Evaluatie

Pilot Weerbare Overheid

Gemeente Tiel

Een pilot met de ministeries BZK, J&V

Het COT

En negen andere Nederlandse gemeenten

Datum	10 augustus 2021
Versie	1.0
Opsteller	Marco Boudewijns

Inhoud

1. Aanleiding

Op 3 oktober 2019 ontving gemeente Tiel een uitnodiging om mee te doen aan een pilot integrale beveiligingsplannen. Het initiatief komt van het ministerie BZK en V&J.
Het doel is om een aantal gemeenten te ondersteunen bij het opzetten van een integrale inzet op

a. De veiligheid van objecten en personen (politieke ambtsdragers, medewerkers en bezoekers)
b. Het integer en veilig werken binnen de organisatie
c. De informatiebeveiliging
d. De continuïteit van bedrijfsvoering

Op 29 oktober 2019 bevestigde de gemeente Tiel per brief deel te willen nemen aan de pilot. De deelname werd door BZK bevestigd per mail van 5 november 2019. In deze mail werd tevens de financiële impuls bevestigd van €105.000,-.

1.1. Cofinanciering

Gemeente Tiel ontvangt van het ministerie een eenmalige financiële impuls van € 105.000,-. Er is sprake van cofinanciering. De cofinanciering vindt plaats door inzet van personeel (projectleider). We verantwoorden onze personele inzet door middel van een (eenvoudige) tijdregistratie.
Het COT evalueert de pilot door middel van een enquête onder de deelnemende gemeenten (zie ook paragraaf 6.8). Met de ingevulde vragenlijsten zal het COT de ministeries van BZK en J&V op de hoogte brengen van de opbrengsten van het traject. De deadline voor het invullen van de enquête is 31 augustus 2021. Het resultaat van de enquête wordt verwacht in oktober 2021.

1.2. Duur van de pilot

De Kick off is georganiseerd op 12 december 2019. De pilot loopt tot medio 2021.

1.3. Deelnemende gemeenten

Tien Nederlandse gemeenten zullen meedoen aan de pilot. Dit zijn:

- Breda
- Tilburg
- Berkelland
- Saba
- Gooisemeren
- Almelo
- Dalfsen
- Haarlemmermeer
- Venlo
- Tiel

2. Doelstellingen pilot

2.1. Algemene doelstelling van gemeente Tiel (zoals door Tiel bevestigd aan BZK)

Tiel wil in de volle breedte een duurzame aanpak ontwikkelen om de impact van ondermijning - en uiteraard de ondermijning zelf - een halt toe te roepen.

2.2. Subdoelstellingen op de punten A tot en met D (zoals door Tiel bevestigd aan BZK)

2.2.1. De veiligheid van objecten en personen (politieke ambtsdragers, medewerkers en bezoekers)

De (balie-)medewerkers van Tiel hebben regelmatig te maken met uitingen van agressie. Dit gebeurt bijna wekelijks. Collega's melden incidenten bij hun leidinggevende. De leidinggevende voert een zogenaamd 'ordegesprek' met de agressor. Tijdens bezoekuren van het gemeentehuis is er een beveiliger aanwezig. We registreren de incidenten maar er vindt geen periodieke evaluatie plaats. Dat is jammer, want een incident is een potentieel leermoment.

Ons doel: Tiel wil 'leren' van de incidenten die plaatsvinden.

2.2.2. Het integer en veilig werken binnen de organisatie

Onze klanten kunnen groot belang hebben bij onze besluitvorming. In sommige gevallen zal de klant de besluitvorming proberen te beïnvloeden. Incidenten in dit kader zijn bijvoorbeeld bedreiging of poging tot omkoping. We besteden hier aandacht aan op ambtelijk en bestuurlijk niveau.

Ons doel: incidenten mogen in géén geval de besluitvorming beïnvloeden.

2.2.3. De informatiebeveiliging

In de gemeentelijke organisatie wordt veel privacygevoelige informatie gedeeld. Niet alleen intern, maar ook met externe partijen. Bij een data-lek denken we meestal aan het werk van een hacker of een storing in het netwerk. Maar dat hoeft niet altijd zo te zijn. Het delen van informatie gebeurt veelal via mail of mondeling. Het onterecht delen van informatie is niet alleen in strijd met privacyregelgeving, maar kan ook gevaarlijke situaties teweeg brengen.

Ons doel: medewerkers gaan zorgvuldig om met informatie en zijn op de hoogte van gevaren en risico's van datalekken.

2.2.4. De continuïteit van bedrijfsvoering

In de gemeente worden veel verschillende processen uitgevoerd. Veel processen zijn termijn gebonden. Sommige kunnen uitstel dulden van slechts enkele dagen. Andere processen hebben een langere doorlooptijd. Een incident kan leiden tot tijdelijke uitval van personeel of van technische middelen.

Ons doel: incidenten mogen er niet toe leiden dat de continuïteit van de bedrijfsvoering in gevaar komt.

3. Opzet van de pilot Weerbare Overheid

De pilot is geïnitieerd door BZK en J&V. De regie op de uitvoering ligt bij het COT (instituut voor veiligheids- en crisismanagement). In de opzet is voorzien in het organiseren van een aantal 'leerkringen'. Hiervan zijn er het afgelopen jaar 6 georganiseerd. Het eindproduct van de pilot/leerkringen is een website met tools, tricks en best practices.

