

Digitale veiligheid in tijden van corona

Inleiding

Als in het voorjaar 2020 Nederland in lock down gaat, reageert de gemeente Heusden snel en effectief. Thuis werken en online vergaderen worden de norm. De dienstverlening aan burgers wordt aangepast; voor de langere termijn onderzoekt men mogelijkheden om met inzet van digitale middelen meer mensen te bereiken. Deze ontwikkelingen roepen ook vragen op over veiligheid en privacy; zeker in het licht van de toenemende dreiging van criminele interventies.

Vanuit haar controlerende taak draagt de gemeenteraad (mede)verantwoordelijkheid voor een adequaat beleid ten aanzien van digitale communicatie. Bovendien vormt de raad zelf een belangrijk onderdeel van de digitale communicatiestructuur.

In deze rekenkamerbrief zet de rekenkamer verschillende, voor de gemeente Heusden relevante aspecten op een rij die onderdeel uitmaken van de digitale weerbaarheid. Hierin geven wij extra aandacht aan de actualiteit omtrent Corona aangezien hierdoor het aandeel van de digitale dienstverlening en digitale ondersteuning van de primaire werkprocessen in korte tijd exponentieel is toegenomen.

Digitalisering heeft een grote impact op de levens van onze inwoners. We leven in een informatie- en netwerksamenleving die steeds complexer wordt. Dorpen en steden ontpoppen zich steeds meer tot 'smart cities' waar digitale kansen volop worden benut. De overheid is in transitie naar een digitaal georiënteerde dienstverlening en bedrijfsvoering. Traditioneel beschikt de overheid over privacy- en concurrentiegevoelige datasets over en voor inwoners en ondernemers. De afgelopen jaren heeft de overheid zich ingespannen om vooral de beveiliging daarvan naar een hoger plan te tillen. Veel gemeenten hebben hier al mooie stappen in gemaakt.

Kwetsbaarheden en dreigingen in het digitale domein nemen echter ook toe, met verstrekken gevolgen in de samenleving. Juist in deze tijd waarin door Corona de digitale werkvormen en dienstverlening steeds vaker het eerste en enige kanaal van contact is tussen overheden, bedrijven en burgers, neemt ook het belang van een goede digitale veiligheid substantieel toe. De risico's beperken zich hierbij niet meer tot de grenzen van de gemeentelijke organisatie, maar doen zich des te meer voor in lokale ketens en netwerken. De verantwoordelijkheid voor de digitale veiligheid van zo'n keten als geheel is nog onontgonnen terrein. Dat is risicovol omdat bij een digitale ontworping de maatschappelijke effecten groot kunnen zijn. De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) onderschrijft dit in haar rapport 'Voorbereiden op digitale ontworping'. Met 'digitale ontworping' doelt de WRR op de ernstige verstoringen van het maatschappelijke leven met zowel digitale als fysieke dimensies. Denk bijvoorbeeld aan de gevolgen van de ransomware aanval op een Oekraïens boekhoudsysteem die in 2017 ook de Rotterdamse haven trof of de landelijke uitval van het noodnummer 112 als gevolg van een KPN-storing in 2019.

Digitale ontworpingen weerspiegelen het belang van slagkracht van bedrijven en instellingen in de gemeente om deze kwesties het hoofd te kunnen bieden. Overheid en bedrijfsleven zijn verantwoordelijk voor een basis 'fitheid' wat betreft digitale veiligheid en een hoge weerbaarheid wanneer zich onverhoopt toch een incident voordoet. Zij moeten onverminderd doorwerken aan het op orde brengen van de eigen digitale weerbaarheid. Om gemeenten en hun bestuurders te ondersteunen bij deze opgave heeft de VNG de Agenda Digitale Veiligheid 2020-2024 opgesteld.

Vragen/aspecten (niet in volgorde van belangrijkheid) van digitale weerbaarheid die we in deze brief zullen beantwoorden zijn:

1. Hoe zit het met de veiligheid van (gratis) applicaties voor videobellen en wat betekent dit voor de gemeente Heusden?
2. Het belang van updaten van software (incl wachtwoorden) en de risico's wanneer je dit niet voldoende doet.
3. Wie of wat bereik je niet met digitale middelen en wat betekent dit voor je dienstverlening, je democratisch proces en je democratische legitimiteit?
4. Wat zijn de belangrijkste risico's qua digitale weerbaarheid voor de gemeente Heusden?
5. Wat is de impact van (regionale) samenwerking met externen voor de digitale weerbaarheid van de gemeente Heusden?

