepassing van de BIO er als volgt uit. Aan de basis staat de baseline-toets met een 'GAP'-analyse (de Engelse term 'gap' staat voor afwijkingen) bij alle organisatorische beheermaatregelen.: Hierbij wordt getoetst in hoeverre voldaan wordt aan een bepaalde set van eisen, zoals de aanwezigheid van een wachtwoordenbeleid. Het verschil tussen de huidige en gewenste situatie is de 'gap'. Bedrijfsprocessen en verantwoordelijken hiervoor worden geïnventariseerd. De BIO gaat uit van risico gestuurd werken. Waar nodig kunnen diepgaande risicoanalyses worden gemaakt. Benodigde beheermaatregelen ('controls' worden organisatorisch goed belegd en vastgelegd in het ISMS (Information securitymanagement system).

Met periodieke monitoring tenslotte wordt bewaakt dat de beveiliging op niveau blijft. Hierbij duikt de term PDCA-cyclus op, dat staat voor Plan-Do-Check-Act, waarmee de lerende organisatie monitort of de controls effectief zijn in het beheersen van - ook nieuwe - risico's.

Landelijke norm 3: Zelfevaluatie met Eenduidige Normatiek Single Information Audit (ENSIA)

In relatie tot de BIO moet ook de nieuwe verantwoordingssystematiek ENSIA (Eenduidige Normatiek Single Information Audit) worden genoemd. Het gaat om een zelfevaluatie om te checken in hoeverre aan de BIO is voldaan. Dit is een initiatief van gemeenten en de ministeries van BZK en SZW en 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. De focus van ENSIA ligt op verantwoording richting de gemeenteraad, het hoogste politieke orgaan van de gemeente. Parallel hieraan leggen gemeenten verantwoording af aan de rijksoverheid waar het gaat om het gebruik van landelijke voorzieningen. ENSIA streeft naar een zo effectief en efficiënt mogelijk ingericht verantwoordings-stelsel voor informatieveiligheid.

Onderstaande afbeelding geeft aan op welke wijze B&W zorgt voor de inrichting en uitvoering van de BIO. Ook wordt visueel duidelijk aangegeven dat verantwoording wordt afgelegd aan de gemeenteraad en het Rijk.



4. Organisatie

4.1 Inleiding

In dit hoofdstuk beschrijft de RMB de organisatorische inrichting van de informatiebeveiliging, waarmee we eigenlijk de 'bouwstenen' van informatieveiligheid benoemen. De CISO maakt hiervan expliciet onderdeel uit. De bevindingen dienen om in hoofdstuk 6 van deze bestuurlijke nota antwoord te geven op de onderzoekvraag: Is de informatiebeveiliging in organisatorische zin zodanig dat deze op orde is en op niveau blijft?

4.2 Aanpak onderzoek naar organisatorische beheermaatregelen

De RMB heeft een extern bureau gevraagd om de organisatorische beheermaatregelen te onderzoeken, die de gemeenten inzetten om de persoonsgegevens van haar burgers te beschermen. Wij hebben bij het onderzoek primair gekeken naar het proces rondom de implementatie van de Baseline Informatiebeveiliging Overheid (BIO). Hierbij wordt de focus gelegd op hoe de gemeente omgaat met de BIO, vanuit de Plan-Do-Act-Check (PDCA) cyclus.

4.3 Positie CISO

Bij Dongen is de CISO in dienst van de gemeente. In Dongen valt de CISO rechtstreeks onder de directie.

Bij Goirle en Hilvarenbeek is de CISO in dienst van de gemeente. Bij Loon op Zand is de CISO ingehuurd bij de IT-leverancier Equalit.

Bij Goirle, Hilvarenbeek en Loon op Zand is de CISO dieper in de lijnorganisatie gepositioneerd.

Het streven van de IT-leverancier Equalit was het om bij iedere gemeente, die IT-diensten afneemt, ook de onafhankelijke functie van CISO te vervullen. Goirle en Hilvarenbeek hebben hier geen gebruik van gemaakt en hebben bewust besloten tot het aanstellen van een eigen CISO.

De CISO van de gemeente Goirle is ook CISO van Hilvarenbeek en Oisterwijk vanwege de GHO-samenwerking. Deze CISO is full time in dienst.

Loon op Zand heeft wel gebruik gemaakt van de optie om de CISO bij Equalit in te huren. De CISO van Loon op Zand vervult deze functie parttime (3 dagen per week).

Het is volgens de RMB de vraag of de plaatsing van de CISO in de lijnorganisatie een onafhankelijke functie kan vervullen. Ook de landelijke IBD heeft aandacht

gevraagd voor de onafhankelijke positionering van de CISO en FG. Dit is qua rolzuiverheid belangrijk.

De CISO's benadrukken dat informatieveiligheid geen specifiek 'feestje' is van de CISO over informatieveiligheid, maar betrekking heeft op ieder onderdeel van de organisatie. Het doel is om de informatie zo goed mogelijk te beschermen. Een middel hierbij een is een integraal risico-management voor alle onderdelen van de organisatie, waarop de CISO dan toezicht kan uitoefenen op informatieveiligheid vanuit zijn (onafhankelijke) positie. De CISO's willen nu de vervolgstap maken naar een goede werking in de praktijk. Zij werken hierbij continu op alle niveaus.

Bij alle onderzochte gemeenten legt de CISO daadwerkelijk verantwoording af aan B&W.

4.4 Uitbesteding aan IT-leveranciers

Gemeenten Dongen, Goirle, Hilvarenbeek en Loon op Zand hebben de IT-diensten uitbesteed.

De samenwerking met de IT-leveranciers (opdrachtnemers) wordt door de vier gemeenten gekenschetst als 'pragmatisch' en daarmee – volgens de gemeenten - passend binnen de mogelijkheden van het beschikbare budget en de aanwezige capaciteit. Het blijkt in de praktijk een uitdaging voor iedere gemeente om binnen de beschikbaar gestelde middelen en vervolgens ook in overleg met de IT-leveranciers een zo hoog mogelijk niveau van gegevens-bescherming te bereiken. Ze zoeken steeds naar een balans tussen kosten en baten.

Dongen heeft de IT-diensten uitbesteed aan de gemeente Tilburg, waarbij de gemeente Dongen gebruik maakt van de IT-systemen van de gemeente Tilburg.

Goirle, Hilvarenbeek en Loon op Zand hebben uitbesteed aan Equalit[1], waarmee iedere gemeente een bilaterale, lichte gemeenschappelijke regeling heeft gesloten. De gemeenten hebben dus de formele rol van opdrachtgever.

De gemeenten Dongen, Goirle, Hilvarenbeek en Loon op Zand leggen de eigen beleidsdocumenten in concept voor aan de IT-leverancier, ter toetsing op consistentie. Gemeenten stellen in de praktijk doorgaans om de 3 jaar het (geactualiseerde) beleid over informatieveiligheid vast, waaronder de implementatie van de BIO. Dit is een verantwoordelijkheid van de colleges van B&W. Gemeenten beschikken daarmee over eigen beleidsmatige uitgangspunten.