Daarnaast zullen twee instructiedocumenten worden opgeleverd:

- Visie document integrale beveiliging
- Governance

Van beide documenten zijn de conceptversies bijgevoegd (versie 28 januari 2021).

4. Het Tielse kernteam m.b.t. weerbare overheid (bij aanvang van de pilot)

- Gemeentesecretaris
- Projectleider pilot
- Medewerker P&O
- CISO
- Programmacoördinator veiligheid
- Regisseur veiligheid
- Teamleider LWD (voorheen publiekszaken)
- Coordinator BHV
- Adviseur financiën
- Teamleider communicatie

De uitbraak van het coronavirus heeft gevolgen gehad voor de deelnemende gemeenten van pilot. Er zijn geen fysieke bijeenkomsten geweest sinds de kick-off. De prioriteiten binnen het veiligheidsdomein zijn bij de meeste gemeenten verschoven.

De opbrengsten uit de leerkringen tot zover zijn door dit kernteam vertaald naar resultaten en activiteiten voor Tiel onder de 4 opgestelde doelen. Deze zijn opgenomen onder de verschillende programma's in de begroting (vnl. programma 9 bedrijfsvoering en organisatie). Een deel daarvan is benoemd in het programma veiligheid onder "weerbare overheid" en als activiteit opgenomen in het uitvoeringsplan veiligheid 2021-2022. Deze worden nog aangevuld wanneer de laatste leerkring heeft plaatsgevonden en de pilot is afgerond.

4.1 Brainstormsessies

In januari 2020 vond een eerste brainstormsessie plaats met de kerngroep van Tiel. De resultaten zijn verwerkt in zogenaamde wordclouds.

5. De leerkringen

Er hebben op dit moment 6 leerkringen plaatsgevonden. Hieronder een overzicht van de inhoud ervan.

5.1 Leerkring 1

31 maart 2020. Thema: kennismaken en inventariseren van de ingevulde vragenlijsten.

De besproken zaken en lessons learned tijdens deze leerkring:

- Gemeenten gaan aan de slag om weerbaarder te worden, bewustzijn te vergroten, risico's te verminderen en fragmentarisch beleid te vormen tot een integrale benadering van veiligheid.
- Onder (integrale) beveiliging valt nu binnen de gemeenten (in volgorde van aanwezigheid): beveiliging (informatie)systemen, beveiliging gebouwen/middelen, een veilige werkomgeving, integriteitsbeleid, continuïteit van bedrijfsvoering, en beveiligen van mensen.
- Van de pilotgemeenten heeft 70% risico's geïdentificeerd/geanalyseerd. 20% niet. Er zijn enkele maatregelen genomen (soms d.m.v. beleid). Restrisico's zijn door 5 gemeenten geaccepteerd.
- Doelen en uitgangspunten zijn bij 9 gemeenten geformuleerd. Voorbeelden: BCM, integriteitsbeleid, voorkomen van informatiebeveiliging/datalekken en bewustwording.
- Om gemeenten weerbaar te maken, gebruiken ze de volgende maatregelen: verplicht training/e-learning volgen, mystery guest/phising actie, instructies bij nieuwe medewerkers en integriteitsbeleid.
- Draagvlak creëren de gemeenten door bestuurlijk draagvlak en bewustzijn van verantwoordelijkheden te stimuleren. O.a. door: e-learning, beleidsdocumentatie, informeren management/bestuur. Verbeterpunt hierin is: gezamenlijke aanpak ontbreekt, ontstaat vaak pas na een incident, geen structurele aandacht.
- Samenwerking/structuur voor (integrale) beveiliging is versnipperd. Soms werken disciplines op thema's samen. Verder met name de lijnorganisatie volgend (bijv. managers/ directieoverleg).
- Bevoegdheden liggen operationeel vast in plannen/functies. Bestuurlijk vaak ook in de lijn per thema.
- Lerende vermogen is beperkt. Vaak reactief/op teamniveau. Actiepunten worden geformuleerd. Niet planmatig ingericht, soms wel interne leertafels.
- Trainingen/educatieve activiteiten voor weerbare organisatie zijn met name: introductiebijeenkomst, I/E-learnings, training integriteit/agressie en campagne informatieveiligheid/privacy.
- Samenwerkingen voor een weerbare organisatie zijn er met name met buurgemeenten (op thema).
- Wat kunnen gemeenten van elkaar leren? Specifieke casuïstiek (specifieke hack, reactie op incident, etc.), korte lijnen tussen afdelingen, bewustwordingsproces en een lange adem.
- Stellingen: weerbaar worden als gemeente kan versterkt worden door scala aan investeringen/verbeteringen. De respondenten reageren bijna op alle stellingen met eens/volledig eens. Enkele keer weet ik niet. Bewustwording en samenwerken/gezamenlijk acteren komt regelmatig terug. Prioriteitendilemma?
- Verwachtingen proces pilot: goede formulering einddoel, actieve deelname alle gemeenten (van elkaar leren), ontvangen kennis/expertise, handvatten via/voor plan/methodiek.
- Verwachtingen bij leerkringen: informatie-, ervaring- en kennisdeling, concrete zaken bespreken, (gezamenlijk) de lat bepalen.
- Opbrengst voor de pilotgemeenten bij pilottraject: Van elkaar leren, kennis en expertise van buitenaf, delen (digitaal pilot platform).