Samenvatting en advies

Met deze rekenkamerbrief willen wij de gemeenteraad een antwoord geven op een aantal relevante vragen ten aanzien van de digitale veiligheid binnen de gemeente Heusden. Vragen die in ieder geval bij de rekenkamer leefden naar aanleiding van de lockdown afgelopen voorjaar. Ten behoeve van deze rekenkamerbrief hebben wij nadrukkelijk niet het totale informatiebeveiligingsbeleid 2019-2021 van de gemeente Heusden grondig en volledig doorgelicht om hier vervolgens conclusies aan te verbinden. Dit zou op een later moment alsnog kunnen plaatsvinden, al dan niet op verzoek van de gemeenteraad.

We hebben de inhoud van deze rekenkamerbrief gebaseerd op gesprekken met betrokkenen en literatuuronderzoek. Op basis hiervan is onze eerste en globale indruk van het beleid in Heusden alsmede de uitvoering hiervan door de afdeling I&A dat dit vooralsnog gedegen is en op een nauwgezette manier wordt uitgevoerd met oog voor de risico's.

Wel heeft de rekenkamer in deze rekenkamerbrief een aantal aandachtspunten voor de gemeenteraad opgenomen. Samengevat zijn dat:

- Raadsleden worden door de afdeling I&A of de griffie vooralsnog niet actief geïnformeerd of geadviseerd over digitale veiligheid. Met name omdat zij gebruik maken van zelf aangeschafte hardware en software en de organisatie hier dus ook geen zicht op heeft. Of deze keuzevrijheid voor raadsleden voor de toekomst nog steeds wenselijk is, is wat de rekenkamer betreft een aandachtspunt.
- De rekenkamer raadt de gemeenteraad aan om te volgen of alle noodzakelijke aanpassingen volgend uit de nieuwe BIO gedurende 2020 daadwerkelijk gedaan zijn zodat, conform de BIO, de gemeente Heusden einde 2020 aan alle eisen voldoet. De rekenkamer stelt voor dat het college hierover rapporteert in de eerste bestuursrapportage 2021.
- De rekenkamer adviseert de gemeenteraad om actief te volgen in hoeverre bij de keuze voor (meer) digitale vormen van communicatie voldoende aandacht wordt gegeven aan de adviezen van de Raad van State ten aanzien van de effecten van de digitalisering voor de rechtstatelijke verhoudingen. Dit zou kunnen als vast onderdeel van de paragraaf bedrijfsvoering in de p&c-documenten
- ENSIA wordt ook binnen de gemeente Heusden al ruim 3 jaar als instrument gehanteerd. Dit helpt de organisatie ook nadrukkelijk bij het omvormen van de oude BIG naar BIO (zie vraag 2), en dit op een risicogerichte wijze. De afdeling I&A geeft wel aan dat het nog wel moet groeien om echt maximaal rendement uit dit instrument te halen. De rekenkamer adviseert de gemeenteraad dan ook om deze ontwikkeling actief te blijven volgen. De rekenkamer stelt voor dat het college hierover rapporteert in de tweede bestuursrapportage 2021.

- Binnen Hart van Brabant bestaat de wens om ten aanzien van de inrichting en vastlegging van informatie meer samen te gaan doen. Het blijkt een zeer complex verhaal en vooralsnog iets voor de toekomst. De rekenkamer adviseert de gemeenteraad om dit, mocht deze wens zich verder ontwikkelen, nadrukkelijk te gaan volgen en hierbij de hiervoor genoemde adviezen van de Raad van State te betrekken.

Antwoorden en bevindingen bij de gestelde vragen

1. Hoe zit het met de veiligheid van (gratis) applicaties voor videobellen en wat betekent dit voor de gemeente Heusden?

Tijdens de lockdown is wereldwijd het gebruik van online applicaties voor videobellen extreem toegenomen, met name voor zakelijk gebruik. Grofweg kun je een onderscheid maken tussen gratis en betaalde applicaties, waarbij veel app's zowel een gratis als een betaalde versie hebben. De betaalde versie biedt dan doorgaans meer gebruikersgemak en scoort veel beter op privacy en veiligheid.

