Informatiebeveiliging
Gemeente Hof van Twente

Rekenkamerrapport

Rekenkamercommissie Hof van Twente

30 mei 2022

De perfecte storm

Auteurs: drs. Etienne Lemmens, mr. drs. Sandra van Breugel

Prae Advies en onderzoek, Utrecht

Inhoudsopgave

Samenvatting, conclusies en aanbevelingen

Samenvatting

Op 1 december 2020 werd de gemeentelijke organisatie van Hof van Twente gewaar dat ze slachtoffer was geworden van een cyberaanval. Naar aanleiding van een verzoek van de gemeenteraad van 1 juni 2021 heeft de Rekenkamercommissie Hof van Twente besloten een onderzoek te laten uitvoeren naar de uitvoering en monitoring van het informatiebeveiligings-beleid van de gemeente in de periode 2019-2020 en daarna. Het doel van het onderzoek is ambtelijk en bestuurlijk te leren van het voorval van december 2020.

In de periode december 2021 tot en met maart 2022 is het onderzoek uitgevoerd op basis van deskresearch en interviews. De bevindingen uit het onderzoek zijn hierna in de hoofdstukken 3 tot en met 11 opgenomen. In deze samenvatting, conclusies en aanbevelingen geven we achtereen-volgens een resumé van de bevindingen, de daarop gebaseerde conclusies en de daaruit voortvloeiende aanbevelingen richting raad en college.

Algemeen

De samenleving maakt een digitale transitie door en gemeenten zijn dienstverleners geworden die grotendeels digitaal georganiseerd zijn. Die transitie biedt geweldige kansen voor gemeenten en de inwoners, bedrijven en instellingen. Tegelijkertijd kent deze transitie ook risico's. Zowel risico's die de veiligheid van de informatiehuishouding van de gemeente zelf raken, als ook risico's voor inwoners, bedrijven en instellingen die van de dienst-verlening van de gemeente afhankelijk zijn. Dat betekent dat er eisen gesteld mogen worden aan de weerbaarheid en het herstelvermogen van de gemeentelijke informatiehuishouding. Anders loopt de gemeente enorme risico's op imago, financieel en politiek-bestuurlijk vlak.

1 december 2020

Vanuit het ambtelijk apparaat werden er in de periode vóór december 2020 rapportages verzorgd naar management en bestuur. Deze gaven geen aanleiding te veronderstellen dat er grote risico’s waren. Na een aantal fouten in de naleving van protocollen en nog niet geïmplementeerd beleid, wat het best omschreven kan worden als een 'perfect storm' [1], wordt op 1 december 2020 duidelijk wat een of meerdere hackers in de systemen hebben aangericht. In een ransomware aanval zijn systemen gehackt, gegevens ontvreemd en servers, gegevens en back-ups vernietigd. Na afweging wordt niet ingegaan op de losgeldeis van de hackers.

Hof van Twente gaat over naar crisismodus en kan relatief snel met behulp van de Informatiebeveiligingsdienst voor gemeenten (IBD), andere

[1] Een 'perfect storm' doet zich voor als een zeldzame combinatie van uiteenlopende omstandigheden tot een extreme gebeurtenis leidt.

gemeenten, de veiligheidsregio en commerciële partijen de hoogst noodzakelijke dienstverlening weer opstarten. De crisisfase wordt afgesloten met een aantal evaluaties waarin het lessen trekken uit de gebeurtenissen centraal staat. Dan begint de projectfase waarin gebouwd wordt aan een robuuste ICT-omgeving. In de loop van 2022 moet deze fase overgaan in een staande gemeentelijke organisatie die in staat is de digitale dienstverlening op niveau uit te voeren. Ondanks het gegeven dat de naweeën van de gebeurtenissen nog voelbaar zijn, onder andere door verlies van gegevens.

Beleid

De gemeente Hof van Twente beschikte in 2020 over een informatie-beveiligingsbeleid dat grotendeels voldeed aan de normen waar gemeenten aan behoren te voldoen. Op basis van een GAP- en risicoanalyse zijn prioriteiten gesteld en jaarplannen met activiteiten op informatiebeveiliging opgesteld. In het collegeprogramma 2018-2022 en de Digitale Agenda 2019 is de digitale dienstverlening van de gemeente, met als onderdeel informatiebeveiliging, een prominent element.

Middelen

De I&A-functie, en daaronder informatieveiligheid werd niet ruim bedeeld in de gemeentelijke begroting. De gemeente was zuinig in vergelijking met een benchmark en daar waren bestuurders en ambtenaren van op de hoogte. Dat besef heeft in 2017 geleid tot structureel en in 2019 incidenteel extra middelen, evenwel zonder op het niveau van de benchmark te komen. Geconstateerd kan worden dat de gemeente geen grote ambities had.

Mede naar aanleiding van de discussie in 2017 is in 2018 het ICT-beheer uitbesteed aan een externe partij. Vanaf 2020 is in het Programma Informatieveiligheid en privacy aandacht geschonken aan het speerpunt informatiebeveiliging uit de Digitale Agenda 2019, met activiteiten op de pijlers bewustwording, verantwoording en ontwikkeling.

Functies

De functies op informatiebeveiliging en privacy waren bezet. Met 8 uur voor de Chief Information Security Officer (CISO) in de stafafdeling, met ondersteuning op technisch gebied door de medewerkers van de afdeling I&A. Tegen het advies van de IBD in had de CISO geen eigen budget.

Volwassenheid

De verantwoordelijkheden voor informatiebeveiliging waren belegd bij de proceseigenaren. Deze moesten op operationeel niveau ondersteund worden door de CISO. De taakvolwassenheid van de proceseigenaren is in het kader van dit onderzoek niet gemeten, maar kan op basis van de bevindingen op maximaal 2 op de 5 puntenschaal van NOREA ingeschat worden (zie bijlage 4). Daardoor ontbreekt de administratieve basis om zicht te krijgen op de uitvoering van het beleid.

Uitvoering

Informatiebeveiliging leek bij de gemeente onder controle, daar deze compliant was op de BIO-richtlijnen. De gemeente voldeed aan 90% van de eisen. Uit het onderzoek blijkt dat informatiebeveiliging bestuurlijk niet

prioriteit nr. 1 was, mede omdat men dacht dat alles op orde was. Er was wel draagvlak voor het onderwerp bij het college. Bewustzijn op en aandacht voor risico's bij medewerkers nam gestaag toe. Net als in veel andere (gemeentelijke) organisaties behoefde en behoeft dat constante stimulering.

De ENSIA-rapportage (ENSIA: Eenduidige Normatiek Single Information Audit) ziet met name toe op opzet en bestaan van (onderdelen van) het informatiebeveiligingsbeleid. De werking wordt in mindere mate gemonitord en daarin zaten de punten die cruciaal bleken met betrekking tot de ransomware aanval. Zoals het back-up & restore beleid en logging die voor 2020 op de rol stonden om geïmplementeerd te worden. De 2-factor authenticatie was weliswaar geïmplementeerd, maar bleek uiteindelijk niet volledig te zijn nageleefd.

Monitoring

De instrumenten voor toetsing en monitoring van de uitvoering waren deels aanwezig. De ENSIA-rapportage is bedoeld voor de verticale verantwoording richting de landelijke toezichthouders. En voor de horizontale verantwoording richting de gemeenteraad. Zoals hiervoor gemeld is deze minder geschikt om de werking van het beleid te monitoren. Deze werd niet uitgevoerd met behulp van een information security management systeem (ISMS).

De accountant waarschuwde meerdere keren voor de risico's op informatiebeveiliging en een mogelijke computeraanval. Een applicatie voor de monitoring van computerdreigingen werd vanwege te hoge kosten niet aangeschaft. Wel werden pentesten uitgevoerd op de systemen, maar ook pas medio 2020 en na advies van de accountant. Uit de rapportage is niet het risico van de ransomware aanval geconstateerd zoals die zich uiteindelijk voltrok.

Externe leverancier

Op operationeel niveau stokte soms de communicatie tussen de gemeente en de externe systeembeheerder. Op tactisch en strategisch gebied ontbrak de aansturing in de relatie met de externe leverancier. Deze relatie was voornamelijk gebaseerd op vertrouwen en er werd sterk geleund op de werkprocessen en kennis van deze partij. De leverancier werd als trusted third party tegemoet getreden, zodat er te weinig controle was op hetgeen de externe partij contractueel verplicht was te leveren. Dat werd opgemerkt en de gemeente was van plan in 2020 meer regie op de relatie te nemen. Dat is er onder andere door de aandacht die de coronapandemie vergde niet van gekomen.

Positionering gemeenteraad

De gemeenteraad is in de periode voorafgaand aan 2020 via de jaarstukken in de P&C-cyclus, ENSIA en twee raadsinformatiebrieven geïnformeerd. In 2017 en 2019 is ICT, de financiering en informatieveiligheid aan bod gekomen in de raad. Met betrekking tot de financiering zijn in 2017 structureel en in 2019 incidenteel middelen ter beschikking gesteld. Er is

geen intensieve bemoeienis van de raad met informatieveiligheid te constateren.

De accountant, met de raad als opdrachtgever, heeft in de management-letters meerdere malen aandacht gevraagd voor ICT in relatie tot de rechtmatigheid van de financiële huishouding van de gemeente. Maar ook ten aanzien van informatieveiligheid, in ieder geval vanaf 2017. Daarbij heeft de accountant onder andere het wachtwoordenbeleid geproblematiseerd en gewaarschuwd voor de risico's van een hack. In 2018 geeft de accountant een 8-tal aandachtspunten, waaronder het informatiebeveiligingsbeleid, toegangs- en autorisatiebeleid en pentesten. In 2019 constateert de accountant dat op een aantal punten vooruitgang is geboekt, en dat nog aandacht nodig is op beheersingsmaatregelen IT en wachtwoordenbeleid.

Na 1 december 2020

Na de ransomware aanval is er veel contact tussen college en de raad. In het begin wordt vanuit het college informatie gedeeld met behulp van vertrouwelijke overleggen. Deze fase eindigt als de evaluaties in een publiek debat eind maart 2021 worden behandeld. Van beide kanten is erkend dat de raad beter in positie gebracht moet worden op informatieveiligheid, vanwege de grote impact van incidenten. In juni 2021 komt het college met een bestuurlijke verantwoording en een dekkingsvoorstel voor de kosten die met de hack en de opbouw van de systemen samenhangen.

Eind 2021 is binnen de auditcommissie een werkgroep op ICT ingericht met raadsleden, wethouder, burgemeester en ambtenaren. De bedoeling is dat in dit gremium diep op de materie kan worden ingegaan.

Van crisisfase > opbouwfase > staande organisatie

Van crisisfase, begin 2020, is in maart 2021 overgegaan naar de opbouw fase. Daarna is het de bedoeling om over te gaan in 2022 naar de staande organisatie. De lessen die de gemeente heeft getrokken uit de gebeurte-nissen en de evaluaties culmineren in een programma met 18 actiepunten. Zo is eind 2021 een nieuwe I&A-visie vastgesteld, dat voorziet in een regiebureau direct onder de algemeen directeur/ gemeentesecretaris.

Er moet ook nog veel ontwikkeld worden, zoals nog ontbrekende beleids-onderdelen op informatiebeveiliging en betere sturingsinformatie. Het huidige informatiebeveiligingsbeleid is nog van 2020-2022, ondanks de ingrijpende gebeurtenis van eind 2020 die noopt tot bijstelling. Intentie is het beleid in de eerste helft van 2022 aan de nieuwe werkelijkheid aan te passen. Audits en pentesten moeten nog gehouden worden.

Conclusies

De bevindingen uit het onderzoek, waarvan hiervoor een korte samenvatting is weergegeven, leiden tot de volgende conclusies.

Vooraf wil de rekenkamercommissie grote complimenten maken aan alle betrokkenen die na de hack op 1 december 2020 op enigerlei wijze hebben meegewerkt aan de werkzaamheden na de hack om de dienstverlening aan inwoners en bedrijven weer mogelijk te maken. Van nul af aan is het ICT-systeem sinds eind 2020 stap voor stap opgebouwd.

Ten tweede is het goed om op te merken dat een hack niet altijd te voorkomen is. Er is veel ontwikkeling op beveiligingsmaatregelen, maar de kwaadwillenden ontwikkelen steeds geraffineerdere methoden om te proberen binnen te komen. Doelstelling van beleid op informatiebeveiliging moet zijn de risico's in beeld te krijgen, de drempels om binnen te dringen zo hoog mogelijk te maken en indien kwaadwillenden toch binnen zijn gedrongen de schade zo beperkt mogelijk te houden.

Hieronder presenteren we de conclusies op de volgende onderdelen: 'beleid, uitvoering en monitoring', kennis ICT, positie CISO, uitbesteding infrastructuur, beschikbaar ICT-budget, prioritering ICT en positie gemeenteraad.

Beleid, uitvoering en monitoring

1. De gemeente Hof van Twente had een beleid op Informatisering en Automatisering vastgesteld. Het beleid was volgens de normen die daarvoor gelden adequaat. De risico's waren wat betreft opzet en bestaan van het beleid in beeld, maar de werking van het beleid en de monitoring ervan kwamen onvoldoende in beeld. De monitoring op de uitvoering van het informatiebeveiligingsbeleid was niet toereikend om de hack periode voorafgaand aan de hack tijdig te detecteren of te voorkomen.

2. In de verantwoordingsrapportages leek de gemeente 'in control' op informatieveiligheid, namelijk te weten wat de risico's zijn en daar maatregelen op te treffen. Onderdelen van het informatiebeveiligingsbeleid waren in 2020 nog in ontwikkeling. Bepaalde onderdelen waren op papier gerealiseerd, zoals het 2FA-beleid en bleken in de praktijk niet consequent te worden uitgevoerd. Er bleek een groot verschil tussen de bestuurlijke werkelijkheid en de dagelijkse praktijk.

Kennis ICT

3. Diepgaande kennis over ICT was niet voldoende aanwezig op sleutelposities in de ambtelijke en bestuurlijke organisatie om de naleving van beleid en protocollen af te dwingen of te controleren. Er kwamen vanaf begin 2019 en in de periode voorafgaand aan de hack via de accountant en een enkele pentest (zomer 2020) signalen op onvolkomenheden op informatieveiligheid binnen bij de organisatie. Deze signalen zijn niet voldoende doorgedrongen bij management, college en de raad. De kennis over informatiebeveiliging was beperkt om de risico's op informatieveiligheid adequaat te duiden en erop door te vragen.

Positie CISO

4. De IBD van de VNG pleitte in 2020 gezien het dreigingsbeeld op informatie-veiligheid voor versterking van de positie van de CISO. De CISO-functie was gepositioneerd in de stafafdeling van de gemeente en was voor 0,2 fte ingevuld. Dat is relatief weinig voor een gemeente als Hof van Twente. De CISO had geen eigen budget, in weerwil van de adviezen van de IBD. Dit gegeven heeft niet geleid tot verminderde activiteit op informatiebeveiliging, maar wierp een onnodige drempel op voor activiteiten die de CISO nodig achtte en leidde niet tot een stevige positie van de CISO.

Uitbesteding Infrastructuur

5. De digitale infrastructuur is in 2018 aan een externe partij uitbesteed. Er waren servicelevel agreements afgesproken met de externe partij waar het ICT-systeembeheer aan was uitbesteed. Op operationeel niveau bleken geringe haperingen in de communicatie en de dienstverlening. Op strategisch en tactisch niveau ontbrak daarop de regie en sturing. De gemeente handelde in de relatie met de leverancier te veel vanuit vertrouwen in plaats van regie, sturing en controle. Een zakelijke samenwerking ontbrak tussen gemeente en de externe leverancier.

Beschikbaar ICT-budget

6. De financiering van ICT en navenant informatiebeveiliging van de gemeente Hof van Twente was beneden de benchmark met vergelijkbare gemeenten. Dat tekent de aandacht voor ICT en draagvlak voor investeringen hierop bij college en raad.

Prioritering ICT

7. Vanwege de grote bestuurlijke, publicitaire en financiële risico's is duidelijk dat ICT en informatieveiligheid op de politieke agenda thuishoren. Fouten op dit terrein kunnen enorme consequenties hebben voor de dienstverlening van de overheid aan inwoners, bedrijven en instellingen, naast de reputatie- en financiële schade voor de overheid en een dalend vertrouwen in de overheid. Dit heeft de gemeente Hof van Twente aan den lijve ondervonden. De indruk bestaat dat de gemeente veel werk heeft verzet na de hack, maar dat de aandacht enigszins verslapt. Dit wordt afgeleid uit het feit dat er sinds de zomer van 2021 geringe aandacht is vanuit de raad voor informatiebeveiliging, de ICT-auditcommissie gestart is in december 2021 en het feit dat slechts twee partijen in hun verkiezings-programma van maart 2022 aandacht geven aan informatiebeveiliging.