4.5 Pragmatisch leveranciersmanagement

Dongen is de opdrachtgever van Tilburg, die IT-diensten aan Dongen levert. Dit is een pragmatische samenwerking. Dongen maakt gebruik van de systemen van de gemeente Tilburg. Het is niet zo dat Tilburg een separaat IT-systeem voor Dongen heeft opgezet en deze afzonderlijk beheert. In de uitvoeringsovereenkomst met Tilburg zijn summiere afspraken gemaakt over serviceniveaus en rapportages. Er is regelmatig overleg met Tilburg, dat volgens ENSIA verantwoording aflegt aan Dongen.

Goirle, Hilvarenbeek en Loon op Zand zijn de opdrachtgevers van Equalit. Iedere gemeente heeft een lichte gemeenschappelijke regeling afgesloten met Equalit. Dus steeds bilateraal. Onder de gemeenschappelijke regeling ligt een dienst-verleningsovereenkomst. De CISO's van alle (11) gemeenten die de IT-diensten van Equalit afnemen overleggen periodiek gezamenlijk, als een opdrachtgevers-overleg (partneroverleg).

Andere diensten die de gemeente afneemt zijn bijvoorbeeld DIGID en SUWINET en vele andere applicaties van grote (Microsoft, Google) en kleinere leveranciers.

Het handelingsperspectief van 'onze' gemeenten is in de huidige markt van IT-aanbieders klein. Sommige leveranciers zijn te groot om vanuit de individuele gemeente aan te spreken (Microsoft, Google), op gebruikersvoorwaarden, bijhouden van back-ups of betrouwbaarheid van gegevensopslag in de Cloud.

Als dit aan de orde zou zijn, nemen de CISO's contact op met VNG/IBD om gezamenlijk een groter gewicht in de schaal te leggen.

Bij alle gemeenten ontbreekt een integraal beleid over leveranciersmanagement. De gemeenten hebben overigens niet de indruk dat zij te afhankelijk zijn van de IT-leveranciers.

4.6 Gelaagde risicoanalyse

De BIO is voor alle overheden de norm. Het management van de gemeenten de IT-leveranciers hebben gekozen voor een focus op BIO en BIO, de 'state of the art' in Nederland voor de gemeenten. Dit is dus voor alle CISO's een hard uitgangspunt. De CISO's voeren risicomanagement uit volgens de BIO; op de risicovolle processen en applicaties in de organisatie. Dit is dus voor alle CISO's een hard uitgangspunt. De CISO's voeren vervolgens hierop het risicomanagement uit.

De risico's bij informatieveiligheid worden in de praktijk op twee niveaus geanalyseerd:

1. Samen met de IT-leveranciers

De CISO's van de gemeenten en de IT-leveranciers stellen voor de IT-systemen (van respectievelijk Tilburg en Equalit) gezamenlijk een risicoanalyse op, met prioriteiten vanuit de deelnemende gemeenten.

De CISO's van de IT-leveranciers bekijken dus gezamenlijk met de CISO's van de gemeenten welke risico's zij lopen bij de IT-dienstverlening. Hierbij is het steeds een zoekproces voor zowel gemeenten als de IT-leveranciers naar een haalbaar evenwicht tussen enerzijds prioriteiten met betrekking tot de informatieveiligheid en anderzijds beschikbare financiële en technische middelen van zowel gemeenten als de IT-leveranciers.

2. Binnen iedere gemeente

De CISO's voeren vervolgens hierop binnen de eigen gemeente het risicomanagement uit (zie 4.7 en 4.8).

4.7 Focus van risicoanalyse binnen de gemeente op 'PIOFACH'

De CISO's werken pragmatisch binnen het beschikbare budget en de beschikbare capaciteit. Eerst richten zij zich op de algemene, organisatorische functies van de gemeente zoals samengenomen in het acroniem PIOFACH[5] om de basis op orde te hebben. Daarna proberen zij zoveel mogelijk te specificeren richting de beleidsinhoudelijke afdelingen (zoals sociaal domein, burgerzaken, belastingen, vergunningen).

De meest recente risicoanalyses, gericht op de organisatiebrede (PIOFACH) processen en de verplichte (repeterende) onderdelen uit de ENSIA, dateren in Dongen van 2021

De meest recente risicoanalyses, gericht op de organisatiebrede (PIOFACH) processen en de verplichte (repeterende) onderdelen uit de ENSIA, dateren in Goirle, Hilvarenbeek en Loon op Zand van 2019.

Deze risicoanalyses zijn dus al enkele jaren oud. Er wordt niet getoetst of deze nog naar behoren functioneren.

4.8 Niet alle processen in beeld bij de risicoanalyse

In de praktijk heeft een gemeente intern tussen de 500 en 800 processen, die gebruik maken van hardware, software en applicaties. Het is voor de gemeenten niet haalbaar om jaarlijks ieder proces te analyseren op eventuele risico's.

[5] PIOFACH staat voor: Personeel, Informatievoorziening, Organisatie, Financiën, Automatisering, Communicatie en Huisvesting

Voor de CISO's is de kern: risico gestuurd werken. Dus kijken waar je 'kroon-juwelen' zitten en focus op die processen. Dus waar de grootste impact zit.

4.9 ENSIA-zelfevaluatie

De gemeenten en de IT-partners gaan ieder uit van ENSIA, dat een zelfevaluatie voorschrijft. Deze is vrijwillig en wordt door de betrokkenen zelf uitgevoerd. Er is in het onderzoek van de RMB vastgesteld dat naast de brede zelfevaluatie op de verplichte onderdelen, ook door een externe auditor onafhankelijk en specifiek wordt getoetst op DigiD en Suwinet. Dit levert op deze onderdelen een verdere ondersteuning van de zelfevaluatie op.

Jaarlijks stellen de CISO's - in de vorm van een IBP - een verbeterplan op. Deze wordt gedeeld met directie en portefeuillehouder. Zij worden periodiek op de hoogte gehouden van de voortgang. Punten die niet worden opgelost komen terug in volgende IBP. Strikt genomen wordt hierbij de PDCA-cyclus niet volledig doorlopen, want men gaat niet meteen tot 'Act' over ofwel men neemt geen actieve maatregelen om geconstateerde tekortkomingen aan te pakken.

4.10 Verantwoording aan B&W

De jaarverslagen van de FG en de CISO worden voorgelegd aan B&W. De risicoanalyse komt bij de portefeuillehouder ter sprake, en zo nodig bij B&W als de portefeuillehouder (burgemeester) het raadzaam acht om deze te delen met de wethouders.

Verantwoording vindt plaats via de ENSIA-systematiek, volgens een gestandaar-diseerde collegeverklaring. Daarin zijn onder meer verwerkt de resultaten van de interne BIO zelfevaluatie en de externe DIGID en SUWINET accountants-verklaringen.

De jaarverslagen en risicoanalyse worden niet gedeeld met de gemeenteraad.

