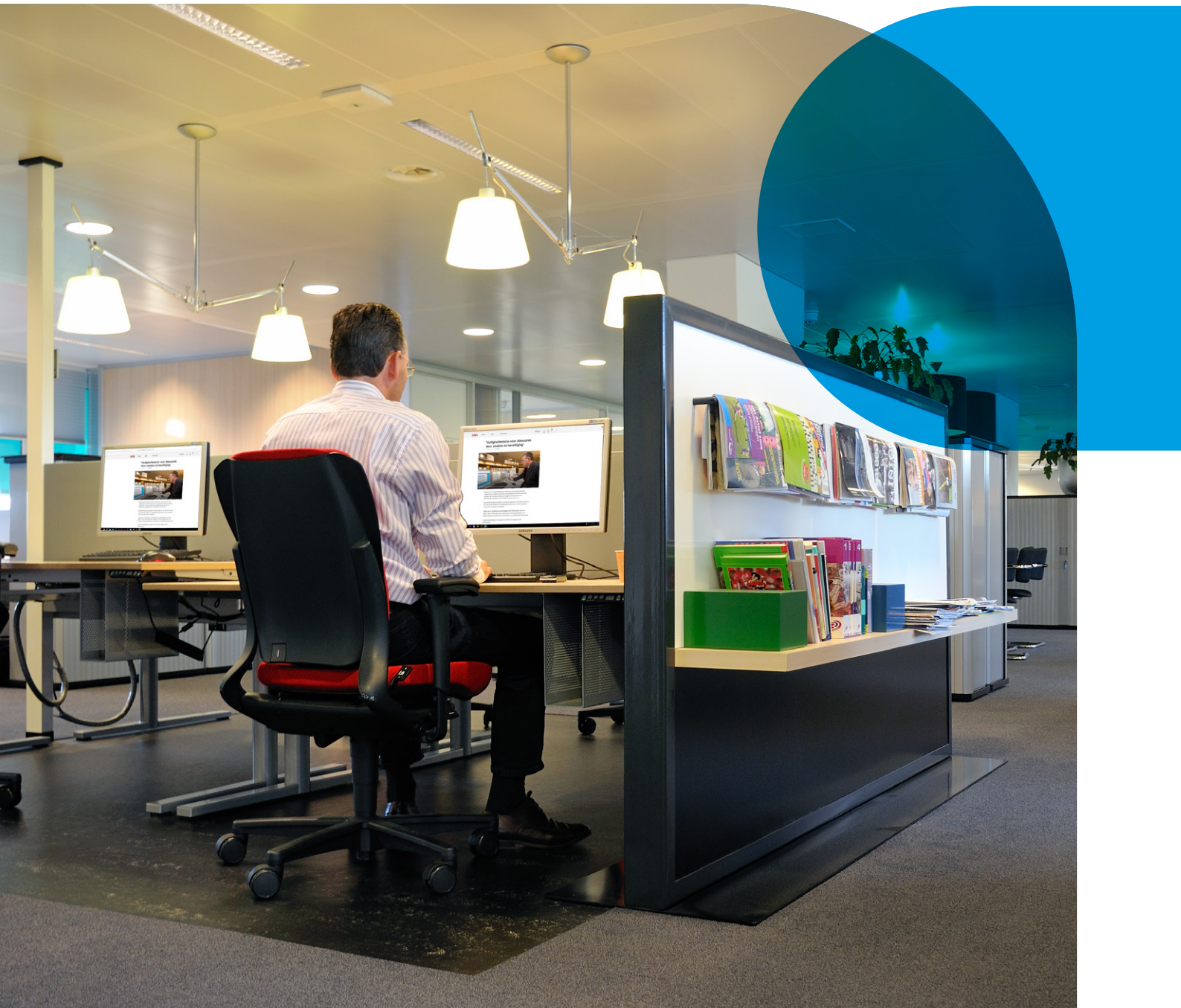
Eindverslag visitatiecommissie Informatieveiligheid
‘Durven leren’