Positie gemeenteraad

8. In de samenwerking tussen college en raad is het college leidend en initiërend. De raad neemt weinig regie en laat zich leiden.

Aanbevelingen

Uit de conclusies vloeien de onderstaande aanbevelingen voort. Daarna volgen een 3-tal aansporingen die door de raad of college kunnen worden opgepakt of worden voortgezet.

1. Monitor op de werking van het informatiebeveiligingsbeleid.
   - Richt de sturingsinformatie in op uitvoering en vastlegging van activiteiten op informatiebeveiliging, maak daarbij gebruik van een ISMS.
   - Voer elk jaar pentesten uit op de techniek en de systemen, de accounts en AD audits op wachtwoordenbeleid en phishing mails enz. Laat dit uitvoeren door steeds andere externen die de externe dienstverleners en elkaar controleren.
   - Maak gebruik van de vrije ruimte die ENSIA biedt om de horizontale verantwoording richting de gemeenteraad in te richten. College en raad moeten daarover met elkaar in gesprek welke informatie de raad nodig heeft om zijn kaderstellende en controlerende rol te kunnen nemen.
2. Organiseer de controle op regievoering van externen en doe dit op drie niveaus (strategisch, tactisch en operationeel),
   - Regiebureau in de staf onder directeur is daarbij goed begin.
   - Plaats de CISO rechtstreeks onder de gemeentesecretaris.
3. Voer een dialoog over de portefeuilleverdeling in het college. Informatieveiligheid is 'chefsache' voor de burgemeester, ICT bij een wethouder die hier echt affiniteit mee heeft.
4. Zorg dat kennis op ICT en informatiebeveiliging in de gemeente geborgd is door:
   - In de ambtelijke organisatie de juiste competenties en kennis op ICT en informatieveiligheid te borgen;
   - Het bestuur (college en raad) te 'scholen' zodat ze op het terrein van ICT en informatieveiligheid de goede vragen kan stellen en kunnen doorvragen.
5. Zorg voor adequate financiering van ICT en informatiebeveiliging, met een eigen toereikend budget voor de CISO.
6. Organiseer tegenmacht binnen de organisatie, tussen organisatie en bestuur en tussen bestuur en raad:
   - Positioneer je als raad in je controlerende en ook kaderstellende rol en neem regie. De ICT-werkgroep is daar een goed middel voor. Aanbevolen wordt dat de raad meer dan alleen maar meedenkt. Draag via een eigen geoormerkt budget in de begroting zorg dat je als raad of commissie een advies of second opinion op raadsvoorstellen kan inwinnen, zonder advisering vanuit de ambtelijke organisatie. Laat eventueel vanuit de ICT-werkgroep pentesten door een externe uitvoeren.

- Geef de accountant de opdracht ICT, informatiebeveiliging en privacy consistent te monitoren en te rapporteren, ook direct aan de raad. Laat rapporteren over de voortgang op de opvolging van de adviezen en geef hierin de griffie een rol om dat te administreren, te bewaken en terug te koppelen aan de raad.

Aansporingen

1. Neem als raad het initiatief om het gesprek aan te gaan over cultuur met het bestuur. Ga daarna als raad met ambtelijke organisatie het gesprek over de gewenste cultuur voeren, neem als raad het college mee en houdt als raad zelf de regie op dit proces. Neem daarbij als raad ook jezelf onder de loep. In hoeverre ben je als raad zelf in staat om dit onderwerp op de bestuurlijke agenda te houden?
2. Verzoek als raad het college om gezamenlijk een keer per jaar met een andere gemeente (of meerdere) uit de regio in gesprek te gaan en laat je informeren over hoe zij de informatiebeveiliging hebben georganiseerd. Laat de andere gemeente ook bij jou kijken, om ideeën en good practices uit te wisselen.
3. Verzoek als raad het college de mogelijkheden te onderzoeken om samen te werken op functies (FG en CISO) met buurgemeenten. En onderzoek de mogelijkheden om op systeembeheer samen te werken, bijvoorbeeld met een gemeente die gastheer wil zijn of via een shared servicecentrum. Regel daarbij de governance adequaat in.

1 Inleiding

Dienstverlening kwetsbaar

De gemeente verleent diensten aan inwoners, bedrijven en instellingen. Ook beheert de gemeente veel (bijzondere) persoonsgegevens van inwoners en vanaf de decentralisaties in het sociale domein van kwetsbare groepen mensen. In toenemende mate is de gemeentelijke dienstverlening afhankelijk van elektronische systemen, hiermee is de gemeente Hof van Twente op rampspoedige wijze geconfronteerd. De gemeente Hof van Twente is zich op 1 december 2020 op brute wijze van de kwetsbaarheid bewust geworden.

1 december 2020

Op die dag werd een ransomware aanval [2] op de gemeentelijke systemen van de gemeente Hof van Twente ontdekt. Dit en de gevolgen ervan hebben een enorme impact gehad op de organisatie. Door de hack werden data vernietigd of onbereikbaar, back-ups konden niet teruggezet worden en de gemeentelijke dienstverlening stokte. De onderzoeken die voor de gemeente voor 1 december 2020 zijn uitgevoerd, zoals audits, pentesten [3] en rapportages, gaven het gemeentebestuur geen zorgwekkende signalen. De noodzaak om te acteren op informatiebeveiliging werd om die reden niet opgemerkt.

Enorme impact

De gebeurtenis in Hof van Twente had een enorme impact op de organisatie, bestuur, gemeenteraad en ook op inwoners. Na de eerste interventies om alles te herstellen, kwam de vraag: Hoe heeft dit kunnen gebeuren en hoe kunnen we dit voorkomen? Zoals te doen gebruikelijk in Nederland zijn er door het College van Hof van Twente verschillende evaluaties verricht om zicht te krijgen op de feiten en omstandigheden van deze hack.

In maart 2021 zijn in opdracht van het College van B&W rapporten verschenen over de technische en organisatorische factoren van de hack.[4] Dat heeft geleid tot een zelfevaluatie door het College om verantwoording af te leggen en lessen te trekken.[5]

Motie 1 juni 2021

In een motie van 1 juni 2021 heeft de gemeenteraad van Hof van Twente de rekenkamercommissie verzocht "(E)en onderzoek in te stellen naar de uitvoering van het informatieveiligheidsbeleid zowel intern als de samenwerking met leveranciers in relatie met de cyberaanval". Naar

---

2 Ransomware, of gijzelsoftware, is schadelijke software die computers en bestanden gijzelt. Criminelen blokkeren of versleutelen computers, bestanden of hele netwerken, en geven die pas weer vrij als losgeld wordt betaald.

3 Een pentest of penetratietest is een toets van een of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden ook werkelijk gebruikt worden om in deze systemen in te breken. Deze testen worden uitgevoerd door zogenoemde ethische hackers.

4 *Te goed van vertrouwen? Duidingsrapportage ransomware-aanval Hof van Twente*, in opdracht van het College, door De Winter Information Solutions, 8 maart 2021; *Rapportage zonder veiligheidsgevoelige informatie. Incident Response & Digitaal forensisch* onderzoek, in opdracht van het College, door NFIR (Nederlands Forensisch Incident Response), 8 maart 2021.

5 *Rapport van Bevindingen. ICT-situatie*, Hof van Twente, 9 maart 2021.

aanleiding van deze motie heeft de rekenkamercommissie van Hof van Twente besloten onderzoek hiernaar te doen. Het resultaat daarvan ligt voor u.

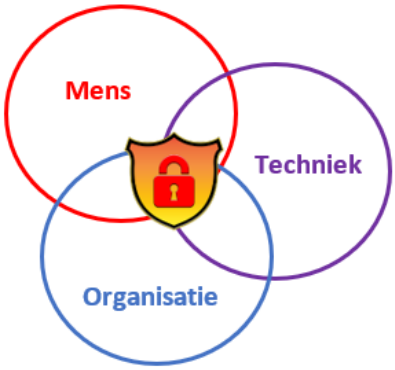
2 Doelstelling en onderzoeksvragen

2.1 Doelstelling

Doelstelling

Doel van het rekenkameronderzoek is bestuurlijk en ambtelijk te leren van de wijze waarop het informatiebeveiligingsbeleid tot stand is gekomen en de wijze waarop het in de praktijk is uitgevoerd en bestuurlijk is gemonitord. Het geeft inzicht in de staat van de informatiebeveiliging van de gemeente Hof van Twente.

De rekenkamercommissie Hof van Twente wil de gemeenteraad inzicht geven in de stand van zaken op het gebied van informatiebeveiliging en privacy in de gemeente. Ten aanzien van informatiebeveiliging spelen drie aspecten een cruciale en op elkaar ingrijpende rol: mens – techniek – organisatie. In het rekenkamer onderzoek wordt ingegaan op deze drie aspecten.



Op de technische infrastructuur zijn door de gemeente zelf onderzoeken en testen uitgevoerd. De rekenkamercommissie heeft Prae Advies en Onderzoek gevraagd met name de organisatorische en menselijke aspecten van informatie-beveiliging en privacy te onderzoeken. Daar waar dat zinvol is wordt in dit rapport ingegaan op de resultaten uit de technische testen die de gemeente zelf heeft uitgevoerd.

2.2 Centrale onderzoeksvraag

Naar aanleiding van de motie van de raad en de onderzoeksopzet van de rekenkamercommissie is de hoofdvraag geformuleerd. De rekenkamercommissie Hof van Twente wil met dit onderzoek de volgende centrale vraag beantwoorden:

“Hoe is het informatieveiligheidsbeleid in de gemeente Hof van Twente in de periode 2019-2020 tot stand gekomen, op welke wijze is deze uitgevoerd en gemonitord en wat is er na een jaar geleerd van het incident dat op 1 december 2020 manifest werd?”

2.3 Onderzoeksvragen

De centrale onderzoeksvraag wordt uitgewerkt aan de hand van de onderzoeksvragen zoals opgenomen in onderstaande tabel 1.

Tabel 1. Onderzoeksvragen

1.	Beschikte de gemeente Hof van Twente in de periode 2019-2020 over een adequaat informatiebeveiligingsbeleid? Welk beleid voert de gemeente Hof van Twente op het gebied van informatiebeveiliging? In hoeverre stuurt het college van B&W op de afspraken die benoemd zijn in de VNG Resolutie 'Informatiebeveiliging, randvoorwaarde voor de professionele gemeente' en in het bijzonder op de implementatie van de Baseline Informatiebeveiliging Nederlandse Overheid (BIO)? [6] Wat zijn de wijzigingen in het beleid sinds 1 december 2020?
2.	Is het informatiebeveiligingsbeleid in die periode adequaat uitgevoerd? Welke risico's bij informatiebeveiliging en privacy heeft de gemeente benoemd? In hoeverre worden risico's beheerst dan wel geaccepteerd? Op welke wijze zijn de (eind)verantwoordelijken aangewezen en de autorisaties geregeld? Welke maatregelen worden genomen om risico's te laten afnemen?
3.	Zijn de functies die van belang zijn op het gebied van informatiebeveiliging in die periode goed ingevuld en gepositioneerd? Welke ontwikkelingen zijn er na 1 december 2020 waar te nemen?
4.	Is de uitvoering van het beleid in die periode adequaat getoetst en gemonitord? Hoe vindt toetsing en monitoring nu plaats
5.	Welke afspraken op informatiebeveiliging zijn gemaakt met externe leverancier(s) en hoe zijn deze gemonitord? Heeft de gemeente in beeld met welke partners informatie en persoonsgegevens worden gedeeld? Op welke manier toetst de gemeente haar partners en leveranciers op privacy- en informatiebeveiligingsaspecten? Met partners en leveranciers zijn afspraken gemaakt op basis van 'privacy by design'.
6.	Is de raad adequaat gepositioneerd geweest om zijn kaderstellende en controlerende rol te kunnen uitvoeren? Op welke manier rapporteert en bespreekt de organisatie het functioneren van informatiebeveiliging op management- en bestuursniveau (college en raad)?
7.	Wat is er gedaan met de aanbevelingen uit de twee onderzoeken die in maart 2021 in opdracht van het college zijn verschenen?
8.	Hoe heeft het informatiebeveiligingsbeleid vorm gekregen na 1 december 2020?
9.	Welke lessen zijn te trekken uit de hack die 1 december 2020 manifest werd en de gebeurtenissen daarna?

Voor de normen bij deze onderzoeksvragen verwijzen we naar bijlage 3.

[6] Gemeenten hebben in 2013 in VNG-verband afgesproken te voldoen aan de maatregelen van de Baseline Informatiebeveiliging Gemeenten (BIG). De BIG is vanaf 2020 vervangen door de Baseline Informatiebeveiliging Overheid (BIO.)
Vanaf 25 mei 2016 schrijft de Algemene Verordening Gegevensbescherming (AVG of GDPR) voor dat passende maatregelen getroffen moeten worden om persoonsgegevens te beveiligen, in het belang van de burger en de gemeenten zelf.

2.4 Aanpak

De onderzoeksvragen worden beantwoord door middel van een analyse van documenten in deskresearch, interviews met bestuur en vertegenwoordigers vanuit de ambtelijke organisatie en tot slot zijn er verschillende gesprekken gevoerd met raadsleden. De documenten bevatten beleid en rapportages van de gemeente Hof van Twente op het gebied van informatiebeveiliging. De documenten die zijn bestudeerd zijn in bijlage 1 opgenomen, evenals de functies van de functionarissen van de gemeente Hof van Twente die zijn geïnterviewd. Aan alle fracties van de gemeenteraad van Hof van Twente is gevraagd of zij een gesprek met de onderzoekers wensten. Alle fracties hebben dit bevestigend beantwoord en de onderzoekers hebben met ten minste een raadslid van elke fractie gesproken. De deskresearch en interviews vonden plaats in de periode december 2021 en januari/ februari/maart 2022.

De nota van bevindingen is op 11 april 2022 aan de gemeentesecretaris aangeboden voor de feitencheck in het kader van de ambtelijke hoor en wederhoor. Naar aanleiding van de feitencheck door de ambtelijke organisatie is de nota van bevindingen deels aangepast. Het rapport, met conclusies en aanbevelingen, is op … mei 2022, voor een bestuurlijke reactie aangeboden aan het college van B&W. Op … 2022 is het rapport via de griffie aangeboden aan de gemeenteraad.

2.5 Leeswijzer

Hieronder volgt in hoofdstuk 3 een korte reprise van de hack van 1 december 2020. Daarna volgen in de hoofdstukken 4 tot en met 11 de bevindingen in de volgorde van de onderzoeksvragen 1 tot en met 8 (zie tabel 1). Onderzoeksvraag 9 bevat de conclusies en aanbevelingen die in 'Samenvatting, conclusies en aanbevelingen' vóór hoofdstuk 1 zijn opgenomen. In de bijlagen volgen respectievelijk een lijst met in ICT veel gebruikte afkortingen en termen, de lijst met geraadpleegde stukken en geïnterviewde functionarissen, onderzoeksvragen en normen en tot slot de volwassenheidsindex van NOREA.

3 De hack – een korte reprise

Er is al veel geëvalueerd en onderzocht met betrekking tot de hack met ransomware die 1 december 2020 bij de gemeente Hof van Twente manifest werd. In het kort beschrijven we hieronder de gebeurtenissen die daartoe leiden en de crisis- en projectorganisatie na 1 december 2020.

Voor 1 december

Door aanpassing van de firewall stond sinds oktober 2019 de poort van een server naar het internet toe open. Daarop draaide een kwetsbare applicatie waardoor het mogelijk was om op afstand in te loggen. Een medewerker heeft op 15 oktober 2020 het wachtwoord van een beheerder-account (admin-account) omgezet naar een eenvoudig wachtwoord. De extra beveiliging met een 2 factor authenticatie (2FA) was voor dit account uitgezet.

Het wachtwoord werd via de open poort naar internet met een brute force aanval gehackt. Dat wil zeggen dat talloze malen werd geprobeerd in te loggen met een variatie aan wachtwoorden. Die aanval werd niet gedetecteerd via logs of via een applicatie dat verdacht verkeer opspoort. Daarbij is het zwakke wachtwoord buit gemaakt.

Het beheerdersaccount had verregaande rechten. De segmentering, dat zijn interne drempels in de systemen zodat iemand die eenmaal binnen is niet overal bij kan, kon het verder doordringen in de systemen niet voorkomen. De hacker kon gedurende 3 weken zijn gang gaan en de ransomware aanval voorbereiden. Ook dat verkeer is niet gedetecteerd of als verdacht naar voren gekomen.

