Rapport van Bevindingen

ICT-situatie

Voorwoord

Op 1 december 2020 is de gemeente Hof van Twente getroffen door een grote computerhack. Onze systemen en data werden vernietigd en back-ups werden door versleuteling ontoegankelijk gemaakt door derden. De impact is enorm en zonder overdrijven kan worden gesproken over een crisis.

Als gevolg van deze crisis heeft de gemeentelijke dienstverlening een aantal dagen stil gelegen. Binnen enkele dagen konden de eerste kritische bedrijfsprocessen weer worden opgestart. Ook na het hervatten van deze dienstverlening kost de wederopbouw van de basisinfrastructuur en data veel tijd en geld.

Vanzelfsprekend moet ook de vraag worden beantwoord hoe dit heeft kunnen gebeuren en op welke wijze de gemeente heeft gehandeld. Ons College heeft aan het begin van de crisis een forensisch cybersecurity specialist opdracht gegeven om hier onafhankelijk onderzoek naar te verrichten, te weten NFIR (Nederlands Forensisch Incident Response). Tevens is het onafhankelijk bureau De Winter Information Solutions gevraagd de gebeurtenissen alsmede de wijze waarop de crisis is aangepakt te duiden. Deze rapporten worden in de loop van het eerste kwartaal van 2021 verwacht.

Daarnaast hebben wij vanuit onze overtuiging een lerende organisatie te zijn vanzelfsprekend ook zelf geëvalueerd. Wij hebben in samenspraak met de operationeel leider van de Veiligheidsregio Twente en de onafhankelijke ICT deskundige van de gemeente Rotterdam hiervoor het voorliggende Rapport van Bevindingen opgesteld. Daarbij staat de volgende vraag centraal:
‘*Op welke wijze heeft de gemeente Hof van Twente voorafgaand aan en tijdens de crisis gewerkt, welke ‘lessen’ kunnen hieruit worden getrokken en hoe vindt de opbouw plaats?*’

Het voorliggende rapport bevat een beschrijving van werkwijzen en inzichten. Deze inzichten vormen de basis voor een routekaart, maar staan niet op zichzelf. Na ontvangst van de hiervoor genoemde rapporten wordt bekeken of en, zo ja, op welke wijze onze aanbevelingen aanvulling behoeven.

Het belangrijkste doel van het voorliggende rapport is om - aanvullend op de hiervoor genoemde rapporten - verantwoording af te leggen en hiervan te leren. Maar het belang is breder. De gevaren van een computer hack zijn groot. Deskundigen zeggen dat het iedereen kan overkomen: ‘hackers komen altijd binnen ...’ Bij ons werd dat werkelijkheid. Vooralsnog zijn er geen aanwijzingen dat er data buit is gemaakt. Echter, het vernietigen van data en de gijzeling van de back-ups heeft enorme gevolgen voor de gemeentelijke bedrijfsvoering. Met transparantie als uitgangspunt, voelen wij het als onze verantwoordelijkheid om deze ‘lessons learned’ te delen. Te delen omdat onze inzichten voor heel bestuurlijk Nederland van belang zijn.

Goor, 9 maart 2021

drs. H.A.M. Nauta-van Moorsel MPM
burgemeester

drs. D. Lacroix
gemeentesecretaris

Inhoudsopgave

Voorwoord 3

Inhoudsopgave 4

0 Managementsamenvatting 5
1 Inleiding 6
2 Context en achtergrond 7
3 De hack 10
4 Project 'Opbouw en Reconstructie 15

Bijlagen
- **Bijlage 1 - Raadsbrief zelfevaluatie informatieveiligheid** 18
- **Bijlage 2 - Informatievoorziening gemeenteraad** 21

0. Managementsamenvatting

In het voorliggende rapport staat de volgende vraag centraal '*Op welke wijze heeft de gemeente Hof van Twente voorafgaand aan en tijdens de crisis gewerkt, welke 'lessen' kunnen hieruit worden getrokken en hoe vindt de opbouw plaats?*'

Afgelopen jaren heeft Hof van Twente veel geïnvesteerd in ICT en Informatieveiligheid. Om de kwetsbaarheid en kwaliteit structureel op een hoger niveau te brengen is het netwerk- en systeembeheer uitbesteed aan een professionele marktpartij. Op het gebied van informatieveiligheid is planmatig gewerkt aan het op orde brengen van processen en wet- en regelgeving. Medewerkers zijn getraind en er is formatie vrijgemaakt binnen bijvoorbeeld I&A, CISO en FG.

Deze constatering wordt niet gedaan om daarmee vast te stellen dat de gemeente het allemaal goed heeft gedaan. Ook in Hof van Twente kunnen en moeten zaken worden verbeterd. Echter, er is meer dan serieus 'werk gemaakt' van deze beleidsterreinen en er was geen indicatie dat de gemeente zaken niet op orde had.

Desondanks vond een hack plaats in Hof van Twente. De impact is niet voor te stellen. Digitale veiligheid is niet alleen een ICT-aangelegenheid, maar raakt de gehele gemeente. Hof van Twente is niet uniek. Deskundigen geven aan dat zoiets iedereen kan overkomen. Ook bestuurlijk is hiervoor steeds meer aandacht. '*Wat in Hof van Twente is gebeurd, kan iedereen overkomen*', zegt burgemeester Weerwind van Almere, tevens voorzitter van de VNG Commissie Informatiesamenleving.

Dat maakt dat Hof van Twente hiervan wil en moet leren, evenals de 355 gemeenten in Nederland. In het voorliggende rapport wordt hiervoor een aanzet gedaan en dit wordt nog aangevuld met de resultaten van de onderzoeksrapporten van NFIR en De Winter Information Solutions.

Gedurende de hack is gewerkt met een crisisorganisatie, waarin snel is opgeschaald en continue is meebewogen met de actuele stand van zaken. Er is gekozen voor een structuur die is gebaseerd op de crisisorganisatie van de Veiligheidsregio Twente onder GRIP 3. Door te werken met heldere en bekende rollen en structuren ontstond rust en overzicht. Dit heeft goed gewerkt. Ook het werken met een hiervoor opgeleide operationeel leider verdient navolging.

Verder is het van belang een specifiek 'digitale incidentenbestrijdingsplan' op te stellen, inclusief het 'lijstje op de gasmeter' waarop de gegevens van de gespecialiseerde bureau's staan vermeld. Het periodiek oefenen en de beschikbaarheid van voldoende budget vloeien hieruit voort.

Tot slot dient het gesprek te worden geïntensiveerd over de mate waarin gemeenten zijn voorbereid op een cyberaanval, welke expertise op dat moment nodig is en op welke wijze deze kan worden gemobiliseerd. De VNG speelt hierin een belangrijke rol. Daarbij dient ook te worden ingegaan op huidige rol/opdracht van de IBD en de mate waarin deze aansluit bij de behoefte van gemeenten wanneer zij te maken krijgen met een ingrijpende digitale calamiteit.