4.11 Verantwoording aan gemeenteraad en toezichthouders Rijk

De programmabegroting en jaarstukken van iedere gemeente bevat een paragraaf Bedrijfsvoering waarin wordt gerapporteerd over informatieveiligheid en privacy. Aan de hand van de ENSIA-zelfevaluatie wordt op hoofdlijnen ingegaan op informatie-beveiliging en privacy. Daarnaast ontvangt de gemeenteraad ieder jaar een uitgebreidere rapportage via een raadsinformatiebrief (RIB).

In onderstaande afbeelding wordt aangegeven op welke wijze B&W verantwoording aflegt aan de gemeenteraad en aan de toezichthouders van het Rijk.

4.12 Dilemma door publieksvriendelijkheid

De CISO's wijzen op het dilemma, dat de gemeenten enerzijds publieks-vriendelijk willen zijn - waarbij zowel fysiek als digitaal de 'deur van het gemeentehuis' openstaat - en anderzijds persoonsgegevens moeten beschermen.

De interne communicatie over informatieveiligheid doet de CISO zelf omdat de CISO binnen de organisatie de centrale functionaris is. De CISO heeft ook nauw contact met de IBD. Van de IBD ontvangt de CISO landelijke dreigingsbeelden met kwetsbaarheidsmeldingen.

In Dongen is de CISO verantwoordelijk voor de communicatie over 'awareness'.

Voor de GHO-gemeenten (Goirle, Hilvarenbeek en Oisterwijk) wordt de communicatie over 'awareness' uitgevoerd door het team informatieveiligheid en privacy, waarvan de CISO voor deze gemeenten deel uitmaakt. Ook bij Loon op Zand is de CISO verantwoordelijk voor de communicatie over 'awareness'.

Communicatie over kwetsbaarheden is behulpzaam om het bewustzijn onder medewerkers, bestuurders en bezoekers te vergroten, maar niet altijd toereikend. Door middel van communicatie en interne 'awareness' trainingen wordt steeds getracht om de 'menselijke factor' te verbeteren.

De gemeenten overwegen om MFA (multi-factor authenticatie) bij steeds meer handelingen in te zetten, zoals de toegang tot bepaalde ruimten (bv. de ruimte waar servers en andere apparaten staan). Hiermee kan de identiteit van de gebruiker op een eenvoudige en niet-ingrijpende wijze gecontroleerd worden.

5. TECHNIEK

5.1 Inleiding

In dit hoofdstuk beschrijft de RMB de aanpak en de uitkomsten van het onderzoek naar de techniek door middel van penetratietesten. De bevindingen dienen om in hoofdstuk 6 van deze bestuurlijke nota antwoord te geven op de onderzoeksvraag: Is de informatiebeveiliging in technische zin zodanig dat deze op orde is en op niveau blijft?

5.2 Aanpak technisch onderzoek met penetratietesten

Om dit onderzoek te kunnen doen heeft de RMB een ethisch hacker ingeschakeld om de IT-beveiliging van de infrastructuur (externe en interne netwerk) te onderzoeken. In het onderzoek is gezocht naar toegang tot vertrouwelijke informatie. Hiervoor is onder strikte voorwaarden bij iedere gemeente een korte 'best-effort' pentest[6] uitgevoerd, waarbij geen technische informatie met de onderzoekers voorafgaand aan het onderzoek werd gedeeld (in vaktermen heet dit een 'blackbox onderzoek'[7]).

De RMB heeft vooraf met Tilburg en Equalit juridische afspraken gemaakt over werkwijze, risico's en uitwisseling van uitkomsten, zodat er geen schade aan techniek en imago uit het onderzoek voortvloeien.

Het onderzoek is een *praktijkoefening* waarvan gemeenten vooral kunnen leren, zonder schadelijke gevolgen. De gemeenten benadrukten dat ze – in samenwerking met de IT-leveranciers - werken in een proces van voortdurende verbetering en dat er altijd iets gevonden zal worden door een hacker. Dit is eigen aan dit beleidsveld. Vanuit dit vertrekpunt hebben de CISO's van de gemeenten en die de IT-leveranciers van begin tot eind positief en constructief meegewerkt aan het onderzoek van de RMB.

Nadat de gemeenten en IT-leveranciers in maart 2023 geïnformeerd zijn over de bevindingen van de RMB (aangetoonde kwetsbaarheden), hebben zij direct maatregelen getroffen.

[6] Met 'best-effort' wordt bedoeld dat de RMB onderzoek heeft laten doen bij onze vier gemeenten (Dongen, Goirle, Hilvarenbeek en Loon op Zand) waarbij de hacker binnen een korte termijn de gelegenheid is gegeven om met een brede aanpak zo veel mogelijk kwetsbaarheden te vinden bij de toegang tot persoonsgegevens, zonder deze vervolgens gericht en diepgaand te benutten.
[7] Black box test: Bij deze test wordt de ethische hacker niet voorzien van informatie. De opdrachtgever verstrekt geen enkele bron van informatie. Op deze manier wordt een cyberaanval van buitenaf zo goed mogelijk nagebootst. De pentester zal de omgeving en kwetsbaarheden in kaart brengen op basis van openbare bronnen.

5.3 Aantallen vastgestelde kwetsbaarheden

	Dongen	Goirle	Hilvarenbeek	Loon op Zand
Kritisch	0	2	1	1
Hoog	5	10	8	8
Medium	10	15	9	6
Laag	13	12	9	12
Info	2	0	0	0

5.4 Regelmatige pentesten door IT-leveranciers

De IT-leveranciers voeren elk ieder jaar een pentest uit op het eigen netwerk. Het onderliggende technische rapport kan door de IT-leveranciers met de gemeenten worden gedeeld met de CISO's van de gemeenten, als zij dit wensen.

5.5 Toegang verkregen tot persoonsgegevens

Uit het onderzoek van de RMB bleek dat bij iedere gemeente het mogelijk was om zowel van buitenaf als van binnenuit toegang te verkrijgen tot persoonsgegevens.

De CISO's van de IT-leveranciers hebben vervolgens meteen maatregelen getroffen om bij de bevindingen met het hoogst geprioriteerde risico openstaande toegangen tot het netwerk te dichten.

Zoals hierboven in de tabel getoond zijn er bij drie gemeenten 'kritische' punten geconstateerd. Pas als er 'kritische bevindingen' zijn, beschouwen sommige CISO's de situatie als onveilig. De RMB meent dat ook de bevindingen van 'hoog' tot 'laag' de gemeenten en de IT-leveranciers aanleiding moeten geven om ook deze 'gaten' te dichten. De RMB onderkent dat veiligheid niet 'zwart/wit' is. Alle issues geven een mate van onveiligheid aan.

5.6 Toegang verkregen tot gebruikersinformatie

De onderzoekers hebben op afstand (van buitenaf) bij iedere gemeente toegang weten te krijgen tot gebruikersinformatie.

De onderzoekers hebben in Dongen op afstand onder andere toegang gekregen tot (privacy)gevoelige informatie, e-mail, wachtwoorden, gedeelde bestanden, en chatberichten. De onderzoekers hebben onder andere toegang verkregen tot gegevens over medische keuringen in het kader van de Wet maatschappelijke ondersteuning (Wmo). Via het dashboard zijn gedetailleerde medische gegevens beschikbaar van burgers.