Daarbij is de informatie op servers deels vernietigd en deels versleuteld. Van de back-ups was geen kopie bewaard op een externe locatie, los van de systemen. De back-ups zijn deels vernietigd en deels versleuteld. Ook de back-ups bij de leverancier die de hosting van een deel van de systemen uitvoerde. Een deel van de systemen was gelukkigerwijs naar de cloud overgebracht en behouden gebleven, zoals het zaaksysteem en intranet.

1-12-2020 en daarna

Op 1 december 2020 gingen de systemen uit de lucht. De volle omvang van het probleem was nog niet direct duidelijk. Eerst werd contact opgenomen met de IBD, maar het duurde even voordat ook daar de impact volledig doordrong. Op 2 december 2020 is aangifte gedaan bij de politie en is bij de Autoriteit Persoonsgegevens (AP) gemeld dat er sprake was van een datalek. Het meldingsformulier voor een datalek bleek niet geschikt om een incident van deze omvang goed te registreren.

Immense impact

De impact bij bestuur en medewerkers is groot. Iedereen die we hebben gesproken heeft het over een afschuwelijke en desastreuze ervaring. Jaren aan verzamelde gegevens zijn kwijt of gecorrumpeerd. Een respondent geeft het als volgt weer: "Er is een bom ontploft in het gemeentehuis, maar

niemand ziet het." Getracht wordt snel de systemen en data opnieuw op te zetten. Op 4 december 2020 zijn uitkeringen aan kwetsbare groepen inwoners uitbetaald, dit had een hoge prioriteit.

In de eerste week is er naast de hectiek van de hack en de wederopbouw van de systemen ook heel veel media-aandacht. Op 1 december 2020 is een crisisteam gestart, waarna het proces werd ingericht vergelijkbaar met Grip 3 van de Veiligheidsregio. In het crisisteam zaten onder andere gemeentesecretaris, communicatie, concerncontroller en afdelingsmanager ICT en vanuit het bestuur de burgemeester en een wethouder. De concerncontroller was vervanger van de CISO, die vanaf begin oktober 2020 met zwangerschapsverlof was. Na verloop van tijd werd er een onderscheid gemaakt tussen een bestuurlijk en ambtelijk deel van het crisisteam.

Op advies van de leverancier werd begin december 2020 een nieuwe server geïnstalleerd en getracht met een eerste scan data te herstellen. In overleg met een forensisch onderzoeksbureau (NFIR) werd daarna gekozen voor een andere leverancier die de nieuwe systeemomgeving heeft opgebouwd.

Ondersteuning

Ondersteuning, direct na de hack, kreeg de gemeente van andere gemeenten, zoals Lochem, Enschede en Rotterdam. En ondersteuning van de IBD en de Veiligheidsregio en van private partijen zoals het forensisch onderzoeksbureau NFIR. Op 10 december 2020 stonden de firewall en de eerste systemen en was de mail weer beschikbaar. Op 4 december 2020 was een eerste begin gemaakt met de opbouw van de ICT-systemen en konden uitkeringen worden betaald. Respondenten herinneren zich dat iedereen erg betrokken was en de schouders eronder zetten.

De hackers zijn door de gemeente niet betaald geworden, hiervoor heeft de gemeente een zorgvuldig proces gelopen waarbij zaken zijn afgewogen vanuit meerdere perspectieven. Omdat de gemeente niet onderhandelt met criminele hackers. En omdat de betrouwbaarheid van de eventueel teruggekochte data niet te garanderen is.

Beeld begin 2022

Het beeld begin 2022 is dat ca. 90% van de systemen weer is hersteld. Medewerkers hebben een jaar lang hard gewerkt om de zaken weer op orde te krijgen en hebben op eieren gelopen. Er heerst bij alle respondenten trots op de organisatie. Met name op het feit dat niet met de vingers naar elkaar wordt gewezen, dat kwetsbare groepen als eerste zijn geholpen, en dat hier heel veel van geleerd kan worden. Ook voor bestuurlijk Nederland buiten Hof van Twente.

4 Informatiebeveiligingsbeleid

Onderzoeksvraag 1	In dit hoofdstuk geven we antwoord op de eerste onderzoeksvraag: In hoeverre beschikte de gemeente Hof van Twente in de periode 2018-2020 over een adequaat informatiebeveiligingsbeleid?
Strategisch informatie-beveiligingsbeleid	In het informatiebeveiligingsbeleid zijn de uitgangspunten en rand-voorwaarden voor informatiebeveiliging neergelegd. In 2017 is dat in het Beleidsplan informatieveiligheid & privacy, met een looptijd van drie jaar. In 2020 is dat vernieuwd in het Strategisch informatiebeveiligingsbeleid 2020-2022. Verantwoordelijkheden, taken en bevoegdheden zijn beschreven, evenals de algemene eisen met betrekking tot de beveiligingsnormen en de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie bij de gemeente.
Verantwoordelijkheden	In het informatiebeveiligingsbeleid is vastgelegd dat de gemeenteraad een toezichthoudende taak is toegekend. De Gemeentewet kent die taak in algemene zin toe aan de raad. Het college is integraal (politiek) verantwoordelijk voor de borging van informatieveiligheid binnen de gemeente. Zij stelt de kaders hierop. De ambtelijke verantwoordelijkheid is gemandateerd aan de gemeentesecretaris. Uiteindelijk is de primaire verantwoordelijkheid in de lijn belegd, wat betekent dat afdelingsmanagers een centrale rol hebben op informatieveiligheid.
2017	In 2017, in aanloop tot het opstellen van het informatieveiligheid- en privacybeleid, is een bestuurlijke discussie met de raad gevoerd over de budgetten voor de I&A-functie. Op basis van een vergelijking met een benchmark werd geconstateerd dat de gemeente zeer zuinig was met investeringen in ICT en informatiebeveiliging. De raad heeft toen structureel middelen ter beschikking gesteld, zij het niet ter gehele dekking van het verschil in de benchmark. Vanaf 2017 is verder gewerkt aan activiteiten op ICT, waarbij informatiebeveiliging werd meegenomen. In 2018 is besloten om een deel van de ICT uit te besteden. Dat wil zeggen dat beheer van de ICT-systemen bij een derde partij werd belegd. Vanwege de schaalgrootte van de gemeente en gebrek aan de benodigde kennis om deze taak zelfstandig uit te voeren. Er is discussie geweest om met andere gemeenten op ICT samen te werken in een Shared Service Centre Netwerk Twente (SSCNT). Dat is er niet van gekomen en uiteindelijk viel de keuze op uitbesteden van het systeembeheer aan een externe professionele partij.
Collegeprogramma 18-22	In het collegeprogramma *2018-2022 Samen Doen!* is informatieveiligheid als onderwerp opgenomen. In hoofdstuk 2 getiteld 'Welke trends zien we en waar gaan we op inspelen?' staat het volgende opgenomen: "Ten eerste hebben steeds meer mensen toegang tot het internet… In de dienst-verlening van de overheid zal de overheid hier proactief op moeten

inspelen, waarbij nadrukkelijk aandacht dient te zijn voor informatie-veiligheid." De ambitie is om daar (nog) meer op in te zetten in een steeds verder digitaliserende samenleving.

Digitale Agenda 2019

In 2019 is de Digitale Agenda vastgesteld, waarin de ambities van de gemeente zijn opgenomen. De agenda ging over het gehele veld van ICT. Met onder andere datagedreven werken als aandachtspunt, wat een relatief nieuw en deels onontgonnen terrein voor gemeenten is. Ook werd informatieveiligheid als speerpunt benoemd. Dat speerpunt is daarna uitgewerkt in drie pijlers van het Programma Informatieveiligheid en privacy (zie hierna). Naar aanleiding van de Digitale Agenda is een stuurgroep gevormd.

Incidentele middelen 2019

De gemeente bleek ook in 2019 minder te investeren in ICT in vergelijking met andere gemeenten in de benchmark. Dat leidde niet tot een structurele verhoging van het budget. De gemeenteraad besloot voor drie jaar incidenteel €1.3 miljoen beschikbaar te stellen om de geformuleerde ambities op ICT en informatiebeveiliging te behalen. De activiteiten ten behoeve van informatiebeveiliging in de drie pijlers (bewustwording, verantwoording en ontwikkeling) zijn opgenomen in een Programma Informatieveiligheid & Privacy 2020 (zie hieronder).

Protocollen/procedures

In 2017 is door het college het Handboek Informatieveiligheid 2017 vastgesteld. Daarin zijn de uitgangspunten voor informatiebeveiliging van de gemeente opgenomen en vormt een naslagwerk voor management en medewerkers. Hierin is de Baseline Informatiebeveiliging Gemeenten (BIG)[7] vertaald naar de gemeente Hof van Twente. Als onderwerpen bevat het handboek de voorschriften van de BIG op onder andere de organisatie van informatiebeveiliging, fysieke beveiliging, de toegangsbeveiliging, beveiligingsincidenten, continuïteitsbeheer en naleving. De uitgangspunten betreffen onder meer de wachtwoorden, compartimentering of segmentering van de systemen back-up beleid enz. De naleving van de maatregelen op informatiebeveiliging is, belegd bij MT en de proces-verantwoordelijken (managers) conform de BIG.

Deze voorschriften en uitgangspunten moeten dan nog uitgewerkt worden in procedures en protocollen. Deze zijn grotendeels meegenomen in de drie pijlers van het Programma Informatieveiligheid en Privacy van 2020: bewustwording, inzicht in de gevolgen van eigen gedrag; verantwoording, met behulp van de ENSIA-rapportage; ontwikkeling, voldoen aan de richtlijnen van BIO en AVG. In een schema van dat programma is opgenomen wat op de drie pijlers in de periode 2017-2019 is gerealiseerd en waar nog inspanningen op gepleegd moeten worden. Op de pijler Ontwikkeling, wat het voldoen aan de richtlijnen van BIO-normen en AVG inhoudt, waren onder andere de volgende resultaten genoemd: invoeren

[7] Vanaf 2019 Baseline Informatiebeveiliging Overheid (BIO).

2FA (tweefactor authenticatie), wachtwoordbeleid, informatiebeveiligings-beleid, zonering (of segmentering) en pentesten. De punten waar de gemeente nog mee bezig was of waar deze nog mee moest starten, betroffen back-up & restore, toegangsbeveiliging, beheerplan en logging.

Bestuurlijke aandacht

Uit de interviews blijkt dat het bestuur aandacht had voor het onderwerp en draagvlak voor investeringen, maar informatieveiligheid was niet een heel groot of structureel terugkerend onderwerp aan de bestuurstafel en in de gemeenteraad. Op de gebruikelijke jaarlijkse rapportagemomenten na, zoals ENSIA. In bilaterale gesprekken tussen bestuur en ambtelijke organisatie is er destijds aandacht geweest voor de risico's op het gebied van informatiebeveiliging, met de kennis van nu blijkt dat dit niet op de juiste wijze heeft plaatsgevonden. Het college en de directie kregen geen signalen dat er mogelijk iets mis was met processen op informatieveiligheid. Informatiebeveiliging wordt omschreven als een technisch onderwerp waar de collegeleden zelf niet veel inhoudelijke kennis van hadden. Er moest in het kader van bedrijfsvoering noodzakelijkerwijs aandacht aan besteed worden. Er werden echter weinig verdiepende vragen over gesteld, behalve naar aanleiding van incidenten elders.

Budget CISO

Opvallend in het strategisch informatiebeveiligingsbeleid 2017 en 2020 is de passage dat de CISO geen eigen budget tot beschikking heeft. In 2020 is daarbij opgemerkt dat dat contrair is aan het advies van de IBD. Gesteld wordt dat als na verloop van tijd blijkt dat dit niet werkt, dit in overleg met de afdeling bedrijfsvoering wordt aangepast. Respondenten geven aan dat dit een pragmatische keuze was en geen principiële keuze. Daarmee werden de uitgaven van de CISO voor activiteiten voor de afdelingen afhankelijk van de betreffende leidinggevenden. Er bestaat een risico dat afdeling overstijgende uitgaven op informatiebeveiliging niet zouden worden uitgevoerd. Voor uitgaven voor algemene maatregelen of activiteiten, zoals pentesten, kon de CISO een onderbouwd beroep doen op het budget van Bedrijfsvoering. Respondenten geven aan dat er, gelet op de grootte van de organisatie, pragmatisch voor gekozen is geen aparte budgetten te hanteren voor centrale organisatievraagstukken waar de concernstaf verantwoordelijk voor is.

5 Uitvoering van het beleid

Onderzoeksvraag 2	De tweede vraag ziet toe op de uitvoering van het informatiebeveiligingsbeleid in de periode voor 1 december 2020. Is het beleid adequaat uitgevoerd?

Op papier	Uit de interviews wordt duidelijk dat op 30 november 2020 de betrokken ambtenaren en bestuurders het idee hadden met informatieveiligheid op de goede weg te zitten. Vanaf 2017 waren extra middelen uitgetrokken voor ICT en informatiebeveiliging, eerst structureel daarna incidenteel. Er waren keuzen gemaakt om netwerk- en systeembeheer uit te besteden. Er was een programma, met onder andere filmpjes over phishing, gestart op basis van de pijlers bewustwording, verantwoording en ontwikkeling (zie hiervoor). De functies op informatiebeveiliging en privacy waren ingevuld en gepositioneerd (zie ook hoofdstuk 6). Er werden geen mogelijke problemen gesignaleerd met betrekking tot de uitvoering van het informatiebeveiligingsbeleid. Ook uit een pentest, medio 2020 is uitgevoerd, kwamen geen hoog kritieke risico's naar voren (zie hoofdstuk 7).
Compliance	Vanaf 2020 was het uitgangspunt voor de gemeente Hof van Twente de Baseline Informatiebeveiliging Overheid (BIO), voorheen Baseline Informatiebeveiliging Gemeenten (BIG). De focus lag op de verbeterpunten die naar aanleiding van de risicoanalyses en de ENSIA werden geconstateerd. De veronderstelling was dat als de gemeente 'compliant' was op de BIO-maatregelen, de gemeente 'in control' was. De gemeente voldeed volgens een van de respondenten voor meer dan 90% aan de formele eisen. Handvat voor de uitvoering van de activiteiten op informatiebeveiliging, en privacy, was in 2020 het Programma informatieveiligheid en privacy.
Pijler Bewustwording	Op de pijler Bewustwording overheerste het gevoel dat de gemeente goed bezig was, ambtenaren ontvingen verschillende trainingen en de gemeente organiseerde activiteiten, zoals de week van informatieveiligheid om de bewustwording bij ambtenaren te vergroten. De CISO kwam 1 à 2 keer per jaar bij afdelingsoverleggen langs om informatieveiligheid onder de aandacht te brengen. Door corona gebeurde dat weliswaar minder, maar de aandacht voor informatiebeveiliging nam volgens de respondenten langzaam maar zeker toe. Bij een aantal activiteiten op bewustwording werd het college door ambtenaren betrokken, zodat duidelijk werd dat het onderwerp bestuurlijk belangrijk werd gevonden.
Pijler Verantwoording	In de pijler Verantwoording waren met name de activiteiten opgenomen met betrekking tot de ENSIA-rapportage richting de landelijke toezichthouders en de gemeenteraad. ENSIA behelst de rapportage over de audits en zelfevaluaties van de verschillende applicaties die de gemeente gebruikt. Zoals de audits voor Suwinet en DigiD en de zelfevaluaties van de

Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en Basisregistratie Ondergrond (BRO). In het kader van ENSIA zijn deze audits in 2020 voor het jaar 2019 uitgevoerd.

Pijler Ontwikkeling

In de pijler Ontwikkeling zaten de activiteiten bedoeld om te voldoen aan de BIO- en AVG-normen. Op informatiebeveiliging ging het om het opstellen van de verschillende protocollen en procedures en uitvoeren van penetratietesten. Afgerond en geïmplementeerd waren wachtwoorden-beleid, beleid telewerken, incidentmanagement en zonering. Voor 2020 stonden op het programma onder andere 'back-up & restorebeleid', toegangsbeveiliging, bedrijfscontinuïteit en wijzigingsbeheer.

Hieronder gaan we nader in op een aantal protocollen die van belang zijn, terugkijkend met de ervaring van de hack die op 1 december 2020 manifest werd.

Incidentmanagement

Incidentmanagement is erop gericht medewerkers incidenten en datalekken te laten rapporteren en ervan te leren. De procedure hiervoor is in 2019 opgesteld. In de teams is de teamcoördinator de proces-verantwoordelijke. Ieder incident dient in Topdesk geregistreerd te worden. Voor de eerste lijn zijn handreikingen beschikbaar om veelvoorkomende incidenten op te lossen. Als het incident daarmee niet opgelost kan worden is er in de tweede lijn een behandelgroep aanwezig met collega's of is er een zogenoemde oplosgroep per applicatie met een functioneel applicatiebeheerder en technisch applicatiebeheerder. Maandelijks dienen de eerste en tweede lijn gezamenlijk de omvang en aard van de meldingen te analyseren en eventueel verbetermaatregelen voor te stellen.