1. Inleiding

In dit rapport staat de volgende vraag centraal: '*Op welke wijze heeft de gemeente Hof van Twente voorafgaand aan en tijdens de crisis gewerkt, welke 'lessen' kunnen hieruit worden getrokken en hoe vindt de opbouw plaats?*'

Het is een brede vraag die een afbakening vereist in breedte en diepte. Hiervoor wordt gebruik gemaakt van het drieluik: verleden, heden en toekomst. In hoofdstuk 2 wordt het beeld geschetst van de wijze waarop de gemeente de afgelopen jaren zowel inhoudelijk als organisatorisch vorm heeft gegeven aan Informatisering & Automatisering alsmede Informatieveiligheid. Dit beeld vormt immers de context waarbinnen deze crisis heeft plaatsgevonden. Vervolgens wordt in hoofdstuk 3 beschreven op welke wijze de gemeente was voorbereid op deze crisis, voor welke aanpak is gekozen en welke inzichten daarbij zijn ontstaan. In het laatste hoofdstuk van het drieluik, hoofdstuk 4, wordt een doorkijk gegeven in de wijze waarop de wederopbouw plaatsvindt.

Tot slot wordt in hoofdstuk 5 een samenvatting gegeven van de gebeurtenissen en inzichten. Deze inzichten vormen het vertrekpunt voor een routekaart en worden op basis van de uitkomsten van de rapporten van het NFIR en De Winter Information Solutions verder aangevuld/aangescherpt.

2. Context en achtergrond

2.1. Inleiding

In dit hoofdstuk 2 wordt het beeld geschetst van de wijze waarop de gemeente de afgelopen jaren zowel inhoudelijk als organisatorisch vorm heeft gegeven aan Informatisering & Automatisering alsmede Informatieveiligheid. Dit beeld vormt de context waarbinnen deze crisis heeft plaats-gevonden.

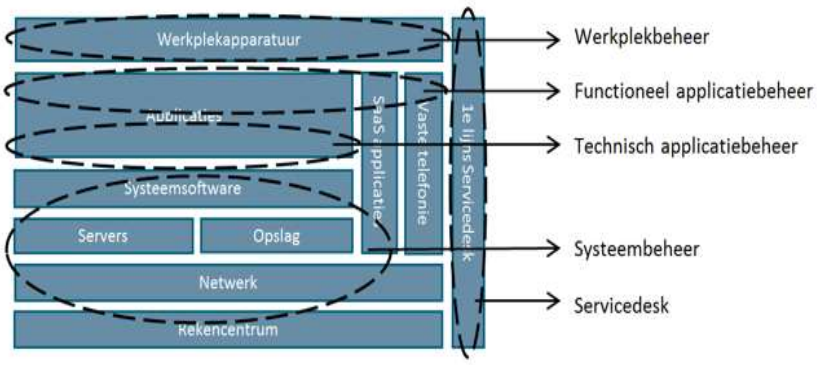
2.2. Informatisering & Automatisering

In 2014 is gestart met een fundamentele discussie over het ambitieniveau en de wijze waarop Hof van Twente haar ICT-taken vorm en inhoud geeft. In dat kader is onderzoek gedaan naar de mate waarin de gemeente in staat is om het volledige ICT-taakpakket zelfstandig uit te (blijven) voeren en in hoeverre intergemeentelijke samenwerking hiervoor een oplossing bood. Tevens ontstond op dat moment het inzicht op basis van benchmark-onderzoek dat de gemeente substantieel minder uitgeeft aan ICT dan gemiddeld. Hiervoor werd een I&A-visie ontwikkeld. Dit heeft ertoe geleid dat het College de Gemeenteraad heeft voorgesteld om vanaf 2017 extra financiële middelen beschikbaar te stellen. De Gemeenteraad heeft structureel €375.000 per jaar en incidenteel €850.000 voor een periode van 3 jaar beschikbaar gesteld.

In 2019 is opnieuw kritisch gekeken naar de ontwikkelingen op het gebied van digitalisering, de ambities op dit onderdeel en de beschikbare middelen. Er werd geconcludeerd dat deze niet in balans waren. Hiervoor is een Agenda Digitalisering opgesteld waarvoor de raad met ingang van 2020 voor 4 jaar een krediet van €1,3 mln. beschikbaar heeft gesteld. De Agenda Digitalisering is een combinatie van activiteiten. Deels om 'bij te blijven' bij de ontwikkelingen en deels om op specifieke onderdelen een stap extra te zetten. In de Agenda Digitalisering staan de volgende 3 pijlers centraal:

- Integrale digitale dienstverlening en bedrijfsvoering, inclusief 'Basis op Orde';
- Informatie-gestuurde organisatie (datagedreven werken);
- Informatieveiligheid.

Parallel hieraan is afgelopen jaren onderzocht op welke wijze de taken worden uitgevoerd om de zogenoemde 3K's (meer Kwaliteit, minder Kwetsbaarheid en lagere Kosten) structureel te verbeteren en borgen. Dit proces is destijds begeleid door M&I adviesbureau en leidde tot het inzicht dat uit-besteding aan een professionele marktpartij noodzakelijk was, om het systeembeheer op een hoger plan te tillen. In 2017 heeft het college besloten het systeembeheer in het algemeen uit te besteden voor een periode van 3 jaar.



Op basis van de eerste ervaringen met de uitbesteding en in het verlengde van het generieke organisatie-ontwikkeltraject, is binnen het team I&A in 2020 een specifiek ontwikkeltraject gestart. Dit ontwikkeltraject is erop gericht om de organisatie en kennis, kunde en vaardigheden adequaat te laten aansluiten op de ambities.

Op basis van een analyse van de I&A-organisatie was reeds begonnen met een doorontwikkeling op strategisch en tactisch niveau. Belangrijk aandachtspunt was en is de wijze waarop de aansturing en het opdrachtgeverschap is ingevuld gekoppeld aan de manier waarop de externe marktpartij haar opdracht invult. Het systeembeheer is immers uitbesteed aan deze marktpartij omdat de gemeente zelf niet over voldoende professionaliteit beschikt in termen van kwaliteit en capaciteit. De afhankelijkheid van deze marktpartij is daarmee groot en vraagt om een goede regievoering. In verband met de juridische positie en belangen van de gemeente wordt hier niet verder ingegaan op de relatie met de betreffende marktpartij.

2.3. Informatieveiligheid en gegevensbescherming

Informatieveiligheid en gegevensbescherming heeft de afgelopen jaren in Nederland steeds meer aandacht gekregen. Vanaf 2014 is de gemeente gestart met de eerste BIG-analyses, het opstellen van beleid en de benoeming van een CISO. De invoering van de Algemene verordening gegevens-bescherming (AVG) per 28 mei 2018 heeft hieraan een extra impuls gegevens. Ook in Hof van Twente.

