Nulmeting informatieveiligheid gemeente Midden-Drenthe

Rapport rekenkamercommissie gemeente Midden-Drenthe

Groningen, 28 april 2017
Versie definitief

insitesecurity

Inhoudsopgave

1 Voorwoord

De rekenkamercommissie heeft een onderzoek gedaan naar de informatiebeveiliging van de gemeente Midden Drenthe. Dit is een onderzoek op de aspecten mens, organisatie en techniek.

De belangrijkste conclusies zijn dat op het thema mens er kwetsbaarheden gevonden zijn. Dit is overigens bij veel organisaties het geval en er zijn vele vormen van bewustwordingscampagnes die ingezet kunnen worden. Op het thema organisatie is de belangrijkste conclusie dat er veel in gang is gezet, maar dat verankering van beleid in werkprocessen e.d. nog geïntensiveerd moet worden. Op het gebied van de techniek zijn een aantal bevindingen gedaan met een hoog risico. Hierop komen we verder in dit voorwoord wat uitgebreider terug.

Het rapport geeft eerst in een management samenvatting een waardering van de bevindingen d.m.v. 'cockpit-meters' met daarna een korte toelichting per thema. Vervolgens wordt in hoofdstuk twee de opdracht, reikwijdte en de methodiek toegelicht. In hoofdstuk drie worden de drie thema's uitgebreid toegelicht, waarbij ook enkele aanbevelingen worden gedaan per thema.

Hieronder staan we expliciet stil bij het thema techniek, omdat dit voor de leek wellicht het lastigste te duiden is. Het is namelijk voor de gemiddelde leek al lastig om een rapport over informatiebeveiliging te lezen. Laat staan dat er een goed beeld ontstaat als er geschreven wordt over de bevindingen van een (technische) pen-test. Daarom hecht de rekenkamer er aan hier wat dieper op in te gaan, zodat er een juiste duiding is van de bevindingen die gedaan zijn op het thema techniek.

De cesuur bij een pen-test is scherp. Er wordt onderscheid gemaakt tussen bevindingen met een hoog -, gemiddeld – of laag risico (hoofdstuk 3.4 aspect techniek). Als er één bevinding gedaan wordt met een hoog risico dan wordt al het predicaat 'zeer onveilig' gebruikt. Dit is logisch vanuit het risico-perspectief, maar wil niet zeggen dat er 'niets deugt' van de technische inrichting van de geautomatiseerde omgeving van een gemeente.

Inmiddels zijn de (technische) bevindingen, die overigens niet in deze rapportage zijn opgenomen, allemaal met de afdeling ICT van de gemeente doorgenomen. De meeste bevindingen zijn inmiddels 'gerepareerd', terwijl andere in de nabije toekomst zijn gepland. Complicerend hierbij is dat sommige bevindingen betrekking hebben op systemen die extern zijn aangeschaft, zodat de beheersmaatregelen alleen in overleg met of door de leveranciers uitgevoerd kunnen worden.

De pen-test heeft voornamelijk betrekking op het interne – en draadloze netwerk. Daarnaast is een beperkte test gedaan op het externe netwerk. Bij dit laatste is gebleken dat er door een menselijke fout documenten met (gevoelige) persoonsgegevens (zoals BSN en naw-gegevens) op de internet-site van de gemeente gepubliceerd zijn. Inmiddels is ook deze bevinding voorzien van een adequate beheersmaatregel. De rekenkamer adviseert wel om n.a.v. deze bevinding een meer uitgebreide pen-test van buiten af te laten uitvoeren.

We willen afsluiten met de opmerking dat vanuit de gemeente goed is meegewerkt aan het onderzoek. Natuurlijk is er discussie geweest over de mogelijkheid en/of de impact van het eventuele voordoen van één van de gevonden risico's. De rekenkamer stelt zich hierbij op het standpunt dat de informatiebeveiliging ‘state of the art’ moet zijn en dat elk risico gemitigeerd moet worden. Dit dient onderdeel te zijn van een goed PDCA-cyclus. Een periodiek onderzoek (audit) zoals nu door de rekenkamer is geïnitieerd kan zeker helpen om het beeld scherp te houden.

Namens de rekenkamercommissie

Albert Vlaardingerbroek

p.s.

Zie bijlage IV voor een technische en bestuurlijke reactie van de burgemeester en wethouders van Midden-Drenthe d.d. 10 april 2017 op het concept onderzoekrapport d.d. 17 maart 2017 naar de informatiebeveiliging van de gemeente Midden-Drenthe, zoals verwoord per brief door de directiesecretaris, de heer A. Gunnink.

2 Managementsamenvatting

2.1 Inleiding

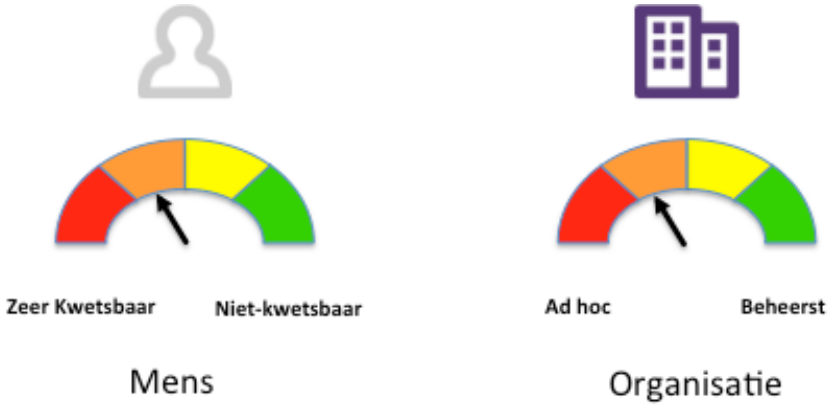
Door de toenemende afhankelijkheid van ICT, is de beveiliging van de gegevens in de systemen van de gemeente Midden-Drenthe ook steeds belangrijker geworden. Zo worden de gegevens van burgers niet meer met de hand geschreven op papieren documenten en in kasten gearchiveerd. Gegevens van burgers worden door de digitalisering nu digitaal bewaard. Bovendien werken gemeenten en burgers steeds meer samen omdat de digitalisering die nieuwe mogelijkheden ondersteund. Tussentijds kunnen burgers bijvoorbeeld de stand van een vergunning digitaal inzien of zelfs aanvullen op verzoek van de ambtenaar. De gemeente Midden-Drenthe heeft met haar zaaksysteem Midnet ook een vergaande digitale samenwerking met haar burgers, want zij hebben daarmee toegang tot hun zaakgegevens. Met de digitalisering heeft de gemeente ook een extra verantwoordelijkheid gekregen om zorgvuldig om te gaan met de gegevens van haar burgers. En dat betreft niet alleen de veiligheid (security) maar ook de privacy. Want de gegevens van burgers mogen niet rondslingeren en in verkeerde handen komen. Bovendien is wettelijk druk daaromtrent ook fors toegenomen. Denk aan de verplichte melding van datalekken aan de Autoriteit Persoonsgegevens en ook aan de recente verhoging van de boetecategorie die de Autoriteit Persoonsgegevens kan opleggen (820.00 euro). Daarnaast wordt met de inwerkingtreding van de Europese Algemene Verordening Gegevensbescherming in mei 2018 de druk op de gemeenten nog groter. Van de gemeenten zal nog meer worden verwacht om de security en privacy van haar burgers aantoonbaar te borgen.

Door de decentralisatie van het sociale domein naar de gemeenten zijn er ook allerlei informatiesystemen toegevoegd. Het betreft veelal complexe systemen die veel persoonsgegevens bevatten en bovendien worden gebruikt door vele betrokkenen.
Tegelijkertijd verandert de wereld om ons heen snel. Ontwikkelingen zoals ‘cloud’ maar ook nieuwe dreigingen zoals ‘phishing’ vragen om een meer proactieve benadering van informatiebeveiliging. En tot slot willen de burgers ook steeds zekerheid over het niveau van informatiebeveiliging van de gemeente Midden-Drenthe en kunnen zij vragen naar de door de gemeente Midden-Drenthe getroffen beveiligingsmaatregelen.

