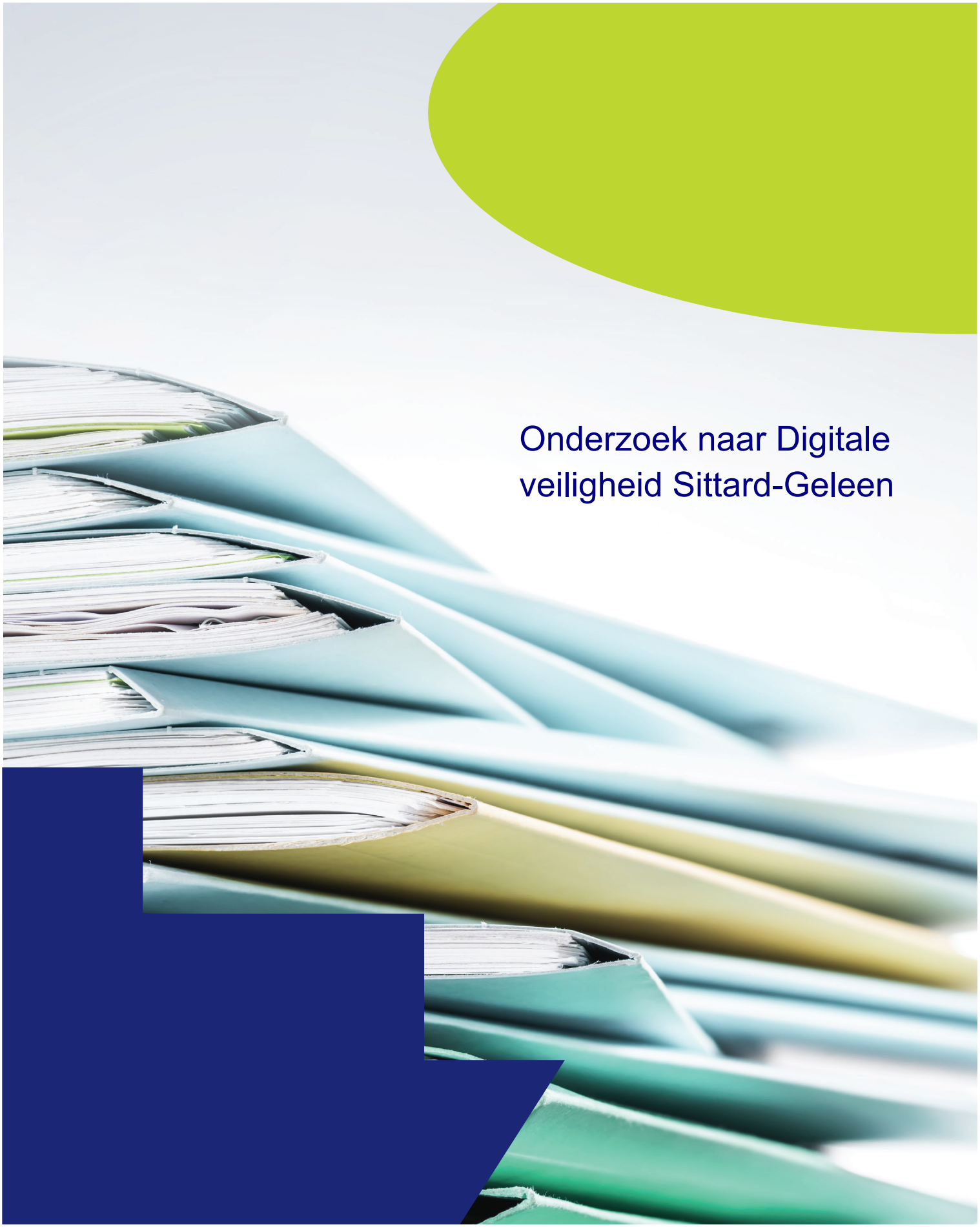


Onderzoek naar Digitale veiligheid Sittard-Geleen

REKENKAMER COMMISSIE SITTARD-GELEEN STEIN

Gemeente Sittard-Geleen Born

Gemeente Stein

REKENKAMER
COMMISSIE SITTARD-GELEEN STEIN

Onderzoek naar Digitale veiligheid Sittard-Geleen

Status: Eindrapport vastgesteld in de vergadering van de Rekenkamercommissie Sittard-Geleen en Stein op 16 maart 2018

Inhoud

1. Voorwoord

Overheden zijn voor de uitvoering van taken massaal overgegaan op de digitale informatieverwerking. Met intranet voor interne dataverwerking en internet voor externe informatie-uitwisseling kunnen data worden geraadpleegd en worden veranderd. De infrastructuur wordt steeds complexer, de techniek geavanceerder en cybercriminelen worden vindingrijker. Het beschermen van digitale informatie is dan ook een kritisch proces geworden dat centraal moet staan bij het handelen van gemeenten. Het is van het grootse belang prioriteit te geven aan Informatiebeveiliging en tegelijk ervoor te zorgen dat alle deelnemers zich bewust zijn van belang en noodzaak van het veilig gebruik van data en het omgaan met digitale informatie(-systemen). Iedereen binnen de organisatie heeft daarin een eigen verantwoordelijkheid en alleen door samenwerking en krachten te bundelen ontstaat een aaneengeschakelde beveiligingsketen.

In de gemeente Sittard-Geleen is dit niet het geval. Informatieveiligheid staat onvoldoende hoog op de agenda en het bewustzijn van belang en risico's rond informatiebeveiliging is te laag. Een ethische hacker heeft vrij eenvoudig gebruikersnamen en wachtwoorden opgehaald en heeft zich toegang tot de mailserver en het netwerk verschaft. De informatiebeveiliging is daarmee onvoldoende gebleken.

De bescherming van de gegevens laat daarmee te wensen over. Technisch gezien is er reden te veronderstellen dat de afdeling ICT zich voldoende bewust is van het belang en de ernst van de technische beveiliging gezien de inrichting van het netwerk en de technische voorzieningen die zijn aangebracht. Informatiebeveiliging speelt echter op alle niveaus binnen de gemeente en vraagt samenwerking van iedereen. Bij de top van de organisatie is onvoldoende gevoel van urgentie aangetroffen. Met name ten aanzien van het gestructureerd en voortdurend aandacht vragen van iedereen om zich bewust te zijn van het belang van informatiebeveiliging, en met elkaar samen te werken aan verbeteringen, dienen slagen gemaakt te worden.
Het risicobewustzijn is te laag.

Het onderzoek was beperkt van opzet om kwetsbaarheden op hoofdlijnen te toetsen. Er is geen nader onderzoek gedaan naar de feitelijke kwetsbaarbaarheid omdat dat aan de afdeling ICT zelf overgelaten kan worden.

De raad van de gemeente dient het thema veiligheid periodiek op de agenda te zetten en te houden. Structurele bestuurlijke aandacht voor informatieveiligheid door de raad en college is vanwege de voorbeeldwerking die daarvan uitgaat nodig om iedereen mee te nemen in dit continu leer- en veranderingsproces.

De Rekenkamercommissie Sittard-Geleen en Stein

2. Bestuurlijke nota

2.1 Inleiding

Aanleiding
De toenemende digitalisering van informatie, de technische ontwikkelingen, de wijze van (externe) opslag van data, nieuwe apparatuur zoals tabletcomputers en mobile apparatuur maken dat overheden en bedrijven bijzondere aandacht moeten gaan geven aan de bescherming van digitaal opgeslagen data.
Recente publicaties over datalekken en onderzoeken van rekenkamers laten zien aan dat gemeenten kwetsbaar zijn en dat het nodig is informatiebeveiliging extra aandacht te geven.

Doel en vraagstelling
De Rekenkamercommissie beoogt met dit onderzoek inzicht te geven in de huidige staat van de technische beveiliging van de gegevens die de gemeente beheert. Het onderzoek richt zich op de technische toegankelijkheid en bescherming van data. Het is een beperkt onderzoek om (gecontroleerd) als kwaadwillende buitenstaander te zoeken naar kwetsbaarheden en toegang tot (vertrouwelijke) informatie te verkrijgen.

De raad krijgt antwoord op de vraag of de gemeenten kwetsbaar is voor cyberaanvallen gericht op vertrouwelijke en persoonsgegevens.

2.2 Conclusies en aanbevelingen

1. De informatiebeveiliging van de gemeente Sittard-Geleen is kwetsbaar gebleken.
   1.1 Door technische onvolkomenheden is toegang tot de mailserver onvoldoende veilig gebleken.
   1.2 De fysieke toegang tot het netwerk is eenvoudig gebleken en vraagt heroverweging.
   1.3 Social en security awareness is te laag.

2. Het Informatieveilgheidsbeleid heeft aandacht van het college.
   2.1 Beleidsplan Informatieveiligheid
   Er is een beleidsplan Informatiebeveiliging geformuleerd (2015), dat mede is gebaseerd op gangbare landelijke afspraken en normenkaders.
   2.2 Sturing en actualiteit van beleid
   De snelle ontwikkeling op dit terrein alsmede de toenemende complexiteit doen dit beleid snel verouderen.
   2.3 Organisatie van verantwoordelijkheden en taakverdeling is volgens landelijk ontwikkelde standaarden ingericht.

3. Er is onvoldoende bewustzijn van belang en de risico's rond informatieveiligheid.
   3.1 Informatieveiligheid is geen specifiek thema van de raad.
   3.2 Structurele en periodieke aandacht van iedereen voor informatieveiligheid ontbreekt.
   3.3 Het urgentiebesef is te laag.
   3.4 Er is geen lerende organisatie.

2.2.1 Toelichting op de conclusies

<u>ad 1.1 Technische beveiliging is kwetsbaar</u>
De pentest die de RKC heeft laten uitvoeren als een quick-scan toont aan dat er kwetsbaarheden zijn. Het bureau dat de ethische hack heeft uitgevoerd constateert, dat er sprake is van 13 kwetsbaarheden waarvan 7 met de kwalificatie: hoog risico voor de gemeente. In het bijzonder is de instelling van de mailserver kwetsbaar gebleken. In combinatie met andere kwetsbaarheden zoals onvoldoende bewustzijn op digitale veiligheid binnen de gemeente Sittard-Geleen vormt dit een serieus probleem. Inmiddels is de instelling van de mailserver aangepast door de afdeling ICT.

De pentest heeft aangetoond dat de afdeling ICT zich bewust is van digitale veiligheid en het op orde hebben van software en de inrichting van het netwerk. De netwerk infrastructuur wordt als gedegen gekwalificeerd. Tegelijk zijn er meerder kwetsbaarheden vastgesteld waarbij is aangegeven welke impact dit kan hebben. In de technische rapportage is dit beschreven voor de afdeling ICT om zo gericht aan oplossingen te werken. Pentesten zijn juist bedoeld om kwetsbaarheden tijdig op te sporen en verbetering aan te brengen.

De onderschepping door de afdeling ICT van de phishing-mail toont aan dat er voldoende oplettendheid bij de afdeling ICT is voor dit soort incidenten. Ook heeft de in gang gezette procedure gewerkt en is de hacker opgespoord. De in gang gezette procedure heeft gewerkt en de hacker is na ongeveer 18 uur getraceerd.
Tegelijk constateert de RKC dat de Phishing aanval succesvol is uitgevoerd omdat de instellingen verkeerd waren.

ad 1.2 Fysieke toegang tot netwerk.
Zowel bij de pentest als de inlooptest heeft de ethische hacker weinig weerstand ervaren.
De hackers zijn met meerdere personen tegelijk te werk gegaan en hebben zich ongestoord en onopgemerkt toegang tot de gebouwen en daarmee tot het netwerk verschaft.
Dat de hackers één dag nadat de phishing was uitgevoerd, toch ongestoord het gebouw zijn binnengegaan en het netwerk hebben gescand, is daarbij opmerkelijk.
In de ambtelijke reactie is aangegeven dat het van belang is om bij het nieuwe huisvestingsconcept rekening te houden met de gedane constateringen en wellicht de tot nu toe gehanteerde uitgangspunten voor de toegankelijkheid van gebouwen te heroverwegen. Hiermee krijgt de fysieke beveiliging van gebouwen en toegang tot het netwerk in de toekomst aandacht.

In de ambtelijke reactie is aangegeven dat beveiliging van de mailserver stond geagendeerd voor het ICT Privacy en Security overleg dat plaatsvond de dag nadat de hack was uitgevoerd en men hierdoor achter de feiten aanliep. Dit laat onverlet dat de instellingen niet juist bleken te zijn. In combinatie met te laag bewustzijn van veiligheidsrisico's bij zowel raadsleden als medewerkers is de gemeente erg kwetsbaar gebleken.

Websites van gelieerde partijen zijn van opvallend lage kwaliteit gebleken. De gemeente is ook hierdoor kwetsbaar. De verantwoordelijkheid voor de veiligheid van de gemeentelijke systemen en gegevens brengt mee dat ook deze positie en rol van gelieerde partijen meegenomen moeten worden in het veiligheidsbeleid.

ad 1.3 Social en security awareness
De aandacht voor het periodiek testen van de systemen is op basis van de informatie die de RKC heeft ontvangen tijdens dit onderzoek beperkt tot audits en vulnerability tests. Deze testen zijn belangrijk en noodzakelijk en moeten ook in de toekomst uitgevoerd blijven worden. Dat daarnaast ook de feitelijke werking van de beveiliging wordt getest en de kwetsbaarheid van buitenaf of van binnenuit wordt opgespoord middels periodieke pentesten, is niet vastgesteld kunnen worden.
Het signaleren van kwetsbaarheden en (voortdurend) preventief zoeken naar verbeteringen krijgt hierdoor te weinig aandacht.