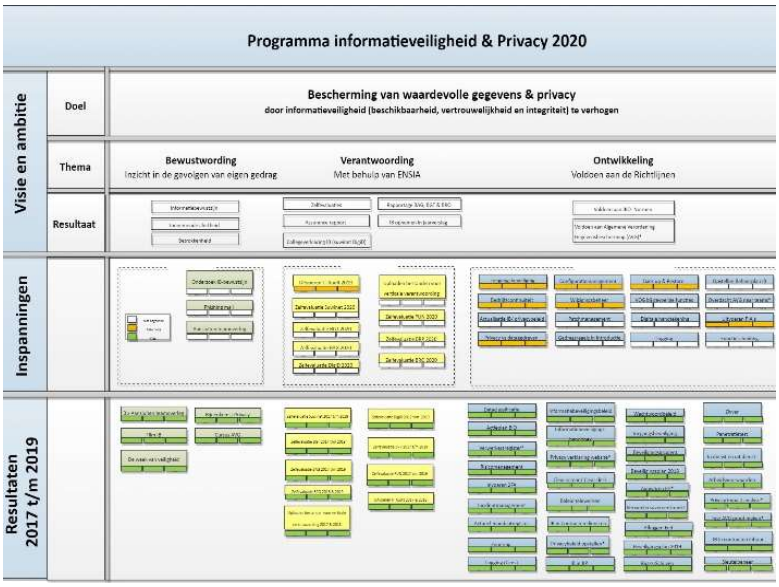
Naast de AVG moet de gemeente vanaf 1 januari 2020 voldoen aan de Baseline Informatie-beveiliging Overheid (BIO). De BIO is de opvolger van de Baseline Informatiebeveiliging Gemeenten (BIG) en biedt een gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid.

Om te voldoen aan de wettelijke vereisten en de informatieveiligheid en gegevensbescherming structureel op een hoger niveau te brengen is in Hof van Twente in 2017 een jaarlijks programma rondom informatieveiligheid gestart. In dit programma is met behulp van jaarplannen een PDCA-cyclus[1] gecreëerd, waarbij de volgende drie programmalijnen centraal staan:

a. Bewustwording
b. Ontwikkeling
c. Verantwoording

Ad a. Bewustwording

Belangrijk onderdeel van informatieveiligheid is de bewustwording, training en coaching van de medewerkers in de ambtelijke organisatie. Doel was / is om de medewerkers bewust te maken van de risico's en te leren hoe hiermee om te gaan. Kortom de digitaal vaardige en veilige medewerker. In dat kader zijn afgelopen jaren verschillende activiteiten uitgevoerd, zoals personeelsbijeenkomsten, trainingen, filmpjes, phishing-mailing, etcetera.



Ad b. Ontwikkeling

Binnen deze programmalijn is wet- en regelgeving vertaald en geïmplementeerd. Processen en geautomatiseerde systemen zijn aangepast om te voldoen aan de eisen die hieraan worden gesteld.

Ad c. Verantwoording

Belangrijk onderdeel van informatie-veiligheid wordt gevormd door uiteen-lopende, veelal wettelijk verplichte, audits en zelfevaluaties om inzicht te krijgen in de mate waarin wordt voldaan aan diverse nomen. Met behulp van deze audits verantwoorden gemeenten zich over informatiebeveiliging en -kwaliteit met behulp van een Eenduidige Normatiek Single Information Audit (ENSIA). Ook in Hof van Twente zijn deze audits periodiek uitgevoerd en hierover heeft het college jaarlijks verantwoording afgelegd aan de raad. In bijlage 1 is de raadsbrief d.d. 17 maart 2020 bijgevoegd.

Naast deze wettelijk verplichte audits is medio 2020 een zogenoemde penetratietest (pentest) uit-gevoerd door een onafhankelijk bureau. Daarbij hebben ethical hackers de gemeentelijke systemen onderzocht om inzicht te krijgen in de risico's en kwetsbaarheden en geadviseerd over de verbeteringen die gericht kunnen worden doorgevoerd. Deze pentest maakt ook onderdeel uit van het jaarplan Informatieveiligheid. Wij gaan er vanuit dat in het rapport van NFIR hierop nader wordt ingegaan.

[1] PDCA-cyclus staat voor plan-do-check-act

2.4. Duiding

Digitalisering

Afgelopen jaren is er binnen Hof van Twente meer aandacht gekomen voor digitalisering. Alhoewel de gemeentelijke investeringen op basis van een recente benchmark nog steeds onder het gemiddelde liggen, is op ambitieniveau, organisatie en financiën een inhaalslag gemaakt.

Vanuit de overtuiging dat Hof van Twente steeds meer een 'ICT-bedrijf met gemeente-licentie' wordt, is het van belang de ingezette koers, momenteel verwoord in de Agenda Digitalisering, voort te zetten, te versnellen en aan te vullen met de specifieke inzichten vanuit de hack. In dat kader vraagt dit uitgangspunt verdere uitwerking.

Informatieveiligheid

De afgelopen jaren is planmatig gewerkt om de informatieveiligheid en gegevensbescherming op het gebied van beleid, processen en mensen op een hoger niveau te tillen. Formele regelingen zoals verordeningen, beleidsregels en een verwerkingenregister zijn opgesteld of geactualiseerd, trainingen zijn georganiseerd en de personele bezetting werd op orde gebracht door de benoeming van een Chief Information Security Officer (CISO) en een Functionaris Gegevensbescherming (FG)[2]. Tot slot heeft de gemeente diverse - doorgaans wettelijke verplichte - zelfevaluaties, audits en een pentest uitgevoerd om inzicht te krijgen en de behaalde resultaten en de ontwikkelpunten voor het jaar daarop. Daarmee is de basis gelegd voor een goede uitvoering. Er wordt aanbevolen om de 'lessons learned' te verankeren in het jaarplan 2021-2022 en daarbij bijzondere aandacht te besteden aan een organisatiebreed trainingsprogramma. Het is belangrijk om de bewustwording, opgedane inzichten en kennis te borgen en, waar nodig, te verbeteren.

[2] De CISO is verantwoordelijk voor het informatiebeveiligingsbeleid. Dit betreft zowel het implementeren van beleid als het toezicht houden op de uitvoering ervan. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de Algemene verordening gegevensbescherming (AVG).

3. De hack

3.1. Inleiding

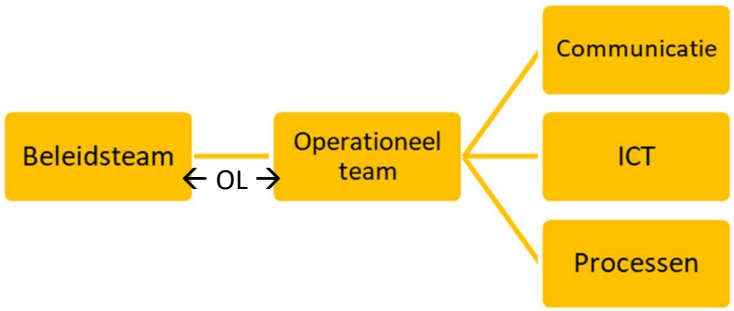
In dit hoofdstuk wordt beschreven op welke wijze de gemeente was voorbereid op deze crisis, voor welke aanpak is gekozen en welke inzichten daarbij zijn ontstaan.