De rekenkamercommissie van de gemeente Midden-Drenthe wil daarom graag weten wat het huidige niveau van informatiebeveiliging is en welke maatregelen gezien de huidige risico’s minimaal noodzakelijk zijn om de risico’s te beperken.

2.2 Resultaten nulmeting informatiebeveiliging

Insite Security heeft een nulmeting informatiebeveiliging uitgevoerd in opdracht van de rekenkamercommissie gemeente Midden-Drenthe. De nulmeting betreft de perspectieven Mens, Organisatie en Techniek. Te samen geven deze perspectieven een beeld van het volwassenheidsniveau omtrent informatiebeveiliging zoals onderstaand is gevisualiseerd voor de perspectieven Mens en Organisatie. De uit de technische nulmeting afkomstige hiaten zijn gelijk opgepakt en verbeterd waarna het continue proces van verbetering in gang is gezet.



Aspect Mens

De resultaten van de nulmeting op het aspect **mens** laten zien dat de zij kwetsbaar zijn voor mensgerichte aanvallen. Binnen een tijdsbestek van een paar uur geeft !0% van de gebruikers van de gemeentelijke systemen haar gebruikersnaam en wachtwoord af naar aanleiding van een phishingmail. Het gemeentehuis is door een ‘mystery visitor’ relatief makkelijk binnen te dringen door mee te lopen met iemand. Vervolgens kan er ongestoord gezocht worden naar vertrouwelijke informatie op bureaus en in kasten. Van de 25 verspreide USB-sticks zijn er 10 USB-sticks (40%) geactiveerd door op de link te klikken.

Aspect Organisatie

Uit de **organisatorische** nulmeting komt naar voren dat de gemeente Midden-Drenthe zich bewust is van het aspect informatiebeveiliging en het toenemende belang voor haar organisatie onderkent. Zij heeft informatiebeveiliging echter nog niet structureel verankerd in haar werkwijzen en ook nog niet vertaald in zichtbare organisatorische functies c.q. rollen. De gemeente Midden-Drenthe heeft wel een veelbelovende aanzet gegeven hiervoor gezien de opzet van het ‘Handboek kwaliteit informatievoorziening’. Dit handboek bevat vele onderdelen van een informatiebeveiligingsplan, zoals voorgeschreven vanuit normenkaders als de ISO27001/2. Het is echter zaak dat de gemeente Midden-Drenthe deze aan ‘gewillig papier’ toevertrouwde organisatorische- en procesinrichting ook daadwerkelijk gaat effectueren. Daardoor kan zij een stap zetten om de informatiebeveiliging onder controle te krijgen. Want de gemeente Midden-Drenthe zal vooral een stap moeten zetten in het opzetten van rapportages (audit controls e.d.) om op basis van (bijna)incidenten de vereiste management verbetercyclus in gang te zetten.

De functies die minimaal benoemd dienen te worden zijn een functionaris gegevensbescherming (ook wel Data Protection Officer) en een (chief) security officer.

Aspect Techniek

Meerdere kwetsbaarheden zijn aangetroffen met een kritisch en hoog risico. Binnen de gegeven tijd is Insite Security erin geslaagd om de beveiliging van het interne en externe netwerk te doorbreken. De inzet van Insite Security was met name gericht op het testen van de beveiliging van het interne netwerk.

Om de technische nulmeting efficiënt uit te voeren is als onderzoeksopzet besloten om Insite Security rechtstreeks toegang te verlenen tot het netwerk (middels een lijst van IP-adres ranges) en ook de beschikking

te geven over een werkplek met toegang tot het interne netwerk van de gemeente Midden-Drenthe. Deze bewuste keuze is ingegeven vanuit de gedachte dat binnendringen in het interne netwerk van de gemeente Midden-Drenthe louter een kwestie van tijd is omdat hackers met voldoende tijd op afstand het interne netwerk op verschillende manieren kunnen bereiken (bijvoorbeeld malware, reverse tunnels, raspberry pi plaatsen etc.). Er wordt er derhalve van uitgegaan dat de mogelijkheid tot verkrijgen tot toegang tot het gemeentelijke netwerk een gegeven feit is en niet aangetoond hoeft te worden.

De beveiliging van het externe netwerk is beperkt getest tijdens het onderzoek.
Wat mogelijk is bij het misbruiken van deze kwetsbaarheden wordt geïllustreerd aan de hand van de volgende situaties.

- Het is mogelijk om de volledige controle over het interne netwerk van de gemeente Midden-Drenthe te bemachtigen. Hierdoor kan een kwaadwillende zo goed als alle informatie op het interne netwerk en andere aangesloten locaties lezen, aanpassen en/of verwijderen.
- Omdat medewerkers document op een verkeerde plek hadden geplaats is mogelijk gedeelde mappen van verschillende afdelingen binnen de gemeente Midden-Drenthe te bereiken. Daardoor kunnen vertrouwelijke documenten met onder andere wachtwoorden, financiële informatie, gebruikersinformatie van personeel en gegevens van Burgerzaken worden ingezien.
- Het is mogelijk om vanaf internet documenten, over aanvragen van inwoners, op te vragen. Deze documenten bevatten onder meer gevoelige persoonsgegevens.

De geconstateerde punten zijn alle opgepakt en vastgelegd in een door de afdeling ICT opgezet actieplan. Na de afronding van het actieplan start de ICT een volgende cyclus van testen en verbeteren, de ‘plan-do-check-act ‘-cyclus.

Verbetermogelijkheden

Op basis van de nulmeting op de aspecten Mens, Organisatie en Techniek en op basis van haar kennis van en ervaring met informatiebeveiliging bij andere organisaties geeft de rekenkamercommissie in samenspraak met Insite Security onderstaand een opsomming van de verbetermogelijkheden en een mogelijke prioritering. De mogelijke verbeterdoelstellingen op basis van de nulmeting voor de gemeente Midden-Drenthe zijn, in volgorde van prioriteit:

Jaar 2017

- Concretiseren en vaststellen van Informatiebeveiligingsbeleid conform het handboek Informatievoorziening;
- Inrichten van de organisatie van informatiebeveiliging, inclusief verbetercyclus[1];
- Benoemen van een Functionaris gegevensbescherming en een (Chief) Information Security Officer;
- Starten en onderhouden van een bewustwordingsprogramma voor de komende drie jaren (zoals e-learning phishing, communicatie, workshops etc.);
- Accorderen van het wachtwoordenbeleid en verbeteren van de rapportages omtrent autorisaties e.d.;
- Voorbereiding op de AVG voorwaarden zoals de Privacy Impact Assessment en Persoonsgegevensregister.

Jaar 2018

- Invoeren en uitvoeren van risicoanalyses vanuit het informatiebeveiligingsperspectief (zoals BIA);
- Benoemen van alle (kritieke) systemen en bijbehorende systeemeigenaren en leg deze vast[2];
- Wijzigingenbeheer voor alle systemen en applicaties uitvoeren;
- Verbeteren van het leveranciersmanagement waaronder bewerkersovereenkomsten;
- Aanscherpen van het beleid ten aanzien van document bewaartermijnen, zoals curriculum vitae;

In dit rapport worden verbeteradviezen gegeven op basis van het onderzoek in opdracht van de rekenkamercommissie.

[1] De ‘plan-do-check-act’ cyclus zoals voorgeschreven door de normeringen

[2] in de Configuratie Management DataBase van ICT,

3 Inleiding

3.1 Opdrachtomschrijving en reikwijdte

De rekenkamercommissie doet onderzoek naar de uitvoering van het gemeentelijk beleid. Hierbij wordt gekeken of de uitvoering efficiënt en volgens de regels heeft plaatsgevonden en of het doel bereikt is. In het kader van haar rol wil de rekenkamercommissie de informatiebeveiliging toetsen op de onderdelen mens, organisatie en techniek.