De rol van de onafhankelijke Chief Information Security Officer is ondergewaardeerd door de positionering binnen de hiërarchische lijnorganisatie. Het ontbreekt aan een autoneem budget waarover de CISO kan beschikken, dat hem in staat stelt specifieke (pen-) testen uit te (laten) voeren die hij vanuit zijn verantwoordelijkheid noodzakelijk geacht.
De rol van de CISO als extra 'veiligheidsklep' die kritisch naar zaken kijkt en aandacht kan vragen van alle verantwoordelijken voor kwetsbaarheden komt niet tot zij recht.

ad 2 Beleid en beheer
Het beleid sluit aan bij gangbare opvattingen en ontwikkelingen en loopt daarmee op hoofdlijnen in de pas. Het beleid is vastgesteld in 2015 en daarmee aan een actualisatie toe. De inrichting van de organisatie en het beheer sluit aan bij de landelijk als algemeen aanvaarde standaarden en de periodiek uitgevoerde audits laten geen ernstige onvolkomenheden zien.

Centrale en periodieke sturing van informatiebeveiligingsbeleid ontbreekt en het veiligheidsbeleid is niet voldoende actueel. Het belang en de urgentie van veiligheidsbeleid vragen om structureel en periodiek aandacht te geven aan actualisatie van het beleid. Een PDCA-cyclus Informatieveiligheid die periodiek aandacht krijgt, ontbreekt op de agenda van de raad.

Audits en kwetsbaarheidstoetsen worden uitgevoerd conform specifieke landelijke richtlijnen en wettelijke ontwikkeling worden gevolgd. Het informatiebeveilingsbeleid loopt hiermee in de pas. De complexiteit en snelle veranderingen vragen aandacht voor een gestructureerde risicoanalyse en door de raad vastgestelde maatregelen voor veiligheid en de beveiliging van met name privacygevoelige gegevens. Informatiebeveiliging als onderdeel van een PDCA-cyclus veiligheid voor bewaking en bijsturing technische beveiliging is niet aangetroffen.

De raad is onzichtbaar als eigenaar van informatieveiligheid. De raad heeft een passieve en volgende rol in dit beleidsdossier. De signaalwerking die hiervan uitgaat stimuleert niet het urgentiebesef en prioriteit voor veiligheid in de organisatie.
Het voornemen om in het kader van ENSIA vanaf 2018 de raad te gaan informeren en mee te nemen kan als een nieuwe start worden gezien.

Bij de inrichting van de beheersorganisatie zijn verantwoordelijkheden toegekend aan specifieke functionarissen. De Chief Information Security Officer (CISO) die een onafhankelijke adviesbevoegdheid vraagt is onvoldoende in positie en rapporteert langs de hiërarchische lijnen. Ook beschikt de CISO niet over een eigen budget om zelfstandig testen uit te (laten) voeren. De onafhankelijkheid en de zelfstandigheid komen onvoldoende tot hun recht waardoor geen zekerheid bestaat over het agenderen van veiligheidsaspecten en het ongefilterd rapporteren over risico's en maatregelen.

ad 3 Bewustwording / bewustzijn

Digitale veiligheid vraagt om permanent aandacht van iedereen in de organisatie en om het bundelen van krachten. De directie heeft daarin een voorbeeldfunctie.

De pentest heeft aangetoond dat het toezicht en het herkennen van risico's te kort schiet en dat kwetsbaarheden te weinig aandacht krijgen. De ethische hacker merkt daarover op dat de gemeente ernstig te kort schiet op gedrag van medewerkers en de toegang tot het netwerk waardoor het eenvoudig is een nieuwe aanval succesvol op te zetten.

De risico's van de slecht beveiligde websites die aan de gemeente zijn gelieerd, zijn onderschat. De fishing aanval heeft aangetoond dat de gemeente kwetsbaar is door slecht beveiligde sites van organisaties die zich presenteren met: sittard-geleen.nl. In de ambtelijke reactie wordt opgemerkt dat het een zorgpunt is dat organisaties waar wij gegevens mee uitwisselen (BsGW) of mogelijk gaan fuseren (Vixia) de beveiliging niet op orde hebben en dat dit nadere actie vergt. Een actief beleid naar derden waarmee wordt samengewerkt op dit punt is noodzakelijk maar eveneens is alertheid geboden naar alle mogelijk aan de gemeente gelieerde sites.

Een gestructureerd communicatieplan en programma's gericht op het periodiek scholen van iedereen, van stagiaires, medewerkers, collegeleden tot raadsleden is niet aangetroffen. Digitale veiligheid is nog geen zaak van iedereen.

In de contacten met de directie rond de uitvoering van het RKC-onderzoek lag het accent meer op nut en noodzaak van een pentest, op zorgen over doublures, op de vraag of een pentest in deze gemeente überhaupt aan de orde is, op bezwaren tegen de werkwijze, de vervelende effecten van de hack en op de uitvoering van de test: kortom de schuldvraag staat steeds centraal. Het accent op de digitale veiligheid zelf en mogelijke leereffecten verschuift naar de achtergrond.

Ook het aanbod van de RKC om leerervaringen rond de pentest te delen is aanvankelijk afgeslagen door de directie. DE RKC komt tot de conclusie dat geen open en lerende houding om permanent en voortdurend te zoeken naar kwetsbaarheden en verbeteringen is aangetroffen.
In tweede termijn is gevraagd om de afdeling ICT alsnog in contact te brengen met het bureau dat de pentest heeft uitgevoerd. In dit constructief overleg zijn de bevindingen en aanbevelingen besproken. Dit gesprek geeft de RKC het begin van het vertrouwen terug, dat intern serieus en oplossingsgericht aandacht gaat worden gegeven aan de bevindingen en aanbevelingen inzake de kwetsbaarheid van de beveiliging.

2.2.2 Aanbevelingen

1. Het verdient aanbeveling een scholings- en trainingsprogramma te maken voor informatieveiligheid en iedereen hierbij te betrekken.
   Structurele aandacht is noodzakelijk om het bewustzijn rond het belang van informatieveiligheid te bevorderen. Dit trainingsprogramma kan als onderdeel van het informatieveiligheidsbeleid jaarlijks worden geactualiseerd. Onbewust zijn van mogelijke risico's maakt kwetsbaar en leidt tot onveiligheid.

2. Het verdient aanbeveling dat informatieveiligheid een zaak van iedereen wordt.
   De raad en het college dienen voorop te gaan in het uitdragen van het belang van informatieveiligheid. De voorbeeldwerking is daarbij essentieel. Door aandacht te geven aan het creëren van dragende krachten voor dit beleid kan draagvlak voor het veiligheidsdenken een belangrijke impuls krijgen.

3. Het verdient aanbeveling de informatieveiligheid voortdurend en structureel aandacht te geven.
   Door een PDCA-cyclus informatieveiligheid in te voeren krijgt dit beleid meer prioriteit en wordt veiligheid een periodiek agendapunt van de raad. Raadsleden worden meegenomen en kunnen invulling geven aan hun sturende en controlerende rol.

4. Het verdient aanbeveling de kwetsbaarheid van de systemen periodiek te testen.
   Voer periodiek pen-testen uit om de specifieke werking van de systemen te testen. Het verdient aanbeveling de CISO te vragen jaarlijks te rapporteren over de uitgevoerde testen en de gevonden kwetsbaarheden ten einde goed inzicht te geven in risicobeheersing. Het uitvoeren van periodieke test op cyberaanvallen van buitenaf en van binnenuit dient onderdeel van het informatiebeveiligingsbeleid te zijn.

5. Het verdient aanbeveling een systematische en actuele risicoanalyse aan de raad voor te leggen.
   Om de raad in staat te stellen te controleren op risicobeheersing van de informatiebeveiliging inclusief de noodzakelijke maatregelen, is een periodieke rapportage aan de raad gewenst. De raad kan hierdoor aandacht geven aan de maatregelen en gewenste of bereikte resultaten. De verantwoordelijkheid voor de veiligheid van de gemeentelijke systemen en gegevens brengt mee dat ook de positie en rol van gelieerde partijen meegenomen moeten worden in het veiligheidsbeleid.
   De raad krijgt hiermee handvaten om te sturen en te controleren.

6. Het is aan te bevelen het informatieveiligheidsbeleid te actualiseren.
   Om extra accent te geven aan veiligheid in zijn algemeen, aan bewustzijn en aan verantwoordelijkheden van iedereen is het aan te raden om naast een technisch

beveiligingsplan een algemeen informatieveiligheidsplan te maken en vast te stellen. Bij dit laatste kan het accent liggen op bewustwording, algemene trends, landelijke wetgeving en kaderstelling etc. Het beveiligingsplan plan is dan meer gericht op de technische aspecten, beveiliging van data en systemen en beheersmaatregelen. Beide plannen vragen een periodieke actualisatie. Het verdient aanbeveling dat de raad hierover expliciete afspraken maakt met het college.

7. Het verdient aanbeveling de positionering van de CISO binnen de gemeente scherper af te bakenen.

   Er is een onafhankelijke rol en positie van de CISIO voorzien. De verantwoordelijkheid en de slagkracht van deze functie is essentieel als waarborg voor kwaliteit en transparantie, over inschatting van risico's en benodigde maatregelen.
   Het is essentieel dat de raad en het college een ongefilterd oordeel van de CISO krijgen en dat deze over een eigen budget beschikt om de nodige onderzoeken en testen te uit te voeren. Dit kan vormgegeven worden door bijvoorbeeld jaarlijks een plan met begroting door de CISO te laten maken en ter accordering voor te leggen. De rapportage dient deel uit te maken van een gestructureerde periodieke rapportage aan de raad (PCDA cyclus informatieveiligheid).

8. De duo-functies van de Security Officer en de Security Manager vragen heroverweging vanwege splitsing van verantwoordelijkheden.

   De schaalgrootte van Sittard-Geleen en het toekennen van hoge prioriteit aan deze taken moeten ruimte kunnen geven om dit te realiseren. De scherpte in de organisatie en daarmee de kwaliteit van het veiligheidsdenken kan toenemen door eigen verantwoordelijkheden duidelijker te stipuleren.

9. Zet informatieveiligheid hoog op de agenda van raad en college.

   Door periodiek aandacht te geven aan informatieveiligheid wordt het goede voorbeeld gegeven. Het perspectief voor een lerende organisatie waarbij verwacht wordt dat iedereen meedoet, zich bewust is (wordt) van zijn verantwoordelijkheid, is sterk afhankelijk van de betrokkenheid vanuit het bestuur van de gemeente. Het is goed zich bewust te zijn van voorbeeldwerking die uitgaat van de visie, gedrag en opvattingen van het directieteam, het college en de raad in dit dossier.

10. Maak veiligheidsdenken tot speerpunt.

    Digitale veiligheid vraagt een bedrijfscultuur waarin "Durven leren" centraal staat. Door periodiek en structureel aandacht te geven en te zorgen voor een open transparante sfeer waarin het samen zoeken naar kwetsbaarheden en het met elkaar verbeteringen realiseren, belangrijker is dan het signaleren van tekortkomingen. Een goede voedingsbodem voor veiligheidsdenken met elkaar en op alle niveaus is cruciaal. Het verdient aanbeveling hierop te sturen.

2.3. Bestuurlijke reactie en nawoord Rekenkamercommissie

Onderstaand treft u de bestuurlijke reactie d.d. 28-2-2018 aan van het college van B&W van Sittard-Geleen.

7

Gemeente Sittard-Geleen
Born

Rekenkamercommissie
Sittard-Geleen en Stein
Postbus 18
6130 AA Sittard-Geleen

Cluster Concern Overig
Uw brief van
Uw kenmerk
Ons kenmerk
Behandeld door
Telefoon
Onderwerp Bestuurlijke wederhoor rekenkameronderzoek digitale veiligheid

Sittard-Geleen, 28 februari 2018

Wij hebben uw rapport inzake het onderzoek naar digitale veiligheid en de begeleidende brief waarin gelegenheid wordt gegeven voor bestuurlijke wederhoor in goede orde ontvangen. Wij hebben kennis genomen van de inhoud van het rapport en hebben de gedane aanbevelingen op hun merites beoordeeld.

Wij verzetten ons ten stelligste tegen uw conclusie, die u nota bene in de titel verwoordt, dat onze gemeente onbewust digitaal onveilig zou zijn. Wij zijn dagelijks bezig om de geautomatiseerde systemen van de gemeente veilig te maken en te houden en durven de stelling aan dat we, zowel qua inspanning als qua effectief resultaat, een voorhoedepositie innemen in gemeenteland. Ten onrechte wekt u de suggestie dat de deuren wagenwijd openstaan en iedere buitenstaander vervolgens overal gemakkelijk bij kan. Het is dan ook geen toeval dat uw hack-poging direct onderschept is, onze systemen direct daarvoor afgesloten zijn en u geen toegang heeft kunnen krijgen tot kwetsbare data.