Samenvattend; wat zou deze pilot voor alle NL gemeenten kunnen opleveren? (weerbare organisatie):

- Programmatische aanpak voor IB
- Methodiek meting (0+1)
- Programma aanpak voor integrale beveiliging (cyclus – pdca)
- Best practise van disciplines
- Modelplan
- Hoe integraliteit te borgen? Start uitvoering pilot gemeente

5.2. Leerkring 2

16 juni 2020. Thema: awareness en draagvlak.

De besproken zaken en lessons learned tijdens deze leerkring:

Voor draagvlak en awareness binnen de organisatie is op vele punten in te zetten. Naast de hierna volgende tips en leerpunten zijn er vijf quick wins om direct mee aan de slag te kunnen. Voor focus en om op korte termijn enkele stappen te kunnen zetten.

- Niet één persoon kan zorgdragen voor awareness of draagvlak door de gehele organisatie. Draag zorg voor 'ambassadeurs'. Informeel of formeel bekend. Zij maken of breken het; zij worden het gezicht en/of zijn voorbeeld voor medewerkers. Denk daarbij ook aan de rol van de controller (intern in te zetten voor het ophalen van informatie/sturing) of griffie (onderwerpen politiek bespreekbaar te maken).
- Draagvlak op strategisch en tactisch niveau is van belang om ook de operatie/medewerker mee te krijgen. Dit begint al bij het zorgdragen voor budget, opstellen beleid, en gaat door bij het zorgdragen voor registreren van incidenten en deze bespreekbaar maken. En waar nodig desbetreffende afdeling/teams ter verantwoording roepen in management/directie.
- Ga als coördinator/verantwoordelijke bij de afdelingen en managers langs. Om punten op te halen voor het beleid, om informatie/aanpak te delen. Of ga bijvoorbeeld per jaar het gesprek met leidinggevenden aan en bespreek dit daarna in het managementteam/directie. Zorg dat het hiermee voor de persoon/manager niet te vrijblijvend is.
- Een e-learning is een middel om te gebruiken om personen inhoudelijk te informeren en de bewustwording te stimuleren. Dit kan op vrijwillige basis of verplicht, waarbij het ook mogelijk is om dit af te ronden met een toets. Waarbij de resultaten ook onderdeel van personeelsdossiers kan worden. Een ander middel is een jaarlijkse enquête/dilemmatraining online en opvolgend groepsgesprekken. Eén keer per jaar gepland. De doelgroep hoeft niet specifiek te zijn, juist breed in de organisatie kan zorgdragen voor het leren van elkaar.
- Leer van de incidenten. Leer van de interne incidenten en als deze er niet/beperkt zijn, leer dan via externe voorbeelden. En of schakel een mystery guest. De inzet van een mystery guest (MG) wordt veel gebruikt om als organisatie een reëel beeld te krijgen over het functioneren van de organisatie in de dagelijkse praktijk.

5.3. Leerkring 3

24 september 2020. Thema: continuïteit gemeentelijke dienstverlening en Kwaliteitsborging/PDCA in gemeenten

De besproken zaken en lessons learned tijdens deze leerkring:

Continuïteitsmanagement binnen de gemeentelijke organisatie draait om het versterken van de weerbaarheid van de organisatie tegen continuïteitsbedreigingen (denk aan geen gebruik kunnen maken van je systemen of locaties). Om zo ook de dienstverlening onder moeilijke omstandigheden te kunnen waarborgen op een vooraf gedefinieerd en geaccepteerd niveau.

Om met continuitsmanagement in de gemeentelijke organisatie aan de slag te gaan, zijn hieronder enkele tips geformuleerd.

- Beredeneer vanuit de impact op de gemeentelijke processen en bepaal welke kritisch zijn voor de dienstverlening. Focus daarbij op kritische processen die bij uitval de belangen van burgers en bedrijven beschadigen (financieel, juridisch, welzijn en continuïteit).
- Zorg voor draagvlak en eigenaarschap binnen het ambtelijk bestuur (gemeentesecretaris, cluster directeuren). Wie houdt zich bezig met dit onderwerp en is een logische sponsor?
- Pas een top-down benadering toe door eerst op strategisch niveau een kader voor continuïteit goed te keuren, waarin de reikwijdte, het doel (waarom willen we dit), de uitgangspunten (wat willen we beschermen?) en de governance (centraal en decentraal) zijn uitgewerkt. Laat dit kader leidend zijn voor de uitrol op decentraal/clusterniveau.
- Werk met een BCM programma/PDCA cyclus om dit te borgen in de organisatie.
- Sluit zoveel als mogelijk aan bij de bestaande structuren, rapportagelijnen en gerelateerde domeinen (zoals Veiligheid, Information Security, crisisplannen, etc.).

5.4. Leerkring 4

14 december 2020. Thema: informatiebeveiliging.