Als blijkt dat escalatie nodig is vanwege een aanpassing van het systeem, wordt een melding gedaan naar de leverancier of een andere derde partij. De leverancier van het systeembeheer gebruikte ook een soort Topdesk, en daar kon mee geschakeld worden als het een incident met betrekking tot systeembeheer betrof. De servicedesk deed vanuit Topdesk een melding richting de leverancier, met een prioriteit erbij. Uit de interviews blijkt dat de ervaring was dat de communicatie over en weer hierop niet optimaal verliep.

Back-up & restore

Het Back-up & restorebeleid stond voor 2020 op de planning. Naar aanleiding van de ervaring van 1 december 2020 (zie hoofdstuk 3) kan geconstateerd worden dat dit beleid, achteraf gezien, nog niet goed functioneerde.

2FA

Het beleid op 2-factor authenticatie was afgerond en geïmplementeerd. In 2019 is met de incidentele middelen die beschikbaar kwamen de mobiele telefonie voor de medewerkers uitgerold. Daarmee kon ingeregeld worden dat met een dubbele authenticatie beveiligd ingelogd kon worden op de systemen. In principe zou dat voor elk account ingesteld moeten zijn

geweest. Geconstateerd kan worden dat dit niet het geval is geweest, in ieder geval niet voor het beheerdersaccount dat gehackt werd.

Volwassenheid

NOREA, de beroepsorganisatie van IT-auditors, hanteert een schaal van 1-5 om de volwassenheid van organisatie op informatiebeveiliging te meten (zie bijlage 5). Bij een volwassenheidsniveau 3 is de gemeente wat betreft beleid op en uitvoering en verantwoording van de activiteiten op informatiebeveiliging in control. Bij 1 zijn de beheersingsmaatregelen aanwezig, maar worden niet consistent toegepast. Bij 2 zijn de beheersingsmaatregelen aanwezig, worden consistent maar informeel toegepast. Uit de documenten en de interviews blijkt dat in het geval van Hof van Twente in 2020 de administratieve basis gedeeltelijk aanwezig en grotendeels informeel werd toegepast waardoor het zicht op de adequate uitvoering van het beleid ontbrak.

6 Functies op informatiebeveiliging

Onderzoeksvraag 3	In dit hoofdstuk beantwoorden we onderzoeksvraag 3: Op welke wijze heeft de gemeente Hof van Twente de functies voor Informatiebeveiliging en privacy in de organisatie ingevuld. Hoe zijn deze functionarissen gepositioneerd?

CISO

De CISO-functie was voor 8 uur per week ingevuld, door degene die daarnaast bestuursadviseur en stafmedewerker bedrijfsvoering was. De CISO-functie werd op strategisch niveau binnen de concernstaf ingevuld, waardoor de onafhankelijkheid was geborgd. De CISO was vooral beleidsmatig en organisatorisch gericht en heeft voor 2020 specifieke opleiding gevolgd. De CISO had geen ICT-achtergrond of diepgaande kennis over ICT of informatiebeveiliging. Die kennis zou door de medewerkers van het team I&A ingebracht worden. Daarnaast werd expertise op ICT en informatiebeveiliging extern gehaald, zoals systeembeheer of pentesten die door derden werden uitgevoerd.

De taak van de CISO zat volgens de respondenten vooral op bewustwording en op het op de kaart zetten van informatieveiligheid in de gemeentelijke organisatie. Daarvoor werd kennis van informatiebeveiliging op hoofdlijnen voldoende geacht. De CISO moest de verbinding zoeken met de afdelingen, de beginselen van de BIG en later de BIO uitleggen en verspreiden. Er is door de CISO een week van de informatieveiligheid georganiseerd, phishing mails uitgezet, langsgegaan bij de teamoverleggen, enzovoorts. Daarnaast stelde de CISO de beleidsplannen en jaarplannen over informatiebeveiliging op, die het management en college vaststelden. En coördineerde ze de ENSIA-rapportages.

Capaciteit

Op de kaart zetten van informatiebeveiliging in de organisatie vergt veel ontwikkel- en opbouwwerk. Protocollen, procedures en processen moeten opgezet en ingericht worden. Dat vergt ook inzet en capaciteit op tactisch en operationeel niveau, zeker met het oog op de ondersteuning van de organisatie met een volwassenheidsniveau tot 2 (zie bijlage 4). Volgens geïnterviewden zou, als de ontwikkel- en opbouwfase voorbij zou zijn, de capaciteit van 8 uur voor de CISO op strategisch niveau voldoende moeten zijn. De huidige stand van zaken is dat de gemeente een CISO werft samen met een buurgemeente voor 1 FTE, voor beide gemeenten 0,5 FTE (18 uur per week).

Budget CISO

Zoals hierboven al is gemeld beschikte de CISO in de periode voor 1 december 2020 niet over een eigen budget, ook al was dat een aanbeveling van de IBD. Als reden wordt aangegeven dat de gemeente Hof van Twente een middelgrote gemeente, is waarbij niet iedereen over een eigen budget beschikt. De CISO heeft daar wel voor gepleit, maar zich er uiteindelijk bij neergelegd en aanvragen gedaan ten laste van het budget van bedrijfs-

voering. Volgens de toenmalige CISO werden alle aanvragen, die goed waren onderbouwd, gehonoreerd en zijn noodzakelijke investeringen wel gerealiseerd.[8]

Overleggen

De CISO had structureel iedere week overleg met de gemeentesecretaris. Daarnaast was de CISO vaak aanwezig bij het driewekelijkse portefeuillehouders overleg. Alleen niet altijd als CISO, maar als stafmedewerker. Informatiebeveiliging was op dat overleg geen vast agendapunt. Door een van de respondenten is aangegeven dat 3-4-maandelijks de CISO en FG aanschoven voor de onderwerpen informatiebeveiliging en privacy. De mogelijkheid was er wel om tussendoor zaken op informatiebeveiliging aan te kaarten. Daarvoor kon de CISO de directe lijn met de secretaris en de burgemeester gebruiken, indien nodig.

De CISO had geen regulier overleg met de medewerkers van de afdeling I&A. Wel was die afdeling voor de CISO onder handbereik en was er bijna dagelijks contact. Verder ging de CISO 1 à 2 keer per jaar langs bij de teamoverleggen, om zaken op informatiebeveiliging door te nemen en bewustwording te bevorderen. Ieder team had een eigen aanspreekpunt, de vertegenwoordiger in het kader van ENSIA. Met hen had de CISO regelmatig overleg.

Team I&A

De inhoudelijke kennis op ICT en informatiebeveiliging moest van de vakmensen van I&A komen en die was volgens respondenten bij enkele medewerkers aanwezig. De afdelingsmanager en de teamcoördinator hadden zelf niet de inhoudelijke kennis en hadden ook geen specifieke rol op informatieveiligheid. De teamcoördinator had voornamelijk een leidinggevende en coachende rol op informatiemanagement, DIV, facilitaire dienstverlening en gebouwen. Het team I&A, met in totaal 12 fte, viel daar ook onder. De afdelingsmanager had onder andere twee keer per jaar contact met de externe partij waar het systeembeheer was ondergebracht (zie ook hoofdstuk 8). Daarbij kwam informatieveiligheid wel aan bod, maar dat overleg betrof met name ICT in het algemeen.

Contract- en leveranciers-management

Omdat het beheer van de systemen werd uitbesteed, en geleund werd op de kennis en werkprocessen bij een externe partij, was er ook behoefte aan kennis specifiek op contract- en leveranciersmanagement. Door respondenten wordt geconstateerd dat die niet aanwezig was in de gemeentelijke organisatie, om goed de regie te voeren op de externe partij.

[8] De huidige CISO gaat hier aandacht voor vragen en ervoor pleiten dat hij een eigen budget krijgt.

7 Monitoring en toetsing van de uitvoering

Onderzoeksvraag 4	De vierde vraag die in dit hoofdstuk wordt beantwoord luidt: Is de uitvoering van het beleid in die periode (vóór 1 december 2020) adequaat getoetst en gemonitord?

Er zijn verschillende manieren waarop de werking van het beleid en de systemen gemonitord en getoetst worden. In het normenkader zijn enkele opgenomen (zie bijlage 3). De werking en effectiviteit daarvan lopen we in dit hoofdstuk na.

ENSIA

Voor de verticale (externe) verantwoording richting landelijke toezicht-houders en de horizontale (interne) verantwoording richting de gemeenteraad is ENSIA opgezet. Daarbij worden de belangrijke applicaties, zoals Suwinet en DigiD, aan een landelijke audit onderworpen. De eisen zijn relatief streng en op herhaalde keren niet voldoen volgt afsluiting van de applicatie. Dan kunnen onderdelen van de gemeentelijke dienstverlening niet meer goed uitgevoerd worden. De gemeente heeft in dat geval een substantieel probleem.

Assuranceverklaring

Het college tekent in het kader van ENSIA voor een verklaring dat bij de gemeente de beoogde en ingerichte beheersingsmaatregelen voldoen aan de geselecteerde normen op Suwinet en DigiD. Een externe auditor stelt daarvoor een Assurance verklaring op. Deze werd afgegeven in 2020 in het kader van de ENSIA-rapportage over 2019. Met dien verstande dat op een onderdeel van Suwinet niet voldaan werd aan de normen. Voorwaarde voor de Assurance verklaring is dan dat het college aangeeft verbetermaatregelen in een plan te hebben opgenomen die belegd en gemonitord worden. Voor de toets op andere applicaties wordt volstaan met een zelfevaluatie.

ENSIA ziet ook toe op de vordering die de gemeente boekt op de maatregelen in de BIO en de AVG. Het gaat dan voornamelijk om de risicobeheersing, of de gemeente de risico's in beeld heeft, en of de maatregelen zoals voorgeschreven in de BIO zijn geïmplementeerd. ENSIA ziet met name toe op de opzet en bestaan van maatregelen, protocollen en procedures, niet op de werking van het beleid. De verantwoording in het kader van ENSIA vindt jaarlijks plaats en is opgenomen in de P&C-cyclus.

In het informatiebeveiligingsbeleid is het lijnmanagement primair verantwoordelijk. Dit om te voorkomen dat een onderwerp als informatie-veiligheid alleen de CISO aangaat. Deze is op strategisch niveau adviseur en onafhankelijk controleur van het beleid en de uitvoering. De CISO is coördinator van de ENSIA-rapportage en wordt daarvoor met informatie gevoed door de contactpersonen in de teams.

Geen ISMS

Voor onder andere het vullen van ENSIA kan een applicatie gebruikt worden, zoals een Information Security Management System (ISMS). Een ISMS is een geautomatiseerd systeem waarin activiteiten en resultaten op informatiebeveiliging worden bijgehouden. Onderdeel van een ISMS is de Plan-Do-Check-Act cyclus (PDCA), waarmee een beleidsleercyclus gevormd wordt. Daar is door de gemeente geen gebruik van gemaakt.

De CISO besprak met de concerncontroller, als leidinggevende, de volledigheid van de ENSIA-rapportage, het totaalbeeld en de conclusies. Mede om de communicatie met college en de raad vorm te geven.

Rapportages

Naast de jaarlijkse ENSIA-rapportage, en onderliggende stukken, kreeg het college in 2019-2020 geen andere rapportages op informatieveiligheid op de bestuurstafel. Bestuurlijk en op papier waren er geen reden om diepgravende vragen te stellen over de stand van zaken op informatie-beveiliging. Ook de gemeentesecretaris kreeg hierop geen signalen en had de indruk dat de processen op informatieveiligheid goed functioneerden.

Afstemming met leverancier

De monitoring op de systemen en het systeembeheer werd door de externe leverancier uitgevoerd, in afstemming met de afdeling I&A. Op operationeel vlak was er contact tussen de medewerkers van de afdeling en de uitvoerende externen. Op strategisch vlak was halfjaarlijks overleg tussen de afdelingsmanager en de leverancier. De CISO had geen structurele rol en werd alleen bij uitzondering en bij incidenten betrokken. De teamcoördinator had geen rol hierop en had, zoals eerder gemeld een meer coachende rol.

Op operationeel terrein ontstond soms ruis in de communicatie tussen gemeente en leverancier. Dat ging vaak over niet tijdig of alert acteren op de onderlinge communicatie en signalen. Daar is op strategisch niveau door de afdelingsmanager over gesproken met de leverancier.

Pentest 2020

In de BIO en het gemeentelijk beleid zijn pentesten op de technische infrastructuur voorzien als middel om de systemen te testen. In de Management Letter 2018 en 2019 constateert de accountant dat er in die jaren geen pentest zijn gedaan. In de zomer van 2020 zijn pentesten door een externe partij uitgevoerd, met ethische hackers. Die partij werd geselecteerd uit een aanbesteding via de VNG.

Met de pentest is getest op toegang tot het domein vanaf internet, toegang tot de achterliggende systemen en aanvullende testen voor toegang tot onderdelen op het domein en andere systemen om gegevens in te kunnen zien, te wijzigen of te vernietigen. In totaal zijn uit de pentest 11 bevindingen voortgekomen, waarvan 1 een middelhoog risico vormde, 5 een laag risico en 5 geen risico. Het middelhoge risico werd gevormd door ontbrekende autorisatie op een SMTP-server voor e-mails. Daarbij werd melding gemaakt van een SMTP-server die open stond naar het internet waardoor het voor iedere kwaadwillende mogelijk was om daar misbruik

van te maken. De FTP-server die al vanaf 2019 open stond is niet expliciet genoemd als risico, noch zijn eventueel andere kritieke risico's gesignaleerd.

Respondenten geven aan dat het ontbreken van specifieke technische kennis een rol heeft gespeeld bij het interpreteren van het pentestrapport, waardoor mogelijke risico's niet goed zijn ingeschat. Er lijkt niet indringend en diepgravend doorgevraagd op eventuele risico's. Mogelijke risico's zijn ook niet doordringend geduid door de testers, in ieder geval is het risico dat leidde tot de hack niet gesignaleerd. Het rapport is door de CISO en de afdeling I&A aangenomen en de aanbevolen activiteiten naar aanleiding van de pentest zijn uitgezet. Er hoefde niet opgeschaald te worden naar secretaris of college, er waren geen kritieke risico's te melden.

Toegangsrechten

In het beleid is afgesproken dat periodiek een uitdraai wordt gemaakt van de toegangsrechten van medewerkers op de applicaties. En dat deze lijst op juistheid en volledigheid wordt gecontroleerd. Uitgangspunt dat zowel de lengte als complexiteit van het wachtwoord volgens het wachtwoorden-beleid in combinatie met de voorwaarde van 2FA adequaat zou moeten zijn als iedereen zich hieraan houdt. Op de complexiteit van wachtwoorden en de implementatie van 2FA wordt niet gecheckt. Tijdens de pentest is ook niet gecheckt of de wachtwoorden en de implementatie van 2FA voldoen aan het vastgestelde beleid en de afspraken. Het simpel te raden wachtwoord waardoor de hacker in november 2020 toegang kreeg tot de systemen voldeed wat betreft lengte aan de eisen, maar niet wat betreft complexiteit. Daar vond geen monitoring op plaats.[9]

Logging en monitoring

Verdacht verkeer in de systemen kan via logging opgemerkt en opgespoord worden. Dat is volgens de respondenten deels geïmplementeerd bij de gemeente, in ieder geval bij de applicaties waarop in het kader van ENSIA strikt toezicht wordt uitgevoerd, zoals Suwinet en DigiD. Het verdachte verkeer van november 2020 is door de externe systeembeheerder niet opgemerkt, althans niet blijkt dat dit gemeld is aan de ambtelijke organisatie.

Door de gemeente is overwogen om via een aanbesteding van de VNG een applicatie voor de monitoring van de computerdreigingen aan te kopen. Dat is een zogenoemde SIEM/SOC (Security Information & Event Management/Security Operations Center). Dat is uiteindelijk niet aangeschaft. Volgens een van de respondenten vanwege de kosten.

[9] De onderzoekers hebben het wachtwoordenbeleid gekregen, maar het is niet gedateerd en het is niet duidelijk of het beleid naar aanleiding van de hack is gewijzigd. 2FA (of multifactor authenticatie, MFA) was voor de gebruikers en de admin-accounts verplicht, ook in de periode voor 1-12-2020. Het wachtwoord dat gehackt is voldeed in ieder geval niet aan de eisen van lengte en complexiteit zoals voorgeschreven in het verkregen wachtwoordenbeleid.

Na 1 januari 2021 wordt op technisch gebied voor de gemeente door NFIR het netwerkverkeer doorlopend gemonitord op basis van een zogenoemd Managed Detection Response (MDR).