Onze stelling wordt bevestigd door meerdere audits en onderzoeken door gecertificeerde IT-audits die de afgelopen periode zijn gehouden en waarvan zgn. vulnerability scans én penetratietesten onderdeel uit hebben gemaakt. Zo zijn wij de eerste van 90 gemeentelijke klanten van de landelijk geselecteerde, onafhankelijke IT-auditor BKBO die het ENSIA[1] assessment met goed gevolg heeft afgerond.

Natuurlijk bedenken hackers steeds nieuwe methoden en technieken. Deze materie is voortdurend in beweging en ontwikkeling. Wat vandaag veilig is kan morgen kwetsbaar zijn. Niet alles kan voorkomen worden maar wel blijken we adequaat te kunnen reageren indien zich toch incidenten voordoen. Om mogelijke schades te beperken zijn binnen de

[1] ENSIA (Eenduidige Normatiek Single Information Audit) heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus.

Postadres: Postbus 18, 6130 AA Sittard-Geleen ☎ 14 046 (vanuit buitenland +31 46 477 77 77) | www.sittard-geleen.nl

ICT-afdeling een beheerorganisatie en beheersproces ingericht waar issues accuraat en doelgericht opgepakt worden. Dat deze werkwijze goed functioneert blijkt ook uit het feit dat de door u ingehuurde hackers gedetecteerd, gelokaliseerd en ontmaskerd zijn. Ondersteuning door landelijke organisaties als de IBD (Informatie Beveiliging Dienst) en het NCSC (National Cyber Security Center) is hierbij eveneens een belangrijk hulpmiddel.

Het bewustzijn van medewerkers is inderdaad een kwetsbaarheid die ook binnen Sittard-Geleen speelt. Hierin is Sittard-Geleen echter beslist niet uniek. Ook landelijk vraagt men aandacht voor de mens als zwakke schakel in cybersecurity. Wij zijn ons er terdege van bewust dat nog het nodige gedaan dient te worden aan bewustzijnsverhoging wat betreft cybersecurity en waarborging van de privacy bij medewerkers, bestuurders en gemeenteraadsleden. Daarvoor is een communicatieplan bewustwording Informatiebeveiliging en Privacy opgesteld waarbij eveneens budget beschikbaar is voor het uitvoeren van activiteiten. Momenteel wordt voor de uitrol van dit plan in SSC-ZL verband een uitvraag gedaan bij firma's die kunnen ondersteunen bij de bewustwordingscampagne(s).

Wij constateren verder dat over een aantal zaken meermalen gedachten en uitgangspunten zijn uitgewisseld tussen uw commissie en medewerkers en directie over procedureafspraken, definities en inbedding van uw onderzoek. Wij constateren hierbij dat de standpunten en de interpretatie van de gemaakte afspraken niet gelijkluidend zijn en dat u - los van de eigen verantwoordelijkheid en de onafhankelijke positie die u heeft en die verder ook niet wordt betwist - op onderdelen een eigen koers heeft gevaren die zich buiten de normaal geldende regels voor ethische hackers begeeft. Ook heeft dit een ernstige verstoring van de bedrijfsvoering tot gevolg gehad, die bij juiste toepassing van regels en procedures niet nodig was geweest. Wij hebben ons ongenoegen daarover in een aantal gesprekken met u reeds kenbaar gemaakt..

Wat hier verder ook van zij, wij rekenen erop dat dit ook voor u een leermoment oplevert. Uiteindelijk dienen we allemaal hetzelfde gezamenlijk belang in deze, namelijk het waarborgen van de veiligheid van de gegevens van onze inwoners, bedrijven en instellingen.

U heeft een tiental aanbevelingen benoemd. Per aanbeveling geven wij hierna een reactie. Voor de overige zaken verwijzen wij kortheidshalve naar de reacties zoals beschreven in de beantwoording van de vragenlijst welke onderdeel uitmaakt van uw rapport als paragraaf 3.8 Bijlage 2 Vragenlijst Digitale Veiligheid Versie 4.

Aanbevelingen:

1. *Het verdient aanbeveling een scholings- en trainingsprogramma te maken voor informatieveiligheid en iedereen hierbij te betrekken.*

Er is reeds een bewustwordingscampagne in voorbereiding die organisatiebreed uitgerold zal worden en alle geledingen inclusief het college van B en W , de gemeenteraad en de burgerraadsleden betreft. Dit gebeurt in afstemming met de gemeenten Maastricht en Heerlen. Deze aanbeveling is derhalve overbodig.

Postadres: Postbus 18, 6130 AA Sittard-Geleen ☎ 14 046 (vanuit buitenland +31 46 477 77 77) | www.sittard-geleen.nl

2. *Het verdient aanbeveling dat informatieveiligheid een zaak van iedereen wordt.*

Met deze aanbeveling stemmen wij in. In de geplande bewustwordingscampagne zal specifiek aandacht worden gevraagd voor deze doelstelling.

3. *Het verdient aanbeveling de informatieveiligheid voortdurend en structureel aandacht te geven.*

Deze aanbeveling nemen wij over. Middels ENSIA wordt de raad in de toekomst structureel geïnformeerd (zie verder punt 5).

4. *Het verdient aanbeveling de kwetsbaarheid van de systemen periodiek te testen.*

Interne pentesten worden maandelijks gedaan en externe pentesten zullen in de toekomst frequenter worden uitgevoerd.
Van 22 - 24 januari heeft reeds de eerste externe pentest van 2018 plaats gevonden. Deze test heeft geen bevindingen en derhalve geen kanttekeningen of opmerkingen opgeleverd. Deze aanbeveling is dan ook overbodig, want dit wordt reeds geruime tijd in praktijk gebracht.

5. *Het verdient aanbeveling een systematische en actuele risicoanalyse aan de raad voor te leggen.*

Hiermee wordt al rekening gehouden bij de implementatie van ENSIA. Risicoanalyses zijn 2 tot 3 jaar geldig, wat betekent dat in 2018 opnieuw een Risicoanalyse dient te worden gedaan. In de PDCA cyclus Informatiebeveiliging is dit opgenomen als activiteit voor 2018. Conform ENSIA voorziet deze Risicoanalyse eveneens in een rapportage die geschikt is om aan de raad voor te leggen. Deze aanbeveling wordt dus reeds in praktijk gebracht.

6. *Het is aan te bevelen het informatieveiligheidsbeleid te actualiseren.*

Het informatieveiligheidsbeleid wordt ieder jaar gereviewd en waar nodig geactualiseerd. Deze aanbeveling is dus al bestaande praktijk.

7. *Het verdient aanbeveling de positionering van de CISO binnen de gemeente scherper af te bakenen.*

Indien nodig en wenselijk rapporteert de verantwoordelijke medewerker rechtstreeks aan de directie. Deze stelt de verantwoordelijk portefeuillehouder en indien nodig ons college onverwijld op de hoogte. Deze aanbeveling nemen we dus niet onverkort over.

8. *De duo-functies van de Security Officer (SCO) en de Security Manager (SM) vragen heroverweging vanwege splitsing van verantwoordelijkheden.*

Deze aanbeveling wordt nader overwogen mede in het licht van komende ontwikkelingen rond ENSIA en de overheveling van taken naar het SSC-ZL.
Om breed draagvlak onder het management te creëren is er reeds een intern Forum Informatiebeveiliging ingesteld. Dit Forum functioneert naar tevredenheid en is benodigd om de PDCA cyclus Informatiebeveiliging goed te kunnen managen, besluiten te nemen op tactisch en operationeel niveau, adviezen te geven aan directie en bestuur en benodigde maatregelen uit te voeren.
Wat betreft controle en audit zijn er meerdere controle- en auditmechanismen die toereikend zijn om de onafhankelijkheid en objectiviteit te waarborgen.

Postadres: Postbus 18, 6130 AA Sittard-Geleen ☎ 14 046 (vanuit buitenland +31 46 477 77 77) | www.sittard-geleen.nl

9. *Zet informatieveiligheid hoog op de agenda van raad en college.*
Deels is dit een aanbeveling voor de raad zelf. Wij adviseren de gemeenteraad deze aanbeveling over te nemen.

10. *Maak veiligheidsdenken tot speerpunt.*
Ook deze aanbeveling nemen we over. Wij onderschrijven een bedrijfscultuur waarin "durven leren" centraal staat en streven naar een open en transparante sfeer waarin het samen zoeken naar kwetsbaarheden en het met elkaar verbeteringen realiseren belangrijker is dan het signaleren van tekortkomingen. Wij zetten hiervoor o.a., interne opleidingstrajecten, bewustwordings-campagnes en Social Intranet in als instrumenten om deze gedragsverandering te bewerkstelligen en te monitoren.

Concluderend verzetten wij ons nadrukkelijk tegen het beeld dat u oproept van de digitale veiligheid van onze gemeente en de aandacht die daaraan besteed wordt voor zover uw aanbevelingen daarop zijn gebaseerd, onderschrijven wij die niet. Voor het overige passen zij in het beleid dat ons college reeds voert dan wel in voorbereiding heeft.

Hoogachtend,

Burgemeester en wethouders van Sittard-Geleen,

drs. G.J.M. Cox,
burgemeester

mr. G.J.C. Kusters,
gemeentesecretaris

Nawoord RKC bij bestuurlijke reactie Digitale Veiligheid Sittard-Geleen

Op 2 maart hebben wij de bestuurlijke reactie ontvangen. Het college geeft eerst in algemene zin haar mening over het rapport en gaat vervolgens in op de aanbevelingen.

> *Het college merkt op dat ze zich ten stelligste verzet tegen de conclusie van de RKC dat de gemeente onbewust digitaal onveilig zou zijn. Dat de titel de suggestie wekt volgens het college dat alle deuren wagenwijd openstaan en iedere buitenstaander overal gemakkelijk bij kan.*

Deze opmerking is een belangrijk punt van overweging voor de RKC.
Het is beslist niet zo dat alle deuren wagenwijd openstaan en dat de RKC van mening is dat de veiligheid in Sittard-Geleen bewust wordt verwaarloosd. Het is beslist niet de bedoeling om deze indruk op te wekken. Het is spijtig dat dit gevoel kennelijk ontstaat. Het leidt bovendien de aandacht af van het doel van het RKC-onderzoek om kwetsbaarheden te signaleren om vanuit dat signaal bij te dragen aan de digitale veiligheid. De energie gaat daardoor uit naar de boodschap in plaats van naar de inhoud.
De RKC heeft de titel dan ook aangepast om de aandacht niet onnodig af te leiden.

De RKC wil in dit verband onder de aandacht brengen dat is geconcludeerd dat de netwerkinfrastructuur op orde is. Dit is een essentieel basisuitgangspunt en er is geconcludeerd dat de afdeling ICT zich voldoende bewust is van het belang en ervoor heeft gezorgd dat dit goed geregeld is.
Tegelijk zijn er echter meerdere kwetsbaarheden gevonden, die in combinatie met elkaar hebben gezorgd voor een onveilige omgeving. De fishingaanval is gelukt door juist gebruik te maken van deze combinatie van de gevonden kwetsbaarheden. De RKC vindt dat voldoende is aangetoond dat de gemeente kwetsbaar is. Geconcludeerd is dat men zich onbewust was van de aangetoonde kwetsbaarheden en dat een lerende en oplossingsgerichte houding ontbrak. De RKC ziet dit als een belangrijk verbeterpunt en heeft enkele concrete aanbevelingen hiervoor gedaan.

> *Het college constateert:' dat de beheersorganisatie en beheersproces zo zijn ingericht dat issues adequaat en doelgericht worden opgepakt. Dat dit goed functioneert blijkt uit het feit dat de hackers zijn gelokaliseerde en getraceerd'.*

De RKC wil hierbij opmerken dat de hacker is opgemerkt en gelokaliseerd. Dit is op zichzelf bezien een adequate en passende aanpak. Echter de hacker heeft minimaal 7 uur ongestoord zijn aanval uit kunnen voeren. In de nabespreking met de afdeling-ICT is aangegeven, dat het lek inmiddels is gedicht.
Het onderzoek heeft zich beperkt tot het aantonen van de kwetsbaarheid maar er is geen toestemming gegeven aan de ethische hacker om feitelijk in de systemen binnen te dringen

door de verkregen wachtwoorden te gebruiken. Hierdoor is feitelijk niet getest of de verkregen wachtwoorden toegang boden tot privacygevoelige informatie. Dit viel buiten de

geformuleerde opdracht. De kwetsbaarheid betreft het gedurende meerdere uren beschikbaar zijn van een groot aantal wachtwoorden in verkeerde handen, terwijl dit een erg opvallende (een zogenaamde luidruchtige) aanval was.

> *Volgens het college is het bewustzijn van medewerkers inderdaad een kwetsbaarheid binnen Sittard-Geleen en is het zich terdege bewust dat er het nodige gedaan dient te worden, waarvoor een communicatieplan bewustwording Informatiebeveiliging en Privacy is opgesteld ook voor bestuurders een gemeenteraadsleden.*

De RKC vindt het een positieve ontwikkeling. Het gaat bij bewustzijn immers om alle eventuele betrokkenen die toegang hebben tot gemeentelijke systemen.
Digitale Veiligheid is een zaak van iedereen.