De rekenkamercommissie van de gemeente Midden-Drenthe heeft Insite Security gevraagd een nulmeting informatiebeveiliging uit te voeren op de aspecten organisatie, mens en techniek.

Het doel van de nulmeting is om het niveau van de IT beveiliging binnen de gemeente Midden-Drenthe in kaart te brengen, de belangrijkste risico's te benoemen en een advies te geven over welke beveiligingsmaatregelen mogelijk kunnen worden getroffen of verbeterd. De nulmeting richt zich op de factor mens, de organisatorische aspecten en op de technische aspecten omtrent de informatiebeveiliging binnen de gemeente Midden-Drenthe en geeft antwoord op de vraag: "Hoe veilig zijn we?" afgezet tegen de bekende kwetsbaarheden die door Insite Security worden geïdentificeerd.

De opdracht 'Nulmeting Informatiebeveiliging' betrof de gehele gemeente Midden-Drenthe. De ondersteuning van Insite Security bestond uit het in kaart brengen van de huidige situatie (nulmeting) voor de aspecten Mens, Organisatie en Techniek.

In dit rapport worden de resultaten van de nulmeting weergegeven en de adviezen die daaruit voortvloeien.

De nulmeting is uitgevoerd in de periode oktober 2016 – november 2016.

3.2 Aanpak

Het doel van de nulmeting was het bepalen in hoeverre de gemeente Midden-Drenthe voldoet aan de geselecteerde (generieke) maatregelen op de aspecten Organisatie, Mens en Techniek. De nulmeting is uitgevoerd aan de hand van een technische scan, het bestuderen van bestaande documentatie, eigen waarneming (bijv. het controleren van bepaalde systeeminstellingen), het houden van een aantal interviews aan de hand van gestructureerde vragenlijsten en een aantal praktijktesten (mystery visit, phishingmail en rondslingerende usb-sticks). Bijkomend effect van de interviews is dat de geïnterviewde medewerkers inzicht in en kennis van informatiebeveiliging is aangereikt, waarmee tevens de eerste bewustwording omtrent informatiebeveiliging in gang is gezet.

Op basis van de nulmeting wordt een globaal advies gegeven omtrent de te treffen of te verbeteren beveiligingsmaatregelen.

3.3 Leeswijzer

Dit rapport is als volgt ingedeeld. Hoofdstuk 1 bevat de management samenvatting. In hoofdstuk 3 worden de uitkomsten van de nulmeting gepresenteerd. De bijlagen bevatten de gedetailleerde bevindingen van de nulmeting en de door ons geraadpleegde bronnen en referenties.

4 Uitkomsten nulmeting

4.1 Inleiding

Dit hoofdstuk beschrijft de bevindingen en aanbevelingen van deze nulmeting en bevat het mensgerichte onderdeel (praktijktesten van gedrag) en het organisatorische onderdeel (analyse interne beheersing). De bevindingen en aanbevelingen van het technische onderdeel van deze nulmeting (penetratietest en kwetsbaarhedenscan) zijn opgenomen in een aparte rapportage die aan de rekenkamercommissie ter beschikking is gesteld.

4.2 Aspect Mens

Aanpak

Het aspect mens is getoetst aan de hand van enkele praktijktesten, die zijn beoordeeld en op niveau zijn ingedeeld aan de hand van de onderstaande classificering.

Niveau 1 **Zeer kwetsbaar**

Bovengemiddeld veel (gevoelige) informatie aangetroffen/verkregen/afgegeven in de praktijktesten van gedrag.

Niveau 2 **Kwetsbaar**

Gemiddelde hoeveelheid (gevoelige) informatie aangetroffen/verkregen/afgegeven in de praktijktesten van gedrag.

Niveau 3 **Minder kwetsbaar**

Minder dan gemiddelde hoeveelheid (gevoelige) informatie aangetroffen/verkregen/afgegeven in de praktijktesten van gedrag.

Niveau 4 **Niet kwetsbaar**

Weinig tot geen (gevoelige) informatie aangetroffen/verkregen/afgegeven in de praktijktesten van gedrag.

Resultaten

De praktijktesten phishing test, mystery guest bezoek en de usb-sticks actie zijn in oktober 2016 uitgevoerd. Onderstaand worden de resultaten beschreven. De menselijke factor in informatiebeveiliging is een risico voor de informatiebeveiliging van de gemeente Midden-Drenthe. De medewerkers en raadsleden zijn kwetsbaar voor dergelijke aanvallen.

Phishing e-mail

Bevindingen:

- Er zijn 365 e-mails (maillijst van de gemeente Midden-Drenthe) verstuurd.
- 10% van de gebruikers (37 unieke gebruikers) heeft data (gebruikersnaam en wachtwoord) gepost. In totaal is de mail 141x bekeken en is er 86x op de phishing-link geklikt;
- Het percentage is waarschijnlijk geflatteerd omdat de (aanstaande) security officer niet op de hoogte was van de test en op eigen initiatief de gebruikers heeft gewaarschuwd waardoor de praktijktest niet volledig kon worden uitgevoerd.
- Diverse gebruikers vullen hun wachtwoord meerdere keren in. Een tweetal hebben het zelfs 4 keer gedaan.
- Er zijn 15 meldingen gerelateerd aan de phishing e-mail geweest bij de servicedesk. De servicedesk was op de hoogte van de test en heeft niet ingegrepen

Rondslingerende USB-sticks

Insite Security heeft eind oktober 25 ‘geprepareerde’ USB-sticks op de locatie van de gemeente Midden-Drenthe achtergelaten. Het gebruiken van USB- sticks waarvan de afkomst niet bekend is, is een risico omdat zo eenvoudig gevaarlijke ‘malware’ op het systeem kan worden geïnstalleerd.

Bevindingen:

- Er zijn 25 sticks verspreid over de afdelingen van de kantoorlocatie (stadhuis);
- Van 10 USB sticks (40%) is op de link geklikt van het bestand: ‘Reorganisatie 2017’;
- Er zijn 9 USB-sticks ingeleverd bij de IT helpdesk.

Mystery guest

Een medewerker van Insite Security heeft in oktober het stadhuis van de gemeente Midden-Drenthe geobserveerd en is er onder kantooruren gezocht naar vertrouwelijke informatie. Hierbij is geprobeerd zonder afspraak of identificering het pand binnen te dringen. Eenmaal binnen is geprobeerd vertrouwelijke informatie te verzamelen door onder andere te zoeken naar fysieke documenten bij printers, werkplekken en archieven.

Bevindingen:

- De mystery guest kon eenvoudig het pand binnengaan door mee te lopen met iemand (het zogeheten 'tailgating') via de personeelsingang aan de achterzijde;
- De medewerkers van de gemeente Midden-Drenthe vertrouwen over het algemeen op de goede bedoelingen van bezoekers. Onze medewerker is eenmaal aangesproken maar deze medewerker kon gemakkelijk worden afgewimpeld;
- Er zijn diverse documenten met vertrouwelijke informatie op bureaus en in kasten aangetroffen;
- Er zijn meerdere onbeheerde niet gelockte schermen aangetroffen, maar deze schermen waren minder goed toegankelijk omdat er collega's in de buurt aanwezig waren;
- Het cleandesk principe wordt na werktijd goed toegepast. Wel zijn er veel werkkasten met vertrouwelijke documenten niet afgesloten;
- Op de kamers van gemeentesecretaris en burgemeester zijn (afgesloten) containers geplaatst voor het afvoeren van vertrouwelijk materiaal;
- Vertrouwelijk materiaal kan worden aangeboden in speciaal hiervoor bestemde afgesloten grijze bakken. Deze bakken waren afgesloten.
- Bij de printers zijn geen vertrouwelijke documenten aangetroffen. Men maakt gebruik van een vorm van secure printen;

Conclusies en aanbevelingen nulmeting mens

De menselijke factor in informatiebeveiliging is een risico voor de informatiebeveiliging van de gemeente Midden-Drenthe. Er zijn zowel 'online' als 'offline' pogingen gedaan om waardevolle informatie buit te maken. De medewerkers en raadsleden zijn kwetsbaar voor dergelijke aanvallen.