(De CISO van de BVOWB heeft deelgenomen aan deze leerkring)

De besproken zaken en lessons learned tijdens deze leerkring:

- Maak risicoanalyses vanuit het belang voor de inwoners van de gemeente. Risicoanalyses zijn niet allemaal hetzelfde voor informatiebeveiliging, laat staan voor integrale beveiliging. Bepaal als gemeente welke wijze van analyseren aansluit bij de ambitie van de gemeente. Tip hierbij is om te beredeneren vanuit de maatschappij/beschikbaarheid voor de samenleving. Wat moet doorgang vinden, waar heeft de maatschappij als eerst nodig of het ergst last van? Hierdoor kan je gericht kijken naar de kritische processen en de prioriteren. Belangrijk gegeven hierbij is dat het uiteindelijke doel niet is om alle risico's uit te bannen, maar om ze terug te brengen tot een acceptabel niveau. Zie hiervoor ook de 3eleerkring over continuïteitsmanagement.
- Ga op afdelings-of teamniveau aan de slag met draagvlak voor informatiebeveiliging. Draagvlak voor informatiebeveiliging en integrale beveiliging blijft een uitdaging; hoe breng je de thema's bij elkaar? Een tip hiervoor is op afdeling/team niveau er mee aan de slag; 'zo gaan wij het doen'. Zo zijn ook per team/afdeling de vertaling te maken naar zelf bepaalde KPI's. Daarnaast werkt de zogenoemde het Adidas-netwerk; meters maken en veel personen (digitaal) spreken en bevragen. Bewustwording van de risico's en het belang van integraliteit; via e-learnings, sessies, mystery guest, etc. zie voor meer tips ook de 2eleerkring over draagvlak en awareness.
- Zorg dat de Informatiebeveiliging-risico's zichtbaar zijn in de begroting en weerstandsparagraaf/ kapitaal. Regelmatig rapporteren –al dan niet via een dashboard –zorgt voor agenderen, bestuurlijke betrokkenheid en informatie voor de gemeenteraad. Dit zorgt voor inzicht en zoals één van de sprekers aangaf: 'alleen druk is niet goed, richting daarbij geven zorgt voor sturing en grip'.

- Bepaal de gezamenlijke taal voor de verschillende thema's van integrale beveiliging. Ga samen aan de slag en maak een 'vertaalslag', zodat we elkaar begrijpen en informatiebeveiliging onderdeel wordt van integrale beveiliging. Zodat ook duidelijk is te bepalen; wat doe je samen en wat apart? Laat ook de CISO's van de pilotgemeenten samenkomen om te bespreken op welke wijze zij informatiebeveiliging zouden vormgeven als onderdeel van Integrale beveiliging. Zo ontstaat er kruisbestuiving naast de leerkringen.
- Blijf als werkgroep met regelmaat bij elkaar komen. Om samen de ontwikkeling door te maken. Let er daarbij op dat je als projectleider/coördinator integrale beveiliging niet voor alles verantwoordelijk bent; je coördineert en stuurt. Samen draag je zorg voor het behalen van de resultaten, ieder vanuit eigen verantwoordelijkheid. Stel daarbij realistische doelen. Dit helpt bij het concreet en haalbaar maken. En, hierdoor is vanaf de start mogelijk om de voortgang erin te houden.

5.5. Leerkring 5

23 maart 2021. Thema: Fysieke en personele beveiliging.

De besproken zaken en lessons learned tijdens deze leerkring

- Werk én treedt de-escalerend op. Bij de fysieke en personele beveiliging gaat het om een goede mix van voorbereiding en inrichting van gebouwen inclusief passende maatregelen en passend optreden. Zo is de inrichting van bijvoorbeeld de ontvangsthal mede bepalend of iemand zich 'anoniem' kan gedragen of voelen of dat alles open en zichtbaar is. Indien de wijze van benadering, aanspreken, gastvrijheid en gezamenlijke 'normen/grenzen' hierop aansluiten versterkt dit elkaar.
- Zorg voor eenduidige registratie systeem/opzet en draag zorg voor gezamenlijke opvolging. Bij fysieke en personele beveiliging is regelmatig sprake van beperkte registratie of verschillende registratiesystemen. Soms geautomatiseerd, soms een gezamenlijk melding emailadres of Excel. De integraliteit ontbreekt regelmatig, waardoor incidenten gefragmenteerd (bijv. door facilitair/beveiliging of personeelszaken/HR-agressie coördinator-) worden opgepakt. Door de incidenten bij te houden, gezamenlijk op te trekken bij de analyse én opvolging én gezamenlijke rapportages te formuleren is afstemming in mogelijke maatregelen te verzekeren. Let wel: het gaat dan om zowel bestuurders als ambtenaren.
- Stem beveiligingsmaatregelen en beleid van gebouwen en medewerkers 'buiten' op elkaar af. Medewerkers van de gemeente werken veelal in het gemeentehuis/stadskantoor en erbuiten. Bij de mensen thuis (sociaal domein), publiek terrein, gelieerde panden, en onderweg van en naar afspraken of het werk. Belangrijk is om met het beleid en de maatregelen rekening te houden met de verschillende situaties en daar één lijn in te trekken. Veilig werken zowel in het kantoor als erbuiten. Let wel: beleid om eigen medewerkers te beschermen ("we doen altijd aangifte"), kan soms haaks lijken te staan op de-escalerend optreden ("kalmeer, ga rustig zitten, we snappen de emotie, we kijken vooruit"). Bepaal daarom uitgangspunten/grenzen in het beleid en stel een heldere norm. Communiceer deze daarna duidelijk onder medewerkers en bezoekers.
- Zorg voor de juist opvolging; preventie, handelen bij een incident en nazorg. Dreiging, escalatie, schelden, etc., het kan zowel fysiek als online plaatsvinden. Er zijn diverse stappen om hieraan te werken. Zie https://www.veiligepubliekedienstverlening.nl/ voor diverse stappen en suggesties om hier mee aan de slag te gaan. Ook staan hier uitgewerkte voorbeelden voor hoe bijvoorbeeld om te gaan met 'coronaspugen', het weigeren van een mondkapje of agressie via sociale media.