Het college geeft vervolgens een reactie op de tien aanbevelingen van de RKC.
Op een zestal punten volgt het college de aanbevelingen van de RKC. Bij vier aanbevelingen worden kanttekeningen gemaakt waarop hieronder wordt ingegaan.

ad 1 De aanbeveling om een scholings- en trainingsprogramma te maken en iedereen erbij te betrekken is volgens het college overbodige omdat er al een bewustwordingsprogramma in voorbereiding is.
De RKC ziet dit op zichzelf als een hoopvolle ontwikkeling.

ad 4 De aanbeveling om kwetsbaarheid van systemen periodiek te testen vindt het college overbodig omdat dit reeds geruime tijd wordt gedaan.
De RKC wil wijzen op het grote belang om periodiek testen uit te voeren. Als dit in de toekomst gaat gebeuren sluit dit goed aan op het gegeven advies.

ad 6 De aanbeveling om het informatieveiligheidsbeleid te actualiseren is volgens het college al bestaande praktijk.
De RKC wil hierbij opmerken dat het actualiseren van het veiligheidsbeleid ook van belang is om de raad te informeren en te betrekken bij de verdere uitbouw van dit beleid, af te stemmen over de te maken keuzes en de raad in positie te brengen op haar controlerende rol. Een actualisatie van het in 2015 vastgestelde informatiebeveiligingsbeleid lijkt hiervoor de aangewezen weg.

ad 7 De Positionering van de CISO scherper afbakenen
Het college wil de aanbeveling niet onverkort overnemen.
In de kern gaat de aanbeveling van de RKC over het vormgeven van de onafhankelijke positie van de CISO. Hierbij is aandacht gevraagd voor de adviesrol en de bevoegdheid om het verantwoordelijke bestuur ongefilterd te adviseren. De organisatorische/ hiërarchische inbedding is daarbij minder leidend.

Tot slot.
De RKC ziet het uitgevoerde onderzoek als een bijdrage aan het verbeteren van het veiligheidsdenken binnen de gemeente. De kunst om cybercriminelen een stap voor te blijven vraagt een transparante en lerende houding van iedereen en het voortdurend bewust zijn van potentiele kwetsbaarheden en risico's. De raad heeft hierin een voorbeeldfunctie door veiligheid hoog op de agenda te zetten.

3. Nota van bevindingen

3.1 Aanleiding van het onderzoek

Gemeenten dragen verantwoordelijkheid voor informatiebeveiliging en in het bijzonder de bescherming van persoonsgegevens. Recente publicaties over datalekken en onderzoeken van rekenkamers laten zien aan dat gemeenten kwetsbaar zijn en dat het nodig is informatiebeveiliging extra aandacht te geven. De Visitatiecommissie informatieveiligheid[1] merkt in haar onlangs gepubliceerde rapport 'Durven leren' op hoe belangrijk het is dat gemeentebestuurders zich eigenaar voelen van informatieveiligheid in hun gemeente. Het belang en bewustwording van informatiebeveiliging is daarmee voldoende aangetoond. De vraag in welke mate de eigen gemeente Sittard-Geleen informatieveilig of -kwetsbaar is, dringt zich op. De noodzaak om vanuit de raad aandacht aan dit onderwerp te geven dringt zich temeer op nu ook de wettelijke kaders aangescherpt zijn en ertoe leiden, dat tot 25-5-2018 de gelegenheid is om het huis op orde te brengen.

Ter ondersteuning van de raad in haar sturende en controlerende rol op dit thema is antwoord gewenst op de vraag: in hoeverre zijn de data veilig en zijn beide gemeenten Sittard-Geleen en Stein beschermd tegen bedreiging van buitenaf. Daarnaast gaat het om de vraag: hoe is de raad hiervan op de hoogte en erbij betrokken.
Bij de oriëntatie is gebleken dat de raad weinig betrokken is geweest bij digitale veiligheid terwijl dit wel verwacht mag worden. Eveneens is de website internet.nl[2] gebruikt om te toetsen of websites van beide gemeenten up to date zijn (ondersteuning biedt voor de moderne internetstandaarden). Dit gaf een eerste indruk.
Het resultaat was:
Website sittardgeleen.nl is up to date voor 73%
Website Stein is up to date voor 87%.

Besloten is in beide gemeenten een globaal onderzoek in de vorm van een QuickScan uit te voeren. Aan een gespecialiseerd bedrijf is gevraagd een black-box penetratietest uit te voeren. De rekenkamercommissie heeft het Bureau Cybersecurit dat gespecialiseerd is in het uitvoeren van ethische hacks verzocht een black box penetratietest (pentest) bij de gemeente Sittard-Geleen en bij de gemeente Stein uit te voeren op de ICT-infrastructuur. De bevindingen worden voor elke gemeente apart gerapporteerd. De pentest is uitgevoerd als een quick-scan om een globaal beeld en een eerste indruk van kwetsbaarheden te krijgen. Het bureau Cybersecurit geeft aan dat de pentest geen garanties biedt voor de veiligheid want daarvoor zijn uitgebreidere en diepgaandere tests nodig.

Een black box onderzoek vereist normaliter om de organisatie onwetend te laten om zo natuurgetrouw mogelijk te werk te gaan. De RKC heeft er in dit geval voor gekozen, ter

[1] Eindverslag visitatiecommissie informatieveiligheid "Durven leren" , https://vng.nl/files/vng/durven-leren_20170906.pdf , september 2017.
[2] internet.nl is een initiatief van de internetgemeenschap en de Nederlandse overheid.

voorkoming van onnodige ongemakken, om in het startgesprek de gemeentesecretaris portefeuillehouder en de afdeling ICT wel te informeren over het onderzoek. Ook is tijdens het interview met de afdeling ICT vooraf de uitvoering van het onderzoek aangekondigd en is stilgestaan bij de bedoelingen van het onderzoek en de positie en afbakening.
Hierbij is afgesproken geen maatregelen te nemen om het onderzoek zo natuurgetrouw mogelijk te laten verlopen.

3.2 Bevindingen

Het onderzoek naar de informatieveiligheid in Sittard-Geleen geeft een eerste indruk van de kwetsbaarheden en de aandacht van de raad voor dit onderwerp.
Dit heeft de navolgende bevindingen opgeleverd.

Bevinding 1
Er zijn assessment-onderzoeken gedaan naar de aanwezigheid van administratieve beheersmaatregelen voor de DigiD aansluiting. Er worden ook vulnerability scans uitgevoerd inzake DigiD beveiliging. Dit is geen pentest naar de werking van de beveiliging. De pentest door de RKC kan een positieve bijdrage leveren aan de interne aandacht voor digitale veiligheid.

Bevinding 2
De informatie aan de raad betreft een paragraaf in het jaarplan en de boardletter van de accountant.

Bevinding 3
Informatieveiligheid is geen specifiek thema op de agenda van de raad en krijgt aandacht als onderdeel van de jaarstukken en de vaststelling van de boardletter van de accountant.

Bevinding 4
De Security Officer rapporteert aan de teammanager en het Forum en niet rechtstreeks aan het bestuur.

Bevinding 5
Het beleid informatiebeveiliging is door het college vastgesteld.
Uitkomsten van uitgevoerde audits, beveiligingsmeldingen (incidenten, datalekken etc.) en de risico- analyses worden niet aan de raad gerapporteerd.

Bevinding 6
Over interne audits wordt intern gerapporteerd en niet gerapporteerd aan raad.

Bevinding 7
De formatie dient nog op niveau te worden gebracht en de onafhankelijke positie van de Functionaris gegevensbescherming is daarbij een belangrijk aandachtspunt.

Bevinding 8
Het beleid informatieveiligheid loopt in de pas met de landelijke aanpak en het landelijk afgesproken normenkader wordt gerespecteerd. Het beleid is door het college vastgesteld in 2015.

Bevinding 9
De beheersregels en -procedures zijn conform landelijk normenkader opgezet en worden gevolgd. Er is geen onderzoek gedaan naar de feitelijke kwetsbaarheid van systemen middels een pentest.

Bevinding 10
- Informatieveiligheidsvraagstukken krijgen geen structurele en periodieke aandacht van de raad.
- Een periodieke rapportage gebaseerd op een structurele en cyclische analyse van de informatieveiligheid aan de raad ontbreekt.
- Niet alle deelnemers in het netwerk worden actief betrokken bij acties rond verbetering van het veiligheidsbewustzijns.
- Cybersecurit geeft aan dat het bewustzijn rond Informatieveiligheid onvoldoende aanwezig is op verschillende niveaus in de gemeente en de veiligheidsrisico's worden onderschat.
- Het testen van systemen geschiedt middels audits waarbij de werking van de systemen en de werking van de beveiliging is uitgesloten. Periodieke penetratietests maken geen deel uit van onderzoek naar de informatieveiligheid.

Bevinding 11
De afdeling ICT is zich bewust van digitale veiligheid en het belang voor de zorg voor actualiteit van software en de inrichting van de netwerkwerk infrastructuur.

Bevinding 12
De netwerkinfrastructuur blijkt geeft van gedegen en doordachte aanpak inzake netwerkbeveiliging.

Bevinding 13
Het bleek mogelijk toegang te krijgen tot apparatuur of computers maar niet tot (privacygevoelige) data in het netwerk.

Bevinding 14
De email server valideert niet of de binnenkomende mail daadwerkelijk afkomstig is van het juiste adres van de afzender. Dit is een kwetsbaarheid met een zeer hoog risico.

Bevinding 15
Er zijn 13 kwetsbaarheden geconstateerd door Cybersecurit waarvan zeven met de kwalificatie hoog[3] risico voor de gemeente. In hoofdlijnen kunnen genoemd worden:
- Het veiligheidsbewustzijn binnen de gemeente als geheel is als volstrekt onvoldoende gekwalificeerd.

[3] Bij de kwalificatie is gekeken naar: de moeite om binnen te dringen, de schade die aangericht kan worden en mogelijk afbreukrisico.

- Ongeautoriseerde toegang tot gebouwen en het netwerk is eenvoudig gebleken.
- De toegang tot gebouwen en tot het netwerk is onvoldoende beveiligd.
- De websites van gelieerde partijen zijn van opvallend lage kwaliteit en zijn gevoelig voor brute force aanvallen, waardoor de gemeente erg kwetsbaar is.
- De gebruikte wachtwoordstructuur is te eenvoudig en daardoor erg kwetsbaar.

3.3 Aanpak en afbakening

Gemeenten dragen verantwoordelijkheid voor informatiebeveiliging en in het bijzonder voor de bescherming van persoonsgegevens. In VNG verband is in 2013 een normenkader afgesproken in de Baseline Informatiebeveiliging Gemeenten (BIG). Het spreekt voor zich dat de normenkaders, de juridische richtlijnen en de vertaling naar organisatorische beleidsmaatregelen de kaders vormen voor het beveiligingsbeleid. De vraag is relevant in hoeverre zijn de data veilig en is de gemeente beschermt tegen bedreiging van buitenaf.

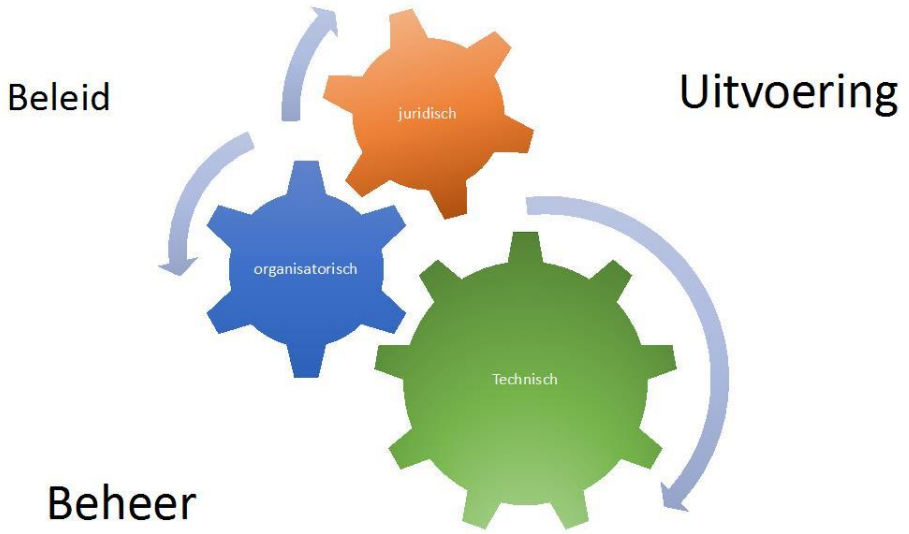
Europese richtlijnen en landelijke wetgeving wordt aangescherpt met name op de bescherming van persoonsgegevens. Gemeenten hebben als gevolg van de decentralisaties in het sociaal domein steeds meer (bijzondere) persoonsgegevens[4] in beheer. Ook wordt steeds meer informatie digitaal opgeslagen en overgedragen en worden systemen en data steeds vaker aan elkaar gekoppeld. Het belang van gemeenten om de informatiebeveiliging op orde te hebben en weerbaar te zijn tegen dreigingen als cybercrime is als gevolg van deze ontwikkelingen aanzienlijk toegenomen.