Het wil overigens niet zeggen dat gratis online vergaderapplicaties niet gebruikt zouden moeten worden. Het is alleen wel van belang op de hoogte te zijn van de risico's die dit met zich meebrengt. De Autoriteit Persoonsgegevens heeft een handig overzicht opgesteld van de meest gebruikte app's voor videobellen met scores voor belangrijke veiligheids- en privacyaspecten. Dit overzicht vindt u in hier:

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/keuzehulp_privacy_en_videobellen.pdf.

Hieronder gaan we nader in op de verschillende toepassingen binnen de gemeente Heusden.

Gemeenteraad Heusden

Voor het online vergaderen van de gemeenteraad heeft de gemeente Heusden in eerste instantie gekozen voor Pexip. De belangrijkste redenen hiervoor waren dat bij Pexip sprake is van Nederlandse hosting (dus meer zicht/focus op de veiligheid) en dat de leverancier een bekende samenwerkingspartner is van de gemeente Heusden en waar men altijd erg tevreden over was. Dit heeft ook in de praktijk erg goed uitgedaan. De gemeente Heusden was een van de eerste gemeenten in Nederland die met haar raadsvergaderingen digitaal ging. Mede door een zeer accurate begeleiding vanuit de afdeling I&A en Pexip konden deze vergaderingen vanaf dag 1 zeer veilig en technisch goed ondersteund doorgang vinden. Echter, enige tijd geleden is de prijs van Pexip substantieel verhoogd door de leverancier. Vervolgens heeft de afdeling I&A een onderzoek gedaan naar alternatieven en gekozen voor Zoom. Zoom heeft het namelijk afgelopen jaar veel aanpassingen gemaakt in hun software zodat het met de juiste instellingen voldoende veilig is om te gebruiken voor online vergaderingen. Vooral het zomaar "inbreken" in een vergadering is niet meer mogelijk. Ook de IBD heeft een positief advies afgegeven:

<https://www.informatiebeveiligingsdienst.nl/product/privacyverklaring-zoom/>

Voor de 'eigen' communicatie kiezen de raadsleden zelf welke applicaties zij hanteren.

Raadsleden kiezen namelijk ook zelf welke hardware zij gebruiken en dit geldt voor de applicaties waar zij mee werken. Hier krijgen zij een budget voor vanuit de gemeente. Voor het raadplegen van de gemeentelijke stukken gebruiken zij wel allemaal Ibabs. Deze applicatie, Cytrix en de verbindingen worden periodiek gecontroleerd door de afdeling I&A inclusief de beveiligingscertificaten. Tevens wordt Ibabs periodiek doorgelicht door de Informatiebeveiligingsdienst (IBD) van de VNG.

Raadsleden worden door de afdeling I&A of de griffie vooralsnog niet actief geïnformeerd of geadviseerd over digitale veiligheid. Met name omdat zij gebruik maken van zelf aangeschafte hardware en software en de organisatie hier dus ook geen zicht op heeft. Dit is voor de toekomst, zeker nu digitaal werken steeds meer een standaard wordt, wat de rekenkamer betreft een aandachtspunt.

College en ambtelijk apparaat gemeente Heusden

Voor het online vergaderen wordt door college en ambtenaren in principe Skype for Business gebruikt. Zoom mag wel gebruikt worden voor overleg, maar dan is het niet toegestaan om documenten te delen. Voor afdelingsoverleggen wordt wel Zoom gebruikt maar dan via een account waarvan de instellingen voor onder meer veiligheid en privacy beheerd worden door de afdeling I&A.

Zoals hierboven al gesteld, heeft de afdeling I&A heeft nadrukkelijk onderzoek gedaan naar Zoom en geconcludeerd dat na de aanpassingen afgelopen voorjaar door de applicatiebouwer de applicatie op zich niet onveilig is, maar dat je het wel onveilig kunt gebruiken. Vandaar eerder genoemde richtlijnen voor het gebruik van Zoom binnen de gemeente. De afdeling I&A blijft de veiligheid van deze en alle andere applicaties actief volgen en neemt ook de signalen die de Informatiebeveiligingsdienst voor gemeenten (IBD) van de VNG hierover verspreid zeer ten harte.