Verhoog het kennisniveau en het risicobesef van de medewerkers en raadsleden door het verzorgen van een bewustwordingsprogramma de komende jaren. In het programma worden onderdelen opgenomen als e-learning, workshops en communicatie uitingen.

Verhoog het kennisniveau van de medewerkers door het aanbieden van bijvoorbeeld e-learning gericht op het onderscheiden van phishing mail van legitieme mail.

4.3 Aspect Organisatie

Aanpak

De organisatorische nulmeting is uitgevoerd aan de hand van gestructureerde vragenlijsten, het bestuderen van bestaande documentatie en het houden van een aantal interviews, zie de bijlage voor lijst geïnterviewden.

De elementen uit de ISO27002 zijn gescoord conform de Cobit versie 4.1. normering (zie de bijlage), met dien verstande dat de status 0 (niet existent) en de status 5 (geoptimaliseerd) buiten beschouwing zijn gelaten omdat deze niet relevant zijn in de onderzoeksopzet. De onderstaande normering is gehanteerd.

Niveau 1 **Ad Hoc**, initieel

Dit normelement krijgt geen/weinig aandacht of er zijn uitsluitend plannen om met dit normelement aan de slag te gaan.

Niveau 2 **Beperkt**

Dit normelement is beperkt gedefinieerd en geïmplementeerd in de organisatie. De controle op doeltreffendheid heeft nog niet plaatsgevonden.

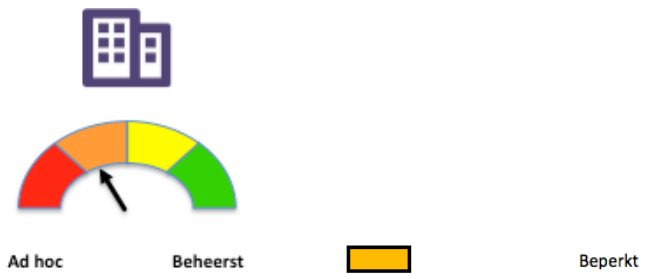
Niveau 3 **Gedefinieerd** en gecontroleerd

Dit normelement is geïmplementeerd op alle, voor informatiebeveiliging, meest kritieke plaatsen en de doeltreffendheid is ten minste één keer door de organisatie gecontroleerd.

Niveau 4 **Beheerst** en Meetbaar

Dit normelement is breed geïmplementeerd en de doeltreffendheid wordt structureel en periodiek door de organisatie gecontroleerd.

Resultaten



De resultaten van nulmeting laten zien dat de gemeente Midden-Drenthe al een groot aantal organisatorische en ook (deels) technische beheersmaatregelen heeft getroffen maar nog niet (periodiek) gecontroleerd worden.

Sterke punten zijn:

- De gemeente Midden-Drenthe werkt aan een *Handboek Kwaliteit informatievoorziening*, een zeer complete beschrijving van alle functies, taken, verantwoordelijkheden, procedures et cetera die relevant zijn om de informatiebeveiliging op orde te krijgen en te houden. Het handboek is enerzijds geïnspireerd op het normenkader van de ISO27001 en anders op de BIG, de Baseline Informatiebeveiliging Gemeenten zoals voorgeschreven door de VNG.
- Het sociaal domein wordt door de interne control periodiek geaudit. Daarmee ontvouwt zich een beeld en is een tijdige signalering van afwijkingen geborgd zodat naar verwachting tijdig bijgestuurd kan worden.
- Een groot aantal beheersmaatregelen zijn reeds geïmplementeerd, zoals werkwijzen omtrent de continuïteit, logging en monitoring, fysieke beveiliging, bescherming tegen malware, netwerkbeveiliging, beveiligd telewerken, etc.
- De gemeente Midden-Drenthe beschikt over een werkende procedure voor het melden van datalekken, zij heeft inmiddels in het jaar 2016 een tiental meldingen gedaan naar de Autoriteit Persoonsgegevens.
- Door de gemeente Midden-Drenthe wordt het credo gehanteerd '*liever kloppelen dan koppelen*'. Hiermee wordt aangegeven dat zij in de eerste instantie de voorkeur geeft aan het handmatig aan elkaar verbinden van applicaties/systemen en pas nadat de noodzaak is aangetoond het '*kloppelen'* wordt omgezet in een geautomatiseerde '*koppeling'*. Deze werkwijze borgt een controle over de koppelingen.
- De gemeente Midden-Drenthe heeft reeds aan een groot deel van de medewerkers privacy trainingen gegeven en geeft daarmee al invulling aan het aspect awareness.
- Het zaaksysteem Midnet (Mozard) is consequent en breed ingezet. Het inzien en bijdragen door derden van aan zaken is qua beveiliging mogelijk gemaakt door middel van een gebruikersnaam en separaat verstrekte pincode. Doordat slechts een koppeling wordt gemaakt met een zaak kan bij een mogelijke beveiligingsincident de koppeling voor de zekerheid ingetrokken worden. Tevens zijn de mails vanuit Midnet reeds technisch beveiligd.
- De gemeente Midden-Drenthe heeft haar autorisaties gekoppeld aan het functieboek van P&O en daarmee is het rechtenprofiel gelijk correct gezet voor de medewerkers.
- De gemeente Midden-Drenthe heeft het 'Mobile Device Management' goed en werkend geïmplementeerd. Daardoor lopen de mobiele apparaten, zoals de iPads en telefoons, geen technisch risico. Voorwaarde is uiteraard dat medewerkers tijdig een melding afgeven van verlies e.d.
- De gemeente Midden-Drenthe-omgeving hanteert een recentelijk opgesteld wachtwoordenbeleid (dat echter nog nader geïmplementeerd, afgedwongen en over gerapporteerd dient te worden).
- Alleen managers zijn verantwoordelijk voor het toekennen, wijzigen en intrekken van autorisaties.

Tegelijkertijd zijn veel zaken niet 'verankerd' in (vastgesteld) beleid, niet goed gedocumenteerd en/of slechts bij één of enkele medewerkers bekend. De gemeente Midden-Drenthe is een organisatie van die van nature op grond van de Drentse tradities van vertrouwen werkt. Het is organisatie die haar beleid en procedures niet zonder 'nut of noodzaak' zal documenteren. Bovendien heeft zij gezien haar beperkte omvang daar ook niet de beschikbare menskracht voor om het uit te voeren.

In onderstaande paragrafen worden adviezen gegeven. Voor deze adviezen is het van belang dat een afweging plaatsvindt tussen de informatiebeveiligingsrisico's die de gemeente Midden-Drenthe loopt en de inspanning in tijd en geld die moet worden geleverd om het advies op te volgen.

Informatiebeveiligingsbeleid en –organisatie

Beperkt

De gemeente Midden-Drenthe heeft haar informatiebeveiligingsbeleid weliswaar reeds beschreven in het handboek kwaliteit (zie document referentie 1), maar dat is nog niet volledig en het is nog niet formeel vastgesteld en niet geïmplementeerd. Een aanzet is gegeven voor de verschillende rollen binnen informatiebeveiliging, zoals de (chief) Information Security Officer en de privacy officer[3)].

Tevens is de opzet van een Information Security Management System (ISMS) verwoord. Dit beleid, het aanwijzen van verantwoordelijken en het ISMS moeten borgen dat informatiebeveiliging binnen de gemeente Midden-Drenthe continu wordt gemonitord en verbeterd.