Informatiebeveiliging is een complex van samenhangende aspecten en risicofactoren. Afbakening van het onderzoeksgebied voor de Rekenkamercommissie is nodig.
Het vraagstuk van informatiebeveiliging richt zich in grote lijnen op organisatorische en technische maatregelen om gemeentelijke informatie te beschermen. De gemeente dient er tevens voor te zorgen dat wordt voldaan aan de nieuwe relevante wet en regelgeving[5].

De gemeenten moeten van de rijksoverheid in dit kader zorgen voor een informatiebeveiligingsbeleid. Dit gaat in op de organisatorische en juridische maatregelen, op bewustwording van mensen als schakel in het proces, op het benoemen van verantwoordelijkheden en het periodiek controleren, middels audits, of aan de kaders wordt voldaan. Het sturen op kwaliteit van informatiebeveiliging betekent structurele en periodieke aandacht in alle geledingen voor beleid, uitvoering en beheer. Gelet op de juridisch organisatorische risico's dient de Raad op hooflijnen op de hoogte te zijn over genomen maatregelen, de stand van zaken en de voortgang in de realisatie van het totale informatiebeveiligingsbeleid.
De samenhang der dingen is toegelicht in onderstaand schema.

[4] Een persoonsgegeven is iedere vorm van informatie die direct over iemand gaat of naar deze persoon te herleiden is. Bij bijzondere persoonsgegevens gaat het om informatie over iemands godsdienst of levensovertuiging, ras, politieke voorkeur, gezondheid, seksuele leven, lidmaatschap van een vakbond of strafrechtelijk verleden. Bijzondere persoonsgegevens mogen niet gebruikt worden, tenzij daarvoor een wettelijke uitzondering geldt. Bron: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens

[5] Wet Bescherming Persoonsgegevens (Wpb), Europese richtlijn persoonsgegevens, Algemene verordening inzake gegevensbescherming, Wet Basisregistratie Personen.



De noodzaak om beleids- en beheersmaatregelen te nemen wordt mede juridisch afgedwongen door meldplicht datalek[6] en door boeteclausules indien niet aan de voorwaarden is voldaan. De boete is nu maximaal € 820.00,= en gaat in 2018 oplopen tot € 20 mln. of 4% van de begroting.

De raad dient vanuit haar sturende en controlerende verantwoordelijkheid nadrukkelijk betrokken te zijn bij de inrichting van het informatiebeveiligingsbeleid en passende maatregelen te laten nemen om te voldoen aan de normenkaders.

Het einddoel is de gemeente te beschermen tegen beveiligingsincidenten (bedreigingen, cybercrime) en het werken met gevoelige informatie te beheersen. De organisatorische en juridische maatregelen vragen veel aandacht om de basis op orde te krijgen.
Vanuit het beveiligingsperspectief is daarbij belangrijk inzicht te hebben in de actuele stand van zaken met betrekking tot de kwetsbaarheden en de toegankelijkheid van data.

De RKC wil onderzoek doen naar de techniek om inzicht te krijgen in de vraag in hoeverre de data van de gemeente op dit moment veilig zijn en beschermd zijn tegen ongewenste aanvallen (of misbruik) van buiten.

Dit onderzoek wordt mede uit efficiencyoverwegingen voor beide gemeenten Sittard –Geleen en Stein tegelijkertijd uitgevoerd.

[6] Wet Bescherming Persoonsgegeven, vanaf 1-1-2016 geldt een meldplicht aan Autoriteit Persoonsgegevens.

3.4 Doelstelling en vraagstelling

Doelstelling

De Rekenkamercommissie beoogt met dit onderzoek inzicht te geven in de huidige staat van de technische beveiliging van de gegevens die de gemeente beheert. Het onderzoek richt zich op de technische toegankelijkheid en bescherming van data.

Met dit onderzoek krijgt de raad antwoord op de vraag of de gemeenten kwetsbaar is voor cyberaanvallen gericht op vertrouwelijke en persoonsgegevens of de beschikbaarheid en integriteit van de systemen gevaar loopt.

Het is een beperkt onderzoek om (gecontroleerd) als kwaadwillende buitenstaander te zoeken naar kwetsbaarheden en toegang tot (vertrouwelijke) informatie te verkrijgen.
De opdracht betreft een 'Black box pentest'[7], waarbij vooraf geen informatie wordt verstrekt over de ICT omgeving.

Tevens wordt aandacht gegeven aan de informatievoorziening aan de raad over digitale veiligheid en de wijze waarop het proces Digitale Veiligheid op de agenda staat in beeld gebracht.

Vraagstelling

De deelvragen die hieruit volgen betreffen:

Algemeen

- Welke informatie is aan de raad verstrekt over informatiebeveiliging?
- Welke aandacht krijgt dit thema van raad, college en ambtelijke organisatie?
- Hoe is de raad in positie op de vaststelling en uitvoering van het informatiebeveiligingsbeleid?
- Welke aandacht wordt gegeven aan audits en rapportage hierover aan de raad?

Technische bescherming Informatie

- Welke kwetsbaarheden zijn er concreet geconstateerd in de ICT-infrastructuur van de gemeente?
- Zijn er datalekken geconstateerd?
- Zijn er datalekken gemeld?
- Welke veiligheidsrisico's doen zich voor in de huidige techniek?

Het onderzoek is vanuit de rekenkamercommissie begeleid door Thijs Heijnen en Bert Holman.

[7] Blackbox Pentest: een binnendringingstest toetst ICT-systemen op kwetsbaarheden waarbij vooraf geen informatie beschikbaar is over het netwerk en de systemen.

3.5 Feitenrelaas informatie aan de raad

1. Toelichting en afbakening

Om inzicht te krijgen in de informatieverstrekking aan de raad en de aandacht die Digitale veiligheid krijgt op bestuurlijk niveau is gebruik gemaakt van een landelijk ontwikkelde 'vragenlijst voor raadsleden'[8]. Hierin staat een tiental vragen die raadsleden op weg kunnen helpen bij hun controlerende rol. De lijst is zeker niet uitputtend en ook niet diepgaand maar geeft wel inzicht en ook aanknopingspunten om verder door te vragen. De RKC heeft deze standaardvragenlijst gebruikt en laten invullen mede om een eerst inzicht te verstrekken en de kwetsbaarheid van digitale veiligheid in Sittard-Geleen te toetsen.

Naast de standaard vragenlijst zijn zes aanvullende vragen gesteld over concrete informatievoorziening en agendering van digitale veiligheid in de eigen gemeente. Dit betreft de eerste vragen in de lijst (In bijlage 2 is de ingevulde vragenlijst integraal opgenomen).
De vragenlijst is ingevuld door de Security Officer/ coördinator ENSIA en de Security manager/ privacy manager (beide dubbelfuncties). Beide functionarissen waren ook aangewezen als de gesprekspartners voor de RKC.

2. Nut en noodzaak Pentest door RKC

Nagegaan is eerst hoe het RKC pentest-onderzoek zich verhoudt tot reeds eerder uitgevoerde pentests door de gemeente Sittard-Geleen.
De onderzoeken die zijn uitgevoerd betreffen de jaarlijks verplichte onderzoeken onder andere in het kader van DigiD. De gemeente heeft de DigiD op eigen servers lopen en moet als gevolg daarvan aan de strenge eisen voldoen. Elk jaar moeten de eisen gecheckt worden. Het onderzoek is uitgevoerd in 2014, 2015 en 2016.
Het onderzoek betreft een toets van de voorwaarden en eisen inzake de inrichting van de systemen, de software en de organisatorische maatregelen.
In de ontvangen rapportages is omschreven als:
"een DigiD beveiligingsassessment is uitgevoerd betrekking hebbend op het onderzoeken van de opzet en het bestaan van maatregelen en procedures gericht op ICT-beveiliging van de webomgeving van DigiD aansluiting Gemeente-Sittard-Geleen2". Er is geen onderzoek gedaan naar de werking van deze beheersingsmaatregelen van DigiD aansluitingen".

Voor deze assessments worden externe bureaus ingehuurd. De bijbehorende vulnerability scan wordt uitgevoerd als grey-test waarbij volwaardige toegang tot het netwerk wordt aangeboden aan de testers. Hierbij wordt de Vulnerability (kwetsbaarheid) getest. Pag. 1 en 2 van het rapport is overhandigd met daarin de samenvatting van de uitkomst.

[8] Raadslid.nu, Informatieveiligheid voor raadsleden, Nederlandse vereniging voor raadsleden.

De uitgevoerde grey-test[9] heeft geen kwetsbaarheden opgeleverd.

De overige twee beveiligingsassessment inzake DigiD zijn van 2017. Er zijn geen bevindingen uit deze testen gekomen inzake de werking van de systemen.

De rapportages melden dat de opzet en het bestaan van beveiligingsmaatregelen is getoetst en er geen onderzoek naar de feitelijke werking van de systemen is gedaan. Eveneens is bij de uitgevoerde assessments geen onderzoek gedaan naar de werking van de interne beheersingsmaatregelen.

Geconcludeerd is in het ambtelijk overleg dat het RKC onderzoek een positieve bijdrage kan leveren aan de interne ontwikkeling en aandacht voor digitale veiligheid en als zodanig zeker niet conflicteert met de interne aandacht en acties.
Het onderzoek wordt gezien als een goede aanvulling.

Bevinding 1

Er zijn assessment-onderzoeken gedaan naar de aanwezigheid van administratieve beheersmaatregelen voor de DigiD aansluiting. Er worden ook vulnerability test uitgevoerd inzake DigiD beveiliging. Dit is geen pentest naar de werking van de beveiliging. De pentest door de RKC kan een positieve bijdrage leveren aan de interne aandacht voor digitale veiligheid.

3. <u>Informatie aan de raad en aandacht voor Digitale veiligheid in Sittard -Geleen.</u>

Het eerste deel van het onderzoek richt zich op de vragen over de informatie aan de raad en de aandacht die de raad geeft aan het onderwerp digitale veiligheid.

Vraag 1. Welke informatie is aan de raad verstrekt over informatiebeveiliging vanaf 2015?

> Er zijn geen specifieke afspraken gemaakt met de raad over hoe Digitale Veiligheid aandacht krijgt. Het college heeft in 2015 het beleidsdocument en plan van aanpak informatiebeveiliging vastgesteld. In het Beleidsdocument Informatiebeveiliging 2015 is een zinssnede opgenomen over de wijze waarop de raad wordt geïnformeerd, te weten: “De gemeente Sittard-Geleen zorgt voor verankering van Informatieveilig-heid, waarbij het college de gemeenteraad informeert. Dit gebeurt door middel van een aparte paragraaf informatieveiligheid in het jaarverslag.”
> In de jaarstukken (jaarplan 2016) wordt aandacht besteed aan informatieveiligheid. (2016: pag. 166).

[9] DigiD Assessment report, 9 februari 2017.

In de Boardletter behorende bij de jaarstukken doet de accountant zijn verslag van bevindingen over de IT-omgeving en Cyber Security.

Meer informatie aan de raad is /wordt niet verstrekt.
Over 2017 wordt in het kader van de ENSIA voorzien in rapportage aan de Raad.

Bevinding 2

De informatie aan de raad betreft een paragraaf in het jaarplan en de boardletter van de accountant.

Vraag 2. Welke aandacht krijgt Digitale Veiligheid van raad?

In de Resolutie informatieveiligheid is aangegeven dat het college de gemeenteraad informeert over informatieveiligheid door middel van een aparte paragraaf informatieveiligheid in het jaarverslag.

Begin 2015 is een thema sessie voor de raad gehouden over de resolutie informatieveiligheid en het plan van aanpak informatiebeveiliging van Sittard-Geleen.
Op 5 november 2015 is de werkgroep Signaal (Sociaal domein) geïnformeerd over informatiebeveiliging.

Bevinding 3

Informatieveiligheid is geen specifiek thema op de agenda van de raad en krijgt aandacht als onderdeel van de jaarstukken en de vaststelling van de boardlettre van de accountant.

Vraag 3. Welke aandacht krijgt digitale veiligheid van college en ambtelijke organisatie?

Op 27-01-2015 heeft het college vastgesteld:
- Beleidsdocument informatiebeveiliging 2015
- Plan van aanpak informatiebeveiliging 2015

Interne rapportage
Intern is een Forum Informatiebeveiliging ingesteld. De Security Officer rapporteert aan de teammanager, die dit doorleidt naar het Forum en de directeur. Vervolgens wordt dit doorgeleid naar de gemeentesecretaris en portefeuillehouder.

De security Officer heeft geen eigen budget en een dubbelfunctie.

Bevinding 4

De Security Officer rapporteert aan de teammanager en het Forum en niet rechtstreeks aan het bestuur.

Vraag 4. Hoe is de raad in positie op de vaststelling en uitvoering van het informatiebeveiligings-beleid?

In het Beleidsdocument Informatiebeveiliging 2015 is het informatiebeveiligingsproces inclusief de rapportage aan de raad beschreven. Het beleidsdocument is door het college vastgesteld.
De rapportage gaat naar de directie c.q. het college. Dit wordt niet doorgeleid naar de raad omdat dit wordt gezien als een interne aangelegenheid. De wisseling van directie laat ruimte voor meer bredere verspreiding van informatie.

Raadsleden zijn niet meegenomen in de enquête bewustwording terwijl ze wel participeren in het digitale systeem.