Tenslotte is de overgang naar thuiswerken over het algemeen erg soepel verlopen, mede doordat alle ambtenaren al thuis konden werken voor de lockdown en er dus al voldoende accounts waren en de manier van werken al gangbaar was, ware het niet op deze schaal.

2. Het belang van updaten van software (incl wachtwoorden) en de risico's wanneer je dit niet voldoende doet

Updaten is in de eerste plaats nodig om met de nieuwste versie van software te werken. Je beschikt dan over de nieuwste functionaliteiten en je krijgt ondersteuning van de leverancier. Daarnaast bevat alle software zwakke plekken. Vaak komt een digitale aanvaller langs die weg een organisatie binnen.

Gemeenten hanteren sinds 1 januari 2020 samen met de rijksoverheid, waterschappen en provincies één uniform normenkader voor informatiebeveiliging: de Baseline Informatiebeveiliging Overheid (BIO). Deze BIO is een 'update' van de Baseline Informatiebeveiliging Gemeenten (BIG). Elke gemeente moet sinds 1 januari 2020 bezig zijn met het invoeren van de richtlijnen voor informatiebeveiliging, om eind 2020 aan de BIO te voldoen. De BIO legt meer nadruk op risicomanagement dan de BIG, die meer gaat over specifieke maatregelen. De rol van de bestuurder en lijnmanager is ten aanzien van risicomanagement explicieter dan de BIG aangaf.

In de BIO worden wachtwoordeisen benoemd. Hierdoor is het volgens de Informatiebeveiligingsdienst voor gemeenten (IBD) van de VNG nodig dat nadere regels worden gesteld over wachtwoordbeleid en ondersteunende processen. Wachtwoordbeleid is geen overbodige luxe bij gemeenten. Bijvoorbeeld om te voorkomen dat er informatie op straat komt te liggen. Alle gebruikers van gemeentelijke informatiesystemen moeten goede wachtwoorden kiezen en zijn verantwoordelijk voor de geheimhouding ervan. En dat is best lastig volgens de IBD. Voor steeds meer diensten zijn verschillende wachtwoorden nodig. Daardoor komt het regelmatig voor dat wachtwoorden worden opgeschreven of opgeslagen op onveilige plaatsen. Of de medewerkers kiezen een wachtwoord dat steeds lijkt op het vorige wachtwoord of met een bepaald patroon, omdat het anders ondoenlijk wordt om te onthouden.

Voor meer informatie over de Baseline Informatiebeveiliging Overheid (BIO) zie link <https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid>

Gemeente Heusden

In het Informatiebeveiligingsbeleid 2019-2021 van de gemeente Heusden is het normstellend (strategisch) beleid vastgelegd en dit is uitgewerkt in het handboek informatiebeveiliging. Met dit beleid werkt de gemeente Heusden aan beveiliging van persoonsgegevens en informatie. Het beleid is gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Inmiddels is er dus sprake van de opvolger van de BIG, zijnde de BIO (zie hierboven). De afdeling I&A is sindsdien het bestaande beleid waar nodig aan het aanpassen met als beoogd resultaat dat einde 2020 het gemeentelijke beleid in lijn is met de BIO.

Meer specifiek wordt binnen de gemeente Heusden het nodige gedaan op het gebied van updaten en wachtwoordbeheer.

Op alle systemen voert de afdeling I&A regelmatig audits uit gebaseerd op de risicoanalyse naar aanleiding van het Informatiebeveiligingsbeleid 2019-2021 en volgt signalen op vanuit de IBD. De updates van de software is automatisch ingeregeld zodat alle eventuele zwakke plekken in de software zo snel als mogelijk kunnen worden gedicht.

Qua wachtwoordbeheer stelt de gemeente Heusden specifieke eisen die de beveiliging bevorderen. Zo is het is als gebruiker via de instellingen onmogelijk gemaakt om een wachtwoord te kiezen dat niet aan deze eisen voldoet. Hiernaast werkt de gemeente Heusden ook met een token als vorm van Multi-Factor Authentication (MFA). Een token is een authenticatie methode

waarbij de gebruiker twee stappen succesvol moet doorlopen om toegang te krijgen. De eerste stap is het invoeren van een gebruikersnaam en wachtwoord. De tweede stap is dat je een aparte code ontvangt (die steeds verandert) en deze gebruikt om in te loggen.