Belangrijk onderdeel van een ISMS is dat de organisatie beheersmaatregelen dient te implementeren op basis van een (vastgelegde) risicoafweging. De nulmeting geeft inzage in de mate van implementatie van alle ISO27001-maatregelen, maar geeft niet voldoende inzicht in de impact van het ontbreken van beheersmaatregelen. Bijvoorbeeld: Er is niet in een risicoanalyse vastgesteld of beschikbaarheid een issue is voor de gemeente Midden-Drenthe, dus het belang van continuïteitsmaatregelen kan niet worden vastgesteld.

Voor de diverse onderdelen van de ISO 27002-norm, zoals bijvoorbeeld wachtwoordbeleid, personeel (gedragscode), beveiliging van mobiele apparaten en informatie-uitwisseling worden wel beheersmaatregelen geïmplementeerd en is een eerste beleid geformuleerd. De volgende stap, de doorvertaling en implementatie dient hierop te volgen. Voor andere ISO27002-onderdelen, zoals autorisatiebeheer en bezoekersregistratie, is de implementatie afhankelijk van de medewerkers die daarmee in aanraking komen. Gevolg is dat de gemeente Midden-Drenthe als organisatie niet kan borgen dat beheersmaatregelen op een juiste manier zijn geïmplementeerd. Adviezen over het opstellen van beleid op deze punten komen in de volgende paragrafen aan de orde.

Advies:

- *Rond het informatiebeveiligingsbeleid af.*
- *Richt een informatiebeveiligingsorganisatie in.*
- *Implementeer een beoordelingscyclus (ISMS) en een continue verbetercyclus.*
- *Voer voor de belangrijkste processen een risicoanalyse uit.*

Systeemeigenaren van de applicaties

Beperkt

Onderdeel van de organisatie van informatiebeveiliging is het benoemen van systeemeigenaren voor alle applicaties. Ieder systeem zou een systeemeigenaar moeten hebben. Deze systeemeigenaar is verantwoordelijk voor de beveiliging van informatie in het systeem. De gemeente Midden-Drenthe heeft deels de systeemeigenaren benoemd.

Advies:

- *Benoem voor alle (kritieke) systemen een systeemeigenaar en geef duidelijk de verantwoordelijkheden aan.*
- *Richt een CMDB[4] in als onderdeel van het incident registratie systeem en leg daarin het eigenaarschap vast.*

[3] Functionaris gegevens bescherming Wbp en Data Protection Officer conform de VG, zie http://eur-lex.europa.eu/legal-content/NL/TXT

[4] Configuratie Management DataBase, hierin worden alle hard- en software elementen vastgelegd.

Beveiliging ICT-voorzieningen

Gedefinieerd

De maatregelen voor de technische ICT-voorzieningen zijn op orde. De technische ICT-voorzieningen worden goed beheerd door de eigen technische medewerkers en de voorzieningen worden bewaakt middels een monitoring systeem. De mobiele apparatuur is goed beveiligd middels Mobile Device Management. De toegang voor externe softwareleveranciers tot het netwerk van de gemeente Midden-Drenthe is gecontroleerd. De (management)rapportages zijn niet structureel waardoor er geen structurele verbetering kunnen worden gedefinieerd en doorgevoerd.

Opmerking: In de technische nulmeting is vastgesteld of er nog kwetsbaarheden aanwezig zijn in de technische ICT-voorzieningen. Zie hiervoor paragraaf 3.4.

Advies:

- *Benoem voor alle (kritieke) systemen een systeemeigenaar en geef duidelijk de verantwoordelijkheden aan.*
- *Richt een CMDB[5] in als onderdeel van het incident registratie systeem en leg daarin het eigenaarschap vast.*
- *Bespreek periodiek de (management)rapportages en stel maatregelen vast om bij te sturen.*

Fysieke beveiliging

Beperkt

De fysieke beveiliging van de ICT/MER is op orde, toegang is alleen mogelijk voor geautoriseerde medewerkers en anderen onder begeleiding.

De fysieke beveiliging van het gebouw van de gemeente Midden-Drenthe is beperkt. Bezoekers moeten zich weliswaar melden bij de receptie, maar er vindt geen registratie plaats. Er worden binnen de gemeente Midden-Drenthe gegevens vastgelegd waarvan de integriteit en de vertrouwelijkheid van belang zijn. Het ontbreken van een fysieke beveiligingsschil is wel belangrijk. In het handboek is een aanzet gegeven voor het beleid.

Advies:

- *Scherp het beleid voor fysieke toegangsbeveiliging enigszins aan en voer dat uit.*

Logische toegangsbeveiliging (Authenticatie en autorisatie)

Beperkt

Logische toegangsbeveiliging betreft niet alleen de toegang tot applicaties, maar ook tot mappen en bestanden op het filesysteem (home-dir en afdelingsmappen) en in de diverse mailboxen.

Er is een aanzet gegeven voor het wachtwoordbeleid voor de gemeente Midden-Drenthe omgeving en er wordt gedacht aan het gebruik van certificaten als authenticatie voor zowel SaaS- als interne applicaties. Toegang tot het gemeente Midden-Drenthe-account wordt momenteel verleend op basis van een gebruikers-ID en (sterk) wachtwoord. Een aantal applicaties is ook te benaderen van buiten het gemeente Midden-Drenthe-account, waarvan sommige zijn beveiligd met een extra SMS-code (soft token). De wachtwoorden worden voor het zaaksysteem netjes ‘gezet’ conform de actuele rechten zodat oude niet meer geldende rechten ook daadwerkelijk verwijderd zijn.

Rapportages omtrent de rechten en het gebruik ervan worden echter niet periodiek verstrekt zodat er geen controle mogelijk is. Dit geldt ook voor de diverse mappen, folders e.d. zoals de U (user) , G

[5] Configuratie Management DataBase, hierin worden alle hard- en software elementen vastgelegd.

(gemeenschappelijk) en I schijf (transfer van documenten). Het ontbreekt aan inzicht in het gebruik van deze schrijven. Aan het gebruik van de I schijf zijn geen restricties verbonden omtrent het plaatsen van vertrouwelijk geclassificeerde data.

Advies:

- *Accordeer het wachtwoorden beleid (procedures voor het aanvragen, wijzigen en verwijderen van toegangsrechten.*
- *Zorg voor two-factor authenticatie[6] op die applicaties of informatiebronnen met integere of vertrouwelijke gegevens.*
- *Rapporteer periodiek over de rechten, het gebruik en de mutaties van accounts en toets of het conform het beleid wordt uitgevoerd.*
- *Rapporteer over het gebruik van de diverse folders en stuur hier op.*
- *Voor periodiek een audit uit over de accounts en folders. Richt met name op de kritische systemen.*

Privacy

Beperkt

De gemeente Midden-Drenthe registreert diverse persoonsgegevens. Aan de registratie van deze persoonsgegevens stelt de nieuwe privacywetgeving strikte eisen, want vanaf 1 januari 2016 is de Wbp[7] aangepast en is het wettelijk verplicht datalekken te melden. De gemeente Midden-Drenthe heeft een eenvoudige en effectieve procedure voor het melden van datalekken aan de Autoriteit Persoonsgegevens. Met ingang van mei 2018 zal tevens nieuwe Europese privacy-verordening van kracht worden, de Algemene Verordening Gegevensbescherming (AVG). Deze wet stelt, onder andere, dat een organisatie die persoonsgegevens verwerkt voor deze registraties een Privacy Impact Assessment (PIA) dient uit te voeren en een register aanlegt van persoonsgegevens. De gemeente Midden-Drenthe heeft (nog) geen PIA's uitgevoerd en beschikt nog niet over een register. Organisaties hebben tot mei 2018 de tijd hun processen aan te passen aan de nieuwe wet. Vanaf dat moment zal de Autoriteit Persoonsgegevens de Europese verordening gaan handhaven.