Compliance

Informatieveiligheid leek bij de gemeente 'in control'. Respondenten geven aan dat de overheersende indruk was dat de gemeente compliant was met de richtlijnen op informatieveiligheid. Op papier leek de gemeente op goede koers te liggen. Bestaan en opzet van beleid waren op orde en de vinkjes konden in ENSIA gezet worden. Op basis van de audits leek ook de werking van het beleid in de praktijk op orde. Respondenten gaven aan dat het medio 2020 ondenkbaar was dat bij de gemeente het systeem kon worden platgelegd, zoals op 1 december 2020 is gebeurd.

Accountant

Accountants schenken de laatste jaren bij de rechtmatigheidscontrole van de gemeenterekeningen ook aandacht aan informatieveiligheid. Sommige gaan zelfs zover om bijvoorbeeld het wachtwoordenbeleid te testen door middel van een audit op de Active Directory. De accountant van de gemeente Hof van Twente heeft bij de interimcontrole over 2019 een beperkte IT-audit uitgevoerd. In de managementletter constateert de accountant dat er verbeteringen nodig zijn op informatieveiligheid en pleit de accountant voor functiescheiding op de verschillende soorten functies. Uit de interviews blijkt dat de gemeente vanwege de schaalgrootte de aanbeveling niet heeft opgevolgd. De interimcontrole over 2020 is door de hack van 1 december 2020 niet meer uitgevoerd.

Cultuur en leidinggeven

De invulling van monitoring en controle hangt ook samen met de cultuur binnen de ambtelijke organisatie. In de gemeente Hof van Twente wordt gewerkt vanuit de kernwaarden leiderschap, eigenaarschap en vertrouwen. Er heerst een zachte manier van leidinggeven, meer coachend en faciliterend van aard, zo geven respondenten aan. Er zijn korte lijnen, niet hiërarchisch en de open cultuur zorgt ervoor dat men elkaar snel vindt. Er heerst vertrouwen in elkaar en naar externen. Respondenten geven aan dat het voor een professionele organisatie randvoorwaardelijk is te controleren en elkaar zakelijk aan te spreken op zaken die niet goed gaan. Daar hoort ook een zakelijke houding en feedback richting externe leveranciers bij.

Monitoring na 1 december 2020

Voor 2021 heeft Hof van Twente de ENSIA-toets met betrekking tot DigiD en Suwinet uit laten voeren door een extern bureau. Dit heeft plaatsgevonden in december 2021 en januari 2022. De resultaten waren begin maart 2022 nog niet bekend. Voor de hack voldeed de gemeente voor 92% aan de BIO-maatregelen, dat is daarna niet meer gemeten.

Jaarverslag 2020 light

Vanwege de hack heeft de gemeente over 2020 een jaarverslag 'light' gepubliceerd. Daarin staat onder andere vermeld dat er 52 meldingen zijn gedaan van 34 verschillende veiligheidsincidenten. De meest bekende is uiteraard de hack van 1 december 2020. In 26 gevallen ging het in 2020 om meldingen van een phishingmail, en daar is snel en adequaat op geacteerd.

Eind 2022	Na oplevering van het programma ‘De Nieuwe Werkelijkheid’ en voltooiing van het ‘Verbeterplan’ bestaande uit 18 actiepunten zal naar verwachting eind 2022 het programma zijn voltooid en zal de veiligheid op orde zijn. Daarna zal het nieuwe systeem worden onderzocht. Reguliere pentesten, phishing mail zullen vanaf dat moment regulier door de gemeente worden uitgevoerd.

8 Externe leveranciers

Onderzoeksvraag 5	In dit hoofdstuk beantwoorden we vraag 5: welke afspraken op informatiebeveiliging zijn gemaakt met externe leverancier(s) en hoe zijn deze gemonitord?

Uitbesteden

In de periode voor 2017 constateerde de gemeente dat een middelgrote gemeente zoals Hof van Twente zou kunnen onderzoeken in hoeverre meer samenwerking met andere gemeenten op ICT een mogelijkheid zou kunnen zijn. Dit is onderzocht en heeft niet tot een gezamenlijke shared serviceorganisatie geleid. Daarom is besloten om ICT-onderdelen van bedrijfsvoering aan een externe commerciële partij uit te besteden. Het uitbesteden heeft plaatsgevonden en er is een contract gesloten met GIBIT-voorwaarden van de VNG. Dit biedt waarborgen voor de gemeente. In dit hoofdstuk ligt de focus op de externe leverancier die ICT voor de afdeling I&A van de gemeente Hof van Twente leverde.

Relatie

De gemeente had twee keer per jaar een strategisch niet-bestuurlijk overleg met de externe partij. De gemeente beschikte ten dele over inhoudelijke ICT-kennis (tactisch beleidsniveau en op uitvoerend niveau) en de indruk uit de interviews is dat de relatie vanuit de gemeente getypeerd kan worden als een relatie van partners op basis van vertrouwen en in mindere mate van opdrachtgever en opdrachtnemer.

Uit de interviews komt naar voren dat de relatie met de externe partij op operationeel niveau moeizaam was. Operationeel niveau hield in dat de vakspecialisten van de gemeente en de uitvoerenden van de externe leverancier contact hadden en dat de communicatie als moeizaam werd ervaren. Vanaf begin 2020 werd dit ook duidelijk bij de leidinggevende en die is aangeschoven bij de reguliere overleggen, als generalist en niet vanuit de inhoud.

Uit de interviews komt een beeld naar voren dat de overige betrokkenen uit de ambtelijke organisatie en bestuur dachten dat het wel goed zat met de externe leverancier. De CISO en controller kregen geen signalen en hadden niet de indruk dat het niet goed ging met de externe leverancier.

Achteraf vragen sommige respondenten zich af waarom er niet opgeschaald is over de communicatie naar strategisch en bestuurlijk niveau. Ook is de vraag gesteld wie de regie had in de relatie opdrachtgever-opdrachtnemer. Respondenten geven aan dat het de gemeente ontbrak aan een adequaat contract- en leveranciersmanagement. De relatie en afspraken met de externe partij waren voor een groot deel op goed vertrouwen gebaseerd.

Een andere gedachte die naar voren is gekomen is de afhankelijkheid van de gemeente bij het uitbesteden van cruciale dienstverlening. Uit de

	interviews komt naar voren dat de suggestie zou kunnen zijn dat de gemeente zich (te) afhankelijk maakt van één partij, dat maakt kwetsbaar.
Monitoring	Er was vertrouwen dat de externe een partner was en goed functioneerde als 'trusted third party'. De gedachte bij de gemeente was dat in principe de externe leverancier de systemen zou monitoren en bij verdacht verkeer een signaal zou geven aan de gemeente of zelf zou optreden. Zoals bij een 'brute force attack' of langdurige handelingen in de achtergrond door een admin-account. De externe partij heeft volgens de betrokkenen geen impliciet en/of expliciet signaal hierover afgegeven aan de gemeente.
Te goed van vertrouwen	Op papier leek alles goed geregeld en in de uitvoering van opdrachtgever en opdrachtnemer, maar dit bleek achteraf onvoldoende te werken. Er was te weinig controle op hetgeen de externe partij contractueel moest doen, blijkt uit de interviews. De vraag is gesteld, ook in de evaluatie: waren we te goed van vertrouwen? Dit is ook de titel van de evaluatie van Brenno de Winter.
Follow up in 2020	Op operationeel niveau was er medio 2020 een proces gestart om dat met de leverancier op te pakken. De externe leverancier bood aan om via de Product Diensten Catalogus (PDC) op operationeel niveau scherpere afspraken te maken. Door corona is dat proces vertraagd.

9 Positionering raad en informatiebeveiliging

Onderzoeksvraag 6	Dit hoofdstuk gaat in op de rol en positionering van de raad. Is de raad adequaat gepositioneerd geweest om zijn kaderstellende en controlerende rol te kunnen uitvoeren?

Inleiding hoofdstuk

In dit hoofdstuk staat de gemeenteraad centraal. Het bestaat enerzijds uit een feitenconstructie over op welke wijze de raad is geïnformeerd en betrokken is geweest bij informatiebeveiliging. In §9.1 de periode tot de hack van 1 december 2020, §9.2 geeft de ontwikkelingen vanaf de hack tot 1 maart 2022 weer. Voor dit onderzoek zijn alle fracties geïnterviewd. Met hen is besproken hoe zij de hack en het proces daarna hebben beleefd en welke reflectie zij hebben op de hack en de informatiebeveiliging van de gemeente. Dit onderdeel van dit hoofdstuk zijn geen feiten. Van iedere fractie is ten minste één raadslid geïnterviewd. Om die reden is er een alinea besteed aan de beleving door de raad. §9.3 gaat over de kaderstellende en controlerende rol van de raad in relatie tot informatieveiligheid van de gemeente.

9.1 Periode vóór 1 december 2020

Rib 20-9-2016

In de periode 2016-2020 heeft het college twee raadsbrieven naar de raad gestuurd waarin informatiebeveiliging aan de orde komt (20-9-2016 en 17-3-2020). De eerste is een wat algemenere brief met informatie over integrale veiligheid. Op 20 september 2016 is naar aanleiding daarvan een raadsbijeenkomst georganiseerd met het onderwerp: ‘Veiligheid doen we’. Op deze avond is de raad geïnformeerd over het Integraal veiligheidsbeleid 2017-2021, politie en veiligheid, en evenementenveiligheid. Ook is die avond een presentatie aan de raad gegeven over informatieveiligheid en privacy.

Vragen 2017

In het Vragenhalfuur op 14 februari 2017 heeft de raad vragen gesteld over de manier waarop Hof van Twente zich voorbereidt op het Shared Services Netwerk Twente (SSNT) en of vanuit de raad een interne werkgroep ter ondersteuning nodig was. Vanuit het college is daarop aangegeven dat het SSNT nog in ontwikkeling was. ICT was daarbij betrokken en het uitgangspunt was dat gemeenten elkaar daarbij versterken en ondersteunen. Voorwaarde was dat de gemeenten het eerst zelf op orde dienden te hebben. Uiteindelijk is het SSNT er niet gekomen.

AVG

In de raadsvergadering van 8 mei 2018 heeft de burgemeester de raad geïnformeerd over de stand van zaken ten aanzien van de invoering van de AVG. Hierop volgend is op 18 mei 2018 de raad in een informele bijeenkomst bijgepraat over informatieveiligheid en privacy, waarbij de CISO een presentatie heeft gegeven. In deze bijeenkomst is ook toegelicht

hoe de verantwoordingsrapportage ENSIA werkt en in welke fase de gemeente Hof van Twente op dat moment was.

Jaarrekeningen 2017-2019 [10]

In 2017, 2018 en 2019 heeft dezelfde accountant van hetzelfde accountantskantoor de jaarrekening van de gemeente Hof van Twente gecontroleerd. Al deze jaren is een goedkeurende verklaring afgegeven. In hoofdstuk 7 is al aangegeven dat de accountant sinds 2017 aandacht vroeg voor informatiebeveiliging. Zo heeft de accountant aandacht gevraagd en een aanbeveling gedaan om functiescheiding beter te organiseren. Uit gesprekken met raadsleden komt naar voren dat ze hier regelmatig, ook in de auditcommissie, aandacht voor hebben gevraagd. Het college en de organisatie gaven aan dat de gemeente te klein was om overal functiescheiding door te voeren.

Management Letter 2017

In de management letter 2017, uit de door de accountant uitgevoerde IT-audit, komt naar voren komt dat op het gebied van automatisering nog verbeteringen mogelijk zijn. Geadviseerd wordt om hieraan prioriteit te geven. Verder blijkt uit de testwerkzaamheden van de accountant dat zij hebben vastgesteld dat het wachtwoordenbeleid voldoet aan de eisen. Er wordt geconstateerd dat van de 750 actieve netwerkaccounts er ongeveer 370 uitgezonderd zijn van de wachtwoord periodiciteit. Hieronder vallen accounts met administrator rechten, het standaard en administrator account en serviceaccounts van de leveranciers. Voor deze accounts die zijn uitgesloten van het wachtwoordenbeleid is een verhoogd risico op onrechtmatige toegang door onbevoegde functionarissen aanwezig, het risico bestaat dat via die accounts toegang verkregen kan worden tot documenten op het netwerk en applicaties. De accountant adviseert in 2017 om alle wachtwoorden, ook die van leveranciers, aan de eis van periodiciteit te laten voldoen. De accountant waarschuwt ook voor de risico's van een hack.

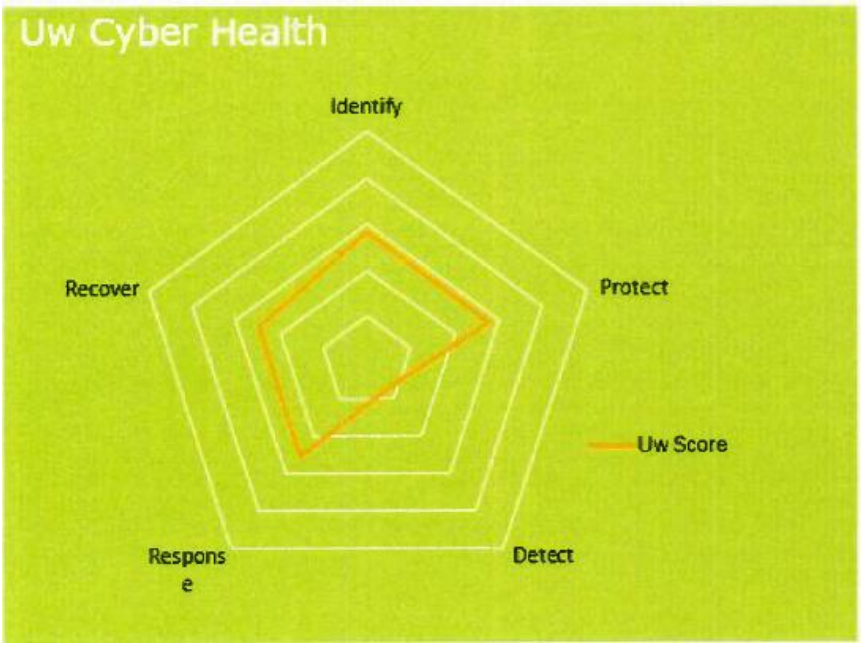
Accountant ML 2018

Eind 2018 heeft de accountant de interimcontrole verricht ter voorbereiding van de controle op de jaarrekening 2018. Op 25 januari 2019 heeft de accountant de Management Letter (ML) 2018 aan de raad aangeboden. In de ML gaat de accountant in op automatisering (hoofdstuk 4). De accountant heeft op basis van interviews een inschatting gemaakt van de kwaliteit van het IT-systeem van de gemeente Hof van Twente. In dat hoofdstuk van de ML is een onderverdeling gemaakt in: voldoende (groen),

[10] Voor dit onderzoek heeft de rekenkamercommissie (rkc) informatie opgevraagd die noodzakelijk was voor dit rkc-onderzoek over informatiebeveiliging. Op grond van art 81 oa Gemeentewet kan de rkc documenten van de betreffende gemeente onderzoeken voor zover opgenomen in de verordening. Niet alle onderzochte documenten kan de rkc openbaar maken. Voor dit onderzoek heeft de rkc onder andere de Management Letter 2018 die door de accountant opgemaakt opgevraagd. Dit document is op 25 januari 2019 aan het college aangeboden. In dit document staat niet vermeld dat dit een vertrouwelijk document is of dat er enige restrictie is opgelegd over de vorm van openbaarmaking dan wel dat de accountant op enigerlei wijze toestemming dient te verlenen voor enige vorm van openbaarmaking uit de Management Letter. Met deze grondslag heeft de rkc voor dit onderzoek en de bijbehorende rapportage passages opgenomen uit de Management Letter.

	benodigd verbetering op (kort) termijn (oranje) en urgente verbetering vereist (rood). De accountant merkt op dat incidenten met cybercrime steeds vaker plaatsvinden en dat bestuurders zich hierop moeten voorbereiden. Om bij te dragen aan de bewustwording is het onderdeel IT door de accountant besproken met de organisatie. In de ML geeft de accountant op 8 aandachtpunten een bevinding over de IT-adviespunten.
IT-beleid, proces, procedures	De structurele monitoring en (IT)beheersing is volgens de accountant goed. Op dat moment is het informatiebeveiligingsbeleid dat in 2017 was vastgesteld en anderhalf jaar oud is als rood beoordeeld. Het gebruikers-beheer Operating systeem (procedure waar bij uitdiensttreding van medewerkers het IT-systeem direct geblokkeerd) is rood beoordeeld. De procedure rondom wijzigingen van applicaties wordt niet vastgelegd, is oranje beoordeeld en vraagt verbetering. Tot slot geeft de accountant aan dat het onderdeel Probleem & Incidentmanagement niet wordt vastgelegd, hiermee kunnen verstoringen worden geïdentificeerd, en is oranje.
Infrastructuur, beveiliging en back up	In 2018 zijn geen Attack en pentesten uitgevoerd, de accountant adviseert om dit periodiek te doen, dat betekent een rode vlag. De uitwijklocatie is ondergebracht bij een externe leverancier. Afspraken zijn opgenomen in een service level agreememt (SLA), dat is als groen gekwalificeerd. Voor de BAG en de Basisregistratie Personen (BRP) heeft in 2018 een recovery test plaatsgevonden, de accountant adviseert dit als een oranje activiteit en adviseert om dit ook voor de andere applicaties uit te voeren. Tot slot oordeelt de accountant groen over Remote Acces: toegang tot het netwerk vindt plaats via twee-factor authenticatie (2FA). Daarnaast vindt lock-out plaats als er een aantal foutieve wachtwoorden worden geprobeerd. Hierdoor is volgens de accountant geen verhoogd risico aanwezig op het raden van wachtwoorden door middel van bijvoorbeeld een bruto-force aanval.
Cybersecurity	In de management letter 2018 zijn aandachtspunten op cybersecurity opgenomen. Het volgende schema over de cyber health van de gemeente Hof van Twente is opgenomen. Op een schaal van 1 (slecht) tot 5 (goed) scoort de gemeente Hof van Twente gemiddeld tussen de 2 en 3.