3.2. Crisisorganisatie

Op 1 december 2020 is direct na het constateren van de problemen het Bedrijfscontinuïteitsplan[3] in werking getreden en is gewerkt met een crisisorganisatie. Daarbij is intern, ambtelijk en bestuurlijk, en extern, met de systeembeheerder, opgeschaald. Ook daarna heeft verdere opschaling plaatsgevonden met gemeenten uit de regio (o.a. Enschede en Oldenzaal), Veiligheidsregio Twente en diverse externe deskundigen van bijvoorbeeld NFIR, de heer De Winter, de gemeente Rotterdam en de politie. Daarbij handelde de gemeente in overleg met de IBD. De Crisisorganisatie heeft continue meebewogen met de actuele stand van zaken en kende vanaf het begin drie tafels:

- een tafel Kritische Bedrijfsprocessen.
- een tafel ICT
- een tafel Communicatie

Tot medio januari is gekozen voor deze structuur die verder volledig is gebaseerd op de crisisorganisatie van de Veiligheidsregio Twente onder GRIP 3 en waarmee we in Twente veelvuldig hebben geoefend. Dat wil zeggen met een Beleids- en een Operationeel team en een Operationeel Leider (OL) die tussen beide teams opereert.



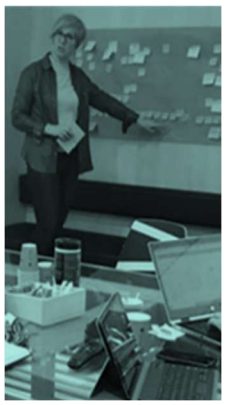
Daarbij is gebruik gemaakt van de ‘Handreiking Cybergevolgbestrijding G4 gemeenten’ uit mei 2020 en de rapporten op de site van de gemeente Lochem naar aanleiding van de cyberaanval die hen trof in juni 2019. Inmiddels heeft deze structuur plaatsgemaakt voor een projectorganisatie die is gericht op herstel en opbouw van de gemeentelijke ICT.

Beleidsteam

Het beleidsteam was verantwoordelijk voor de bestuurlijke aansturing van de tafels en het nemen van de besluiten over de vragen/voorstellen/adviezen welke door de OL vanuit de verschillende tafels werden voorgelegd. De burgemeester en gemeentesecretaris verzorgden tevens de noodzakelijke bestuurlijke en ambtelijke opschaling, bijvoorbeeld naar de minister en CdK alsmede naar leveranciers. Deze communicatie werd al in de eerste crisisweek opgepakt.

[3] Vastgesteld door het College op 04 februari 2020.

Tafel Bedrijfskritische processen



Belangrijkste uitgangspunt was het hervatten van de dienstverlening. Als basis hiervoor is gebruik gemaakt van het gemeentelijk Bedrijfscontinuïteitsplan, waarin alle gemeentelijke dienstverleningsprocessen zijn geïnventariseerd en gecategoriseerd. Dit plan heeft de gemeente in staat gesteld om gestructureerd te werken aan de meest kritische bedrijfsprocessen en de dienstverlening op deze cruciale onderdelen weer op te starten. Zo konden op 04 december 2020 de geplande voorschotten van de uitkeringen worden betaald. Feitelijk was binnen 10 dagen de meest kritische dienstverlening weer in de lucht. Dat neemt niet weg dat 'achter de schermen' er een nieuw netwerk moet worden gebouwd, ingericht en gevuld. Volgens deskundigen neemt dit een half jaar tot twee jaar in beslag.

In dit verband zijn Burgerzaken, Werk & inkomen, Zorg, Financiën en Archief zwaar getroffen. Binnen deze onderdelen werd gewerkt met applicaties die op de servers stonden. Voor Burgerzaken zijn de noodzakelijke processen met een noodvoorziening weer in de lucht. Daardoor konden ook de voorbereidingen van de verkiezingen worden opgepakt te samen met onze partners. De betaalprocessen van Financiën (facturen), uitkeringen Werk & Inkomen, facturen van zorgaanbieders WMO en Jeugd, worden via een zogenaamde work-around (vooral handmatig) uitgevoerd. Aanvragen op gebied van Werk & Inkomen, WMO en Jeugd worden in behandeling genomen en daar waar geen systeem meer is voor afhandeling, worden aanvragen voorlopig of met een voorschot afgehandeld.

Tafel ICT

Vanaf het begin lag de hoogste prioriteit bij het voortzetten en weer op gang brengen van de gemeentelijke dienstverlening. De ICT tafel is verantwoordelijk voor het faciliteren hiervan. Zowel intern als bij de externe dienstverlener zijn direct na het ontdekken van de problemen met de hoogste urgentie ICT-teams samengesteld. De nadruk lag op dat moment op de volgende onderdelen:

- Het veiligstellen van netwerk en systemen
- Het verkrijgen van inzicht in de aard en ernst van de problemen
- Onderzoek naar mogelijkheden data-recovery door gespecialiseerd bureau uit Zweden[4]
- Strafrechtelijk en forensisch onderzoek

Op donderdag 3 december 2020 heeft de gemeente de 1e resultaten van het data-recovery onderzoek ontvangen. De resultaten geven aan dat snelle data-recovery niet mogelijk lijkt. De data op de eigen servers en systemen (inclusief de back-up) lijkt onherstelbaar beschadigd en de 'back-up op afstand' is niet meer toegankelijk (gegijzeld). Omwille van de dienstverlening wordt op dat moment besloten door het Crisisteam om te starten met de opbouw van een nieuw netwerk. Slechts een beperkt aantal gecertificeerde organisaties zijn in staat om forensisch onderzoek te doen. In de eerste crisisdagen zijn deze partijen geraadpleegd en kon hiervoor op vrijdag 4 december 2020 NFIR gecontracteerd worden met de volgende opdracht:

- Herstel data
- Opbouw nieuw netwerk en systemen, inclusief security
- Forensisch onderzoek

Hierdoor kon binnen 10 dagen een nieuw en veilig (nood-)netwerk beschikbaar zijn waarop de dienstverlening verder kan worden uitgebouwd. Voor de hardware is op een externe locatie in die week een zogenoemde 'installatiestraat' ingericht, waar medewerkers met hun laptops naartoe konden om deze door te laten lichten en deze hardware veilig te verklaren voor gebruik.

[4] Het bureau is in de nacht van dinsdag op woensdag gestart met het onderzoek. Dit zou ongeveer 24 uur duren.

Tafel Communicatie

Vanuit het uitgangspunt transparantie en dat de communicatie naar binnen ook de communicatie naar buiten is ('intern <=> extern'), is op verschillende manieren gecommuniceerd over de ontstane situatie (persberichten, persgesprekken, social media en website). De communicatielijn behelsde informatievoorziening, schadebeperking en betekenisgeving. Daarbij is de noodzakelijke terug-houdendheid betracht gelet op het lopende strafrechtelijk onderzoek en andere juridische trajecten. De burgemeester werd tijdens de crisis bijgestaan door een externe communicatie adviseur. Wat betreft de interne communicatie, zijn de gemeenteraad en de fractievoorzitters periodiek door de burgemeester bijgepraat over de ontwikkelingen (zie bijlage 2) en zijn de medewerkers met behulp van filmpjes door de gemeentesecretaris en periodieke interne nieuwsbrieven op de hoogte gehouden.