De onderzoekers wisten bij de gemeenten Goirle, Hilvarenbeek en Loon op Zand toegang tot persoonsgegevens te verkrijgen. Deze gegevens hebben betrekking op het sociaal domein, belastingen, burgerzaken en vergunningen.

Daarbij hebben zij onder andere toegang gekregen tot desktops, vertrouwelijke en privacygevoelige informatie, e-mail, (beheer) wachtwoorden van services en fileshares.

Ook is toegang (het kunnen raadplegen van gegevens) verkregen tot persoons- en belastinggegevens van burgers en juridische procedures van de gemeenten.

5.7 Geen toegang verkregen tot beheerrechten

De onderzoekers hebben tijdens het onderzoek geen toegang gekregen tot beheerrechten (de zogenoemde Admin-functie). Zie ook 5.12.

5.8 Onvoldoende segmentatie in systemen van de IT-leveranciers

Onderzoekers hebben laten zien dat de scheiding van de verschillende gemeentelijke IT-omgevingen onvoldoende is.

Vanuit de IT-omgeving van gemeente Dongen was toegang mogelijk tot gegevens van de gemeente Tilburg, omdat beide gemeenten samen 1 systeem vormen. Hieronder kunnen kwetsbaarheden impact hebben op de gehele infrastructuur. Er is wel netwerk-segmentering, maar geen firewall tussen beide gemeenten. Tilburg verleent diensten aan Dongen en behandelt Dongen als een 'afdeling' van Tilburg. Vanaf het begin van de samenwerking is het ook nooit het doel geweest om een firewall tussen Tilburg en Dongen in te richten.

Vanuit de IT-omgevingen van Goirle, Hilvarenbeek en Loon op Zand was toegang mogelijk tot gegevens van de andere samenwerkingspartners van Equalit. De oorzaak van het verkrijgen van toegang was: de "gehackte" medewerker had rechten tot deze applicatie, zodoende heeft men toegang.

De scheiding van de IT-omgevingen van Equalit-partners bleek onvoldoende. Deze kwetsbaarheden hebben impact op de gehele infrastructuur.

De onderzoekers hebben zich, volgens de gemaakte afspraken met de RMB, beperkt tot de IT-omgevingen van Dongen, Goirle, Hilvarenbeek en Loon op Zand. Vooraf was aan de onderzoekers meegegeven dat zij zich geen toegang mochten verschaffen tot de andere IT-omgevingen en daar aanwezige gegevens van de overige Equalit-partners.

5.9 Meer aandacht voor segmentering

De netwerkzonering is bij Tilburg een permanent aandachtspunt. Hier wordt op projectbasis aan gewerkt. Het is een meerjarenproject. Het is een continu traject.

De deelnemersraad van bij Equalit aangesloten gemeenten neemt in gezamenlijkheid besluiten over het plaatsen van 'digitale schotten'. Uiteindelijk is het Equalit die deze besluiten uitvoert en risicodrager is.

De conclusie van de pentester was: er is niet voldoende segmentatie aanwezig. Dit wordt ook door Equalit onderkend, en wordt later opgepakt door middel van microsegmentatie. Deze microsegmentatie is afhankelijk van de voorgenomen cloudgang.

De gemeenten en Equalit streven naar een evenwicht tussen veiligheid en laagdrempelige samenwerking, soepele bedrijfsvoering en gebruikersgemak. Het is een thema in het partneroverleg van de CISO's binnen het verband van Equalit. Samenwerken is goed en het delen van informatie is ook goed, maar een kwaadwillende hacker moet binnen het netwerk niet te makkelijk kunnen bewegen.

Prioriteit gaat op dit moment vooral uit naar het isoleren van de kritische processen binnen het netwerk. Dit stond al op de risicolijst van het partneroverleg van de CISO's, met een lage prioriteit vanwege een kostenafweging. Door toedoen van het RMB-onderzoek komt het nu hoger te staan op de prioriteitenlijst van het partneroverleg.

Equalit heeft netwerksegmentatie uitgevoerd conform de BIO eisen. Microsegmentatie staat dit jaar (2023) nog niet op de roadmap, maar dat volgt later.

Het door de RMB uitgevoerde onderzoek heeft de CISO's geleerd dat de segmentering binnen het netwerk verbeterd moet worden. Dit had al de aandacht, maar dit onderzoek benadrukte het belang.

5.10 Vergrendeling van persoonlijke apparaten veelal in orde

Persoonlijke apparaten zoals laptops waren correct vergrendeld bij afwezigheid van de werknemer. Toch waren gedeelde apparaten soms niet vergrendeld en

waren gebruikers nog ingelogd waardoor de onderzoeker de sessie kon voortzetten en bij data kon.

5.11 Gebrekkige alertheid van de gebruikers

De ICT-medewerkers van Tilburg en Equalit zijn afhankelijk van de alertheid van de gebruikers van de gemeenten. Tijdens het onderzoek zijn enkele voorbeelden aangetroffen van onzorgvuldig handelen door gebruikers.

ICT-medewerkers kunnen in zulke gevallen de mogelijke schade van een eventuele aanvaller niet meer voorkomen of beperken.

De faciliterende organisaties (gemeente Tilburg en Equalit) hebben de hacker, die namens de RMB-onderzoek deed, niet kunnen opmerken, omdat hij zich voordeed als een reguliere gebruiker. De onderzoeker kon zich toegang verschaffen tot de autorisaties die aan de betreffende gebruiker zijn toegewezen.

Daarbij zijn geen beheertaken of 'Adminrechten' (zie ook 5.7) overgenomen of zijn rechten van de gehackte gebruiker aangepast. Vandaar dat er ook geen alarm is geslagen. De IT-leveranciers Tilburg en Equalit stellen dat dit wel zou zijn gebeurd als de rechten waren gemuteerd.

5.12 Fysieke beveiliging, 'Clean desk' en 'clean screen

De fysieke beveiligingsmaatregelingen bij een van de gemeentehuizen waren ontoereikend. Volgens de gemeenten is de fysieke beveiliging een lastige opgave bij publieke organisaties, zoals gemeenten. De gemeenten zetten technische hulpmiddelen in, zoals druppelsysteem met zonering. Zij zoeken naar een praktisch en effectieve middenweg tussen beveiliging en publieksvriendelijkheid. Immers, de toegang tot de gemeentehuizen moet voldoen aan de eisen vanuit de BIO. Dat maakt dat er zonering nodig is – en dat met name de gevoelige apparatuur van bv. burgerzaken in een goed beveiligde zone moet staan waar onbevoegden geen toegang hebben.

In Dongen was de patchruimte weliswaar op slot, maar de sleutel hing onbeveiligd buiten de daartoe bestemde kast. Bovendien was het patch paneel toegankelijk.

Daarnaast kon de onderzoeker in Dongen op de kamer van burgemeester in een geopende kast komen bij een bakje gelabeld 'privé'. De hacker heeft de documenten van de burgemeester vanzelfsprekend niet ingezien (een ander had dit wel kunnen doen).