Afbeelding 1. Score op aandachtspunten cybersecurity, Management Letter 2018 Gemeente Hof van Twente, 25-1-2019.



De score op 'detect' is laag, beneden 1. Dit houdt in dat er maatregelen dienen te worden genomen om de gemeente te beschermen tegen een aanval. Binnen Hof van Twente zijn volgens de accountant, begin 2019, niet afdoende maatregelen getroffen om mogelijke incidenten tijdig te detecteren.

Toegangsbeveiliging

Tot slot besteedt de ML aandacht aan aandachtpunten voor een logische toegangsbeveiliging. Het wachtwoordenbeleid is als groen aangegeven. Het autorisatiebeheer is nagenoeg geheel rood (van de 9 items is er één groen en acht items zijn rood).

Januari 2019 auditcommissie

Het college kondigde aan met de bevindingen en de aanbevelingen van de accountant aan de slag te gaan. De auditcommissie had er vertrouwen in dat dit werd opgepakt en heeft niet meer gevraagd naar de realisatie van de maatregelen.

Accountantsverslag 2018

In het accountantsverslag behorend bij de jaarrekening 2018, gedateerd op 29 mei 2019, staat bij de bevindingen interne beheersing een passage opgenomen over automatisering. De accountant meldt dat IT een steeds belangrijker onderdeel van de bedrijfsvoering wordt en daarmee ook van de jaarrekening-controle. De accountant meldt dat uit hun IT-audit naar voren komt dat op het gebied van automatisering verbeteringen mogelijk zijn. De accountant adviseert het college hier prioriteit aan te geven.

Raadsvergadering

Op 18 juni 2019 bespreekt de raad de jaarrekening 2018. Over ICT is een passage genoemd: 'De gemeente heeft goed aandacht voor ICT, belangrijk voor de toekomst'. Een ander raadslid refereert aan de management letter, namelijk dat er geen Attack- en Pentest is uitgevoerd en er geen autorisatiebeheer wordt uitgevoerd. Een raadslid benadrukt de aandacht voor ICT.

Vragen 2019

Op 28 mei 2019 zijn tijdens het Vragenhalfuur vragen gesteld over gegevensuitwisseling in relatie tot datasamenwerking binnen het kader van de AVG op het niveau van WMO en Jeugdzorg. Hierop heeft het college de raad geïnformeerd.

Management Letter 2019

Het valt op dat de Management Letter 2019 een andere systematiek kent dat in 2018 en in 2017. Op die wijze is het lastig na te gaan in hoeverre de aandachtspunten van de accountant zijn opgevolgd. Wel is het autorisatie-beheer van grotendeels rood naar oranje gegaan, wat een adviespunt inhoudt waarop aanscherping mogelijk is. Verder meldt de accountant dat het IT-beleidsplan verouderd is. Jaarlijks wordt er wel een informatie- en beveiligingsplan opgesteld. Ten aanzien van de beheersingsmaatregelen op IT zijn er verbeteringen mogelijk en wordt een periodieke controle op het wachtwoordenbeleid geadviseerd. In 2019 heeft de gemeente geen Attack en Pentest gehouden, terwijl dat wel op de agenda stond. In de Management Letter 2019 staat: "alleen door een aanbesteding heeft u de test niet kunnen laten uitvoeren, aangezien de door u gekozen partij niet voorkomt in de leverancierskeuze volgens de VNG" [11]. In 2018 besteedt de accountant aandacht aan 'cyber health' en geeft de gemeente Hof van Twente een cijfer op een vijftal indicatoren (zie hoofdstuk 7). Dat komt niet voor in de Management Letter 2019.

Rib 17-3-2020

Op 17 maart 2020 ontvangt de raad de raadsinformatiebrief (rib) ‘Zelfevaluatie informatiebeveiliging 2019’ van de portefeuillehouder. Daarin is de stand van zaken over informatiebeveiliging in het jaar 2019 opgenomen.

Twee raadsbijeenkomsten

Van de twee raadsbijeenkomsten over (informatie)veiligheid en de AVG in 2016 en 2018 is alleen de agenda beschikbaar, een weergave via schrift of via beeld en geluid is niet beschikbaar. Dit hangt samen met de verdwenen informatie door de hack.

9.2 1 december 2020 en de periode daarna

Hack 1 december 2020

Op de ochtend van 1 december 2020 wordt de hackpoging duidelijk. Sommige raadsleden kunnen niet meer bij hun mail komen, anderen merken op dat moment nog niets. De burgemeester informeert de raadsleden persoonlijk. Vanaf dat moment praat de burgemeester iedere twee weken de raad en fractievoorzitters bij. In het begin veelal via besloten bijeenkomsten, omdat veel nog onduidelijk is en er een forensisch onderzoek naar de hack gaat lopen c.q. loopt. Op dat moment is informatie voornamelijk vertrouwelijk en niet openbaar.

24 maart 2021

Op 24 maart 2021 spreekt de raad in een spoeddebat voor het eerst in het openbaar over de cyberaanval van 1 december 2020. Het spoeddebat is

[11] Management Letter 2019, pagina 22. In het schema Beveiliging onder het aandachtspunt’ monitoring’.

door raadsleden aangevraagd. Dit naar aanleiding van het Rapport van Bevindingen van 9 maart 2021, de evaluaties en andere documenten die onder geheimhouding aan de raad zijn verstrekt. Resultaat van de bespreking is het voornemen dat er een extra onderzoek komt, de vorm moet nog nader worden bepaald.

Vanaf maart 2021

De evaluaties over de hack en de gevolgen dateren van begin maart 2020. In maart 2021 en de maanden daaropvolgend zijn de rapporten aan de raad toegelicht en met hen besproken. Toen is onderkend dat de raad op informatiebeveiliging beter in positie dient te worden gebracht. Hieronder volgt een overzicht.

Motie financiën

Op 13 april 2021 komen de gevolgen van de hack in de openbare reguliere agenda van de raad aan bod. Er wordt een motie over de financiële gevolgen van de hack ingediend. Gevraagd wordt om voor eind april 2021 inzicht te krijgen in de financiële gevolgen van de hack en een eventuele begrotingswijziging. De indieners baseren zich op het budgetrecht van de raad (artikel 189 Gemeentewet). De raad dient eerst te beslissen over het budget en het college kan daarna tot uitvoering overgaan. Op 14 april 2021 bespreekt de raad de motie. De wethouder zegt toe dat er in april 2021 een financieel overzicht komt, hetgeen al is toegezegd in het seniorenconvent in februari 2021. De drie indienende fracties trekken de motie in. Op 11 mei 2021 zal de raad hierover verder spreken.

11 mei 2021

In de raadsvergadering van 11 mei 2021 spreekt de raad meningsvormend over het ICT Verbeterplan, de verantwoording over de hack en de financiële gevolgen van de hack. Door raadsleden wordt het college in overweging gegeven voor een wisseling van portefeuilles, tussen burgemeester en wethouders. Het college geeft aan dit te bezien na de gemeenteraads-verkiezingen van 2022.

Bespreking 1 juni 2021

Op 1 juni 2021 spreekt de raad, besluitvormend, over de ICT-situatie (financiën, verbeterplan en verantwoording). In deze bijeenkomst wordt de begroting cyberaanval met dekkingsvoorstel door de raad vastgesteld [12], wordt kennisgenomen van de ‘Bestuurlijke verantwoording behorend bij het Rapport van bevindingen’ en heeft de raad het ICT Verbeterplan

[12] In de raadsvergadering van 1 juni 2021 bespreekt de raad de gevolgen van de cyberaanval en neemt hieromtrent besluiten. De vergaderstukken zijn bijgevoegd en te raadplegen op de site van de gemeente bij de agenda. Het raadsvoorstel noemt 3 bijlagen. Bijlage 1 is de begroting cyber aanval behorende bij raadsvoorstel 20 april 2021. In de openbare agenda van de raad van 20 april staat niets geagendeerd over de ICT of een begroting over de cyberaanval, er is geen enkel document bij de agenda van 20 april gevoegd. Wel is te lezen dat de motie over de financiële gevolgen hack is ingetrokken. In de besluitenlijst van 20 april 2021 staat opgenomen: ‘wethouder zegt toe dat we hier 11 mei over gaan debatteren’. Op 11 mei 2021 staat onder agendapunt 8 (meningsvormend) de ICT-situatie (financiën, verbeterplan en verantwoording), maar de stukken ontbreken op de website. Aan de hand van de mondelinge verhandeling en in de verschillende vergaderingen blijkt niet dat voornoemde stukken vertrouwelijk zijn. Wel staat op de agenda van 1 juni 2021 een begroting cyberaanval behorende bij raadsvoorstel 20 april 2021. Het Verbeterplan wordt vastgesteld door de raad op 1 juni 2021. Het Verbeterplan ontbreekt bij de te raadplegen stukken op de site bij de gemeenteraad (bijlage 2 bij raadsvoorstel 1 juni 2021).

vastgesteld. Deze besluiten zijn genomen naar aanleiding van de evaluaties over de cyberaanval.

Motie rkc-onderzoek

In een motie van 1 juni 2021 heeft de gemeenteraad Hof van Twente de motie aangenomen om de rekenkamercommissie te verzoeken "(E)en onderzoek in te stellen naar de uitvoering van het informatieveiligheids-beleid zowel intern als de samenwerking met leveranciers in relatie met de cyberaanval". De motie wordt unaniem aangenomen. Ook dienen drie fracties in de raadsvergadering van 1 juni 2021 een motie van afkeuring in als reactie op de hack en het proces daarna. De motie wordt verworpen met 19 stemmen tegen en 5 stemmen voor (1 raadslid was afwezig bij de stemming).

Openbare vergaderingen

In de periode maart 2021 tot en met juni 2021 heeft de raad vier keer in het openbaar vergaderd over de hack en de gevolgen ervan. In juni 2021 behandelt de raad het jaarverslag 2020 'light'. In het jaarverslag zijn de onderwerpen tekstueel toegelicht, zonder financiële gegevens.

Log4J, december 2021,

De ervaring van respondenten is dat de raad alerter op dit dossier is geworden, maar na de zomer van 2021 wordt het stil. Totdat in december 2021 het volgende ICT-incident voor wereldwijde reuring zorgt, namelijk de Log4J-kwetsbaarheid. Hof van Twente besluit om de site offline te halen en de digitale dienstverlening on hold te zetten. Hierover is via WhatsApp contact tussen college en raadsleden. Over Log4J zijn geen vragen vanuit de raad gekomen, terwijl de gemeente besloot de gemeentelijke dienst-verlening enige dagen offline te halen. Met uitzondering van het contact via WhatsApp was er geen communicatie tussen bestuur en raad.

ICT-auditcommissie

Eind 2021 is er een raadswerkgroep ICT ingesteld, de ICT-auditcommissie. Daarin komt informatieveiligheid aan de orde. Dit overleg bestaat uit 15 personen met onder andere vertegenwoordigers van de raadsfracties, CISO, TISO, burgemeester, controller, gemeentesecretaris, griffier en plaats-vervangend griffier en ook de secretaris rkc. Volgens een aantal respondenten kwam het initiatief tot de ICT-auditcommissie vanuit de driehoek burgemeester-secretaris-griffier. Anderen menen dat dit initiatief vanuit de raad kwam, naar aanleiding van een motie uit de raad na een raadsdebat. De ICT-auditcommissie is gestart op 8 december 2021 met een 2^{e} overleg eind januari 2022.

Zoals gemeld is de raad meer betrokken op het onderwerp informatie-beveiliging dan voor 1 december 2020. Dat is begrijpelijk na de heftige gebeurtenis. De raad is zich veel meer bewust geworden van de risico's op informatieveiligheid. De verwachting bij respondenten is dat dit onderwerp op de agenda blijft. Aangegeven wordt dat de raad ook nauwer betrokken wenst te worden. Drie fracties zijn echter afwezig bij de ICT-auditcommissie van december 2021. Dat zijn de fracties die in juni 2021 een motie van afkeuring hebben ingediend. Als reden komt uit de interviews onder andere naar voren dat drie maanden voor de verkiezing van een nieuwe raad geen

goed moment is om een dergelijk overleg te starten. De kans is groot dat er na maart 2022 nieuwe raadsleden zitting hebben in de raad en dit onderwerp in portefeuille krijgen.

Jaarrekening 2020 en 2021

In het najaar van 2022 komt naar verwachting de jaarrekening met accountantscontrole over de kalenderjaren 2020 en 2021. Bij het schrijven van dit rapport is onduidelijk in hoeverre de accountant een kwalificatie zal geven over de financiële verslaglegging over de kalenderjaren 2021 en 2022 of over de stand van informatiebeveiliging.

9.3 Kaderstellende en controlerende rol met een reflectie door raadsleden

Kaderstellende rol raad

In het ICT-beleid is afgesproken dat de raad vooral een controlerende rol heeft. Tot de hack in 2020 heeft de raad geen expliciete kaderstellende rol gepakt, omdat het bedrijfsvoering betrof dat voornamelijk wordt gezien als een aangelegenheid van het college. Wel heeft de raad het budgetrecht, en in die zin heeft de raad twee keer extra middelen ter beschikking gesteld (1x structureel en 1x incidenteel.) In de periode tot 1 december 2020 heeft de raad vragen gesteld, maar deze zijn niet vanuit de specifieke kaderstellende rol aan de orde geweest. Het college had het initiatief en was leidend op informatiebeveiliging en privacy.

Controlerende rol raad

In de periode 2016 -2020 is de raad geïnformeerd over informatie-beveiliging en privacy via de reguliere verantwoordingcyclus en zijn er geen specifieke vragen gesteld anders dan hierboven is beschreven. De raad ontvangt jaarlijks ENSIA-verantwoording in een raadsbrief. Die heeft de raad meestal voor kennisgeving aangenomen. In de interviews komt naar voren dat de indruk bestaat dat de techniek van ICT ver van de raad afstaat. De verschillende fracties hebben wel woordvoerders die affiniteit met en kennis over het onderwerp hebben. Er ontstaat soms een discussie, maar niet diepgaand over de risico's op informatiebeveiliging.

Extra budget ICT

Uit de interviews komt het beeld dat de gemeente Hof van Twente, zeker voor de hack, een zuinige gemeente was. Over het algemeen deed het college voorstellen aan de raad en die werden, wat betreft bedrijfsvoering, door de raad meestal goedgekeurd. Zo ook op het gebied van ICT. Zoals eerder geconstateerd heeft de raad in 2017 en 2019 nog extra budget beschikbaar gesteld om investeringen te doen in ICT, waaronder informatie-beveiliging. In 2017 waren dat structurele middelen voor de periode 2018 en daarna, in 2019 incidentele middelen vanaf 2020. Beide keren is de raad gemeld dat de investeringen voor een gemeente als Hof van Twente onder de benchmark van vergelijkbare gemeenten zat. Uit de interviews blijkt dat de raad er niet op gewezen is dat mogelijke onder financiering gevolgen zou kunnen hebben voor de informatieveiligheid van de gemeente. Het is een niet te beantwoorden 'als-dan'-vraag of de aanval met de ransomware zou zijn voorkomen als de raad akkoord was gegaan met meer en structurelere

middelen. Er ligt in ieder geval geen directe relatie tussen een niet uitgevoerde investering en de geslaagde hack van 1 december 2020.