Een belangrijke sleutel om je organisatie te beschermen tegen aanvallen van buiten is en blijft toch ook het gedrag van de gebruikers. Aanvallers van buiten komen steeds vaker binnen via het zogenaamde phishing. Phishing is een vorm van internetfraude waarbij internetcriminelen proberen persoonlijke gegevens of wachtwoorden te stelen. Een medewerker heeft op een verkeerde link geklikt, een verkeerde bijlage geopend of misschien verkeerd gereageerd op een e-mail waardoor de aanvallers de organisatie binnen kunnen dringen. Om dit zoveel als mogelijk te kunnen voorkomen, zetten de Chief Information and Security Officer (CISO) en de Privacy Officer (PO) in op educatie en bewustwording. Regelmatig worden alle medewerkers geïnformeerd via presentaties en sessies op specifieke onderwerpen die van belang zijn voor de beveiliging van de informatie. Ten behoeve van de bewustwording worden ook periodiek nep-phishingmails verstuurd met als doel om medewerkers bewust te maken van de listigheid van sommige criminelen. Ook worden regelmatig crisisgames vanuit de IBD gedaan om te simuleren wat er gebeurt bij een cyberaanval. Ook dit helpt enorm bij de bewustwording. Dit alles is en blijft echter wel een continue proces dat dus ook blijvend aandacht verdient.

Het volledig uitsluiten van een aanval van cybercriminelen is overigens onmogelijk. Dit gevaar dreigt namelijk voor alle organisaties, wereldwijd. In tegenstelling tot bijvoorbeeld water- of energieleveranciers lijken (kleinere) gemeenten zoals Heusden voor cybercriminelen niet bijzonder interessant om volledig plat te leggen, maar ontregelen kan soms ook een doel zijn. Dit zagen we ook bij het Kiddovirus dat de gemeente Heusden trof in 2008 waardoor alle systemen werden platgelegd. Dit heeft intern wel tot bewustwording van de gevaren geleid. In het geval van een dergelijke aanval zal apparatuur opnieuw geïnstalleerd moeten worden met schone software en werk je verder vanuit de laatste backup. Binnen de gemeente Heusden wordt iedere nacht een backup van alle gegevens gemaakt op 2 verschillende locaties. Ook wordt periodiek de digitale omgeving gescand op zwakke plekken en risico's.

De rekenkamer raadt de gemeenteraad aan om dit actief te blijven volgen. En meer specifiek te volgen of alle noodzakelijke aanpassingen volgend uit de nieuwe BIO gedurende 2020 daadwerkelijk gedaan zijn zodat, conform de BIO, de gemeente Heusden einde 2020 aan alle eisen voldoet. De rekenkamer stelt voor dat het college hierover rapporteert in de eerste bestuursrapportage 2021.

3. Wie of wat bereik je niet met digitale middelen en wat betekent dit voor je dienstverlening, je democratisch proces en je democratische legitimiteit?

Algemeen

Allereerst de beantwoording van de vraag wat het effect van digitalisering is als je kijkt naar mensen die niet digitaal vaardig zijn. Steeds meer diensten en producten van gemeenten worden namelijk digitaal aangeboden. Het grootste deel van de burgers heeft hier veel baat bij. Was de visie tot een aantal jaren geleden nog 'digitaal, tenzij...', inmiddels verandert dat naar 'digitaal waar het kan en persoonlijk waar het moet'. Het besef is er namelijk dat niet iedereen mee kan en/of wil in de digitale transformatie. Zo publiceerde de nationale ombudsman in 2017 het rapport "Hoezo MijnOverheid?". Hierin wordt kritisch gekeken naar de digitalisering van de overheidsdienstverlening en wordt een oproep gedaan om te zorgen dat er voor (kwetsbare) groepen alternatieven zijn voor digitaal zaken doen. Zo stelt de ombudsman: "Burgers mogen zich niet gedwongen voelen om gebruik te maken van een digitaal kanaal als zij dat niet kunnen of willen. Het is van belang om de verschillende groepen gebruikers en hun behoeften te onderscheiden". Digitale uitsluiting vindt plaats wanneer mensen geen materiële toegang hebben tot ICT of wanneer zij door verschillen in vaardigheden en gebruik niet de gewenste informatie digitaal kunnen vinden, ophalen en/of aanleveren. De vraag rijst: hoe zorgen we voor toegankelijke (digitale) dienstverlening voor inwoners met minder digitale vaardigheden?