Bovendien had de onderzoeker met opzet de bezoekerspas niet zichtbaar gedragen en is vervolgens hierop door geen enkele medewerker aangesproken.

Bij Goirle, Hilvarenbeek en Loon op Zand bleek tijdens het onderzoek dat op de interne netwerken testomgevingen toegankelijk waren. Als voorbeeld: er slingerde een papiertje met inloggegevens van 1 test/training omgeving waardoor de hacker zich toegang kon verschaffen tot die omgeving.

De gemeenten zien hierin aanleiding om de gedragsregels wederom onder de aandacht van de medewerkers te brengen. Dit in een poging om de 'menselijke factor' tot een hoger bewustzijn te brengen. Volgens de gemeenten wordt de factor 'menselijk gedrag' steeds onderschat.

De praktijk is nu dat een incident pas helpt om bij de leiding van de organisatie, de medewerkers en de gemeentebesturen aandacht te vragen voor goed gedrag bij informatieveiligheid.

6. Conclusies en aanbevelingen

6.1 Inleiding

De RMB constateert dat de vier gemeenten en de IT-leveranciers (Equalit en Tilburg) constructief met ons hebben meegewerkt aan:

- Technisch onderzoek, in de vorm van een pentest
- Organisatorisch onderzoek, in de vorm van een quick scan

Technisch onderzoek

Bij het technisch onderzoeken hebben de betrokkenen de uitkomsten van de pentesten ter harte genomen en actie ondernomen dan wel de geconstateerde onveiligheden op een actielijst gezet. De mate van uitvoering van deze actiepunten heeft de RMB niet nader onderzocht. Dit is een verantwoordelijkheid van de gemeente en de IT-leverancier.

Organisatorisch onderzoek

Bij het organisatorische deel van het onderzoek viel het de RMB in de eerste plaats op, dat de gemeenten nauw samenwerken met hun voornaamste IT-leveranciers, Tilburg en Equalit. Ten tweede viel het de RMB op dat er tijdens het organisatorische onderzoek en bij het ambtelijk wederhoor belangwekkende verschillen van inzicht op kernbegrippen naar voren kwamen.

6.2 Beantwoording centrale onderzoeksvraag

De centrale onderzoeksvraag is: *Kunnen de gemeenteraad en de burgers ervan op aan dat de persoonsgegevens zijn beschermd?*

Op basis van het uitgevoerde onderzoek kan de RMB deze vraag niet met een eenvoudig ‘ja’ of ‘nee’ beantwoorden. We hebben gezien dat de organisaties van de gemeenten en de IT-leveranciers hun best doen om de persoonsgegevens te beschermen. Dit doen zij binnen de middelen die de besturen beschikbaar hebben gesteld.

En toch is in het onderzoek gebleken dat de onderzoekers van de RMB toegang hebben gekregen tot deze persoonsgegevens. Uit het onderzoek van de RMB eind 2022/begin 2023 blijkt namelijk dat de ethisch hacker, die door de RMB was ingehuurd, zich toegang heeft verschaft tot persoonsgegevens van burgers en medewerkers. De hacker heeft geen beheerrechten verworven. De techniek vertoont feitelijke onveiligheden, waardoor – strikt genomen - het wettelijke doel van bescherming van persoonsgegevens (zie AVG) niet gegarandeerd is.

Hebben we hier nu te maken met enkele - nu eenmaal - onvermijdelijke onveiligheden in het systeem of hebben we te maken met een falend systeem?

De RMB belicht deze vraag hieronder, genuanceerd langs drie lijnen:

- Wat gaat goed? Zie paragraaf 6.3.
- Zijn er niettemin risico’s? Zie paragraaf 6.4.
- Wat kan beter? Zie paragraaf 6.5.

6.3 Wat gaat goed?

Gemeenten volgen nadrukkelijk de landelijke 'state of the art'

Het referentiekader van de ambtelijke organisatie is:

- BIO = norm + risico gestuurd werken + zelfevaluatie
- ENSIA = verantwoording, met jaarlijkse raadsinformatiebrief/RIB (desgewenst voor gemeenteraad)
- Jaarlijkse verbeterplannen per gemeente = PDCA-cyclus
- Overleg met de IT-partner = samenwerking = PDCA-cyclus

De RMB onderkent dat dit op grove hoofdlijnen de 'state of the art' is bij de gemeenten in Nederland. De gemeenten stellen BIO en ENSIA centraal.

B&W stelt iedere drie jaar het beleid vast

De gemeenten hebben in de bestuurlijke besluitvorming stappen gezet door periodiek het beleid over informatieveiligheid te laten vaststellen door B&W. Door de RMB wordt dit als een positieve ontwikkeling gezien.

Samenwerking met IT-leveranciers verloopt goed

De gemeenten hebben de IT-dienstverlening uitbesteed aan deskundige partijen, wat verstandig is voor kleinere gemeenten, die op zichzelf over beperkte capaciteit en kennis beschikken. De gemeenten Dongen, Goirle, Hilvarenbeek en Loon op Zand hebben voor informatieveiligheid dus een raamwerk opgezet in samenwerking met de IT-leveranciers en zij hebben met deze IT-partners een gezamenlijk proces van voortdurende verbetering ingericht. De betrokken functionarissen van de gemeenten en de IT-leveranciers besteden veel aandacht aan de inrichting van zowel het raamwerk als het verbeterproces.

Scope risicomanagement is goed, als startpunt voor doorontwikkeling

De BIO is een goed startpunt, maar het blijft zaak om risico's bij alle processen continu en structureel te blijven beoordelen, zeker gezien de veranderlijke omgeving van een gemeente.

Verantwoording wordt afgelegd aan B&W en gemeenteraad

Aan B&W wordt door de CISO verantwoording afgelegd op basis van ENSIA. B&W legt vervolgens aan de gemeenteraden verantwoording af in de P&C-documenten (paragraaf Bedrijfsvoering) en in jaarlijkse raadsinformatiebrieven over informatieveiligheid. De gemeenteraad kan hierdoor toezicht houden.

6.4 Zijn er niettemin risico's?

Gewenste beleidseffect wordt niet bereikt

Het gewenste effect van het beleid is de bescherming van persoonsgegevens, vanuit de AVG als hoogste norm. De uitkomsten van het onderzoek geven aan dat de huidige aanpak van de gemeenten en de IT-leveranciers niet het gewenste effect heeft bereikt, want buitenstaanders kunnen bij de persoonsgegevens komen. De RMB heeft overigens de indruk dat de gemeenten en de IT-leveranciers binnen de financiële en personele mogelijkheden het maximale doen, maar ook dat zij wellicht de grenzen van hun financiële en personele mogelijkheden hebben bereikt.

Een vervolgstap lijkt noodzakelijk, waarbij de gemeenten hun eigen positie zelfbewuster en doeltreffender kunnen gaan invullen, ook tegenover de IT-leveranciers.