De gemeente Midden-Drenthe heeft nog geen Functionaris Gegevensbescherming. De FG is de persoon die bewaakt of de organisatie voldoet aan de Wbp. Via internet (https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming) is een uitgebreide beschrijving van de rol en de bevoegdheden van de FG te downloaden.

Belangrijk onderdeel van de privacywetgeving is het bewaar- en vernietigingsbeleid. Het is aan te bevelen dat de gemeente Midden-Drenthe haar in het handboek Kwaliteit verwoorde beleid en procedures voor het bewaren en vernietigen van (persoon) gegevens controleert.

Advies:

- *Voer voor de kritieke persoonsregistraties een Privacy Impact Assessment uit (art. 35 AVG).*
- *Begin in 2017 met het aanleggen van een persoonsgegevens register (art. 30 AVG).*
- *Benoem een Functionaris Gegevensbescherming (Wbp) / Data Protection Officer (art. 37 AVG).*
- *Controleren van het beleid ten aanzien van bewaar- en vernietigingstermijnen.*

[6] Het vaststellen van de identiteit van de gebruiker op basis van twee factoren, namelijk kennis (van een wachtwoord) en bezit (van een token of smartphone) .

[7] Wet Bescherming Persoonsgegevens.

Beveiliging informatie-uitwisseling

Beperkt

De applicaties die door de gemeente Midden-Drenthe worden gebruikt staan voornamelijk in het eigen rekencentrum en sommige staan 'in-the-cloud', de SaaS-applicaties die specifiek door de gemeente Midden-Drenthe worden gebruikt. Voor de koppelingen met die systemen zijn de volgende beheersmaatregelen geïmplementeerd:

- Wederzijdse authenticatie: Beide kanten van de 'lijn' moeten zeker weten dat ze contact hebben met het juiste systeem, dan wel de juiste persoon.
- Versleuteling van het gegevensverkeer.
- Logging van het berichtenverkeer (niet de inhoud, wel het feit dat verkeer heeft plaatsgevonden).

De gemeente Midden-Drenthe gebruikt reeds certificaten en voor het berichten verkeer en is van plan om dat volledig in te voeren.

Beveiliging van de uitwisseling van gegevens betreft ook het via de e-mail of telefonisch verstrekken van informatie aan externe partijen of andere betrokkenen. De gemeente Midden-Drenthe heeft haar medewerkers gewezen op de gevaren van het verzenden van (vertrouwelijke) e-mail door middel van privacy trainingen. De gemeente Midden-Drenthe heeft voorzieningen getroffen om op een beveiligde manier documenten als bijlage via e-mail te versturen. Het zaaksysteem Midnet/Mozard maakt een beveiligde en gecontroleerde toegang mogelijk door derden (via de gebruikers ID en aparte pincode). Voor die berichten die als vertrouwelijk worden geclassificeerd zal daarom altijd via een zaak op een veilige wijze worden gecommuniceerd.

Advies:

- *Implementeer volledig het gebruik van certificaten voor het (digitale) berichten verkeer.*
- *Controleer periodiek of de voorziening voor het veilig verzenden van e-mail altijd wordt gehanteerd.*

Overeenkomsten ten aanzien van informatie-uitwisseling

Beperkt

Naast de beveiliging van de informatie-uitwisseling dient met name de gemeente Midden-Drenthe de afspraken over de uitwisseling met de diverse partijen vast te leggen in bewerkers-overeenkomsten (art. 14 Wbp). In deze overeenkomsten dienen o.a. de volgende zaken te worden vastgelegd:

- Beschrijving van de gegevens die worden uitgewisseld.
- Welke partij (voor en na de uitwisseling van de gegevens) verantwoordelijk is voor de beveiliging.
- De wederzijdse verplichting tot het melden van datalekken.
- In hoeverre de betrokkene toestemming heeft verleend voor de uitwisseling.
- Het doel waarvoor de gegevens gebruikt mogen worden.
- Bewaar- en vernietigingstermijnen.

De gemeente Midden-Drenthe zal minimaal voor alle kritische systemen een overeenkomst dienen af te sluiten. Uit de interviews is gebleken dat er in enkele gevallen wel een overeenkomst is, maar Insite Security heeft niet vast kunnen stellen of overeenkomsten conform bovenstaande bepalingen zijn opgesteld en heeft ook de volledigheid niet kunnen vaststellen, want gezien het aantal leveranciers en applicaties is dat buiten de scope van de opdracht. Veelal zullen leveranciers het initiatief nemen tot het actualiseren van de overeenkomst. Het is echter aan de gemeente Midden-Drenthe om voor de kritische systemen, vanuit het beveiligingsperspectief bezien, juridisch gezien haar zaken op orde te hebben.

Advies:

- *Stel een beleid op voor welke applicaties/leveranciers en gegevensuitwisselingen waarvoor vanuit informatiebeveiliging perspectief bewerkersovereenkomsten opgesteld dienen te zijn. Controleer deze aan de minimale juridische aspecten zoals genoemd in de Wbp.*

Beveiligingsincidenten

Beperkt

De gemeente Midden-Drenthe heeft een procedure geïmplementeerd voor het melden van datalekken aan de Autoriteit Persoonsgegevens (AP).

Bij de afhandeling van de reguliere incidenten wordt door de gemeente Midden-Drenthe echter nog geen extra aandacht besteed aan de aspecten van informatiebeveiliging. Want het ontbreekt aan een beleid bij het melden door medewerkers of leveranciers van beveiligingsincidenten. De ISO27001 schrijft voor dat organisaties dienen te leren van beveiligingsincidenten en derhalve zullen alle meldingen geregistreerd dienen te worden. Het naderhand periodiek analyseren van de achterliggende oorzaak van een beveiligingsincident (Root-cause-analysis) is hierbij ook een belangrijk element. De gemeente Midden-Drenthe heeft dat niet geborgd in een procedure.

Advies:

- *Stel een aanvullend beleid op voor het (melden,) registreren, afhandelen en analyseren van beveiligingsaspecten bij de reguliere incidentmeldingen.*

Continuïteitsmaatregelen

Beperkt

De gemeente Midden-Drenthe heeft (ruim) voldoende beheersmaatregelen geïmplementeerd om de continuïteit van de ICT-voorzieningen te borgen. Er wordt gebruik gemaakt van moderne virtuele servers, waarmee de continuïteit van de servervoorzieningen in grote mate is geborgd. De noodstroomvoorzieningen zijn op orde. Hetzelfde geldt voor de (gescheiden) backup- en restorevoorzieningen. De toetsing en controle hiervan heeft echter nog niet plaatsgevonden.

De gemeente Midden-Drenthe kent een zogeheten kernteam dat in geval van calamiteiten bijeen geroepen wordt.

Advies:

- *Plan periodiek oefeningen in om de effectiviteit van het kernteam te verifiëren, te beoordelen en te evalueren.*

Gedrag(scode)

Beperkt

Ten aanzien van het gedrag van medewerkers heeft de gemeente Midden-Drenthe haar medewerkers (formeel) op de hoogte gesteld van de eisen die de organisatie stelt ten aanzien van informatiebeveiliging gezien de privacy trainingen.

Belangrijk element in het bewustzijn van medewerkers is het besef dat zij (integere/vertrouwelijke) gegevens beheren die vaak niet in systemen zijn opgeslagen. Zij zijn zelf verantwoordelijk voor de beveiliging van opslag, gebruik en transport van die gegevens. Medewerkers moeten worden ondersteund bij het classificeren van deze gegevens en met de middelen om opslag en transport van die gegevens adequaat te beveiligen. Dit kan door het hanteren van een classificatierichtlijn. Deze geeft medewerkers inzicht in hoe zij kunnen bepalen of een document openbaar, vertrouwelijk of geheim is en hoe zij een vertrouwelijk of geheim document moeten,

dan wel mogen behandelen. De gemeente Midden-Drenthe heeft classificatie genoemd in haar handboek Kwaliteit Informatievoorziening echter zij heeft deze nog niet omgezet praktische richtlijnen.