3.3. Uitgangspunten en scenario's

Vanaf het begin van de crisis is gewerkt met een aantal uitgangspunten die centraal stonden bij de aanpak en keuzen. Het Beleidsteam heeft de volgende uitgangspunten vastgesteld:

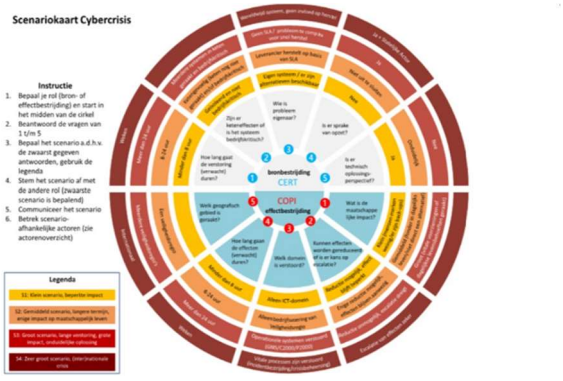
1. Hervatten dienstverlening
2. Data-recovery
3. Forensisch onderzoek
4. Strafrechtelijk onderzoek politie
5. Juridisch en financieel weer in control komen
6. Transparantie

Deze uitgangspunten zijn medio december nogmaals herbevestigd en staan ook in het vervolg centraal. Hoewel deze bestuurlijke uitgangspunten door het OT niet in detail zijn geoperationaliseerd, golden ze als kader waarbinnen werkzaamheden geprioriteerd werden uitgevoerd.

In de Crisisorganisatie is verder gewerkt met een scenariokaart Cybercrisis aan de hand waarvan 3 scenario's zijn onderscheiden. Deze scenario's geven - oplopend in ernst - inzicht in de situatie en bepalen daarmee de prioriteiten, risico's en activiteiten. Het gaat om de volgende drie scenario's:

a. Herstelde veilige en werkende ICT
   Het systeem is veilig en werkt weer. Verder herstel gaat gepaard met de nodige tegenslagen waar veel werk en tijd in gaat zitten en dat veel geld kost. De capaciteit van het netwerk, het aantal bijgeschakelde applicaties en het aantal werkplekken wordt gestaag uitgebreid.

b. Informatie gegevens 'op straat' en imagoschade
   Dit scenario is van kracht wanneer privacy-gevoelige gegevens openbaar worden. Media berichten hierover en de tendens is negatief. Belangen worden geschaad. Dit heeft zijn weerslag op de inwoners en relaties van Hof van Twente. Schadeclaims en rechtszaken behoren tot de mogelijkheden.



c. Misbruik van informatie en gegevens
   Hier is sprake van een verergering van scenario 2 doordat het datalek misbruik tot gevolg heeft zoals identiteitsfraude, afpersing, phishing, valsheid in geschrifte et cetera.

In de crisisorganisatie is aan de hand van een hiervoor ingerichte monitor een inschatting gemaakt van het voorliggende scenario. Dagelijks is een inschatting gemaakt en consequent is geadviseerd om uit te gaan van scenario 1. Daarbij werd gebruik gemaakt van:

- het gemeentelijke 'Security Operations Centre' dat inmiddels in ingericht en waarin gemeentelijke computer- en netwerkactiviteiten worden gemonitord;
- monitoring van het Darkweb;
- informatie van het Centraal Meldpunt Identiteitsfraude en -fouten van het Ministerie van Binnenlandse Zaken & Koninkrijksrelaties;
- overige signalen uit de samenleving, politie, OM, et cetera.

Er waren en zijn vooralsnog geen aanwijzingen dat persoonlijke gegevens door de daders van de cyberaanval zijn buitgemaakt. Dit is dagelijks gemonitord en de komende maanden wordt dit voortgezet en ondergebracht binnen de Concernstaf. Op basis van een risicobeoordeling wordt het verantwoord geacht om een lagere frequentie aan te houden. Verder staat de gemeente in contact met de Autoriteit Persoonsgegevens en zijn voorbereidingen getroffen voor het geval er onverhoopt persoonlijke gegevens van inwoners toch op straat belanden als gevolg van de cyberaanval. Mocht zich in de komende tijd een situatie voordoen waaruit blijkt dat identiteitsgegevens van inwoners zijn gehackt of misbruikt, dan treedt de gemeente direct in contact met politie, Informatiebeveiligingsdienst, Centraal Meldpunt Identiteitsfraude en de Autoriteit Persoonsgegevens om de getroffen personen terzijde te staan.

3.4. Betrokken instanties

Naast de activiteiten die binnen de hiervoor genoemde 'tafels' hebben plaatsgevonden, is een aantal – deels wettelijk verplichte – activiteiten uitgevoerd.

Allereerst is het bij een cyberaanval en hack van belang dat een aantal instanties formeel wordt geïnformeerd en betrokken. Direct na het constateren van de problemen is dan ook contact opgenomen met de Autoriteit Persoonsgegevens (AP), de Informatiebeveiligingsdienst (IBD), het NCSC (Nationaal Cyber Security Centrum) en de politie. De dag daarop is formeel aangifte gedaan bij de politie en op grond van de meldplicht is een voorlopige melding gedaan van een datalek bij de AP.

Vanaf het begin zijn de juristen van de gemeente betrokken geweest bij de crisisorganisatie. Ter ondersteuning is in december 2020 First Lawyers ingehuurd om de gemeente juridisch bij te staan en eventuele aansprakelijkheidsclaims voor te bereiden.

Tot slot hebben de burgemeester en de gemeentesecretaris op een aantal momenten bestuurlijk en ambtelijk afstemming gezocht met de provincie en het ministerie. Het is van belang geweest om deze instanties betrokken te houden bij de situatie in Hof van Twente.

De Informatiebeveiligingsdienst (IBD)

De IBD van de VNG fungeert als Computer Emergency Response Team (CERT) voor gemeenten en is verantwoordelijk de uitwisseling van informatie over dreigingen, incidenten en kwetsbaarheiden. Zij zijn verantwoordelijk voor de informatievoorziening richting NCSC en overige gemeenten en hebben dit ook als zodanig opgepakt. Zij kunnen deze informatie delen met de organisaties en instanties die bij hen zijn aangesloten, zodat een groot deel van Nederland efficiënt is geïnformeerd en - zo nodig - maatregelen kan treffen.

Conform het Bedrijfscontinuïteitsplan is op 1 december dan ook contact opgenomen met de IBD. Ook de dagen daarna hebben de ICT-manager en concerncontroller / CISO wnd. herhaaldelijk contact gezocht met de IBD. De gemeente had vooral behoefte aan deskundige ondersteuning (een incident response team) om de impact van het cyber incident voor de gemeente zo snel mogelijk tot een minimum beperken. De verwachtingen dat de IBD deze ondersteuning direct operationeel en ter plaatse levert, bleken onjuist. Na enkele dagen is contact geweest tussen de directeur IBD en de gemeentesecretaris en werd de ondersteuning vanuit de IBD verder opgeschaald. In de weken daarna heeft dagelijks afstemming plaatsgevonden tussen de IBD en de gemeente en in voorkomende gevallen is ook ter plaatse adequate ondersteuning geleverd.

Ook was de ondersteuning van de IBD in die eerste fase primair gericht op de informatievoorziening naar het NCSC en andere gemeenten. De gemeente heeft geconstateerd dat parallel hieraan ook diverse parallelle opschalings- en informatiestructuren ontstonden. Op welke wijze dat heeft plaatsgevonden is voor de gemeente nog niet duidelijk. Wel is duidelijk geworden dat de IBD hierop heeft geïntervenieerd.