Vervlechting met IT-partners wordt te groot

B&W heeft de verwerkingsverantwoordelijkheid. De kleine gemeenten lopen hierbij het risico van vervlechting met de grotere IT-partners en ongemerkt "het beleid van de IT-partner" te volgen. De RMB signaleert dit als een mogelijk risico, waarbij in de praktijk het 'haalbare' de overhand kan krijgen boven het 'wenselijke'. De gemeente dient hierbij te bepalen wat het 'wenselijke' is, vanuit de AVG als hoogste norm.

Governance is niet zuiver

De inrichting van de organisatie ziet er 'op papier' redelijk uit, maar gemeenten beschikken over een beperkte capaciteit om hier praktisch de nodige invulling aan te geven. De uitvoering van het door B&W vastgestelde beleid is in wording, omdat de uitvoering van beleidsplannen noodgedwongen gespreid in de tijd (jaren) ter hand wordt genomen. Ondanks de motivatie van de betrokken functionarissen wordt niet stelselmatig gevolg gegeven aan actiepunten. Hierdoor wordt het beheersproces ('PDCA-cyclus') niet volledig doorlopen.

Integraal risicomanagement is niet haalbaar in de praktijk

Iedere gemeente heeft wel een vorm van risicoanalyse uitgevoerd, maar evalueert en actualiseert deze niet jaarlijks. Het uitvoeren van een integrale risicoanalyse (op basis waarvan de BIO moet worden geïmplementeerd) is niet structureel geborgd in de gemeenten.

De verantwoording is slechts gebaseerd op een zelfevaluatie

De informatie die aan de gemeenteraad wordt verstrekt - in de voornoemde P&C-documenten en de raadsinformatiebrieven - is gebaseerd op de interne ENSIA-zelfevaluatie, opgesteld door de gemeentelijke organisatie zelf. Met andere woorden: er heeft geen externe, onafhankelijke toets (of iets dergelijks) plaatsgevonden.

De fysieke beveiliging verdient steeds aandacht

Zo bleek in Dongen de fysieke beveiliging van het gemeentehuis ontoereikend. De patchruimte was niet afgesloten en de onderzoeker kon zich toegang verschaffen tot vertrouwelijke documenten in de kamer van de burgemeester.

6.5 Wat kan beter?

Vanuit de huidige praktijk ziet de RMB verbetermogelijkheden, in de zin van het nemen van maatregelen tegen de risico's die de RMB in het vorige hoofdstuk heeft beschreven. De RMB beveelt B&W aan met de gemeenteraad te reflecteren over twee cruciale onderwerpen.

Aanbeveling 1: B&W bespreekt (beeldvormend) met de gemeenteraad de scope en de integraliteit van de risicoanalyse bij informatieveiligheid.

Aanknopingspunten voor de beeldvormende bespreking met de gemeenteraad zijn:

Integraliteit: Willen we alle processen in kaart hebben? Of volstaan we met de grootste risico's vanuit het huidige 'risico gestuurd werken'? De eerstverantwoordelijke is de gemeentesecretaris, want die is verantwoordelijk voor het integrale risicomanagement. De IBD zegt hierover in het Dreigingsbeeld 2023-2024 (blz. 18): *"De gemeentesecretaris voert de regie over het risicomanagement en de CISO/privacyfunctionaris zijn de eerste adviseurs die helpen bij een veilige bedrijfsvoering en dienstverlening."* Het is aan de gemeentesecretaris om er expliciet op te sturen dat risicomanagement over informatieveiligheid expliciet onderdeel is van het concernbrede, integrale risicomanagement. Hierdoor wordt richting de organisatie uitdrukkelijk bevestigd dat informatieveiligheid een gezamenlijke verantwoordelijkheid is van allen die werkzaam zijn in de organisatie; en niet een taak is van een specifieke functionaris.

Normenkader: Motiveer in de integrale risicoanalyse het wettelijke doel van het gemeentelijke beleid en volsta niet met volgen van de landelijke praktijk.
Het doel van de wet is: bescherming van persoonsgegevens. Durf daarbij – los van de dagelijkse praktijk en het dilemma van de haalbaarheid met de huidige middelen - na te denken over de wenselijkheden om te komen tot: *een goed gepositioneerde informatiebeveiliging binnen de gemeenten, waarbij het beleid helder is, de organisatorische inrichting en techniek op orde zijn en waarbij ook sprake is van een goede control, ingebed in het primaire proces als onderdeel van het concern risicomanagement.*

Urgentie: Beargumenteer in de integrale risicoanalyse de urgentie voor de gemeente van de actuele dreiging, zoals bijvoorbeeld de IBD aangeeft. Probeer daarbij te simuleren welke de schadelijke gevolgen voor de gemeente kunnen zijn van actuele dreigingen. Denk tijdig na over de urgentie van de dreigingen en wacht niet tot het te laat is.

Objectivering evaluatie: De voornaamste basis voor de verantwoording aan B&W en de gemeenteraad is nu een (subjectieve) zelfevaluatie. De huidige externe audits richten zich nu op DigiD en Suwinet, wat meestal een onderdeel is van het totale informatie-beveiligingslandschap van de gemeente (en daar worden vaak ook niet de grootste risico's gelopen). Naast de zelfevaluatie met behulp van ENSIA kunnen externe audits of andere vormen (zoals peer review of visitatie) het kritische vermogen van de gemeente versterken, waardoor de beschikbare bestuurlijke informatie (voor B&W en gemeenraad) objectiever wordt onderbouwd.

Aanbeveling 2: B&W bespreekt (beeldvormend) met de gemeenteraad de invulling van macht en tegenmacht, in de professionele samenwerking met de externe 'IP-partner'.

Aanknopingspunten voor de beeldvormende bespreking met de gemeenteraad zijn:

Leveranciersmanagement: De samenwerking met de 'IP-partner' (resp. Equalit en Tilburg) is zo hecht dat de opdracht gevende gemeente en de opdracht nemende IT-leverancier dicht op elkaar zitten.

Hierdoor komt het beoogde governance-systeem van 'checks and balances' of 'macht en tegenmacht' mogelijkerwijs niet goed uit de verf. Voor alle gemeenten geldt dat ze "steunen" op de IT-partner. Dat is logisch, maar aan de andere kant heeft de gemeente ook de belangrijke rol om in het kader van leveranciersmanagement kritisch te zijn op haar IT-leveranciers.

Opdrachtgeverschap als mindset: geef namens de gemeente steeds zelfbewust invulling aan het opdrachtgeverschap richting de IT-leveranciers en de leveranciers van andere diensten. Dit betekent aan de voorkant goed nadenken over afspraken (contracten) en servicelevels en aan de achterkant processen implementeren waarmee bewaakt kan worden dat de IT-partner levert wat is afgesproken.