Advies:

- *Zet het geformuleerde beleid in het handboek Kwaliteit Informatie voorziening ten aanzien van classificatie om in praktische richtlijnen en controleer hierop.*

Wijzigingenbeheer

Beperkt

Het proces rondom wijzigingenbeheer ten aanzien van wijzigingen in de infrastructuur is op orde. Het wijzigingenbeheer binnen de gemeente Midden-Drenthe ten aanzien van wijzigingen in de applicatie-voorzieningen is ad hoc georganiseerd. Nieuwe versies van software worden getest en vaak met een kopie van de productie gegevens, waarmee een risico wordt genomen dat door ondeugdelijke software (het moet immers nog getest worden) de productiegegevens onbedoeld op straat komen te liggen.

Het wijzigingenbeheer is van belang om te voorkomen dat onbedoeld of onbeheerst (dus niet voldoende getest) applicatiewijzigingen worden uitgevoerd. Registratie van wijzigingen is van belang om achteraf te kunnen vaststellen welke aanpassingen zijn gedaan, bijvoorbeeld in het geval er problemen optreden.

Advies:

- *Voer een (beperkte) registratie in van de wijzigingen in de belangrijkste applicaties.*
- *Onderzoek of het mogelijk is om voor vertrouwelijke systemen aparte test-sets te creëren.*

Indienst/Uitdienst

Gedefinieerd

De gemeente Midden-Drenthe heeft haar processen rondom het in/uit dienst treden goed op orde. Zij bewaart de documenten in het personeelsdossier dat alleen toegankelijk voor geautoriseerde medewerkers is. Tevens maakt zij gebruik van het zaaksysteem zodat de berichtgeving beveiligd is. Een aandachtspunt is het bewaren van de curriculum vitae van sollicitanten (deze dienen tijdig verwijderd te worden, binnen één maand voor een reguliere sollicitatie en binnen één jaar voor een open sollicitatie)). Bij uitdiensttreding wordt gerefereerd aan de gemaakte afspraken (via de zaak) en worden de in te leveren gemeentelijke spullen gezamenlijk doorgenomen. Hiervoor geldt echter nog een kleine inhaalslag, want niet alle medewerkers zijn geregistreerd.

Een speciaal aandachtspunt betreft de situatie waarin er zich een dispuut voor doet met de medewerker en er derhalve sprake is van extra vertrouwelijke documenten. Het is wenselijk om die extra te versleutelen.

Advies:

- *Completeer de registratie van werkafspraken met alle medewerkers in het zaaksysteem.*
- *Verwijder de curriculum vitae van sollicitanten die niet aangenomen zijn.*
- *Onderzoek een mogelijk voor versleuteling van extra vertrouwelijke berichten/documenten.*

4.4 Aspect Techniek

Aanpak

De rekenkamercommissie van de gemeente Midden-Drenthe heeft besloten de beveiliging van het interne en externe netwerk te laten toetsen. Onderdeel hiervan was een penetratietest (hierna pentest) op het interne, externe en draadloze netwerk van de gemeente Midden-Drenthe. Onderzocht is of het mogelijk is op enigerlei wijze toegang te krijgen is vanaf binnen en buitenaf tot de systemen en gegevens. Met andere woorden hoeveel moeite kost het om de beveiliging te doorbreken en wat kun je zien als dit gelukt is.

Daarnaast wordt een risicoaanduiding gegeven en wordt een mogelijke oplossing gegeven die de kwetsbaarheid wegneemt. In een gegeven hoeveelheid tijd —time-box— zijn zoveel mogelijk zwakke plekken in kaart gebracht. Zo is er onderzocht of bijvoorbeeld netwerk segmentatie aanwezig is. Zijn er kritische kwetsbaarheden aanwezig? Wat kan een kwaadwillende gebruiker misbruiken om toegang te krijgen tot gevoelige informatie?

De onderstaande indeling is gehanteerd om de uitkomsten van de kwetsbaarheden scan te waarderen.

Niveau 1 **Zeer onveilig**

Eén of meerdere bevindingen met een hoog risico zijn aangetroffen.

Niveau 2 **Onveilig**

Eén of meerdere bevindingen met een gemiddeld risico zijn aangetroffen en geen hoog risico.

Niveau 3 **Veilig**

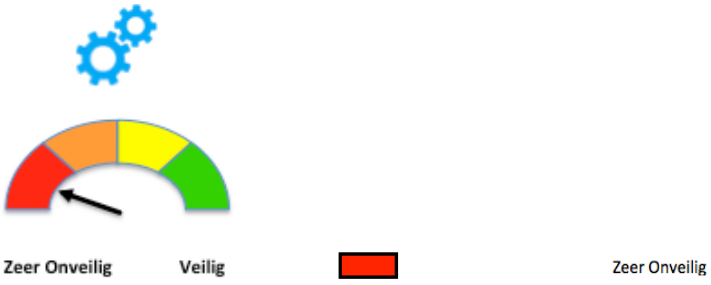
Eén of meerdere bevindingen met een laag risico zijn aangetroffen en geen gemiddeld en/of hoog risico

Niveau 4 **Zeer veilig**

Geen bevindingen met enig risico zijn aangetroffen.

Resultaten

Op basis van de bevindingen van de penetratietest wordt de beveiliging van het interne, externe en draadloze netwerk van de gemeente Midden-Drenthe beoordeeld als '**zeer onveilig**' op het moment van de nulmeting.



Er zijn meerdere kwetsbaarheden aangetroffen met een kritisch en hoog risico. Binnen de gegeven tijd is Insite Security erin geslaagd om de beveiliging van het interne en externe netwerk te doorbreken. De inzet van Insite Security was met name gericht op het testen van het interne netwerk. De beveiliging van het externe netwerk is beperkt getest tijdens het onderzoek.
Wat mogelijk is bij het misbruiken van deze kwetsbaarheden wordt geïllustreerd aan de hand van de volgende situaties.

- Het is mogelijk om de volledige controle over het interne netwerk van de gemeente Midden-Drenthe te bemachtigen. Hierdoor kan een kwaadwillende zo goed als alle informatie op het interne netwerk en andere aangesloten locaties lezen, aanpassen en/of verwijderen.
- Omdat medewerkers documenten op een verkeerde plek hadden geplaatst was het mogelijk gedeelde mappen van verschillende afdelingen binnen de gemeente Midden-Drenthe te bereiken. Daardoor kunnen vertrouwelijke documenten met onder andere wachtwoorden, financiële informatie, gebruikersinformatie van personeel en gegevens van Burgerzaken worden ingezien.
- Het is mogelijk om vanaf internet documenten, over aanvragen van inwoners, op te vragen. Deze documenten bevatten onder meer gevoelige persoonsgegevens.

Er zijn op korte termijn verbeteringen noodzakelijk om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te kunnen garanderen. Hierbij moet er rekening worden gehouden met bijvoorbeeld het patchmanagement, configuratiemanagement en segmentatie van het netwerk.

Gezien de vertrouwelijkheid van de informatie wordt voor de verdere technische rapportage verwezen naar het separaat opgeleverde technisch rapport.