Impact na de hack

Net als het college en de ambtelijke organisatie was de raad ontredderd, zo bestaat het beeld bij de respondenten. College en ambtenaren moesten snel overgaan naar de doe-modus. De raad wilde meer betrokken worden en de raad moest daarop ook worden gevoed. Volgens de geïnterviewden uit de organisatie heeft de raad na 1 december 2020 de goede vragen gesteld. Het seniorenconvent was actief en werd geregeld door burgemeester/college bijgepraat over de ontwikkelingen rond de hack. Ook werd de raad bijgepraat via besloten raadsbijeenkomsten/vergaderingen.

Bestuur/organisatie

Na de hack heeft het college en de organisatie de raad ervaren als het bestuurlijk gremium dat volwassen heeft gereageerd op het incident. Kritisch richting het college en de ambtenaren, zonder wijzende vinger. De eerste weken na 1 december 2020 is de raad met grote regelmaat geïnformeerd en de ervaring is dat de raad constructief was richting bestuur en de ambtelijke organisatie.

Politieke dimensie

Vanaf maart 2021, toen de eerste onderzoeken gereedkwamen, moest verantwoording worden afgelegd. Toen kwam er een politieke dimensie bij. De raad leek te schrikken van wat er mis was gegaan. De kwesties die speelden waren: waar ligt schuld, bij de gemeente of bij de leverancier? Gaat de gemeente losgeld betalen en het risico lopen om afhankelijk te worden van criminelen? Het college was van meet af aan van plan geen losgeld te betalen om niet afhankelijk te worden van een kwaadwillende. Mede omdat de integriteit van eventueel teruggekochte data niet gegarandeerd zou zijn. Het college besloot het hele systeem opnieuw op te zetten en dat kost veel geld.

Perspectief raad

Raadsleden zijn wisselend hoe zij de communicatie in de periode na de hack hebben ervaren. Het ene raadslid vindt dat gezien de crisis er goed is gecommuniceerd door betrokkenen. Anderen vinden dat de communicatie van college en organisatie tekort is geschoten. Veel mocht niet verteld worden, omdat er juridische claims liepen (en lopen). Een deel van de raad is van mening dat de communicatie erg defensief was. Aangegeven wordt dat de schuld door het college werd gezocht bij ambtenaren, terwijl bestuur en directie zelf buiten schot bleven, zo leek het. In nagenoeg alle gesprekken die in het kader van dit onderzoek zijn gehouden met raadsleden komt de passage van de burgemeester terug: "het had iedereen kunnen overkomen". Enkele fracties namen dat de burgemeester kwalijk. Na navraag geven zij aan, dat de uitspraak de indruk wekte dat er geen verantwoordelijkheid door college en organisatie werd genomen. In meerdere gesprekken is naar voren gekomen dat het (te) lang heeft geduurd voordat de burgmeester excuses heeft aangeboden voor de gang van zaken en bestuurlijke verantwoordelijkheid nam. Dit gebeurde na druk vanuit een (deel van) de raad.

Financiën na de hack

Bijzondere aandacht is gevraagd door sommige raadsleden in de interviews voor de financiële component na de hack. De raad is pas in maart/april 2021 door het college in de openbaarheid betrokken bij de financiële consequenties van de hack. Meerdere raadsleden brachten in de interviews naar voren dat onmiddellijk na de hack het college op eigen gezag verplichtingen is aangegaan om onderzoek te doen naar de hack en de dienstverlening aan inwoners en bedrijven weer op te bouwen. Het college heeft hierbij geput uit het budget dat beschikbaar was voor informatie-beveiliging. De raad is hierover niet geïnformeerd, ook de auditcommissie is hierbij niet betrokken geweest. De raad had het, achteraf gezien, op prijs gesteld dat zij hierover tijdig in de openbaarheid waren geïnformeerd door het college, niet pas in maart/april 2021.

Reflectie raad

In de interviews komt naar voren dat raadsleden reflecteren op hun eigen rol voor en na de ransomware aanval. Ze vragen zich af of ze niet, achteraf gezien, meer en kritischere vragen hadden moeten stellen over informatie-veiligheid. Zij hadden de indruk dat op dit gebied alles op orde was. Verder kwam naar voren dat de raad informatiebeveiliging een lastig en vooral technisch onderwerp vindt. Lastig om te controleren, omdat raadsleden over het algemeen niet over de benodigde kennis beschikken zich een oordeel te vormen over de technische inhoud.

Rol griffie

Uit de interviews met raadsleden blijkt dat de griffie geen actieve rol heeft gespeeld in het dossier van informatiebeveiliging. De burgemeester, ook portefeuillehouder, onderhield de contacten met de raad en fractie-voorzitters. De griffie werkt voornamelijk ‘op verzoek van raadsleden’. In de communicatie na de hack heeft de griffie richting de raad geen rol van betekenis vervuld. In dit onderzoek zijn de raadsbijeenkomsten beluisterd en de documenten voor zover opgenomen in de raadagenda bestudeerd. Het valt op dat er documenten ontbreken zoals bijlage bij het raadsvoorstel op 1 juni 2021, het door de raad vastgestelde Verbeterplan. Ook de door de raad in het najaar van 2021 vastgestelde visie op I&A is niet te vinden bij de agenda op de site van de raad. De raadsvergadering (waarin kennelijk informatie is gegeven over de kwetsbaarheid over Log4J) van 14 december 2021 is digitaal beschikbaar, maar stopt na 12 minuten en begint opnieuw.

10 Opvolging lessen geleerd uit de hack

Onderzoeksvraag 7	In dit hoofdstuk geven we antwoord op vraag 7: Welke lessen komen voort uit de twee onderzoeken die maart 2021 verschenen in opdracht van het college? Wat is met deze lessen gebeurd?

Evaluaties

In maart 2021 zijn 3 onderzoeken/evaluaties/rapportages verschenen die de hack van 1 december 2021 analyseren en conclusies en aanbevelingen formuleren. De onderzoeken zijn:

- NFIR Onderzoek Incident response & Digitaal forensisch onderzoek van 8 maart 2021. Een technische analyse wat vooraf is gegaan aan de hack, inclusief een tijdlijn, de activiteiten van de gemeente na ontdekking van het incident op 1 december 2020 en een analyse hoe het zo ver heeft kunnen komen met conclusies en aanbevelingen.
- Duidingsrapportage door Brenno de Winter, 'Te goed van vertrouwen' van 8 maart 2021. Een duiding van het NFIR-rapport en een analyse van het proces dat de gemeente na de hack heeft doorgemaakt.
- Rapport van bevindingen Hof van Twente ICT-situatie 9 maart 2021, door het College van de gemeente Hof van Twente. Deze bijdrage gaat vooral in hoe de gemeente in control leek te zijn tot 1 december 2021, hoe informatiebeveiliging en ICT waren georganiseerd, de communicatie naar alle betrokkenen over het incident: gemeenteraad, leveranciers en inwoners en bedrijven, een reflectie op het gebeuren en tot slot hoe de dienstverlening na het incident vorm heeft gekregen.

Aanbevelingen

Met de aanbevelingen is de organisatie aan de slag gegaan. Uit de verschillende rapporten heeft de organisatie 35 aanbevelingen geformuleerd en deze samengevat in 18 actiepunten.

Verbeterplan

Deze 18 actiepunten vormen het Verbeterplan van het programma de Nieuwe Werkelijkheid. Op 1 juni 2021 heeft de gemeenteraad dit Verbeterplan vastgesteld. De actiepunten uit het Verbeterplan zijn naar verwachting medio 2022 uitgevoerd, sommigen daarvan worden structureel in de organisatie ingebed. De gemeenteraad wordt via de ICT-auditcommissie geïnformeerd over de vorderingen. Dat is voor het laatst in februari 2022 gebeurd.

De 18 actiepunten

De 18 actiepunten heeft de gemeente als volgt geformuleerd, waarbij DNW voor De Nieuwe Werkelijkheid staat. Per actiepunt is een verantwoordelijke benoemd, meestal een MT-lid. De gemeentesecretaris is overall verantwoordelijk, dit laatste was soms de vraag bij respondenten, zij vroegen zich af wie een integraal zicht heeft op de 18 actiepunten, waarop soms ook een overlap te constateren valt.

Tabel 2. 18 actiepunten, wie verantwoordelijk is en de planning. Versie februari 2022.

Actiepunt	Titel actiepunt	Verantwoordelijk	Planning gereed
1	Back up 3-2-1	Programma DNW	Gereed in december 2021
2	Wachtwoordenbeleid	Project DNW	Niet bepaald
3	IT-securitybeleid	Project DNW	Gereed in december 2021
4	Netwerksegmentatie	Project DNW	Gereed december 2021
5	Actieve monitoring	Project DNW	Externe partij: NFIR monitort, komt in dashboard, dashboard is in ontwikkeling
6	Organisatie I&A	Gemeentesecretaris	Plan vastgesteld door de raad in september 2021, reorganisatie I&A planning in 2022 [13]
7	Stuurinformatie	CISO/ hoofd concernstaf	Na 1e kwartaal 2022 gereed
8	Incidentenplan en oefenen	CISO/ hoofd concernstaf	1e helft 2022 incidentenplan gereed Oefenen na de oplevering DNW, medio 2022
9	Security audits en pentests	CISO/ hoofd concernstaf	In uitvoering, zie ook actiepunt 5 NFIR monitort als externe partij Na oplevering DNW, eind 2022
10	Informatieveiligheidsbeleid	CISO/ hoofd concernstaf	1e helft 2022
11	Contract & Leveranciersmanagement	Manager Leefomgeving	1e helft 2022 project met studenten van Saxion Hogeschool
12	Rollen, verantwoordelijkheden en taken I&A	Manager Bedrijfsvoering	2e helft 2022
13	Bewustwording, kennis en professionaliteit	Manager Sociaal Domein	Plan: gereed eind 2021 Uitvoering is gestart in eerste kwartaal van 2022
14	Training en kunde	CISO	Projectplan digitale transformatie, gereed eind 2021
15	Bevragen beveiliging en organiseren tegenspraak	Gemeentesecretaris	Na reorganisatie I&A medio 2022 Stuurgroep ICT; onafhankelijke deskundige toegevoegd aan de stuurgroep (is gebeurd)

[13] Deze gegevens komen uit de interviews. We hebben de besluitvorming en het plan niet op de site van de gemeente aangetroffen.

16	Bestuurlijke expertise ontwikkelen	Burgemeester, gemeentesecretaris en griffier	De 1e raads-auditcie is gestart op 8 december 2021 2e bijeenkomst ICT raads-auditcie is geweest in februari 2022, dit Verbeterplan besproken
17	Project DNW en visievorming	Niet bepaald	Medio 2022 afgerond, na reorganisatie I&A
18	Externe communicatie en lessons learned	Niet bepaald	In 2021 24 bijdragen geleverd, afgerond

Opvolging aanbevelingen

De gemeente is voortvarend aan de slag gegaan met de actiepunten en maakt regelmatig rapportages om de voortgang van deze punten te bewaken. Hierna volgt het overzicht van de stand zaken in januari 2022 [14]. Zoals gemeld zijn volgens planning de 18 actiepunten medio 2022 uitgevoerd en eindigt het Programma Verbeterplan. Een aantal actiepunten zal daarna structureel worden opgepakt en geborgd in de organisatie. De lijn moet dan de operationele uitvoering van informatiebeveiliging overnemen.

[14] De gemeente Hof van Twente heeft 18 (actie) punten geformuleerd na de hack. Regelmatig maakt de gemeente een overzicht hoe de 18 punten worden opgepakt en geïmplementeerd. De laatste versie van de verbeterrapportage stand van zaken dateert van januari 2022 en neemt dit onderzoek als uitgangspunt om te bepalen in hoeverre de gemeente de aanbevelingen heeft uitgevoerd en wat de stand van zaken is.

Tabel 3. 18 actiepunten, een overzicht van wat is uitgevoerd (groen) en wat nog in uitvoering is (oranje). Versie februari 2022.

1	Back-up 3-2-1	
2	Wachtwoordbeleid	
3	IT-securitybeleid	
4	Netwerksegmentatie	
5	Actieve monitoring	
6	Organisatie I&A	
7	Stuurinformatie	
8	Incidentenplan & oefenen	
9	Security audits/ pentests	
10	Informatieveiligheidsbeleid	
11	Contract- en leveranciersmanagement	
12	Rollen, verantwoordelijkheden en taken I&A	
13	Bewustwording, kennis en professionaliteit	
14	Kennis en kunde	
15	Bevragen op beveiliging/ tegenspraak	
16	Bestuurlijk expertise ontwikkelen	
17	Project De Nieuwe Werkelijkheid/ incl. visie	
18	Externe Communicatie & Lessons Learned	

De meest essentiële activiteiten die direct verband houden met het incident van 1 december 2020 zijn gerealiseerd, zoals het back-up- en wachtwoordbeleid, de netwerksegmentatie en de actieve monitoring. De externe communicatie en lessons learned zijn ook gerealiseerd. De andere actiepunten hebben een wat langere adem nodig, zoals de bewustwording, kennis en kunde.

11 Informatiebeveiliging huidige beleid

Onderzoeksvraag 8	In dit hoofdstuk geven we antwoord op vraag 8: Hoe heeft het informatiebeleid vorm gekregen na 1 december 2020?

Opnieuw ontwikkeld	Sinds de hack op 1 december 2020 is vanaf de basis het ICT-systeem opnieuw opgebouwd. De essentiële dienstverlening van de gemeente is binnen een week operationeel geworden. In de periode daarna is langzamerhand de dienstverlening gekomen tot op een niveau dat inwoners en bedrijven op de gebruikelijke wijze een beroep konden doen op de gemeente.
Informatiebeveiligingsbeleid	Zoals uit tabel 3 (zie hoofdstuk 10) blijkt is er nog geen nieuw informatie-beveiligingsbeleid geformuleerd. Het vigerende is het Informatie-beveiligingsbeleid 2020-2022. De intentie is in de 1e helft van 2022 nieuw beleid te formuleren. Een van de punten die heroverwogen worden is voor de CISO een eigen budget voor activiteiten op informatiebeveiliging te bestemmen.
IT-securitybeleid	De gemeente had geen expliciet IT-securitybeleid. Op advies van het NFIR ontwikkelt de gemeente nu het securitybeleid en heeft het voornemen om dit expliciet vast te leggen. Dat is nog niet gerealiseerd, zie ook tabel 3.
I&A-visie	Een nieuwe I&A-visie is in 2021 vastgesteld. Deze gaat uit van een regie-bureau I&A die direct onder de gemeentesecretaris is gepositioneerd. Daar gaat het cluster I&A van bedrijfsvoering naar toe. Plan is om daarnaast een aantal informatiemanagers aan te stellen om de regiefunctie van de gemeente op dit terrein te versterken. Ten tijde van het onderzoek werd een regiemanager als kwartiermaker voor het proces geworven. Deze zou het plan verder moeten gaan uitwerken.
Beleid in progress	Ten aanzien van de volgende onderdelen is er beleid in ontwikkeling, waarbij vermeld zij dat veelal de uitgangspunten door de gemeente eerder waren geformuleerd: audits en pentesten, oefeningen (fysiek en digitaal), sturingsinformatie, monitoring en contract- en leveranciersbeleid.
Nu en in de toekomst	De contouren van de nieuwe situatie op informatieveiligheid van de gemeente Hof van Twente beginnen zichtbaar te worden, er is de afgelopen anderhalf jaar hard gewerkt. Contouren waarin de lessen zijn opgenomen die de gemeente in 2020 en daarna heeft getrokken. Er zijn evenwel nog fundamentele vraagstukken die het gemeentebestuur zal moeten adresseren zoals bijvoorbeeld de inrichting van de organisatie, monitoring op een structurele wijze van de ICT-processen en met name de werking van processen evalueren. Zo is er bijvoorbeeld tot op heden nog geen pentest uitgevoerd.

De gemeente Hof van Twente heeft een turbulente periode achter de rug en is daarvan grotendeels hersteld, maar nog niet helemaal. De ontwikkeling vanaf 1 december 2020 is dat van incident naar crisisorganisatie en uiteindelijk projectorganisatie. Management en medewerkers hebben hard gewerkt om de dienstverlening weer op gang te brengen. Informatiebeveiliging, en alle maatregelen daarop, behoorde bij het crisismanagement en de projectorganisatie. Dat zal ook weer in reguliere lijnorganisatie moeten gaan landen, waarbij de lijn weer eindverantwoordelijk wordt voor informatieveiligheid, zoals bedoeld in het informatiebeveiligingsbeleid.

In de crisis- en projectfase is noodzakelijkerwijs gebruik gemaakt van ingehuurde kennis en expertise. De kosten voor de wederopbouw van de systemen zijn bekend, namelijk €3,9 miljoen. Dat is nog niet alles. Externen ondersteunen Hof van Twente 24/7 onder andere met cloudservices en monitoringapplicaties. Deze brengen hoge kosten met zich mee en de vraag is hoe lang de gemeente dat bestedingsniveau op ICT en informatie-beveiliging kan volhouden.