Van Aa en Hunze tot Zwolle: Twee jaar in gesprek over gemeentelijke informatieveiligheid



Colofon

Samenstelling commissie

De visitatiecommissie
Frans Backhuijs (voorzitter). Frans is burgemeester van Nieuwegein en voorzitter van de visitatiecommissie Informatieveiligheid. Eerder was hij respectievelijk wethouder in Eindhoven en burgemeester in Oldenzaal. Frans is als vicevoorzitter van de commissie Dienstverlening & Informatiebeleid nauw betrokken bij de digitalisering van gemeenten.
Maarten Ruys. Maarten is voormalig gemeentesecretaris Groningen. Eerder was Maarten onder meer voorzitter a.i. bij de Nederlandse Zorgautoriteit en Secretaris-Generaal bij het ministerie van Sociale Zaken en Werkgelegenheid.
Wim Blok. Wim is directeur Publiekszaken, Handhaving en Veiligheid in de gemeente Leiden. Daarnaast is hij voorzitter van de Vereniging Directeuren Publieksdiensten. Wim heeft diverse lijnfuncties vervuld binnen zowel landelijke instellingen als de lokale overheid

De commissie dankt Rein Zijlstra (wethouder Zeewolde) en Nausikäa Efstratiades (hoofd IBD) op wie zij in voorkomende gevallen een beroep heeft kunnen doen ter deskundige vervanging bij incidentele afwezigheid van één van de commissieleden.

Secretaris
Jeroen Boot ondersteunt de commissie als secretaris. Dank gaat uit naar Eric Warners, secretaris in de periode tot april 2016 en Arie-Jan Baan die in voorkomende gevallen insprong als vervanger.

Secretariaat
Meta van den Brandhof verzorgt het secretariaat.

Begeleiding vanuit VNG
Remco van Vliet, Youri Lammerts van Bueren en Peter van Dijk.

September 2017

Inhoud

De visitatiecommissie Informatieveiligheid: Wim Blok, Frans Backhuijs (voorzitter) en Maarten Ruys (vlnr.)

Voorwoord

De visitatiecommissie Informatieveiligheid heeft in de afgelopen twee jaar met bestuurders en CISO's gesproken, door het hele land heen, van Aa en Hunze tot Zwolle. Al die gemeenten maken gelukkig in meer of mindere mate werk van informatieveiligheid. De bezochte gemeenten hebben in hun gesprek met de visitatiecommissie een grote openheid getoond rond dit gevoelige thema. Gemeenten kregen een verslag met bevindingen van het bezoek van de commissie en gingen daarmee aan de slag. Het bezoek van de visitatiecommissie heeft bij de bezochte gemeenten gewerkt als impuls om het thema informatieveiligheid beter te verankeren.

Technische bedreigingen nemen toe en zijn steeds complexer van aard. Goede technische voorzieningen die tijdig eventuele bedreigingen signaleren worden onontbeerlijk. Om daaraan invulling te geven is samenwerking noodzakelijk. Vanuit onze informatiebeveiligingsdienst voor gemeenten (IBD) worden hieraan landelijk aanzetten gegeven, maar ook samenwerking in de eigen regio noemt de visitatiecommissie een belangrijk thema.

Informatiebeveiliging is mensenwerk. Niet voor niks hamert de visitatiecommissie op het belang van een structurele bestuurlijke aandacht voor dit thema. Van inhuurkracht tot raadslid, iedereen moet zich bewust zijn van zijn of haar verantwoordelijkheid.

Het is aan de bestuurder van de gemeente om dit thema steeds weer onder de aandacht te brengen en te houden. De visitatiecommissie laat zien dat het gaat om een continu leer- en veranderingsproces. Niet voor niets heeft dit rapport de titel 'Durven leren'.