Bevinding 5

Het beleid informatiebeveiliging is door het college vastgesteld. Uitkomsten van uitgevoerde audits, beveiligingsmeldingen (incidenten, datalekken etc.) en de risico- analyses worden niet aan de raad gerapporteerd.

Ad 5 Welke aandacht wordt gegeven aan audits en rapportage hierover aan de raad?

Audits zijn jaarlijks terugkerend. Er vinden meerdere toetsen en interne audits jaarlijks plaats. Genoemd kunnen worden de DigiD audit, zelfaudit Suwinet, BRP en PNIK. Tevens doet de accountant jaarlijks een audit in het kader van de jaarrekening en rapporteert dit in de boardlettre.
Er wordt gerapporteerd aan teammanager, forum Informatiebeveiliging en directeur; De hogere echelons rapporteren vervolgens aan de gemeentesecretaris en Portefeuillehouder overleg. De rapportages worden besproken in het Forum.

Uitkomsten van de interne audits worden niet aan de raad gerapporteerd.

Bevinding 6

Over interne audits wordt intern gerapporteerd en niet gerapporteerd aan raad.

4. Overige beleidsaspecten voor de raad

In de landelijke vragenlijst voor raadsleden over digitale veiligheid krijgen diverse aspecten aandacht zoals: het normenkader, de interne organisatie en verantwoordelijkheden, bewustwording, risico's, het hanteren van de cyclus van informatieveiligheid en de melding van incidenten.
Deze vragenlijst is door de RKC gebruikt om informatie voor de raad te inventariseren. In de bijlage is deze vragenlijst opgenomen met de verkregen antwoorden, waarnaar wij verwijzen.

Onderstaand wordt ingegaan op meest relevante aspecten voor de raad.

A) Organisatie
De Security Officer en Security Manager hebben duo functies. Uitbreiding met een functionaris voor Privacy en een Functionaris Gegevensbescherming (verplichting volgens de AVG die per 25-5-2018 operationeel wordt), is in voorbereiding. De interne positionering van deze nieuwe functies en bijbehorende bevoegdheden moeten nog ingevuld worden. De Functionaris Gegevensbescherming dient eveneens een onafhankelijke positie te krijgen door rechtstreeks aan het college te rapporteren.

Bevinding 7

De formatie dient nog op niveau te worden gebracht en de onafhankelijke positie van de Functionaris gegevensbescherming is daarbij een belangrijk aandachtpunt.

B) Normenkader
De resolutie 'Digitale Veiligheid, randvoorwaarden voor de professionele gemeente' is overgenomen in het Beleidsdocument Informatiebeveiliging 2015 evenals het Normenkader zoals op VNG niveau is afgesproken. De audits wijzen uit dat onder andere de beheersmaatregelen voor DigiD afdoende zijn ingevoerd. De zelfaudits worden ook jaarlijks uitgevoerd volgens plan waarbij de resultaten worden gerapporteerd aan het Forum.
Ook is invulling gegeven aan het opstellen van procedures voor datalekken, ICT gerelateerde stroringen en beveiligingsincidenten. Verder wordt samengewerkt met IBD van de VNG voor preventie en het oplossen van incidenten.

Bevinding 8

Het beleid informatieveiligheid loopt in de pas met de landelijke aanpak en het landelijk afgesproken normenkader wordt gerespecteerd. Het beleid is door het college vastgesteld in 2015.

C) Aandacht voor Kwetsbaarheid

De gemeente heeft de datacentra verdeeld over twee locaties waardoor uitwijkmogelijkheid bestaat en databestanden gespiegeld kunnen worden bijgehouden. Ook zijn er technische voorzieningen aangebracht en is er een meldingssysteem tegen een verstoring actief.

Er is door de ICT-afdeling van de gemeente geen test gedaan op Business Continuity Management (cyberaanval).

In enig jaar waren 7 mogelijke datalekken gesignaleerd waarvan één lek is gemeld aan de Autoriteit Persoonsgegevens. Hierbij is de formele procedure gevolgd en is gehandeld conform de beleidsregels van de Autoriteit Persoonsgegevens.

Bevinding 9

De beheersregels en -procedures zijn conform landelijk normenkader opgezet en worden gevolgd. Er is geen onderzoek gedaan naar de feitelijke kwetsbaarheid van systemen middels een pentest.

D) Bewustwording

Een van de belangrijkste aspecten van digitale veiligheid is de wijze waarop mensen ermee omgaan. Hierbij gaat het om houding en gedrag maar ook over bewustzijn van de risico en de gevolgen. Alle deelnemers in het netwerk zijn relevant.

Kijkend vanuit het perspectief dat de visitatiecommissie schets, kan in Sittard-Geleen het volgende beeld worden opgemaakt:

- Raadsleden en burgerraadsleden worden niet meegenomen in acties (enquête) gericht op bewustwording.
- De Security Officer rapporteert langs de formele lijn aan een teammanager en niet rechtstreeks aan het bestuur.
- De Security Officer heeft geen eigen budget om gericht testen uit te voeren.
- Informatiebeveiliging is geen frequent/ periodiek agendapunt van de raad.
- Een gestructureerde cyclische rapportage aan de raad gebaseerd op de PDCA-cyclus Digitale Veiligheid ontbreekt.
- Digitale veiligheid wordt gezien als aangelegenheid van het college en de directie.
- De aandacht voor informatiebeveiliging is niet evenredig met de aandacht voor financiën.

- Er worden audits/ assessment onderzoeken uitgevoerd en geen periodieke pentesten.
- De ambtelijke reactie op de uitgevoerde pentest is gericht op bezwaren tegen de door de RKC gekozen aanpak, op de vervelende effecten van de geslaagde Phishing aanval en op het ontbreken van informatie of waarschuwingen vooraf. De schuldvraag staat centraal.
- Het aanbod van de RKC om leerervaringen rond de pentest te delen is afgeslagen door de directie.

De RKC heeft tijdens het onderzoek nog andere ervaringen opgedaan die vraagtekens oproepen inzake veiligheidsbewustzijn.

- In interne mails (o.a. mail van de secretaris over digitale veiligheid) worden mailadressen van alle medewerkers zichtbaar vermeld. Volgens de ICT-afdeling is dit in strijd met interne spelregels.
- Een A4 met gebruikersnaam en wachtwoord is aangetroffen in vergaderruimte waarmee ook hackers toegang tot netwerk wordt geboden.
- Het verkrijgen van een wachtwoord om in te loggen op het netwerk is telefonisch verstrekt zonder legitimatie. Het is een medewerker van de gemeente gelukt (na enig aandringen) in meerdere pogingen nieuwe wachtwoorden te ontvangen om in te loggen op het netwerk. Hier is verder geen onderzoek naar gedaan.

Bevinding 10

- Informatieveiligheidsvraagstukken krijgen geen structurele en periodieke aandacht van de raad.
- Een periodieke rapportage gebaseerd op een structurele en cyclische analyse van de informatieveiligheid aan de raad ontbreekt.
- Niet alle deelnemers in het netwerk worden actief betrokken bij acties rond verbetering van het veiligheidsbewustzijns.
- Cybersecurit geeft aan dat het bewustzijn rond Informatieveiligheid onvoldoende aanwezig is op verschillende niveaus in de gemeente en de veiligheidsrisico's worden onderschat.
- Het testen van systemen geschiedt middels audits waarbij de werking van de systemen en de werking van de beveiliging is uitgesloten. Periodieke penetratietests maken geen deel uit van onderzoek naar de informatieveiligheid.

3.6 Feitenrelaas Pentest Digitale Veiligheid

Om de veiligheid van informatie te testen is in overleg met de gemeente besloten een Black box penetratietest uit te laten voeren. Hiertoe is aan een extern bureau gevraagd om te zoeken naar kwetsbaarheden zoals ongeautoriseerde toegang tot de systemen en naar de bescherming van privacygevoelige informatie. Gekozen is voor een black box benadering hetgeen betekent dat het onderzoeksbureau geen enkele informatie vooraf krijgt over de gemeente en de gebruikte systemen maar ook dat de organisatie onwetend blijft van een dergelijk onderzoek. De RKC heeft er in dit geval voor gekozen het onderzoek vooraf wel aan te kondigen in het startgesprak met de gemeentesecretaris. In een nader overleg met de Security Officer en de Security Manager is dit vervolgens nader toegelicht en is afgesproken dat geen extra beschermingsmaatregelen door de ICT-afdeling genomen zouden worden om zo de werkelijkheid goed in beeld te krijgen.

Het onderzoek is breed en globaal van opzet en geeft geen zekerheid over de veiligheid indien er niets gevonden wordt. Het gaat om het blootleggen van zichtbare lekken.
De eerste oriëntatie legde een zevental kwetsbaarheden bloot die nader onderzoek vereisen.

	Kwetsbaarheid	Doel	Slagingskans	Impact
1	Phishing mail	Verkrijgen inlog gegevens	90%	Zeer groot
2	Mystery guest	Koppelen aan het netwerk en afluisteren privacygevoelige informatie	85%	Zeer groot
3	Memory dump uitlezen	Het geheugen uitlezen	40%	Groot
4	VPN portaal	Toegang tot netwerk door 2 kwetsbaarheden	30%	Gemiddeld
5	Brute Forcing	Wachtwoord verkrijgen met toegang tot portalen	15%	Zeer groot
6	HTML injectie	Verkrijgen informatie van bezoekers van website	45%	Gemiddeld
7	Wachtwoorden	Wachtwoorden gebruiken voor toegang tot diverse systemen	45%	Laag

Hierop is besloten om verder onderzoek te beperken tot de twee aspecten met de grootste kwetsbaarheid en de grootse impact. Dit betrof een Phishing e-mail campagne en een Mystery guest bezoek om toegang tot het netwerk (privacy gegevens) te krijgen. De overige gesignaleerde aspecten verdienen eveneens nader onderzoek maar zijn nu door de rekenkamer

niet meegenomen. In de vertrouwelijke technische rapportage is hierover gerapporteerd. Vervolgonderzoek op deze punten is aan de organisatie zelf.

1. Phishingtest

De mail is op 25 september 16.24 uur verzonden. Er is gebruik gemaakt van de 'luidruchtige'[10] methode om de pakkans voor de ICT-afdeling zo groot mogelijk te maken. Het exacte tijdstip dat de ICT-afdeling de mail heeft onderschept en heeft ingegrepen is niet gemeld aan de RKC en is ook niet achterhaald. De laatste inloggegevens zijn om 23.30 uur ontvangen.
De afdeling ICT heeft de Pishingtest ontdekt en het team van onderzoekers opgespoord en vervolgens maatregelen genomen. De RKC is op 26 september om ca 12.30 uur door het onderzoeksbureau op de hoogte gebracht van hun contact met de afdeling ICT en de onderschepping van de phishingtest door de gemeente Sittard-Geleen. De RKC heeft hierop besloten de Phishingtest direct te laten stoppen. Er is geen onderzoek gedaan naar de wijze waarop de ICT-afdeling heeft gereageerd en naar de effecten van de genomen maatregelen.

Resultaat phishingtest:

- De Phishingtest is succesvol uitgevoerd:
- In korte tijd (ca 30 minuten) is een substantieel aantal gebruikersnamen (13% van de steekproef) met bijbehorende wachtwoorden opgehaald.
- Gedurende zeven uur zijn gegevens van medewerkers opgehaald
- Via een ingebouwde code kon elk stap van de ontvanger zet worden gevolgd.
- De complexiteit van de wachtwoorden is zeer laag.

Van de mogelijkheid om via webmail.sittard-geleen.nl in te loggen op de accounts van de betreffende medewerkers of raadsleden is geen gebruik gemaakt conform de gemaakte (ethische) afspraken.

2. Mystery guest test

Onderzoek is gedaan naar de toegankelijkheid van de gebouwen en de mogelijkheid ongestoord binnen te dringen. De bedoeling was om te onderzoek of het mogelijk was apparatuur te koppelen aan het netwerk, om wachtwoorden en gebruikersnamen te testen ten einde het netwerk van buitenaf te benaderen.
Deze test is uitgevoerd in de periode 22 tot en met 26 september.

Aanval 1. Fysieke penetratie om een geprepareerde USB-stick met assistentie van een medewerker aan een pc te koppelen.
Aanval 2. Fysieke penetratie om geprepareerde apparatuur aan het netwerk te koppelen om verbinding te maken met internet.

[10] Bij een luidruchtige aanval worden alle mails in een keer en tegelijk verzonden naar alle mail-adressen. Bij een stille aanval waarbij de maisl een voor een verzonden wordt is de pakkans veel lager en het risico voor de organisatie veel groter (de hacker heeft dan veel meer tijd).

Aanval 3. Fysieke penetratie om apparatuur te koppelen aan het netwerk om een scan van het netwerk uit te voeren en toegang tot privacygevoelige informatie af te luisteren.