Het in eigen huis organiseren van kennis en capaciteit op ICT en informatie-veiligheid, met bedreigingen die 24/7 doorgaan, is eveneens kostbaar. Op de huidige overspannen arbeidsmarkt is expertise daarop moeizaam en duur te verwerven. Dat vraagt innovatieve oplossingen.

Bijlage 1. In informatiebeveiliging en privacy veel voorkomende termen en afkortingen

2FA	Twee factor authenticatie, zo wordt op 2 verschillende manieren gecheckt of degene die inlogt degene is die hij/zij aangeeft te zijn
2-staps-verificatie	zie 2FA
Active Directory (AD)	De Active Directory is een database waarin onder andere accounts en inloggegevens zijn opgenomen
AP	Autoriteit Persoonsgegevens
Applicatie	Softwareprogramma, zoals de BAG, BRP, SUWInet enz.
Attack en Pentest	Zie pentest
AVG (GDPR)	Algemene Verordening Gegevensbescherming, Europese regelgeving die de privacyregels in de Europese lidstaten harmoniseert (GDPR = General Data Protection Regulation)
BAG	Basisregistratie Adressen en Gebouwen, applicatie met onder andere gegevens over adressen en gebouwen in de gemeente
BIG	Baseline Informatiebeveiliging Gemeenten, maatregelen voor de informatiebeveiliging bij gemeenten, in 2013 als standaard afgesproken in VNG-verband
BIO	Baseline Informatiebeveiliging Overheid, verwachting is dat hier de BIR en BIG in zullen opgaan vanaf 2020
BRP	Basisregistratie Personen, applicatie met persoonsgegevens van de inwoners
Brute force attack	Een brute-force attack is een digitale aanval waarbij de aanvaller systematisch wachtwoorden en encryptiesleutels uitprobeert totdat er één blijkt te werken
CISO	Chief Information Security Officer
Cloud	De cloud staat voor een netwerk van computers die een soort 'wolk van computers' vormt, waarbij de eindgebruiker niet weet op hoeveel of welke computer(s) de software draait of waar die computers precies staan
DPIA (ook PIA)	Data protection impact assessment, analyse op risico's in verband met privacy en gegevensbescherming bij verwerkingsprocessen. Onder de AVG verplicht bij gegevensverwerking met waarschijnlijk een hoog privacy risico.
ENSIA	Eenduidige Normatiek Single Information Audit, eenmalige informatieverstrekking en eenmalige IT-audit voor de horizontale (richting gemeenteraad als toezichthouder) en verticale verantwoording (richting landelijke toezichthouders)
FG	Functionaris gegevensbescherming, verplicht voor overheden.
Firewall	Een firewall is een systeem dat de middelen van een netwerk of computer kan beschermen tegen misbruik van buitenaf.
GAP	Is de Engelse term voor ‘kloof’. Dat betekent hier het verschil tussen de bestaande situatie en de gewenste situatie
GAP-analyse	Controle of en in welke mate de maatregelen uit de BIO geïmplementeerd zijn
GDPR	General Data Protection Regulation (zie AVG)
GBA	Gemeentelijke Basisadministratie
IBD	Informatiebeveiligingsdienst voor gemeenten
ICT	Informatie- en communicatietechnologie
ISMS	Information securitymanagement system

Log4J	In Apache Log4j, software die veel gebruikt wordt in webapplicaties en allerlei andere systemen, is december 2021 een kwetsbaarheid aangetroffen waardoor een aanval op IT-systemen mogelijk is
MDR	Managed Detection Response, daarmee kunnen digitale aanvallen ontdekt worden en tijdig worden gereageerd.
ML	Management Letter, interimcontrole door de accountant. Jaarlijks op te maken ter voorbereiding op de controle van de jaarrekening
P&C-cyclus	Planning & Control cyclus
PDCA	Plan-Do-Check-Act beleidsleercyclus
Pentest	Een pentest of penetratietest is een toets van een of meer computer-systemen op kwetsbaarheden, waarbij deze kwetsbaarheden ook werkelijk gebruikt worden om in deze systemen in te breken. Deze testen worden uitgevoerd door zogenoemde ethische hackers.
Phishing mail	Vorm van internet oplichting en fraude, door middel van een vals e-mail bericht 'hengelen' naar inlog- of andere persoonsgegevens
PIA (ook DPIA)	Privacy impact assessment, analyse op risico's in verband met privacy en gegevensbescherming bij verwerkingsprocessen. Onder de AVG verplicht bij gegevensverwerking met waarschijnlijk een hoog privacy risico.
Privacy by default	Onderdeel van privacy by design, waarbij de standaardinstellingen zo privacy-vriendelijk mogelijk zijn ingesteld
Privacy by design	Betekent dat bij het ontwerp van producten en diensten nagedacht wordt over privacy
SIEM/SOC	Security Information & Event Management/Security Operations Center. Applicaties die computerdreigingen, zoals hackpogingen of malware, monitort en in kaart brengt.
Verwerkingsregister	Register waarin de gemeente bijhoudt welke persoonsgegevens de gemeente en de verwerkers die deze inschakelt verwerkt
VNG Realisatie	Kwaliteitsinstituut van de VNG (voorheen KING)
VPN	Virtueel privé netwerk (versleutelde beveiligde verbinding)

Bijlage 2. Lijst geraadpleegde stukken en lijst respondenten

De geraadpleegde stukken en de geïnterviewde personen zijn hieronder weergegeven. Een aantal stukken is vernietigd door de hackpoging, vandaar dat we niet alles hebben kunnen traceren.

Geraadpleegde stukken

- 2019_stafmedewerker bedrijfsvoering (CISO)
- Agenda informerende bijeenkomst raad 20 september 2016
- Agenda informerende bijeenkomst raad 30 mei 2018
- Algemene Instructies beveiliging Hof van Twente 25-04-2018
- Assurance rapport ENSIA 2019 Gemeente Hof van Twente v1.0
- Bakertilly, Accountantsverslag 2017 [15]
- Bakertilly, Management Letter 2017
- Bakertilly, Accountantsverslag 2018
- Bakertilly, Management Letter 2018
- Bakertilly, Accountantsverslag 2019
- Bakertilly, Controleverklaring 2019
- Bakertilly, Management Letter 2019
- BBV Collegevoorstel
- BBV-raadsbrief zelfevaluatie informatieveiligheid 2019
- Bedrijfscontinuïteitsplan gemeente Hof van Twente v4
- Beleid incidentmanagement 1.1, 11 september 2019
- Beleidsplan Informatieveiligheid Privacy 2017 (oud)
- Besluiten m.b.t. informatieveiligheid Hof van Twente
- Bijlage Inhuur- en detacheringsovereenkomst
- Binnenlands Bestuur, Weinig ICT in partijprogramma's gehackte gemeenten, 16 februari 2022
- Collegeprogramma 2018-2022 'Samen doen!'
- Collegeverklaring-ENSIA-2019-inzake informatiebeveiliging DigiD en Suwinet HvT AtA
- Collegevoorstel, zelfevaluatie informatieveiligheid 2019 van 10 maart 2020
- Contactoverzicht informatiebeveiligingsaangelegenheden
- Handboek Informatiebeveiliging 2017
- Integriteitbeleid versie 2011
- Jaarverslag 2020 light 'Kiezen voor de toekomst', behandeld in de raad van juni 2021.
- Overdracht van Crisisorganisatie naar Projectorganisatie

[15] Voor dit onderzoek heeft de rekenkamercommissie (rkc) informatie opgevraagd die noodzakelijk was voor dit rkc-onderzoek over informatiebeveiliging. Op grond van art 81 oa Gemeentewet kan de rkc documenten van de betreffende gemeente onderzoeken voor zover opgenomen in de verordening. Niet alle onderzochte documenten kan de rkc openbaar maken. Voor dit onderzoek heeft de rkc onder andere de Management Letter 2018 die door de accountant opgemaakt opgevraagd. Dit document is op 25 januari 2019 aan het college aangeboden. In dit document staat niet vermeld dat dit een vertrouwelijk document is of dat er enige restrictie is opgelegd over de vorm van openbaarmaking dan wel dat de accountant op enigerlei wijze toestemming dient te verlenen voor enige vorm van openbaarmaking uit de Management Letter. Met deze grondslag heeft de rkc voor dit onderzoek en de bijbehorende rapportage passages opgenomen uit de Management Letter.

- Procedure afvoer ICT-middelen
- Procedure mobiele gegevensdragers
- Programma Informatieveiligheid en Privacy 2020
- Raadsbrief 17 maart 2020 door portefeuillehouder (Burgemeester). Over ENSIA aan te passen en als uitgangspunt te nemen BIO
- Rapportage pentest juni 2020
- Routekaart Actiepunten uit verbeterplan
- Strategisch informatieveiligheidsbeleid 2020-2022
- Taakbeschrijving Stafmedewerker bedrijfsvoering (Ciso), datum niet vermeld in document
- Toegangsbeveiliging 2020
- Verbeterplan Suwinet en Digid, 30 maart 2021
- Verbeterplan Hack stand van zaken, versie januari 2022
- Verbeterrapportage hack stand van zaken, versie februari 2022
- Verslag ICT-auditcommissie 8 december 2021
- Visie regievoering I&A, 2022-2026
- Wachtwoordenbeleid, passwords

Evaluaties

- 'Te goed van vertrouwen', Brenno de Winter, 8 maart 2021
- Rapportage zonder veiligheidsgevoelige informatie, Incident response & Digitaal forensisch onderzoek, NFIR, 8 maart 2021
- Rapport van Bevindingen, ICT-situatie, gemeente Hof van Twente, 9 maart 2021
- Lessen uit de hack bij Hof van Twente, IBD

Andere bronnen

- Interview Klein Tank aan RPO Journaal VNG, 1 april 2021 (online te bekijken VNG.nl)
- Interview Rob Mellegers, TISO, Binnenlands Bestuur
- Weergave verschillende raadsvergaderingen periode 2019 – 2022 met bijbehorende documenten

Functies van geïnterviewde respondenten

- Afdelingsmanager
- Burgemeester
- CISO (in dienst tot augustus 2021)
- CISO (in dienst vanaf 15 januari 2022)
- Controller
- Gemeentesecretaris
- Griffier
- 6 gesprekken met verschillende raadsleden (in totaal zijn 8 raadsleden van alle 7 fracties geïnterviewd)
- Teamcoördinator

Bijlage 3. Onderzoeksvragen en normen

De onderstaande normen zijn voornamelijk ontleend aan de BIO en de AVG. Mogelijk kunnen de gemeentelijke beleidsplannen aanvullende normen opleveren, waaraan de uitvoering van de informatiebeveiliging getoetst wordt.

Onderzoeksvragen	(Concept)Normen
1. Beschikte de gemeente Hof van Twente in de periode 2018-2020 over een adequaat informatiebeveiligingsbeleid?	- Het college stelt het integrale beleid ten aanzien van informatiebeveiliging en privacy vast. - Er vindt sturing plaats op basis van de BIO. - Het informatiebeveiligingsbeleid is opgesteld aan de hand van een GAP-analyse. Jaarlijks wordt op basis van een risicoanalyse het informatiebeveiligingsplan ingevuld. De gemeente neemt maatregelen om risico's te verlagen. - Op onderdelen van informatiebeveiliging is beleid geformuleerd en zijn richtlijnen opgesteld, zoals gebruik van wachtwoorden, 2 factor authenticatie, mobiele datadragers, autorisaties en monitoring, wijzigingsbeleid enz. - Gegevens zijn goed beschermd tegen ongewenste invloeden van buitenaf.
2. Is het informatiebeveiligingsbeleid in die periode adequaat uitgevoerd?	- De maatregelen uit het jaarlijkse informatiebeveiligings-plan worden uitgevoerd. - Het bestuur en medewerkers dragen het beleid ten aanzien van informatiebeveiliging actief uit. - De gemeente heeft procedures om te leren van beveiligingsmeldingen met als doel beheersmaatregelen te verbeteren. - Medewerkers weten wat ze wel en niet mogen/moeten doen met gegevens en herkennen incidenten en rapporteren deze ook daadwerkelijk.
3. Zijn de functies die van belang zijn op het gebied van informatiebeveiliging in die periode goed gepositioneerd?	- De CISO is gepositioneerd en geëquipeerd om diens taak adequaat uit te voeren. - De teamhoofden Bedrijfsvoering en I&A zijn goed gepositioneerd en geëquipeerd om hun taak adequaat uit te voeren.
4. Is de uitvoering van het beleid in die periode adequaat getoetst en gemonitord?	- Het Information Security Management System (ISMS), indien aanwezig, is gekoppeld aan de PDCA-cyclus. - Over het functioneren van informatiebeveiliging wordt gerapporteerd aan het management, bij voorkeur op basis van een ISMS. - Er worden periodiek (pen)testen uitgevoerd op de systemen en de infrastructuur. - De autorisaties voor toegang tot de systemen en data zijn actueel en worden periodiek gecontroleerd. - Op de systemen is logging geïnstalleerd en er is capaciteit aanwezig om deze te monitoren. - Er is een procedure vastgesteld voor de wijze waarop informatiebeveiligingsgebeurtenissen en zwakke plekken in de beveiliging worden beheerd en gerapporteerd.
5. Welke afspraken op informatie-beveiliging zijn gemaakt met externe leverancier(s) en hoe zijn deze gemonitord?	- De afspraken met de externe leverancier zijn afgestemd op de rollen en taken op ICT en informatiebeveiliging die de gemeente en de externe leverancier(s) uitvoeren. - Afspraken over incidenten en datalekken zijn vastgelegd en worden gemonitord door de CISO en FG.

6. Is de raad adequaat gepositioneerd geweest om zijn kaderstellende en controlerende rol te kunnen uitvoeren?	- Over het functioneren van informatiebeveiliging wordt gerapporteerd aan de raad, op zijn minst jaarlijks in het kader van ENSIA. - De raad krijgt grote beveiligingsincidenten en datalekken gerapporteerd.
7. Wat is er gedaan met de aanbevelingen uit de twee onderzoeken die in maart 2021 in opdracht van het college zijn verschenen?	- Op 1 december 2021 is er beargumenteerd zicht in hoeverre aanbevelingen zijn of worden overgenomen. - Van de overgenomen aanbevelingen is (het begin van) implementatie zichtbaar.
8. Hoe heeft het informatiebeveiligings-beleid vorm gekregen na 1 december 2020?	- In 2021 is gestart met een nieuwe GAP- en risicoanalyse op basis waarvan een nieuw informatiebeveiligingsbeleid wordt vastgesteld.
9. Welke lessen zijn te trekken uit de hack die 1 december 2020 manifest werd en de gebeurtenissen daarna?	- Geen normen

Bijlage 4. Volwassenheidsniveau NOREA

Niveau	Naam	Omschrijving	Indicatieve criteria
1	Initieel	Beheersingsmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.	• Geen of beperkte controls geïmplementeerd. • Niet of ad-hoc uitgevoerd. • Niet /deels gedocumenteerd. • Wijze van uitvoering afhankelijk van individu.
2	Herhaalbaar	Beheersingsmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd.	• Control is geïmplementeerd. • Uitvoering is consistent en standaard. • Informeel en grotendeels gedocumenteerd.
3	Gedefinieerd	Beheersingsmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst.	• Control gedefinieerd o.b.v. risico assessment. • Gedocumenteerd en geformaliseerd. • Verantwoordelijkheden en taken eenduidig toegewezen. • Opzet, bestaan en effectieve werking aantoonbaar. • Rapportage van uitvoering van beheersingsmaatregel aan management. • Effectieve werking van controls wordt periodiek getoetst, gebaseerd op het risicoprofiel van de organisatie. • De toetsing toont aan dat de control effectief is.
4	Beheerst en meetbaar	De effectiviteit van de beheersingsmaatregelen wordt periodiek geëvalueerd.	• Periodieke (control) evaluatie en opvolging vindt plaats. • Evaluatie is gedocumenteerd en geformaliseerd. • Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de onderneming en is minimaal jaarlijks. • Rapportage van de evaluatie aan management.
5	Continu verbeteren	De beheersingsmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering.	• Continu evalueren van de beheersingsmaatregelen om de effectiviteit te verbeteren. Gebruik makend van resultaten uit Self-assessment, gap en root cause analyses. • De getroffen beheersingsmaatregelen worden gebenchmarkt en zijn 'Best Practice' in vergelijking met andere organisaties. • Real time monitoring. • Inzet automated tooling.

Bron: Handreiking bij Volwassenheidsmodel Informatiebeveiliging, januari 2019, NBA.