- Werk met een integrale 0-meting/analyse. Bovenstaande punten laten zien dat diverse diensten/afdeling betrokken zijn voor zowel inrichting, faciliteiten, opvolging et c. Zorg dat je als gemeente de diverse punten inzichtelijk maakt, al dan niet door een externe partij, om zo integraal te bepalen waar aanpassingen nodig zijn, maar ook waar dit mogelijk impact heeft op andere terreinen.

5.6. Leerkring 6

14 juni 2021. Thema: Terugblik en vooruitkijken. (eindproduct van de pilot)

Tijdens deze laatste leerkring hebben we met elkaar gesproken over hoe we deze pilot hebben ervaren. Wat hebben we van elkaar geleerd? En hoe kunnen we andere gemeenten helpen?

Het eindproduct van de pilot wordt – zoals gezegd in paragraaf 3 – een website met tips, tools en tricks. De website zal worden gelanceerd in oktober 2021. De website zal worden opgebouwd met een aantal bouwstenen. De globale opbouw is als volgt:

- Homepage Integrale beveiliging
- Bouwsteen Informatiebeveiliging
- Bouwsteen Fysieke beveiliging
- Bouwsteen Personele beveiliging
- Bouwsteen Awareness en draagvlak (inclusief integriteit)
- Bouwsteen Preparatie en raakvlak met incidenten- en crisismanagement
- Bouwsteen Raakvlak met continuïteit

6. Lessons learned, maar wat deden we er mee in Tiel?

Het afgelopen jaar leek alles maar om één ding te draaien: Corona. De collega's in de tien deelnemende gemeenten zagen prioriteiten verschuiven. Bijeenkomsten van de pilot gingen niet meer door, totdat er een online oplossing werd gevonden. En heel eerlijk… de pilot is minder goed uit de verf gekomen dan we hadden verwacht.

Toch bleef het werk op de verschillende thema's van de pilot niet stil liggen.

Een overzicht:

6.1. Projecten Baseline Informatieveiligheid Overheid (BIO)

Baseline Informatiebeveiliging Overheid (BIO) is één normenkader voor informatiebeveiliging voor alle overheidsorganisaties en vervangt daarmee de bestaande richtlijnen zoals de Baseline informatiebeveiliging Gemeente (BIG). Dit normenkader betekent wel een aantal veranderingen. Een belangrijke verandering is dat de rol van de bestuurder en lijnmanager ten aanzien van risicomanagement explicieter is. De BIO bestaat uit verplichte maatregelen en risico-gebaseerde maatregelen.

Wat is er tot nu toe gedaan?

Er is een analyse BIO voor de verplichte maatregelen uitgevoerd. Dit heeft geresulteerd in de definiëring van een aantal projecten voor 'grote' onderwerpen. De gemeentes hebben budget gereserveerd voor deze projecten. De overige onderwerpen die uit de analyse BIO zijn gekomen worden in de 'lijn' opgepakt door onder andere de CISO en ICT BWB.

Welke projecten zijn er voor de BIO opgestart?

1. **Opstellen beleid en procedures voor informatiebeveiliging**

Er zijn voor de BIO diverse beleidskaders en procedures rond informatiebeveiliging noodzakelijk. De huidige beleidskaders zijn gebaseerd op de BIG. De procedures dienen ook geupdate te worden. Voor de beleidskaders is BMC gevraagd om deze op te stellen. De meeste beleidskaders en procedures zullen door BWB worden getoetst.

Indien het beleidskader of de procedure ook impact heeft voor de gemeente Tiel zal de proceseigenaar gevraagd worden om deze te toetsen.

2. **Kwaliteitssysteem BIO (ISMS)**

Het ISMS is het kwaliteitssysteem voor verantwoording en verwerkingen. BWB zorgt voor de inrichting en goedkeuring van verwerkingen uitgevoerd door proceseigenaar van BWB.

De proceseigenaar van de gemeente Tiel keurt de eigen verwerkingen goed. De eerste ronde van verwerkingen start in Q2 2021. Dit houdt in dat zij in een applicatie een aantal vragen krijgen over vereisten vanuit de BIO. Per proces(onderdeel) moet dan worden aangegeven of voldaan wordt aan

de eis. Indien dat niet het geval is, dient hier een motivatie voor te worden opgegeven en een verbeterplan voor te worden opgesteld. De betrokkenen krijgen hiervoor instructie.

3. Bewaken netwerkverkeer (SIEM/SOC)

SIEM/SOC is het bewaken van activiteiten en het gedrag op de ICT-infrastructuur door KPN. Dit is afname dienstverlening via GGI-veilig (aanbesteding VNG). BWB verzorgt de inrichting en het beheer.

Het doel van de inrichting van SIEM/SOC is dat malafide activiteiten en/of dreigingen op het netwerk gemonitord worden en in een vroeg stadium kunnen worden afgewend.

Er is geen impact voor de gemeente Tiel.