Resultaten Mystery guest test:

- De gebouwen van de gemeenten zijn goed toegankelijk gebleken en de hackers hebben ongestoord en onopgemerkt hun aanval kunnen doen.
- De test van de Mystery guest om apparatuur aan het netwerk te koppelen bleek eenvoudig uitvoerbaar.
- Bij de eerste aanval op 22 september is een USB-stick gekoppeld aan het netwerk op de pc van een medewerker. De test om verbinding vanuit het netwerk naar het internet op te zetten is mislukt.
- Bij de tweede aanval op 25 september is geprobeerd apparatuur te koppelen aan het netwerk en verbinding naar buiten te maken. Dit is niet gelukt.
- Bij het derde bezoek op 26 september is apparatuur aan het netwerk gekoppeld en is een scan van het interne netwerk uitgevoerd. Er is een IP-adres ontvangen. Er zijn alleen Thin-clients zijn aangetroffen en er is een RDP verbinding gemaakt. Er kon geen verbinding met de windows- server worden gemaakt en er kon geen verbinding met het internet worden gemaakt. Dit onderzoek heeft ca 30 minuten geduurd.
- De gegevens verkregen met de Phishingtest bleken onbruikbaar gemaakt nadat de phishingtest was gedetecteerd.
- Er zijn wijzigingen in het netwerk geconstateerd tijden de pentest. Niet bekend is of dit bewuste acties van de afdeling ICT zijn of dat dit toeval is.
- Tijdens de pentest was een eerder gebruikt toegangspunt afgesloten voor gebruik.

3. Het onderzoeksbureau concludeert dat:
    1. De gemeente ernstig tekort schiet op gedrag van medewerkers en de toegang tot het netwerk. Met een geldige gebruikersnaam en wachtwoord zullen beveiligingsmaatregelen geen effect hebben
    2. Met de opgedane ervaring het eenvoudig is voor het bureau of voor hackers een nieuwe aanval succesvol op te zetten.
    3. De grootste dreiging voor de gemeente Sittard-Geleen is een totaal gebrek aan security awareness en de daaruit voortvloeiende zwakheid voor social-engineering aanvallen is.
    4. Gelieerde websites van opvallend lage kwaliteit zijn met grote zwakheden.

4. Het bureau adviseert om:
    1. De huidige gesignaleerd kwetsbaarheden op te lossen met nadruk op de gevonden problemen binnen het e-mailverkeer
    2. Om diepgaandere testen uit te voeren om illegale toegang te voorkomen. De nu uitgevoerde testen zijn te beperkt qua zwaarte.

3. Vooraf vastgestelde delen van de infrastructuur regulier te testen want dit verkleint het risico van gehackt te worden en verhoogt het beveiligingsbewustzijn van de verantwoordelijken. Aangeraden wordt deze test periodiek te herhalen.
4. Het veiligheidsbewustzijn van alle gekoppelde personen verhogen via trainingen verdient prioriteit. Dit geldt zowel voor de toegang tot gebouwen, fraude herkenning als het verhogen van bewustzijn en gedag.
5. Websites van gelieerde partijen zijn kwetsbaar gebleken en vragen om actie. Deze zijn vatbaar voor Cyberaanvallen met als gevolg schade voor de gemeente. De website van de gemeente behoeft eveneens aanpassingen maar dit heeft lagere prioriteit.

Bevinding 11

De afdeling ICT is zich bewust van digitale veiligheid en het belang voor de zorg voor actualiteit van software en de inrichting van de netwerkwerk infrastructuur.

Bevinding 12

De netwerkinfrastructuur blijkt geeft van gedegen en doordachte aanpak inzake netwerkbeveiliging.

Bevinding 13

Het bleek mogelijk toegang te krijgen tot apparatuur of computers maar niet tot (privacy gevoelige) data in het netwerk.

Bevinding 14

De email server valideert niet of de binnenkomende mail daadwerkelijk afkomstig zijn van het juiste adres van de afzender. Dit is een kwetsbaarheid met een zeer hoog risico.

Bevinding 15

Er zijn 13 kwetsbaarheden geconstateerd waarvan zeven met de kwalificatie hoog[11] risico voor de gemeente. In hoofdlijnen kunnen genoemd worden:

- Het veiligheidsbewustzijn binnen de gemeente als geheel is als volstrekt onvoldoende gekwalificeerd.
- De toegang tot gebouwen en tot het netwerk is onvoldoende beveiligd.
- De websites van gelieerde partijen zijn van opvallend lage kwaliteit en zijn gevoelig voor brute force aanvallen, waardoor de gemeente erg kwetsbaar is.
- De gebruikte wachtwoordstructuur is te eenvoudig en daardoor erg kwetsbaar.

[11] Bij de kwalificatie is gekeken naar: de moeite om binnen te dringen, de schade die aangericht kan worden en mogelijk afbreukrisico.

3.7 Bijlage 1. Ontwikkelingen rond digitale veiligheid op hoofdlijnen.

De RKC wil enkel belangrijke ontwikkelingen beschrijven om een overzichtsbeeld te schetsen voor de raad. Het is niet de intentie om compleet te zijn en uitgewerkte details te beschrijven. Dit hoort thuis in een beleidsplan.

Normenkader

Er zijn algemene normen ontwikkeld voor digitale veiligheid die elke gemeente dient te hanteren. Dit betreft onder ander de internationale ISO-normen en de BIG[12].
In 2013 is door de VNG de 'Resolutie Informatieveiligheid randvoorwaarde voor de professionele gemeente' aangenomen. Deze resolutie kan gezien worden als vertrekpunt en basiskader voor het gemeentelijke informatiebeleid. Afgesproken is:

1. Informatieveiligheid wordt onderdeel van de collegeambities 2014-2018 en opgenomen wordt in de portefeuille van het college van B&W.
2. Gemeenten zorgen voor verankering van informatieveiligheid op de gemeentelijke agenda, waarbij het college de raad informeert in een aparte paragraaf in het jaarverslag.
3. Gemeenten gaan de BIG als basisnormenkader hanteren.
4. Gemeenten stellen Informatiebeveiligingsbeleid vast.
5. Informatieveiligheid borgen door aan te sluiten bij de planning en control cyclus.
6. Gemeenten maken informatieveiligheid transparant voor burgers.

De bedoeling van de resolutie is dat gemeenten hun beleid inzake informatiebeveiliging formuleren op basis van dit normenkader.

Juridische kaders

Daarnaast gelden juridische kaders die bepalen welke bescherming vereist is en welke maatregelen nodig zijn.
De Wet Bescherming Persoonsgegevens (Wbp) geeft aan dat alle bedrijven en overheden die persoonsgegevens gebruiker een plicht hebben om deze goed te beveiligen (artikel 13 Wbp). In de 'richtsnoeren beveiliging persoonsgegevens' geeft de Autoriteit Persoonsgegevens aangeduid dat beveiliging van systemen gedurende de tijd dat ze in gebruik zijn (tot en met de laatste update) aandacht moet hebben en dat dit in de periodieke PDCA cyclus informatiebeveiliging getoetst wordt. Bovendien is sinds 1 januari 2016 de meldplicht datalekken van kracht die de Autoriteit Persoonsgegevens de bevoegdheid geeft een boete op te leggen van maximaal € 810.000,= als blijkt dat wettelijke regels niet worden nageleefd.
De Wet basisregistratie persoonsgegevens regelt het gebruik, de bescherming en beveiliging van persoonsgegevens die zijn opgenomen in de basisregistratie personen. De maatregelen die de gemeente neemt ter beveiliging van de gegevens worden vastgelegd in een Beheerregeling Basisregistratie Personen. De Wet bescherming persoonsgegevens(Wbp) is de Nederlandse uitwerking van de Europese richtlijn bescherming persoonsgegevens[13]

[12] Baseline Informatiebeveiliging Gemeenten

[13] De Algemene Verordening Gegevensbescherming is in werking getreden op Europees niveau. De verordening zal in mei 2018 van kracht worden waarna de Wet bescherming persoonsgegeven (Wbp) dan niet meer geldt.

De Algemene Verordening inzake Gegevensbescherming (AVG) is een Europese verordening die gaat over bescherming van personen in verband met de verwerking van persoonsgegevens. Deze verordening is in mei 2016 in werking getreden en overheden hebben tot 25 mei 2018 de tijd om hun de bedrijfsvoering in overeenstemming met de AVG te brengen. De maximale boete die kan worden opgelegd is 20 miljoen euro.

Verder staan op de Agenda Digitale veiligheid 2020 de Wet Generieke Digitale Infrastructuur en het Programma Kwaliteit en Innovatieve Rechtspraak.

Controle en bewaking van informatieveiligheid
Een ander aspect binnen de kaderstelling is het afleggen van verwantwoording. Hierbij kan gedacht worden aan de wettelijke verplichting om periodiek audits uit te voeren. Elk jaar moeten gemeenten zich verantwoorden over de kwaliteit van de informatieveiligheid van diverse systemen. In juli 2017 is de nieuwe audit systematiek van kracht, om slim en in één keer verantwoording af te leggen. De bedoeling is dat verticale audits die tot juli jl. los van elkaar werden uitgevoerd onder dit nieuwe systeem gestructureerd en gecoördineerd kunnen gaan verlopen. Deze audits vervallen niet maar worden in onderling verband gebracht. Het gaat dan om de Eenduidige Normatiek Single Information Audit (ENSIA).
ENSIA regelt de coördinatie van de audits:

1. Basisregistratie personen (BRP)
2. Paspoortuitvoeringsregeling PUN)
3. Basisregistratie Adressen en Gebouwen
4. Basisregistratie Grootschalige Topografie(BGT)
5. Structuur Uitvoeringsorganisatie Werk en Inkomen (Suwinet)
6. Digitale Persoonsidentificatie (DigiD)

Om dit proces in goede banen te leiden en vorm te geven is in VNG verband afgesproken dat het noodzakelijk is een coördinator implementatie ENSIA aan te wijzen.

Ook is afgesproken dat periodiek (eens in de vijf jaar) een visitatie wordt uitgevoerd om te onderzoeken of de zelfregulering bij gemeente voldoende serieus wordt genomen. De visitatiecommissie heeft in september 2017 gerapporteerd.
Enkele belangrijke aanbevelingen zijn:

- Actieve betrokkenheid van het bestuur is van groot belang voor interne prioriteitstelling. Dit verdient in algemene zijn versterking en door ENSIA wordt dit nog meer noodzakelijk.
- Het op een hoger plan brengen van informatieveiligheid vraagt het goed positioneren van de Chief Information Security Officer (CISO) die in elk geval een onafhankelijke positie krijgt.
- De verantwoordelijkheid voor informatieveiligheid geldt over de hele linie van inhuurkracht tot raadslid en samenwerkingspartners. Informatieveiligheid vraagt structureel aandacht en invoering van een Information Security Management System (ISMS).
- Gemeenten moeten krachten bundelen. Samenwerking is de Crux.
- Wees transparant over incidenten en zet leerervaring centraal.
- Beschouw Informatieveiligheid als even belangrijk als financiën

- Voor bestuurders is het van belang te weten welke vragen moet ik stellen en welke deskundigheid is nodig.
- Voer periodiek een penetratietest (pentest) uit.

Integriteit, informatieveiligheid, privacy, en continuïteit van dienstverlening vragen sterke professionalisering op het gebied van informatieveiligheid. Hiervoor moeten de CISO en de controller een vergelijkbare – onafhankelijke – rol en positie in de organisatie hebben.

Instrumentarium
In VNG verband vindt afstemming plaats over de aanpak van digitale veiligheid en worden afspraken gemaakt over een gezamenlijke aanpak, het ontwikkelen van hulpmiddelen en instrumenten. Zo is er een Informatiebeveiligingsdienst voor Gemeenten de IBD[14] opgericht om bij calamiteiten op te treden en gemeenten daarbij te ondersteunen. Tevens is het de verbindende schakel met het Nationaal Cyber Security Centre NCSC).
Er is het kwaliteitsinstituut voor Nederlandse Gemeenten (KING) dat gemeenten ondersteunt bij hun informatiemanagement en de implementatie daarvan alsmede met de beveiliging van informatie.
In de Digitale Agenda 2020 zijn afspraken gemaakt om de toekomstige ontwikkelingen gezamenlijk aan te pakken. Genoemd kunnen worden:

- Het Platform samenleving
- Internet of Things
- De Gemeentelijke Gemeenschappelijke Infrastructuur (GGI)
- Blockchain

In de Roadmap is een overzicht te vinden van de belangrijkste toekomstige ontwikkelingen https://www.da2020.nl/roadmap

[14] DE IBD treedt op als CERT: Computer Emergency Respons Team

3.8 Bijlage 2 Vragenlijst Digitale Veiligheid Versie 4

Onderzoek richt zich op de periode sinds 2015. Relevante aspecten in voorafgaande periode rond het informeren van de raad inzake Digitale Veiligheid (DV) vermelden. Informatie ontvangen van Chief information Security Officer.