3.5. Duiding

Door de medewerkers van de organisatie is tijdens de crisis met veel inzet, creativiteit en saamhorigheid gewerkt om de dienstverlening te hervatten en de geautomatiseerde systemen op te bouwen. Daarbij heeft de gemeente ondersteuning gehad van diverse instanties zoals collega-gemeenten, de Veiligheidsregio en overige overheidsinstanties en bureau's.
De gemeente is hen veel dank verschuldigd.

Crisisorganisatie

Vanaf het begin is gewerkt met een crisisorganisatie, waarin snel is opgeschaald en continue is meebewogen met de actuele stand van zaken. Er is gekozen voor een structuur die is gebaseerd op de crisisorganisatie van de Veiligheidsregio Twente onder GRIP 3, waarbij drie 'tafels' zijn onderscheiden: ICT, Communicatie en Kritische bedrijfsprocessen. De heldere rollen en structuren zijn bekend en hiermee is veelvuldig geoefend. Hierdoor ontstond rust en overzicht en dit heeft goed gewerkt. Het werken met een hiervoor opgeleide operationeel leider verdient navolging.

Gemeentelijke voorbereiding en aanpak: een digitale incidentenbestrijdingsplan

Het Bedrijfscontinuïteitsplan voorzag niet in een specifieke uitwerking van een crisisorganisatie voor een situatie van deze omvang en met deze impact. Deze inrichtingsvraagstukken moesten daarom in de eerste dagen worden opgepakt. De burgemeester en de gemeentesecretaris hebben hiertoe het initiatief genomen. Het verdient aanbeveling het bedrijfscontinuïteitsplan op dit onderdeel uit te breiden en een specifiek digitaal incidentenbestrijdingsplan op te stellen en hiermee periodiek te oefenen. Dat betekent tevens dat hiervoor budget moet worden vrijgemaakt. De samenwerking tussen de CISO, de functionaris Bedrijfscontinuïteit en de AOV-er wordt hiervoor geïntensiveerd.

Vanaf het moment dat de aard en ernst van de situatie duidelijk werd, is opgeschaald en gezocht naar adequate ondersteuning. De gespecialiseerde bureau's, die in staat waren om de gevraagde ondersteuning en expertise te bieden in termen van capaciteit en kwaliteit, moesten worden gezocht en dit heeft onnodig veel tijd gekost. Het Bedrijfscontinuïteitsplan wordt aangevuld met het zogenoemde 'lijstje op de gasmeter'.

Intergemeentelijke voorbereiding en Emergency Response

De verwachting dat de IBD direct en ter plaatse ondersteuning levert, is een onjuiste. Hieraan was wel behoefte. Het verdient aanbeveling om in VNG-verband het gesprek aan te gaan over de mate waarin gemeenten zijn voorbereid op een cyberaanval, welke expertise op dat moment nodig is en op welke wijze deze kan worden gemobiliseerd c.q. welke rol de IBD hierin aanvullend op zijn huidige 'opdracht' kan spelen. De rol die de Veiligheidsregio's hierin kunnen spelen moet hierbij worden betrokken.

4. Project ‘Opbouw en Reconstructie’

4.1. Inleiding

Na de afbouw crisisorganisatie is een project gestart voor de opbouw van systemen en het reconstrueren van data. In dit hoofdstuk 4 wordt een doorkijk gegeven in de wijze waarop de wederopbouw plaatsvindt.

4.2. Opdracht

Tot medio januari 2021 is gewerkt met een crisisstructuur die vergelijkbaar is met de structuur van de Veiligheidsregio bij een GRIP-3 situatie. Deze crisisstructuur heeft ervoor gezorgd dat de meest urgente bedrijfsprocessen in korte tijd weer konden worden opgestart. Hierdoor is de crisissfeer verdwenen en kan de crisisorganisatie plaatsmaken voor een projectorganisatie.

Deze projectorganisatie moet ervoor zorgen dat de gemeentelijke dienstverlening en alle ICT systemen en gegevens in de volle breedte weer op orde komen. Dus niet alleen ‘aan de balie’ maar ook achter de schermen. Tevens willen we een stap naar voren maken, leren van hetgeen is gebeurd en deze ‘lessons learned’ zowel intern als extern uitdragen. De opdracht voor de projectorganisatie omvat drie onderdelen:

a. Herstel: korte termijn (2021)

Draag zorg voor het herstel van de dienstverlening door de hiervoor benodigde systemen en gegevens in de meest brede zin op orde te brengen. Het wederopbouwen van de waardeketens zoals deze voor het incident van kracht waren, alsmede het eventuele ontvlechten van ICT systemen die voor de opbouw van de noodvoorziening benodigd zijn geweest. Alle (kritische) bedrijfsprocessen moeten weer van A-Z en veilig worden opgestart en ingericht. Met name het inrichten van processen, systemen en gegevens vraagt het komende jaar prioriteit. Daarnaast het inrichten van een governance structuur op de extern verworven dienstverlening.

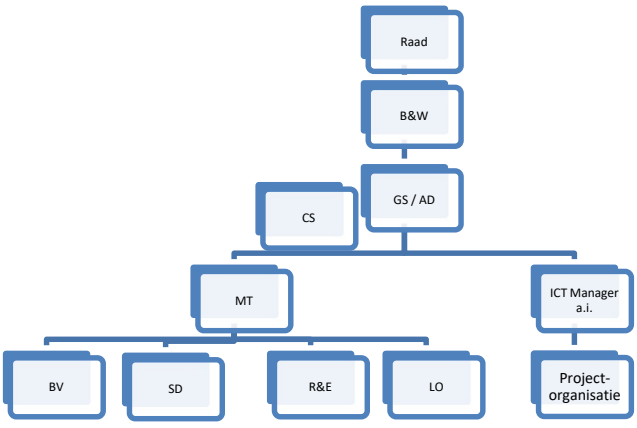
b. Opbouw: middellange termijn (2022 e.v.)

Ontwikkel een visie op basis waarvan eind 2021 een gefundeerd bestuurlijk besluit kan worden genomen over de wijze waarop de gemeente I&A op middellange termijn vorm en inhoud kan geven. Hieraan is onlosmakelijk het vraagstuk verbonden welke rol de gemeente hierin zelf neemt.

c. ‘Lessons learned’

De gemeente wil leren en er geldt een maximale inspanningsverplichting om herhaling te voor-komen. In het project worden dan ook alle bestaande inzichten en nieuwe inzichten actief betrokken, vertaald en geïmplementeerd. Het voorliggende rapport, het overdrachtsdocument van de Operationeel Leider en de nog te verschijnen rapportages van NFIR en De Winter Information Solutions vormen hiervoor de basis.

De projectorganisatie wordt direct opgehangen onder de gemeentesecretaris / AD en krijgt de status van bestuurlijk project.



4.3. Duiding

Lessons learned in de praktijk

De gemeente hof van Twente wil de inzichten en ervaringen meteen in de praktijk brengen. Om die reden worden de conclusies en aanbevelingen actief en expliciet onderdeel gemaakt van het project Opbouw en Herstel en een hiervoor op te stellen routekaart. Dat geldt voor de ‘harde’ onderdelen, zoals de inrichtring van de systemen en security. Ook de ‘zachte’ onderdelen krijgen hierin een plaats, zoals de culturele aspecten van de organisatie.