Rol CISO: Positionering van de CISO onder het lijnmanagement – zoals bij Goirle, Hilvarenbeek en Loon op Zand het geval is - is geen goede zaak, waardoor binnen de organisatie de interne kritische tegenkracht van de CISO mogelijkerwijs onvoldoende wordt benut. De positie van de CISO wordt versterkt door de CISO niet meer te plaatsen onder het lijnmanagement, maar direct en onafhankelijk onder gemeentesecretaris/B&W in een strategische staffunctie; respectievelijk geen externe CISO in te huren bij de eigen IT-leverancier. De RMB meent dat een invulling van de CISO-functie door de IT-leverancier niet de juiste oplossing is. Een dergelijke constructie lijkt op gespannen voet te staan met de gewenste functiescheiding tussen het opdrachtgeverschap van de gemeente en de opdrachtnemersrol van de IT-leverancier.

Structurele monitoring op verschillende risiconiveaus: De gemeenten (en de IT-leveranciers) hebben de neiging te reageren op de onveiligheden die tijdens ons technische onderzoek als 'kritische kwetsbaarheden' werden gekwalificeerd (zie par. 5.3). Dit is goed, maar in het onderzoek is ook aan de gemeenten geadviseerd om zo snel mogelijk ook alle bevindingen met 'Hoog', 'Middel' en 'Laag' risico te verhelpen en deze vervolgens te laten hertesten. Tijdens het onderzoek heeft de RMB gemerkt dat deze bereidheid ook bestaat bij de organisatie, ook al is budget/geld soms een beperkende factor om deze ambitie in praktijk te brengen. Het verhelpen van de bevindingen met een 'Hoog', 'Midden' en 'Laag' risico komt de gelaagde beveiliging van het netwerk ten goede.

6.6 Slotopmerkingen

De RMB heeft de aanbevelingen aan het college van B&W geformuleerd vanuit twee vertrekpunten:

1. *Het doel is een goed gepositioneerde informatiebeveiliging binnen de gemeenten, waarbij het beleid helder is, de organisatorische inrichting en techniek op orde zijn en waarbij ook sprake is van een goede control, ingebed in het primaire proces als onderdeel van het concern risicomanagement.*
2. *De IBD[8] stelt iedere twee jaar een dreigingsbeeld op voor gemeenten. In het rapport Dreigingsbeeld Informatiebeveiliging 2023-2024 constateert de IBD dat de risico's voor gemeenten groeien. Gemeenten doen – volgens de IBD - al veel om hun informatie goed te beveiligen, maar er is meer nodig om gelijke tred te houden met de dreiging. De IBD constateert dat het aantal ransomware-aanvallen groeit en dat deze ook steeds professioneler worden uitgevoerd. Bij zo'n aanval versleutelen criminelen bestanden om vervolgens losgeld te eisen om ze weer beschikbaar te stellen. Ook ziet de IBD steeds meer en ernstigere fouten in software. Het lukt criminelen zo om toegang te krijgen tot gemeentelijke systemen. Het rapport van de IBD benadrukt het belang van investeringen in informatieveiligheid.*

De RMB heeft hierbij het wettelijke doel in gedachten (bescherming van persoonsgegevens). En de RMB wil de gemeente behoeden voor wat andere gemeenten en organisaties al eerder is overkomen: afpersing en gijzeling van gegevens. Wat de ethische hacker ons heeft geleerd is dat een kwaadwillende hacker bij 'onze' gemeenten veel schade had kunnen aanrichten. Dit is helaas geen suggestieve opmerking, maar een serieuze waarschuwing.

[8] Als onderdeel van de VNG draagt de IBD (informatiebeveiligingsdienst) namens gemeenten bij aan de deskundigheid over informatiebeveiliging en brengt het kennisproducten hierover uit, zoals het Dreigingsbeeld 2023-2024. Voor meer uitleg zie paragraaf 3.4 van deze nota.

Deel B BESTUURLIJKE REACTIES B&W

DONGEN

29 augustus 2023

Wij zijn blij met het initiatief voor een dergelijk onderzoek, de uitkomsten helpen ons om onze informatieveiligheid verder aan te scherpen. Het speelveld van informatieveiligheid is immers continu in beweging. Dit soort onderzoeken, maar ook eigen onderzoeken, audits, scans en steekproeven helpen ons alert te blijven. 100% veiligheid is niet haalbaar, daarom besteden we naast preventie ook aandacht aan crisisbeheersing en het BCM (business continuity management).

De leesbaarheid van de rapportage is verbeterd met het uiteen halen van de opmerkingen voor Dongen enerzijds en de andere drie gemeenten anderzijds, zoals ambtelijk geadviseerd. Daarvoor dank.
Naar aanleiding van de door u doorgevoerde aanpassingen hebben we nog de volgende opmerkingen:

- Pagina 22 ("De techniek vertoont … gegarandeerd is."): Wij volgen net als andere gemeenten de landelijke baseline in het kader van onze weerbaarheid. Deze kent drie aspecten: techniek, mens en fysiek (3 verdedigingslinies). Dit is een continu proces. Digitale veiligheid is niet louter middels technische maatregelen te bereiken.
- Pagina 29: De paragraaf 'Rol CISO' lijkt uitsluitend betrekking te hebben op de andere drie gemeenten, niet op Dongen.
- Pagina 25 en 26 (§6.2 en 6.3): De vraag "Kunnen de gemeenteraad en de burgers ervan op aan dat de persoonsgegevens zijn beschermd? " is inderdaad moeilijk met ja of nee te beantwoorden. We moeten continue alert zijn en de techniek up-to-date houden om de risico's te beperken. En we moeten blijven werken aan de bewustwording (veilig en vaardig digitaal werken) onder medewerkers. Dat is een doorlopend proces. Maar de focus moet niet alleen liggen op preventie. Met voldoende middelen zullen er altijd mogelijkheden zijn om digitaal in te breken. Daarom besteden we ook tijd en aandacht aan de voorbereiding op een incident. We oefenen crisissituaties en werken aan onze bedrijfscontinuïteit.
- In met name hoofdstuk 5 staan gevoelige gegevens en conclusies, die niet naar buiten mogen worden gebracht. Daarom willen we graag met u afspreken dat dit rapport onder geheimhouding wordt gedeeld met de raad en als zodanig wordt besproken.

Tot slot hechten we er belang aan om te benadrukken dat we met de in de pentest gevonden kwetsbaarheden (direct) aan de slag gegaan zijn. Hierbij kijken we niet alleen naar de mitigatie van de feitelijke bevindingen, maar proberen we ook eventuele onderliggende oorzaken aan te pakken.
We pakken ze (uiteraard) op van hoog (high) naar laag (low). In de bijlage treft u een overzicht aan van de stand van zaken (het spreekt voor zich dat deze informatie onder geheimhouding met u wordt gedeeld).

We wensen u succes bij de verdere uitwerking tot het definitieve rapport.

GOIRLE

22 augustus 2023

Informatieveiligheid staat in onze gemeente hoog op de agenda. Wij danken de Rekenkamercommissie Midden-Brabant voor het onderzoek en de inzichten die het ons heeft opgeleverd.

Informatieveiligheid is een onderwerp van ons allemaal. Wij onderschrijven dan ook de twee aanbevelingen waarin u adviseert om de gemeenteraad in een beeldvormende bijeenkomst deelgenoot te maken van de wijze waarop wij met dit onderwerp omgaan. Ook awareness op het niveau van de gemeenteraad draagt bij aan een goede beveiliging van onze gegevens.