5 Bijlagen

I Bronnen en afkortingen

De volgende personen waren betrokken bij de nulmeting:

Naam	Rol/Functie
Jacobus Koops	Security Manager (ai)
Reinder Pepping	Technisch Beheerder
Jan Schroteboer	ICT Manager
Berend Iwema	Technisch specialist koppelingen
Dylan Kamoen	Functioneel consultant sociaal domein
Johan Homan	Hoofd Samenlevingszaken
Tinette de Boer	P&O
Jannie Bijker	P&O

Insite Security heeft de volgende documenten geraadpleegd voor de nulmeting:

Nr	Titel	Bestandsnaam
1.	Handboek Kwaliteit Informatievoorziening	RKMD 03 Handboek Kwaliteit Informatievoorziening (Nieuwe Stijl).docx
2.	Applicatie lijst	RKMD 02 lijst met applicaties

Verklaring van gebruikte afkortingen:

Afkorting	Verklaring
AP	Autoriteit Persoonsgegevenvs
AVG	Algemene Verordening Persoonsgegevens
BIA	Business Impact Assessment
CMDB	Configuation Management Data Base
FG	Functionaris Gegevensbescherming
ISMS	Information Security Management System
PIA	Privacy Impact Assessment
SaaS	Software as a Service
WBP	Wet Bescherming Persoonsgegevens

II Cobit Framework versie 4.1. Maturity Model

APPENDIX III—MATURITY MODEL FOR INTERNAL CONTROL

Maturity Level	Status of the Internal Control Environment	Establishment of Internal Controls
0 Non-existent	There is no recognition of the need for internal control. Control is not part of the organisation's culture or mission. There is a high risk of control deficiencies and incidents.	There is no intent to assess the need for internal control. Incidents are dealt with as they arise.
1 Initial/*ad hoc*	There is some recognition of the need for internal control. The approach to risk and control requirements is *ad hoc* and disorganised, without communication or monitoring. Deficiencies are not identified. Employees are not aware of their responsibilities.	There is no awareness of the need for assessment of what is needed in terms of IT controls. When performed, it is only on an *ad hoc* basis, at a high level and in reaction to significant incidents. Assessment addresses only the actual incident.
2 Repeatable but intuitive	Controls are in place but are not documented. Their operation is dependent on knowledge and motivation of individuals. Effectiveness is not adequately evaluated. Many control weaknesses exist and are not adequately addressed; the impact can be severe. Management actions to resolve control issues are not prioritised or consistent. Employees may not be aware of their responsibilities.	Assessment of control needs occurs only when needed for selected IT processes to determine the current level of control maturity, the target level that should be reached and the gaps that exist. An informal workshop approach, involving IT managers and the team involved in the process, is used to define an adequate approach to controls for the process and to motivate an agreed-upon action plan.
3 Defined	Controls are in place and are adequately documented. Operating effectiveness is evaluated on a periodic basis and there is an average number of issues. However, the evaluation process is not documented. Whilst management is able to deal predictably with most control issues, some control weaknesses persist and impacts could still be severe. Employees are aware of their responsibilities for control.	Critical IT processes are identified based on value and risk drivers. A detailed analysis is performed to identify control requirements and the root cause of gaps and to develop improvement opportunities. In addition to facilitated workshops, tools are used and interviews are performed to support the analysis and ensure that an IT process owner owns and drives the assessment and improvement process.
4 Managed and measurable	There is an effective internal control and risk management environment. A formal, documented evaluation of controls occurs frequently. Many controls are automated and regularly reviewed. Management is likely to detect most control issues, but not all issues are routinely identified. There is consistent follow-up to address identified control weaknesses. A limited, tactical use of technology is applied to automate controls.	IT process criticality is regularly defined with full support and agreement from the relevant business process owners. Assessment of control requirements is based on policy and the actual maturity of these processes, following a thorough and measured analysis involving key stakeholders. Accountability for these assessments is clear and enforced. Improvement strategies are supported by business cases. Performance in achieving the desired outcomes is consistently monitored. External control reviews are organised occasionally.
5 Optimised	An enterprisewide risk and control programme provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements.	Business changes consider the criticality of IT processes, and cover any need to reassess process control capability. IT process owners regularly perform self-assessments to confirm that controls are at the right level of maturity to meet business needs and they consider maturity attributes to find ways to make controls more efficient and effective. The organisation benchmarks to external good practices and seeks external advice on internal control effectiveness. For critical processes, independent reviews take place to provide assurance that the controls are at the desired level of maturity and working as planned.

Voor meer informatie zie: http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx

III Onderzoeksbureau:

Het onderzoek is uitgevoerd door de consultants van Insite Securtiy:

Naam	Onderdeel
drs. Lourens W. Dijkstra MMC CISM	Onderdeel mens en projectleiding
drs. ing. David van der Meer	Onderdeel organisatie
Khalid Latifi CEH	Onderdeel techniek

IV Technische en bestuurlijke reactie coll. B&W

GEMEENTE MIDDEN-DRENTHE

Postadres Postbus 24, 9410 AA Beilen
Telefoon (0593) 53 92 22
Internet www.middendrenthe.nl
E-mail gemeente@middendrenthe.nl

Bezoekadres
Beilen Raadhuisplein 1
ma, di, vr 8.30 – 12.00
wo 8.30 – 16.00
do 8.30 – 20.00
Smilde Hoofdweg 24
ma, do 8.30 – 12.00
Westerbork B.G. van Weezelplein 10
di 8.30 – 12.00

de Rekenkamercommissie
t.a.v. De heer E. De Lange

Datum: 10 april 2017
Behandeld door: Allard Gunnink
Zaaknummer: 777030
Onderwerp: Bestuurlijke en technische reactie op onderzoek Rekenkamercommissie Informatiebeveiliging

Uw brief van: 17 maart 2017
Uw kenmerk:
Bijlagen:
Verzonden op: 11 april 2017

Geachte heer De Lange,

In uw brief van 17 maart 2017 verzoekt u ons om een technische en bestuurlijke reactie te geven op uw concept onderzoekrapport naar onze informatiebeveiliging. U heeft dat onderzoek uitgevoerd binnen onze ambtelijke organisatie, het college en de gemeenteraad. We geven met deze brief graag gevolg aan uw verzoek.

Technisch
Onze medewerkers hebben vastgesteld dat er in uw rapport geen feitelijke onjuistheden staan. Verder hebben zij in een eerder stadium al kunnen kennisnemen van de technische bevindingen van de onderzoekers. Zij hebben op basis daarvan een technisch plan van aanpak gemaakt, dat ze ook aan de onderzoekers hebben overhandigd.
In uw onderzoeksrapport verwijst u ook naar deze eerdere uitwisseling van informatie.

Bestuurlijk
We zijn u als college erkentelijk dat u ons een gedegen onderzoeksrapport aanbiedt over onze informatiebeveiliging. U maakt ons daarin duidelijk dat we als organisatie, college en raad stappen te zetten hebben op dit thema.

We zijn er ook blij mee dat u in uw voorwoord de resultaten van het onderzoek op een heldere manier nader duidt. We vatten dat voor onszelf zo samen: we doen als gemeente al een heleboel dingen gewoon goed, tegelijk is er nog werk aan de winkel en dat blijft ook wel zo in de dynamische digitale wereld.

We beseffen daarbij dat het om een belangrijk thema gaat waarin we als lokale overheid een grote verantwoordelijkheid dragen. Het is juist vanwege dit besef dat we de uitkomsten van het onderzoek voortvarend oppakken.

KvK 01182848
BTW 806300449B.01
E-mail nota's factuur@middendrenthe.nl
IBAN NL10BNGH0285078712

We nemen als college al uw aanbevelingen ter harte. Dat betekent ook dat we over ongeveer een jaar opnieuw een extern onderzoek zullen laten uitvoeren. In dat onderzoek laten we in elk geval nagaan wat we op dat moment feitelijk gedaan hebben met alle aanbevelingen.

We gaan ervan uit dat we in onze planning- en controlcyclus standaard aandacht zullen geven aan dit onderwerp.

We vertrouwen er op dat u met deze bestuurlijke reactie verder kunt in uw rapportage naar de gemeenteraad.

Informatie
Voor meer informatie kunt u contact opnemen met Allard Gunnink, directiesecretaris, te bereiken op maandag tot en met vrijdag via telefoonnummer (0593) 53 93 10 of via het mailadres a.gunnink@middendrenthe.nl.

Met vriendelijke groet,
burgemeester en wethouders van Midden-Drenthe,

de secretaris, de burgemeester.

2