4. Beheren (zakelijke) telefoons en tablets / mobile device managementMDM)

Een MDM-oplossing moet leiden tot het in control te komen voor het beheer van de apparaten (smartphones en tablets (iOS en Android)) van BWB en de gemeente Tiel, Culemborg en West Betuwe. Dit zijn op dit moment 750 smartphones (Android) en 223 tablets (142 iOS en 81 Android).

Dit beheer betreft het zorgen voor ondersteuning van updates, wachtwoorden etc. In het project MDM zal deze ondersteuning worden ingericht.

Er is voor gekozen om te beginnen met de zakelijke telefoons en tablets. Daarbij is gekozen voor een gefaseerde invoer, beginnend met BWB (pilot en eerste uitrol), daarna volgen de gemeentes (de ambtelijke organisatie). De projectmanager zal nog een advies opstellen of en zo ja, hoe B&W en de gemeenteraad in de vervolgfase meegenomen kunnen worden.

Impact voor de medewerkers van de gemeente Tiel is dat er wijzigingen op de zakelijke telefoons en tablets doorgevoerd gaan worden. Welke dit precies zijn, wordt tijdens de inrichting bepaald en naar de medewerkers gecommuniceerd.

In Q1-Q2 worden ook afspraken maken over de apparaten welke vallen onder de bring your own device (BYOD) regeling en het beheer van de apps van BWB in een zakelijk deel van de privé telefoons. Deze zijn nog geen onderdeel van de invoering van MDM.

5. Toegangsadministratie netwerk en applicaties / identity access management (IAM)

Een IAM-oplossing moet leiden tot het in control te komen voor toegang en autorisatie voor medewerkers. Deze moet de in-, door-, en uitstroom processen ondersteunen en (via Topdesk) ondersteuning bieden voor het wijzigen van toegang en autorisaties tot applicaties. Gekozen is om de huidige oplossing met AFAS en Topdesk uit te breiden.

Impact voor de gemeente Tiel is dat de functioneel applicatiebeheerders van de gemeente Tiel ondersteunt worden bij de in-, door- en uitstroom van medewerkers.

6. Bedrijfscontinuïteitsbeheer (BCM)

Een BCM plan beschrijft hoe de kritieke diensten worden geleverd in geval van een ramp (op het gebied van ICT en informatiebeveiliging). Dit plan wordt opgesteld voor de kritische ICT processen en ICT applicaties.

Indien de kritische ICT processen en ICT applicaties ook voor gemeente Tiel gelden zullen de proceseigenaren en applicatiebeheerders meegenomen worden in het BCM plan.

6.2. Werkgroep privacy- en informatieveiligheid

De Algemene Verordening Gegevensbescherming (AVG) trad in werking op 25 mei 2018. Dat betekent dat er vanaf die datum in de hele Europese Unie (EU) dezelfde privacywetgeving geldt. De Wet bescherming persoonsgegevens (Wbp) geldt niet meer.

Een belangrijke eis in de AVG is dat de gemeente de naleving van privacyregels op *aantoonbare* wijze borgt en daarover *verantwoording* aflegt. Dit betekent onder meer dat hiervoor processen ingeregeld moeten zijn en dat de benodigde documentatie aanwezig is. Dit wordt ook wel privacymanagement genoemd en dit dient blijvend te worden onderhouden. Alle documentatie tezamen wordt hier verder de privacy en informatieveiligheid administratie (PIVA) genoemd. Uit deze administratie dient de opzet (beleid, ontwerp), het bestaan (de implementatie) en de effectieve werking van de beheersmaatregelen te blijken.

De gemeente dient haar bedrijfsvoering in overeenstemming te hebben met de verplichtingen die voortvloeien uit de AVG. Het niet of deels voldoen aan de AVG kan grote gevolgen hebben voor de gemeente in termen van reputatieschade, boetes en schadeclaims. Dat niet alles op korte termijn gerealiseerd kan worden komt doordat de gemeente opereert in een omvangrijke en complexe omgeving. Er is tijd nodig om als organisatie te wennen aan nieuwe dan wel aangescherpte procedures, richtlijnen en regels en sommige zaken zoals de onderbouwingen van het verwerkingsregister (werkprocessen) en Data Protection Impact Assessments (DPIA's) vergen veel capaciteit.

In 2020 is de werkgroep Privacy- en informatieveiligheid opgericht. Deze bestaat uit de Functionaris Gegevensbescherming (BVOWB), de Privacy Officer, en enkele Privacybeheerders.

In het werkplan privacy 2020 – 2021 zijn de activiteiten opgenomen die in de komende periode nodig zijn om op een aantoonbare wijze naleving van de privacywetgeving te borgen binnen de gemeente Tiel.

Het doel van dit werkplan is drieledig:

- Implementeren van een Privacy Control Framework (PCF) dat de criteria van de AVG vertaalt naar een kwaliteitscyclus voor gegevenbescherming en privacy. Zo ontstaat een beeld van wat de organisatie al gedaan heeft en wat nog moet gebeuren om aantoonbaar aan de AVG te voldoen;
- Cyclisch evalueren en daar waar nodig verbeteren van de zaken die inmiddels zijn gerealiseerd;
- Implementeren van maatregelen die nog genomen moeten worden om geheel te kunnen voldoen aan de AVG. Dit kunnen ook zaken zijn die gemeentebreed meerdere jaren omvatten. Nadat dit voor enkele processen / voor enkele teams is gedaan ligt het in de bedoeling om de overige processen middels de verbeterplannen in de kwaliteitscyclus (Plan-Do-Check-Act) op te pakken.