Uit onderzoek in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties uit 2017 wordt ingeschat dat minimaal driekwart (75%- 80%) van de burgers digitaal zelfredzaam is. Daarnaast is circa 95% redzaam met ondersteuning. Er is een kleine groep (5%) die niet digitaal redzaam is. Daarbij dient opgemerkt te worden dat een groot deel hiervan vermoedelijk ook niet digitaal redzaam zal worden in de toekomst. Dit betekent dat 3,4 miljoen Nederlanders zonder ondersteuning moeite hebben met het digitaal zakendoen met de overheid. Voor de gemeente Heusden heb je het dan over ruim 7.000 mensen van boven de 18 jaar. Een deel van hen zal altijd hulp nodig hebben bij (digitale) dienstverlening van gemeenten. Een ander deel heeft wél de mogelijkheid om digitale vaardigheden te leren. De drie voorwaarden om digitaal vaardig te kunnen worden zijn:

- het spreken van de taal;
- het kunnen lezen en schrijven;
- het beschikken over een computer en internet.

Uit het onderzoek 'De digitale (zelf)redzaamheid van de burger: ondersteuning bij de Digitale Overheid 2017' van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties blijkt dat de groep minder digitaalvaardige Nederlanders een gevarieerde groep is. Hierin zitten bijvoorbeeld mensen die onvoldoende digitale vaardigheden bezitten, maar ook mensen die bijvoorbeeld de taal onvoldoende beheersen of mensen die door een stressvolle levensgebeurtenis (tijdelijk) niet in staat zijn om digitaal adequaat te reageren. De grootste risicogroepen zijn 'ouderen van 65+' (35%) en 'laagopgeleide oudere vrouwen' (32%).

Andere en misschien minder vanzelfsprekende risicogroepen zijn: 'relatief jonge werkende of studerende mensen' (11%), 'werkende mannen van middelbare leeftijd met een hoog inkomen' (14%) en 'langdurig werklozen' (8%) (Van Duimel en Notenboom, 2007).

Wanneer de digitale vaardigheden van inwoners toenemen, wordt een duurzame oplossing gecreëerd voor het probleem, omdat inwoners in de toekomst beter in staat zijn digitale dienstverlening van de overheid af te nemen. Het is gemeenten dan ook aan te raden om hier de komende jaren nadrukkelijk aandacht aan te geven. De VNG heeft begin 2019 bijvoorbeeld een notitie met betrekking tot Digitale Inclusie opgesteld met daarin onder andere goede voorbeelden van gemeenten die hiermee aan de slag gegaan zijn. Voor meer informatie hierover zie de brochure van de VNG over Digitale Inclusie (https://vng.nl/sites/default/files/2020-03/def-brochure-digitale_inclusie-2020.pdf)

Een ander interessant advies in dit kader is dat van De Raad van State over de effecten van de digitalisering voor de rechtstatelijke verhoudingen (2018). Juist op het gebied van democratische waarden en de rechtsstatelijke verhoudingen biedt deze publicatie steun. Het helpt lokale bestuurders in hun beleidskeuzes op het terrein van de informatiesamenleving, om maatschappelijke doelen voorop te stellen en te handelen vanuit publieke waarden, zoals privacy, zelfbeschikking, het tegengaan van sociale uitsluitingen en toezicht op technologie. Daadwerkelijk contact met de overheid is nodig. Van onze inwoners wordt steeds meer verwacht dat zij langs de digitale weg contact met de overheid kunnen onderhouden. Van die zelfredzaamheid blijkt echter in een aantal gevallen geen sprake (zie ook hierboven). De Raad van State adviseert daarom een nieuw beginsel van behoorlijk bestuur te ontwikkelen: het recht op toegang tot- en zinvol contact met de overheid. Onder dit beginsel moeten burgers inhoudelijk te woord worden gestaan, waarbij het contact kan leiden tot het bijstellen van voornemens of handelingen. In aanvulling hierop adviseert de Raad van State de overheid een effectieve uitvoering van de Algemene Verordening Gegevensbescherming (AVG) waar te maken door bestuursorganen actief te ondersteunen bij het operationaliseren van de daarin neergelegde rechten en waarborgen. Het gaat hierbij in het bijzonder om het recht op inzage en correctie van gegevens (in ketens) van overheidsorganisaties. Wij zien dat met de verwezenlijking van dit recht de positie van de inwoner tegenover de overheid bij digitale dienstverlening kan worden versterkt.