Agenda digitalisering

Het Project ‘Opbouw en Herstel’ kent een overduidelijke overlap met de Agenda Digitalisering en de hierin opgenomen pijlers. Gezien de ontwikkelingen is het wenselijk om de Agenda digitalisering te integreren in het Project, waarbij de bestaande pijlers ‘Informatieveiligheid’ en ‘Basis op Orde’ de hoogste prioriteit krijgen. De gevolgen voor de ambities en middelen van de Agenda Digitalisering moeten hiervoor in kaart worden gebracht.

BIJLAGEN

Bijlage 1: Raadsbrief zelfevaluatie informatieveiligheid

Gemeente Hof van Twente

Raadsbrief

Onderwerp	Zelfevaluatie informatieveiligheid 2019
Zaaknummer	19243
Datum	17 maart 2020
Portefeuillehouder	drs. H.A.M. Nauta-van Moorsel MPM
Medewerker	Apperloo, E.S. (Esther)

Aanleiding

Als gemeente werken we veel met waardevolle en privacygevoelige informatie. Informatiebeveiliging en dus ook het nemen van allerlei beheersmaatregelen om de risico's te beperken, zijn daarom steeds belangrijker geworden.
Sinds 2017 is ENSIA geïmplementeerd bij alle gemeenten. Dit is een Eenduidige Normatiek Single Information Audit (ENSIA) om in één systematiek de verantwoording te bundelen over:

- Basisregistratie Personen (BRP)
- Paspoortuitvoeringsregeling Nederland (PUN)
- Digitale persoonsidentificatie (DigiD)
- Gezamenlijke Elektronische Voorzieningen Structuur Uitvoeringsorganisatie Werk en Inkomen (Suwinet)
- Basisregistratie Adressen en Gebouwen (BAG)
- Basisregistratie Grootschalige Topografie (BGT)
- Basisregistratie Ondergrond (BRO)

Deze systematiek gaat onder meer uit van de Baseline Informatiebeveiliging Gemeenten (BIG) en vanaf 1 januari 2020 van de Baseline Informatiebeveiliging Overheid (BIO). Dit is een normenkader waar de gemeenten aan moeten voldoen. ENSIA sluit aan op de gemeentelijke planning- en controlcyclus voor informatiebeveiliging. Hierdoor heeft het gemeentebestuur meer overzicht over de informatieveiligheid van de gemeente en kan het college beter sturen en verantwoording afleggen aan de gemeenteraad en betrokken ministeries.

Met deze raadsbrief wordt u geïnformeerd over de resultaten van de zelfevaluatie 2019 en de verplichte verantwoording op het gebied van Suwinet, DigiD, BAG, BGT & BRO. Tevens wordt u kort geïnformeerd over wat er in 2019 is gedaan omtrent de Algemene Verordening Gegevensbescherming (AVG).

Inhoudelijke boodschap

Resultaten zelfevaluatie 2019
De zelfevaluatie van de BIG is een onderdeel van de ENSIA-systematiek. Voor 1 januari 2020 zijn de resultaten van de zelfevaluatie ingeleverd via ENSIA bij de betrokken ministeries. Met onze inzet hebben wij ervoor gezorgd dat wij voor **92% voldoen** aan de 303 normen van de BIG. Dit is een toename ten opzichte van 2018. Toen hadden wij een score van 86%. De acties die dit jaar op het programma staan om onze informatieveiligheid te vergroten, zijn te vinden in de bijlage 'Programma Informatieveiligheid & Privacy 2020'. Vanaf 2020 dienen wij ons te verantwoorden over de nieuwe normenkader: Baseline Informatiebeveiliging Overheid (BIO).

Suwinet & DigiD
Het college dient een verklaring af te leggen of wij voldoen aan de geselecteerde normen inzake DigiD en Suwinet. Deze verklaring betreft de onderdelen van de ENSIA-systematiek waarover goedkeuring (Assurance) wordt gevraagd van een onafhankelijke IT-auditor. In de collegeverklaring staat dat wij **voldoen** aan de DigiD normen en de Suwinet normen op het gebied van Werk en Inkomen. Ook staat er dat wij **niet voldoen** aan de Suwinet normen op het gebied van Burgerzaken. De oorzaak hiervoor is dat de aansluiting voor Suwinet-Inkijk voor adres bevragingen door Burgerzaken pas medio 2020 door het team Burgerzaken gebruikt gaat worden. Omdat er in 2019 wel vanwege een test is ingelogd, dient deze aansluiting wel meegenomen te worden in de audit. Er is een verbeterplan opgesteld voor het gebruik van Suwinet-Inkijk door het team Burgerzaken om daarmee in 2020 wel te voldoen aan de Suwinet normen.

De auditor heeft de collegeverklaring onderzocht tijdens de audit op 18 en 19 februari 2020 en geoordeeld dat deze naar juistheid is ingevuld. Het assurancerapport (van de auditor) en de collegeverklaring dienen voor 1 mei 2020 ingeleverd te worden via ENSIA bij de ministeries (verticale verantwoording). Met deze raadsbrief willen wij u hier graag over informeren. De collegeverklaring en het assurancerapport kunt u vinden in de bijlage.

Tevens dienen wij het Beveiligingsplan Suwinet jaarlijks te evalueren en indien nodig te actualiseren. In de bijlage bevindt zich het door het college vastgestelde Beveiligingsplan Suwinet 2020. De belangrijkste wijzigingen ten opzichte van het plan van 2019 zijn:
- Het beveiligingsplan is geactualiseerd (o.a. verwijzingen naar ons nieuwe intranet (JIP)
- Een nieuwe paragraaf 1.2 over het gebruik van Suwinet-Inkijk door team Burgerzaken
- Verwijzing naar het Personeelshandboek 2020 van de gemeente Hof van Twente waarin onder gedragscode voor werknemers een artikel is opgenomen over het gebruik van Suwinet (artikel 6)
- Verantwoording over het gebruik van Suwinet over 2019 en 2020 i.v.m. de Baseline Informatieveiligheid Overheid (BIO) vanaf 2020.
- Wijziging periode voor uploaden van burgerservicenummers ten behoeve van de whitelist naar 2-wekelijks.

BAG, BGT & BRO
Voor de verantwoording over BAG, BGT & BRO geldt dat de door het college vastgestelde verantwoordingsrapportages voor 1 mei 2020 via ENSIA moeten worden geüpload naar het Ministerie van BZK voor de verticale verantwoording. Tevens dient de raad hierover te worden geïnformeerd. Dit wordt gedaan met behulp van deze raadsbrief.

In de verantwoordingsrapportages is te lezen hoe de gemeente Hof van Twente scoort op de borging, tijdigheid, volledigheid en juistheid van BAG, BGT & BRO op het gebied van informatieveiligheid. De minimale score waar de gemeente aan moet voldoen is 75%.