Het streven is om de borging van privacy uiteindelijk onder te brengen in de bestaande Planning & Control (P&C) cyclus.

Naast het werkplan heeft de werkgroep de volgende producten opgeleverd:

- Privacy governancestructuur
- Taakverdeling privacybeheerders en privacyofficer
- Register van verwerkingen (lopend proces)
- Standaard model DPIA
- Procedure Datalek met toelichting

Binnen de verschillende domeinen is een eerste start gemaakt met het vullen van het register van verwerkingen en het opstellen van de DPIA's (bijvoorbeeld cameratoezicht in de publieke ruimte en het IGP).

6.3. Bewustwording

Een van de belangrijke pijlers in de pilot is bewustwording. Dat geldt voor zowel personeelsleden (intern en extern), raadsleden als ook de bestuurders. Het is een continu-proces. Veel plannen, procedures en protocollen vallen of staan met de naleving ervan.

In de afgelopen periode is een aantal berichten verschenen op JIP.

6.3.1. Aandacht voor phishingmails door het versturen van een nep-mail

Boodschap: hoe herken je een phishing mail?

De oude phishing mails in gebrekkig Engels zijn vaak makkelijk te herkennen. Tegenwoordig zijn phishing mails ook heel vernuftig waardoor ze slecht herkenbaar zijn als spam. Het afzend e-mailadres kan zelfs worden nagemaakt waardoor het lijkt alsof het van een vertrouwde afzender komt. Er zijn wel zaken waar je een phishing mail mogelijk aan kan herkennen:

• Verwacht je een mail van de afzender?

• Is de inhoud logisch?

• Zit er tijdsdruk in de mail (klik op deze link voor datum x)? Dat is vaak een teken dat het spam betreft.

Bij twijfel, nergens op klikken maar eerst verifiëren of de afzender daadwerkelijk is wie hij zegt te zijn. Dit kun je doen door via een ander medium (zoals de telefoon) contact te zoeken om te vragen of de mail van hem afkomstig is.

6.3.2. Verplichte E-learnings

De afgeslopen periode is er een aantal verplichte E-learnings beschikbaar gesteld. De laatste was medio december 2020.

6.3.3. Veilig mailen

Sinds medio 2020 is SmartLockr geïntroduceerd. Met deze applicatie kunnen medewerkers van Tiel op een beveiligde manier mailen. Via JIP werd een handleiding en instructiefilmpje beschikbaar gesteld.

6.3.4. Scherm vergrendelen

Aandacht op JIP voor het vergrendelen van je PC scherm.

Boodschap: Ga je even weg van je werkplek? Lock dan je computer met de toetsencombinatie “windowsknop” + “L”.

6.3.5. AVG

Vanuit de werkgroep privacy- en informatiebeveiliging is een aantal berichten geplaatst op JIP. Daarin werd aandacht gevraagd voor het doel en belang van de AVG.

6.4. Veilig en integer werken

Dit protocol is onderdeel van het grotere arbobeleidsplan van de gemeente Tiel en is (met instemming van OR) vastgesteld in 2019. Het beschrijft de norm (NOMA, Niet Omgaan Met Agressie) en beschrijft preventieve maatregelen om wangedrag te voorkomen.

Het protocol bevat maatregelen en procedures bij wangedrag zoals voorbeeldbrieven voor een gebouwontzegging. Hier zitten ook instructies voor medewerkers bij (ook voor verdachte omstandigheden/pakketjes)

In 2019 is iedereen binnen de gemeente Tiel opgeleid conform dit protocol. De volgende opleidingen zijn gegeven:

- Themabijeenkomst: voor alle medewerkers en bestuurders;
- Kernprogramma: per team;
- Locatietraining (balie, spreekkamer en locatie): Medewerkers in de publieke dienstverlening;
- Ordegesprekken: Voor leidinggevenden en medewerkers met mandaat om ordegesprekken te voeren.

Conform het arbobeleidsplan (waar dit protocol onderdeel van is) worden deze trainingen en opleidingen 1x per 3 jaar herhaald. Voor nu betekent dat dat in 2022 dit traject weer wordt doorlopen. Hiervoor is geld gereserveerd in de begroting van Tiel (Arbobudget).

6.4.1. Aantal agressie incidenten 2020

Bijna wekelijks vinden gevallen van ongewenst/intimiderend gedrag plaats. In 2020 hebben vier serieuze agressie incidenten plaatsgevonden. Al deze gevallen vonden plaats bij de frontoffice. Er zijn geen gewonden gevallen.
De manager van het team frontoffice heeft deze meldingen opgepakt en afgehandeld. Er is tevens een agressieprotocol aanwezig.

6.5. BHV

Hierin werken we samen met Werkzaak en UWV. Er is één plan voor de hele Stadhuiscampus. Vanwege het thuiswerken in 2020 tot en met nu zijn de volgende acties ondernomen:

6.5.1. Introductie software programma Multibel halverwege 2020

MultiBel is een automatisch oproepsysteem (via mobiel, tablet en pc) waarmee snel en eenvoudig een groep personen wordt gealameerd bij incidenten, calamiteiten, storingen en crisis. Een snelle en effectieve alarmering bespaart tijd, beperkt de vervolgschade en zorgt voor continuïteit.