Verder adviseert de Raad van State:

- de beginselen van behoorlijk bestuur, en in het bijzonder het motiveringsbeginsel en het zorgvuldigheidsbeginsel, verscherpt te interpreteren in de context van digitalisering. Dat betekent onder meer dat in een besluit moet worden toegelicht welke beslisregels (algoritmen) zijn gebruikt en welke gegevens zijn overgenomen van andere bestuursorganen. Daarmee kan de positie van de burger bij geautomatiseerde en ketenbesluitvorming worden versterkt;
- maatwerk en "menselijke" heroverweging in de bezwaarfase van geautomatiseerd tot stand gekomen besluiten te bevorderen.
- In algemene zin terughoudend te zijn met zogenoemd techniekonafhankelijk wetgeven;
- ICT en uitvoering vanaf het begin onderdeel te doen zijn van het (multidisciplinair) voorbereiden van wet- en regelgeving en daar het wetgevingsproces op in te richten.

Voor het gehele advies van de Raad van State zie <https://www.raadvanstate.nl/@112661/w04-18-0230/>

Gemeente Heusden

De dienstverlening van de gemeente Heusden is vanaf het eerste moment van de lockdown in het voorjaar prioriteit geweest voor de organisatie. In het dagelijkse continuïteitsoverleg was de dienstverlening en hoe deze toch doorgang kon vinden een vast agendapunt. In het begin was het wel lastig dat de telefooncentrale niet vanuit huis bediend kon worden. Dit betekent dat er, in tegenstelling tot de richtlijn dat mensen zoveel als mogelijk thuis moesten werken, toch steeds mensen fysiek op het gemeentehuis dienden te zijn om de telefoon te beantwoorden. Dit is overigens inmiddels opgelost waardoor het nu wel mogelijk is om de telefoon te bedienen vanuit huis.

Ook voor de dienstverlening aan de balie zijn nieuwe richtlijnen gekomen. Zo moet voortaan in de middag op afspraak gewerkt worden en kent alleen de avondopenstelling een vrije inloop, al proberen medewerkers vanuit de dienstverleningsgedachte hier wel zo flexibel mogelijk mee om te gaan. Aan de andere kant zijn de openingstijden van de milieustraat juist verruimd.

De gemeente Heusden heeft niet exact in beeld in hoeverre de lockdown en de nieuwe richtlijnen aan de balie hebben geleid tot het niet (meer) bereiken van specifieke doelgroepen. Echter na de lockdown is wel een duidelijke piek opgetreden in de aanvragen in het sociaal domein. Hierbij speelt natuurlijk ook een rol dat veel mensen gedurende de lockdown ook minder naar de huisarts gingen en de reguliere zorg deels werd stilgelegd.

Qua participatie ziet de gemeente Heusden echter ook kansen. Binnen de organisatie wordt momenteel actief onderzocht in hoeverre digitale middelen voor communicatie nog meer kunnen helpen bij het betrekken van zoveel mogelijk mensen in de gemeente Heusden. Het GVVP (gemeentelijk verkeer en vervoersplan) en omgevingswet lopen hier natuurlijk in voorop. De rekenkamer adviseert de gemeenteraad om hierbij actief te volgen in hoeverre voldoende aandacht wordt gegeven aan onder meer de adviezen van de Raad van State zoals hierboven beschreven.