We streven naar een niveau van volwassenheid op het gebied van informatieveiligheid, waarbij kwaliteitszorg goed geborgd is in de processen en waarbij zelfevaluatie in de toekomst kan overgaan in een goede interne en externe audit. U hebt zelf kunnen ervaren tijdens het onderzoek, dat we continu leren en ontwikkelen. Dit vakgebied staat nooit stil met alle technologische ontwikkelingen van deze tijd. Juist door dit soort onderzoeken en onze eigen scans en steekproeven, blijven we alert. Hoewel we graag alle mogelijke situaties willen ondervangen en alles zouden willen afdekken, is dit niet mogelijk. Honderd procent veiligheid bestaat niet. Wij besteden daarom ook veel aandacht aan bedrijfscontinuïteit en crisisbeheersing, met andere woorden: wat te doen wanneer je gehackt bent?

Kortom, we werken toe naar een volwassen kwaliteitszorg in onze organisatie, waarbij maatregelen ingebed zijn in het primaire proces en het toezicht goed gepositioneerd en op orde. Daarbij maken we dankbaar gebruik van de uitkomsten van uw onderzoek.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd, zodat u de fase van bestuurlijke wederhoor naar tevredenheid kunt afronden.

HILVARENBEEK

29 augustus 2023

Informatieveiligheid staat in onze gemeente hoog op de agenda. Wij danken de Rekenkamercommissie Midden-Brabant voor het onderzoek en de inzichten die het ons heeft opgeleverd.

Informatieveiligheid is een onderwerp van ons allemaal. Wij onderschrijven dan ook de twee aanbevelingen waarin u adviseert om de gemeenteraad in een beeldvormende bijeenkomst deelgenoot te maken van de wijze waarop wij met dit onderwerp omgaan. Ook awareness op het niveau van de gemeenteraad draagt bij aan een goede beveiliging van onze gegevens.

Uw eerste aanbeveling behandelt de onderwerpen integraliteit, normenkader en de urgentie van informatieveiligheid. We streven naar een niveau van volwassenheid op het gebied van informatieveiligheid, waarbij kwaliteitszorg

goed geborgd is in de processen en waarbij zelfevaluatie in de toekomst kan overgaan in een goede interne en externe audit. U hebt zelf kunnen ervaren tijdens het onderzoek, dat we continu leren en ontwikkelen. Dit vakgebied staat nooit stil met alle technologische ontwikkelingen van deze tijd. Juist door dit soort onderzoeken en onze eigen scans en steekproeven, blijven we alert. Hoewel we graag alle mogelijke situaties willen ondervangen en alles zouden willen afdekken, is dit niet mogelijk. Honderd procent veiligheid bestaat niet. Wij besteden daarom ook veel aandacht aan bedrijfscontinuïteit en crisisbeheersing, met andere woorden: wat te doen wanneer je gehackt bent?

Uw tweede aanbeveling gaat over een professionele samenwerking met de IT partner. Een goed contract- en leveranciersmanagement is daar één van. Wij zijn ons bewust van de rol van de gemeente als opdrachtgever richting Equalit. De governance binnen de Equalit samenwerking heeft de aandacht in het strategisch en tactisch overleg in deze samenwerking. Binnen onze gemeente is ook de positionering van de CISO en FG een punt van aandacht. Samen met het vraagstuk over de benodigde capaciteit, wordt dit in GHO verband bekeken.

Kortom, we werken toe naar een volwassen kwaliteitszorg in onze organisatie, waarbij maatregelen ingebed zijn in het primaire proces en het toezicht goed gepositioneerd en op orde. Daarbij maken we dankbaar gebruik van de uitkomsten van uw onderzoek.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd, zodat u de fase van bestuurlijke wederhoor naar tevredenheid kunt afronden.

LOON OP ZAND

3 oktober 2023

Informatieveiligheid staat in onze gemeente hoog op de agenda. Wij danken de Rekenkamercommissie Midden-Brabant voor het onderzoek en de inzichten die het ons heeft opgeleverd. Wel merken wij op dat het rapport in eerste instantie onjuistheden bevatte. De RMB heeft, op aangeven van de Ciso's (Chief Information Security Officer), besloten na te gaan om welke onjuistheden het ging.

De onjuistheden die o.a. besproken zijn, zijn:
• Het niet juist benoemen van beveiligingsmaatregelen
• Toepassen van segmentatie (Netwerksegmentatie is het opknippen van het totale netwerk in kleinere segmenten, met tussen de segmenten een beveiligd koppelvlak. Dit zorgt ervoor dat kwaadwillende die zich in een netwerksegment bevindt niet direct ongehinderd toegang heeft tot andere netwerksegmenten)
• Een oordeel over het functioneren van medewerkers
Deze zijn inmiddels besproken, afgestemd en naar tevredenheid van de Ciso's gewijzigd. Het college heeft daarna kennis genomen van de tekstuele wijzigingen in het rapport.

Informatieveiligheid is een onderwerp van ons allemaal. Wij onderschrijven dan ook de aanbevelingen waarin u adviseert om de gemeenteraad in een beeldvormende bijeenkomst deelgenoot te maken van de wijze waarop wij met

dit onderwerp omgaan. Ook awareness op het niveau van de gemeenteraad draagt bij aan een goede beveiliging van onze gegevens.

De aanbeveling waarin u adviseert met de gemeenteraad de invulling van macht en tegenmacht, in de professionele samenwerking met de externe 'IP-partner' te bespreken in een beeldvormende bijeenkomst nemen wij niet over. De onderwerpen waar de rekenkamer commissie het college op attendeert zoals het verder professionaliseren van het leveranciersmanagement, nemen wij zeer ter harte. Aangezien het hier gaat om een uitvoeringskwestie, gaan we dit niet beeldvormend bespreken met de gemeenteraad.

We streven naar een niveau van volwassenheid op het gebied van informatieveiligheid, waarbij kwaliteitszorg goed geborgd is in de processen en waarbij zelfevaluatie in de toekomst kan overgaan in een goede interne en externe audit. U hebt zelf kunnen ervaren tijdens het onderzoek, dat we continu leren en ontwikkelen. Dit vakgebied staat nooit stil met alle technologische ontwikkelingen van deze tijd. Juist door dit soort onderzoeken en onze eigen scans en steekproeven, blijven we alert. Hoewel we graag alle mogelijke situaties willen ondervangen en alles zouden willen afdekken, is dit niet mogelijk. Honderd procent veiligheid bestaat niet. Wij besteden daarom ook veel aandacht aan bedrijfscontinuïteit en crisisbeheersing, met andere woorden: wat te doen wanneer je gehackt bent?

Kortom, we werken toe naar een volwassen kwaliteitszorg in onze organisatie, waarbij maatregelen ingebed zijn in het primaire proces en het toezicht goed gepositioneerd en op orde. Daarbij maken we dankbaar gebruik van de uitkomsten van uw onderzoek.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd, zodat u de fase van bestuurlijke wederhoor naar tevredenheid kunt afronden.