6.5.2. Uitstellen van ontruimingsoefeningen

Voor 2020 zijn vanwege de coronamaatregelen de oefeningen uitgesteld. In overleg met de gemeentesecretaris is deze naar eind 2021 verplaatst vanwege aanhoudende coronamaatregelen.

Opleidingen hebben plaatsgevonden door middel van e-learning. Alle bhv'ers zijn momenteel bij met de trainingen en opleidingen.

6.5.3. Samenwerking met Culemborg en West Betuwe

BHV coördinatoren en het hoofd BHV hebben maandelijks overleg om activiteiten af te stemmen voor verhoogde efficiëntie en effectiviteit van beide BHV organisaties.

Verder is er een hoofd BHV bijgekomen die de verantwoordelijkheid zal dragen voor Tiel. Voorheen was er een gedeeld hoofd BHV voor zowel Tiel als Culemborg.

6.5.4. Alarmknopprocedures:

Enkele overlegruimten op de begane grond zijn uitgerust met een alarmeerknop in geval van een incident. Deze staan in verbinding met de receptie waar te allen tijde een beveiliger (ingehuurd via securitas) aanwezig is. Deze loopt ook regelmatig langs de betreffende ruimtes ter controle.

6.6. Fysieke beveiliging

Het toegangscontrole systeem van de gemeente is toe aan vervanging, dit geldt niet alleen voor gemeente Tiel maar ook voor gemeenten Culemborg en West Betuwe. Deze aanbesteding wordt dan ook vanuit inkoop en facilitaire zaken als een gecombineerde aanbesteding aangevlogen.

Momenteel loopt een selectieprocedure van de zoektocht naar een geschikte veiligheidsadviseur (selectie tussen 3 partijen) omdat de benodigde specialistische kennis niet in onze organisatie aanwezig is. Deze gaat ons dan ook meenemen in onze adviesvragen zoals wat er speelt in de markt, toekomstbestendigheid, knelpunten, etc.

Als deze is geselecteerd dan zal deze gaan inventariseren (locaties/systemen/wensen van de partijen) en dan ons uiteindelijk begeleiden in het aanbestedingstraject.

6.7. Eindproducten van de pilot

Zoals gesteld onder paragraaf 3 zal het eindproduct van de pilot/leerkringen een website zijn met tools, tricks en best practices.

6.7.1. Weerbareoverheid.pleio.nl

Het eindproduct van de pilot zal te vinden zijn op Pleio. Dit is een beveiligde omgeving waar deelnemende gemeenten hun ervaringen kunnen delen. De website zal gereed zijn in oktober 2021.

6.7.2. Visie en governance integrale beveiliging

Naast de website is er ook gewerkt aan een tweetal documenten om gemeenten te helpen met het vaststellen van een strategisch kader en een governance (kwaliteitssysteem).

Bij deze voortgangsrapportage zijn de volgende documenten gevoegd:

- Instructiedocument voor het uitwerken en vaststellen van het strategisch kader voor integraal beveiligingsbeleid voor gemeenten (visie, beveiligingsdoelen, uitgangspunten en kwaliteitsborging) (januari 2021)
- Instructiedocument voor governance en kwaliteitssysteem van integrale beveiliging gemeenten (januari 2021)

Deze documenten zijn nog in de status ‘concept’. Bij de lancering van de website (oktober) zullen de definitieve versies worden toegevoegd (actie COT).

6.8 Evaluatie van de pilot

Na anderhalf jaar zijn we aan het einde gekomen van deze pilotfase. Het COT heeft een vragenlijst opgesteld ter evaluatie van de pilot. De vragenlijst dient ter verantwoording aan de ministeries van BZK en J&V.

De vragen in deze 1-meting gaan in op de volgende onderdelen:

- Huidige inzichten en ontwikkelingen integrale beveiliging.
- Integrale thema’s en bouwstenen, zoals risico inventarisatie, gedrag, organisatiestructuur, samenwerking, draagvlak en lerend vermogen.
- Evaluatie pilot(proces) en eindproduct.

7. Relevante documenten

Over de thema's weerbare overheid en ondermijning zijn al protocollen en rapportages aanwezig.

A. Protocol integer en veilig werken
   Dit protocol is opgesteld door de BVOWB. Het beschrijft de norm (NOMA, Niet Omgaan Met Agressie) en beschrijft preventieve maatregelen om wangedrag te voorkomen. Tenslotte bevat het protocol procedures bij wangedrag zoals voorbeeldbrieven voor een gebouwontzegging.
B. Programma Veilige Publieke Taak Tiel (2016)
   Beschrijft de rol van de gemeente bij het programma VPT. Drie opzichten: als werkgever, publieke ambtsdragers en als regisseur veiligheid.
C. Ondermijningsbeeld Tiel
   Het RIEC leverde medio 2019 het ondermijningsbeeld op. In het rapport werd een aantal aanbevelingen gedaan. Het college nam deze aanbevelingen over.

8. Bijlagen

- Instructiedocument visie integrale beveiliging (conceptversie 28 januari 2021)
- Instructiedocument governance integrale beveiliging (conceptversie 28 januari 2021