De BRO is dit jaar voor het eerst een verplicht onderwerp in de zelfevaluatie en wij zijn ons ervan bewust dat wij op dit onderwerp niet hoog scoren. Hieronder een samenvatting van onze score en de te nemen verbetermaatregelen:
- **BAG -> Score 85%**. Ten aanzien van tijdigheid wordt in 2020 de koppeling gerealiseerd met BAG/BGT/BRO. Dit zorgt ervoor dat wij structureel inzicht krijgen in de in te meten panden en beter gebruik maken van het kwaliteitsdashboard. Om de volledigheid en juistheid te verbeteren streven we ernaar om de luchtfotovergelijking jaarlijks te gaan doen.
- **BGT -> Score 93%.** De koppeling met BAG/BGT/BRO heeft als voordeel dat wij sneller zien welke panden gereed zijn en dat de melding openbare ruimte sneller afgehandeld wordt. Ten aanzien van volledigheid en juistheid vindt in 2020 een nieuwe aanbesteding plaats voor het inwinnen van topografie. Hier wordt de luchtfotovergelijking in meegenomen. Dit betekent dat panden en andere topografie worden opgespoord en ingemeten. Dit willen we meer terrestrisch laten inmeten. Terrestrisch gemeten topografie heeft een grotere nauwkeurigheid en juistheid dan topografie ingewonnen uit luchtfoto's.

- **BRO -> Score 33,3%**. Dit is een toename vergeleken met de nulmeting van vorig jaar (8%). De BRO is een nieuwe basisregistratie en in 2020 wordt gestart met het formeel beleggen van de rol in de organisatie, zodat de eigenaar van de BRO deze registratie goed gaat ontwikkelen. Er komt dan aandacht voor het inrichten van het proces, zodat daarna de actualiteit en tijdigheid verbeterd kan worden. Wanneer het proces ingericht loopt, worden er steekproeven gehouden om periodiek de BRO te controleren.

Algemene verordening gegevensbescherming (AVG)
In mei 2018 is de Algemene Verordening Gegevensbescherming in werking getreden. De AVG gaat over het rechtmatig omgaan met persoonsgegevens. Zo bepaalt de wet dat persoonsgegevens alleen mogen worden verwerkt op basis van één van de wettelijke grondslagen, er niet meer gegevens mogen worden verzameld dan noodzakelijk voor het uitvoeren van het vastgestelde doel en dat de gegevensverwerking op een passende manier moet worden beveiligd. De positie van degene over wie de gegevens worden verwerkt is verstevigd.

In 2018 is gestart met de implementatie van de AVG. Dit is in 2019 voortgezet en heeft geleid tot het volgende:
- Een ronde langs alle teams om de AVG (opnieuw) onder de aandacht te brengen en mogelijke knelpunten en casussen te bespreken.
- Uitbreiding en invulling van het verwerkersregister, met behulp van de verantwoordelijke proceseigenaren.
- Actualisatie van de standaard-verwerkersovereenkomst.
- Versteviging van de Kerngroep AVG binnen de organisatie (= intern overleg van bij de AVG direct betrokken medewerkers van diverse afdelingen).
- Beantwoording van uiteenlopende vragen over de AVG met in sommige gevallen wijziging van proces, formulieren of werkwijze tot gevolg.
- Opstellen van een ‘Privacy Governance’ (= beschrijving van rollen, taken en verantwoordelijkheden ten aanzien van privacy)

Het komend jaar is bedoeld om de communicatie rondom de AVG levendig te houden maar ook om inhoudelijke zaken rond privacy bij de afdelingen/teams te beleggen. Zij hebben immers de inhoudelijke kennis en verantwoordelijkheid op hun eigen beleidsterrein: privacy valt daar onder (net als bijvoorbeeld financiën en communicatie).

Conclusie
Zoals u hebt kunnen lezen zijn wij op de goede weg met betrekking tot informatieveiligheid en privacy. We voldoen aan de verplichte normen van Suwinet en DigiD en scoren goed op het gebied van BAG en BGT. BRO is dit jaar een aandachtspunt en wordt opgepakt in de organisatie, zodat we volgend jaar voldoen aan de normen. Tevens is en blijft de AVG een belangrijk aandachtspunt in de organisatie. In het jaarverslag 2019 bij paragraaf bedrijfsvoering staat tevens de informatie over de stand van zaken met betrekking tot informatieveiligheid en privacy.

Burgemeester en wethouders van Hof van Twente,

de secretaris,	de burgemeester,
drs. D. Lacroix	drs. H.A.M. Nauta-van Moorsel MPM

Bijlage 2: Informatievoorziening gemeenteraad

Vanaf 01 december 2020 is de Gemeenteraad op verschillende manieren geïnformeerd over de ICT-hack. Hieronder in chronologische volgorde:

- 02 december 2020: fractievoorzitters afzonderlijk telefonisch geïnformeerd door de burgemeester:
  Een toelichting op de stand van zaken en de ernst van de situatie.

- 03 december 2020: fractievoorzitters afzonderlijk telefonisch geïnformeerd door de burgemeester:
  Een toelichting op de stand van zaken en de ernst van de situatie.

- 04 december 2020: fractievoorzitters per WhatsApp geïnformeerd door de burgemeester:
  Een toelichting op de stand van zaken en het inschakelen van NFIR voor o.a. forensisch onderzoek.

- 05 december 2020: raadsbrief (103203):
  Toelichting op de stand van zaken en stappen die zijn gezet.

- 05 december 2020: Seniorenconvent (digitaal):
  Een toelichting op de stand van zaken en de opdracht aan NFIR.

- 05 december 2020: fractievoorzitters per WhatsApp geïnformeerd door de burgemeester:
  Een toelichting op de communicatie en persnummer.

- 06 december 2020: fractievoorzitters per WhatsApp geïnformeerd door de burgemeester:
  Een toelichting op de stand van zaken, het interview met de Volkskrant en de positie van de betreffende journalist.

- 07 december 2020: Seniorenconvent (digitaal):
  Een toelichting op de stand van zaken, vragen die leven, dienstverlening, losgeld, crisisstructuur, back-up systemen en het doorgaan van de reguliere raadsvergadering van december.

- 09 december 2020: Informerende raadsbijeenkomst (fysiek):
  In bijzijn van de heer Van der Sluis, directeur NFIR de gemeenteraad geïnformeerd over het forensisch onderzoek en de stand van zaken (ICT, Communicatie en Dienstverlening). Tevens het dilemma van losgeld en de formele bevoegdheden toegelicht. Zodra het betalen van losgeld een optie wordt, komt het college terug bij de raad;

- 11 december 2020: fractievoorzitters per WhatsApp geïnformeerd door de burgemeester:
  Een toelichting op de stand van zaken en dienstverlening.

- 18 december 2020: Informerende raadsbijeenkomst (digitaal)

- 07 januari 2021: seniorenconvent (digitaal):
  Een toelichting op de stand van zaken en het project ‘Opbouw en herstel’

- 03 februari 2021: informerende raad (digitaal):
  Een toelichting op de stand van zaken, dienstverlening, project ‘Opbouw en herstel, juridische en financiële gevolgen en communicatie.

de Höfte 7, 7471 DK Goor
Postbus 54, 7470 AB Goor
0547 – 85 85 85
info@hofvantwente.nl