	Vraag	Reactie
1	Welke informatie is aan de raad verstrekt over informatiebeveiliging vanaf 2015?	In de jaarstukken (jaarplan 2016) wordt kort aandacht besteed aan informatieveiligheid. (2016: pag. 166). In de Boardletter behorende bij de jaarstukken doet de accountant zijn verslag van bevindingen over de IT omgeving en Cyber Security. Meer informatie aan de raad is /wordt niet verstrekt
2	Welke aandacht krijgt digitale veiligheid van raad?	Er zijn geen specifieke afspraken gemaakt met de raad over hoe DV aandacht krijgt. In de resolutie informatieveiligheid is aangegeven dat het college de gemeenteraad informeert over informatieveiligheid door middel van een aparte paragraaf informatieveiligheid in het jaarverslag. Begin 2015 is een thema sessie voor de raad gehouden over de resolutie informatieveiligheid en het plan van aanpak informatiebeveiliging van Sittard-Geleen. Op 5 november 2015 is de werkgroep Signaal (Sociaal domein) geïnformeerd over informatiebeveiliging.
3	Welke aandacht krijgt digitale veiligheid van college en ambtelijke organisatie?	Op 27-01-2015 heeft het college vastgesteld: • Beleidsdocument informatiebeveiliging • Plan van aanpak informatiebeveiliging

	Vraag	Reactie
4	Hoe is de raad in positie op de vaststelling en uitvoering van het informatiebeveiligingsbeleid?	Zie vraag 3. In het beleidsdocument informatiebeveiliging is het informatiebeveiligingsproces inclusief de rapportage aan de raad beschreven. De rapportage gaat naar de directie cq college. Dit wordt niet doorgeleid naar de raad omdat dit wordt gezien als een interne aangelegenheid. De wisseling van directie laat ruimte voor meer bredere verspreiding van informatie. NB. raadsleden zijn niet meegenomen in de enquête bewustwording terwijl ze wel participeren in het digitale systeem.
5	Welke aandacht wordt gegeven aan audits en rapportage hierover aan de raad?	Audits zijn jaarlijks terugkerend (voor verdere detaillering zie vraag 13). Er wordt gerapporteerd aan teammanager, forum Informatiebeveiliging en directeur; De hogere echelons rapporteren vervolgens aan de gemeentesecretaris en PHO. Over audits wordt niet aan raad gerapporteerd.

	Vraag	Reactie
6	Hoe heeft college de resolutie ‘Digitale Veiligheid, randvoorwaarden voor de professionele gemeente’ opgepakt?	Zie beleidsdocument informatieveiligheid De raad is begin 2015 tijdens een themasessie geïnformeerd over de resolutie informatieveiligheid en het plan van aanpak informatiebeveiliging Sittard-Geleen.
7	Wordt de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) als normenkader gehanteerd?	Ja dit is in het beleidsdocument informatiebeveiliging verankerd.

	Vraag	Reactie
8	Wie zijn er als verantwoordelijken aangesteld?	Theo Derhaag (Security officer) Paul Janssen (Security manager/Privacy manager) De formatie voor informatieveiligheid is uitgebreid. Voor Privacy moet nog een extra FTE Privacy-Officer komen. Per 25 mei 2018 geldt de Algemene verordening gegevensbescherming (AVG). Vanaf dit moment is de gemeente verplicht een functionaris voor de gegevensbescherming (FG) aan te stellen. De positionering in de organisatie moet nog ingevuld worden. In de King/ VNG notitie: "Rol en taken van de FG" staat aangegeven: "De FG dient in alle onafhankelijkheid zijn werkzaamheden te kunnen uitvoeren en ontvangt daarbij geen instructies vanuit de gemeente en verwerkers. Wel rapporteert de FG rechtstreeks aan het college van B&W over zijn werkzaamheden." De onafhankelijke positie van de FG (directe rapportage aan het college) is daarbij een belangrijke en essentieel aspect. De onafhankelijkheid kan ook vormkrijgen door een externe plaatsing. Overleg met Maastricht en Heerlen loopt op dit punt. Het Forum Informatiebeveiliging is een functioneel overleg waarin alle verantwoordelijken zijn vertegenwoordigd op tactisch niveau. Dit overleg functioneert onder verantwoordelijkheid van de algemeen directeur die deze bevoegdheid heeft gedelegeerd aan de adjunct-secretaris /directeur. Het Forum Informatiebeveiliging is in beginsel besluitvormend binnen de door B&W op strategisch niveau vastgestelde kaders. Besluitvorming vindt plaats op basis van consensus, met escalatie naar B&W. De besluitvorming wordt nadat het getoetst is aan de vastgestelde kaders vastgesteld door de B&W. Daar waar de kaderstelling nog ontbreekt wordt de voorgenomen richting voorgelegd aan B&W. Naast de besluitvormingsrol heeft het overleg een adviserende rol naar het strategisch niveau, en een controlerende rol naar operationeel niveau. Het Forum Privacy is op dezelfde wijze opgezet.

	Vraag	Reactie
9	Is er aandacht voor bewustwording?	Bewustwording informatieveiligheid is een nadrukkelijk aandachtspunt van het Forum informatiebeveiliging. Er is een plan van aanpak bewustwording informatieveiligheid en privacy opgesteld. Concrete acties uit het plan worden stap voor stap uitgevoerd.

	Vraag	Reactie
10	Welke risico's accepteert het college voor de eigen gemeente en welke niet?	In de in 2015 gedane Risicoanalyse (RA) welke is gebaseerd op de z.g. CRAMM methodiek is een risicoprofiel opgesteld voor de Gemeente Sittard-Geleen. De risico's op het gebied van beschikbaarheid, (elektronische) integriteit en vertrouwelijkheid van gegevens zijn benoemd. Bijzondere aandacht krijgen de risico's waarbij de kans dat deze zich voordoen hoog is en/of de impact groot is. Er zijn maatregelen gedefinieerd die genomen moeten worden om risico's te beperken. Het betreft maatregelen op het gebied van datacommunicatie, fysieke risico's, logische risico's, menselijk falen en technische storingen. De te nemen maatregelen zijn onderwerp van bespreking in het Forum Informatiebeveiliging en het Forum Privacy. In het Forum wordt dit jaar bezien of dit onderzoek herhaald wordt (volgens eerdere besluitvorming in 2017 of 2018) De risicoanalyse is uitgevoerd door een extern gespecialiseerd bedrijf. Het Cramm onderzoek bevat veel criteria waaruit de gemeente een selectie maakt van toepasselijke risico's voor de eigen gemeente. (Dit betreft ca. 6.800 maatregelen van de ca 20.000) Er wordt niet over de risico's gerapporteerd aan de raad. De rapportage van de gedane Risico analyse (RA) is niet geschikt voor brede verspreiding. Als deze informatie openbaar wordt neemt de kwetsbaarheid toe derhalve is er voor gekozen deze niet breed uit te zetten. Ter illustratie ook auditors krijgen alleen inzage in de inhoudsopgave van de RA

	Vraag	Reactie
11	Welke politiek-bestuurlijke en maatschappelijke gevolgen kan dit hebben in geval van een incident? Is de privacy van onze burgers gegarandeerd?	Incidenten kunnen nooit helemaal voorkomen worden en kunnen diverse gevolgen hebben waaronder bijvoorbeeld imagoschade. Er is een escalatiemechanisme geïmplementeerd: 'hoe te handelen in geval van incidenten en datalekken' Kopie wordt aangereikt (PJ) De gebruikte systemen hebben een signaleringsmodule ingebouwd die signaleert waarna IBD of softwareleverancier ingeschakeld wordt. De IBD signaleert ook vaak zelf welke acties nodig zijn om de veiligheid te borgen. Er zijn wel afspraken over verantwoordelijkheden van teammanagers vastgelegd. Deze moeten actie nemen en opschalen indien nodig. Er zijn ook virusscanners geïnstalleerd. Er is geen apart protocol of procedure bij een aanval of hack vastgelegd omdat dit soort incidenten beschouwd kan worden als een majeur ICT Incident waarvoor reeds opschalingsmechanismen zijn ingericht. Daarnaast is er de mogelijkheid om bij een aanval of hack de ondersteuning van de IBD in te schakelen.

	Vraag	Reactie
12	Functioneert de cyclus van informatieveiligheid binnen onze gemeente?	In het beleidsdocument informatiebeveiliging is het 'Proces Informatiebeveiliging' beschreven. Op hoofdlijnen wordt dit proces gevolgd. Maandelijks wordt op onderdelen gerapporteerd aan het forum informatiebeveiliging. De PDCA cyclus DV: dit geschiedt via rapportage (via directie) aan het college. Forum adviseert jaarlijks en incidenteel bij bijzonderheden. Ook gebeurt dit in de vorm van een presentatie aan de portefeuillehouder. E.e.a. is ontwikkelpunt bij de inrichting van het SSC met Heerlen en Maastricht

	Vraag	Reactie
13	Vindt er een jaarlijkse toetsing plaats om na te gaan of uw gemeente in control is op het gebied van informatieveiligheid? Wat zijn de resultaten van deze toetsing? Wordt de cyclus jaarlijks bijgesteld op basis van lessons learned?	Ja, er vinden diverse toetsen en interne audits plaats waaronder: • de Digid audit waarvoor tevens jaarlijks een Vulnerability Scan en een Penetratietest wordt uitgevoerd. • Daarnaast is er jaarlijks een zelfaudit BRP, PNIK en Suwinet waarover wordt gerapporteerd aan de bevoegde instanties en waarover steekproefsgewijs controles kunnen worden uit gevoerd. Zo is in 2016 door Panteia (onderzoeksbureau uit Zoetermeer) in opdracht van het ministerie de zelfevaluatie PNIK gecontroleerd. Doel van de controle was om na te gaan of de uitkomsten van de Zelfevaluatie PNIK een juiste afspiegeling vormen van de werkelijke situatie. Doel hierbij was de validatie van de uitkomsten van de zelfevaluatie. • Daarnaast vindt er een audit /evaluatie IB plaats door de accountant in het kader van de jaarrekening • Tenslotte komt het Forum Informatiebeveiliging maandelijks bijeen om de stand van zaken inzake IB te bespreken en indien nodig zaken bij te stellen of acties te ondernemen. Dit is een doorlopend proces.

	Vraag	Reactie
14	Zijn binnen de gemeente procedures opgesteld voor incidenten?	Binnen Topdesk, (meldingen systeem van de gemeente (voor datalekken en ICT gerelateerde storingen)) is een procedure ingericht voor het afhandelen van beveiligingsincidenten en het voorkomen van kwetsbaarheden. Voor het melden van datalekken en het afhandelen van IBD meldingen zijn eveneens procedures opgesteld.
15	Welke risico's loopt de gemeente in geval van verstoring of cyberaanval, ook wanneer deze verstoring elders in de keten plaatsvindt?	Zie vraag 11. Cyberaanval Er is een signaleringssysteem ingebouwd en er is een actie-protocol. Cyberaanval: er zijn geen tests gedaan Business continuity management is niet ingevoerd. In het kader van BRP PUN zijn er aanvullende voorzieningen en afspraken hoe te handelen bij een verstoring. : Doordat we de beschikking hebben over 2 locaties en 2 datacentra, een in Sittard en een in Geleen is uitwijk naar een andere locatie en het gespiegeld bijhouden van databestanden mogelijk Hierdoor zijn we in vergelijking met een aantal andere collega gemeenten minder kwetsbaar.

	Vraag	Reactie
16	Hoeveel incidenten zijn er geweest? Melden wij die incidenten bij de IBD?	Zie bijlage rapportage Incidentbeheer. Er waren in 2016: 7 mogelijke datalekken In het register worden 9 mogelijke datalekken vermeld. Er is in 2016 één mogelijk datalek gemeld aan de Autoriteit Persoonsgegevens Dit betreft een mogelijk datalek dat zich niet heeft vertaald in een werkelijk risico of lek. De melding is volgens de procedure gedaan en de betreffende personen die te maken konden krijgen met het datalek zijn op de hoogte gebracht. Hierbij is gehandeld conform de beleidsregels van de Autoriteit Persoonsgegevens. De rapportage is alleen aan de Directie gedaan. Er hebben zich geen incidenten voorgedaan waarvan melding aan de IBD noodzakelijk was.
17	Overige relevante informatie m.b.t. sturing en control door de raad inzake Digitale veiligheid?	Bewustwording informatieveiligheid en privacy is ook van belang voor raadsleden en burgerraadsleden. Dit aspect dient intern nadere aandacht te krijgen in beleid digitale veiligheid en bij de interne trainingen.

3.9 Bijlage 3 Lijst met begrippen

AVG	De Algemene Verordening Gegevensbescherming. Is in werking getreden op Europees niveau. De verordening zal in mei 2018 van kracht worden waarna de Wet bescherming persoonsgegeven (Wbp) dan niet meer geldt.
BIG	Baseline Informatiebeveiliging Gemeenten
Blackbox Pentest	Penetratietest waarbij de onderzoeker voor het testen geen informatie krijgt over het netwerk of de computer die getest wordt.
DigiD	Digitale code voor burgers. Gebruikersnaam en wachtwoord. Elektronische Herkenning om in te loggen bij overheden, verzekeringen, zorginstellingen, pensioenfondsen etc.
ENSIA	Eenduidige Normatiek Single Information Audit
Hacken	Illegaal inbreken op computers
Pentest	Penetratie test een binnendringingstest toetst ICT-systemen op kwetsbaarheden
Social engineering	Personen verleiden om informatie vrij te geven die in principe niet toegankelijk is voor derden.
Suwinet	Services om gegevens van burgers en bedrijven digitaal bij andere overheidsorganisaties op te vragen en naar elkaar door te sturen.
Vulnerability scan	Kwetsbaarheid scan
White box pentest	Penetratietest waarbij de onderzoeker voor het testen wel informatie krijgt over het netwerk of de computer die getest wordt.