4. Wat zijn de belangrijkste risico's qua digitale weerbaarheid voor de gemeente Heusden?

Algemeen

Informatiebeveiliging is een proces van plannen, uitvoeren, controleren en bijstellen (Plan-Do-Check-Act). Gemeenten groeien steeds meer in volwassenheid van informatiebeveiliging. De focus verschuift van reageren op incidenten naar het herkennen en voorkomen van incidenten. Een digitaal weerbare gemeente kan potentiële incidenten vroegtijdig signaleren en de gevolgen ervan beperken, omdat de juiste maatregelen zijn getroffen. Als de basis door implementatie van de BIO (zie vraag 2) op orde is, verhoogt dit de digitale weerbaarheid van gemeenten.

ENSIA is een instrument dat gemeenten hierbij kan gaan helpen. ENSIA (Eenduidige Normatiek Single Information Audit) heeft tot doel het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid gebaseerd op de BIO (zie vraag 2).

ENSIA helpt gemeenten in één keer slim verantwoording af te leggen over informatieveiligheid. De verantwoordingssystematiek over de Basisregistratie Personen (BRP) en wet- en regelgeving Reisdocumenten (PUN en PNIK), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootchalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet) is samengevoegd en gestroomlijnd.

Uitgangspunt is het horizontale verantwoordingsproces aan de gemeenteraad. Dit vormt de basis voor het verticale verantwoordingsproces aan nationale partijen die een rol hebben in het toezicht op informatieveiligheid. Bij het afleggen van verantwoording wordt het principe van single information single audit toegepast; alle informatie die noodzakelijk is voor verticale verantwoording is ook onderdeel van het horizontale verantwoordingsproces. Voor meer informatie zie www.ENSIA.nl

Gemeente Heusden

Op het eerste gezicht lijkt de digitale weerbaarheid van de gemeente Heusden goed op orde. Echter, er moet nog wel een forse slag gemaakt worden in het vastleggen van de processen. Veel informatie en kennis zit in de hoofden van mensen en doordat betrokkenen elkaar doorgaans makkelijk vinden, lijkt de noodzaak tot het vastleggen en actueel houden van deze processen ook niet zo groot. Zeker in tijden waarin de druk op de operatie zo groot is als die de afgelopen maanden was. Echter, dit maakt het geheel wel kwetsbaar. De afdeling I&A is zich hiervan terdege van bewust en heeft al een analyse gemaakt van wat er moet gebeuren.

ENSIA wordt ook binnen de gemeente Heusden als ruim 3 jaar gehanteerd om de raad goed te kunnen informeren. Dit helpt de organisatie ook nadrukkelijk bij het omvormen van de oude BIG naar BIO (zie vraag 2), en dit op een risicogerichte wijze. De afdeling I&A geeft wel aan dat het nog wel moet groeien om echt maximaal rendement uit dit instrument te halen. De rekenkamer adviseert de gemeenteraad dan ook om deze ontwikkeling actief te blijven volgen.

5. Wat is de impact van (regionale) samenwerking met externen voor de digitale weerbaarheid van de gemeente Heusden?

Algemeen

Gemeenten in Nederland werken steeds meer samen. Met andere gemeenten en met andere organisaties binnen en buiten de eigen gemeentegrenzen. De samenwerking binnen Hart van Brabant is hier natuurlijk een mooi voorbeeld van. Deze samenwerking brengt op het gebied van het omgaan en delen van informatie wel specifieke aandachtgebieden met zich mee. En zorgen. Welke informatie willen en kunnen we delen en hoe gaan andere partijen met deze informatie om?

Gemeente Heusden

Over het algemeen is het beleid binnen de regionale samenwerkingsverbanden waarin de gemeente Heusden actief is dat iedereen met zijn eigen systemen en eigen applicaties werkt. Dit maakt dat er vooralsnog weinig risico is met betrekking tot de informatieveiligheid maar dat het soms wel lastig is om elkaar goed en snel te vinden. Er bestaat dan ook de wens, bijvoorbeeld binnen Hart van Brabant om ten aanzien van de inrichting en vastlegging van informatie meer samen te gaan doen, maar de vraag is nog wel hoe dit dan zou moeten en kunnen. Het blijkt een zeer complex verhaal en vooralsnog iets voor de toekomst. De rekenkamer adviseert de gemeenteraad om dit, mocht deze wens zich verder ontwikkelen, dit nadrukkelijk te gaan volgen.