Binnen de vereniging blijven we ons de komende jaren inzetten om met u informatieveiligheid verder te verbeteren. Het verder inrichten van een CISO-netwerk; het komen tot een aanpak om vroegtijdig dreigingen te signaleren en het ondersteunen van een transparante verantwoording over informatieveiligheid zijn daar voorbeelden van.

De visitatiecommissie levert met haar bezoeken en dit rapport een belangrijke bijdrage aan het verbeteren van het (bestuurlijk) bewustzijn rond dit thema. Namens de vereniging wil ik Frans Backhuijs, Wim Blok en Maarten Ruijs zeer bedanken voor de betrokken wijze waarop zij hun werk hebben gedaan En dat geldt ook voor Eric Warners, Jeroen Boot en Meta van den Brandhof die in de afgelopen twee jaar de visitatiecommissie hebben ondersteund.

Jantine Kriens
Algemeen directeur VNG

Inleiding door de voorzitter van de visitatiecommissie

Ruim twee jaar geleden begonnen Wim, Maarten en ik aan onze rondtocht langs 120 gemeenten als "visitatiecommissie informatieveiligheid". Praktisch betekende dit dat we iedere twee weken drie gemeenten bezochten. Het doel van onze bezoeken was drieledig: de aandacht voor informatieveiligheid vasthouden en versterken, het handelingsperspectief van gemeenten vergroten en toetsen of verplichtende zelfregulering werkt. Kortom, we zijn geen visitatiecommissie in de klassieke zin, maar een commissie die het leren van gemeenten moet bevorderen.

De afgelopen twee jaar hebben we een enorme ontwikkeling gezien en doorgemaakt. We hebben bij gemeenten een onmiskenbare ontwikkeling waargenomen, maar ook wij zelf kregen in de loop van onze bezoeken steeds beter inzicht. Het onderwerp informatieveiligheid is in de afgelopen twee jaar ook steeds nadrukkelijker in de media opgepikt en heeft aan relevantie gewonnen. De laatste bezoeken merkten we, anders dan bij de eerste bezoeken, dat het belang van het onderwerp niet meer ter discussie staat. Informatieveiligheid komt inmiddels vrijwel iedere week terug op de voorpagina's van de kranten; hierdoor is dat dus overigens ook niet vreemd.

Gemeenten zijn sinds de 'wake up call' in 2011 naar aanleiding van DigiNotar en Lektober aan de slag gegaan met het onderwerp informatieveiligheid. In de afgelopen periode zijn aanzienlijke stappen gezet. Zo is in de afgelopen jaren de Informatiebeveiligingsdienst voor gemeenten (IBD) voor gemeenten uitgegroeid tot een vertrouwde en professionele partner van gemeenten. Parallel aan de toegenomen aandacht voor informatieveiligheid bij gemeenten dringt zich ook het besef op dat er nog veel te doen is. De bekendheid met de risico's neemt toe, zo constateren wij, maar er zijn ook continu nieuwe en grotere risico's. Het werken aan informatieveiligheid is dus 'nooit af'. Een gevaar van die constatering is dat het beeld kan ontstaan dat er te weinig zou gebeuren bij gemeenten. Dat is niet juist: er gebeurt veel, maar dat geldt ook voor de ontwikkelingen die op de gemeenten afkomen. We zullen als gemeenten dus geen rust kunnen nemen op het onderwerp informatieveiligheid. Ons eindverslag heeft dan ook niet als focus om te beschrijven 'wat er allemaal bereikt is', maar biedt een aanzet voor wat de logische vervolgstappen zijn.

We willen dit eindverslag evenmin gebruiken om 'lijstjes' van koplopers en achterblijvers te maken. Voor zover we een foto hebben kunnen maken met onze bezoeken, is het beeld bewegend: de gemeenten die wij twee jaar terug bezochten zullen inmiddels progressie hebben geboekt. Een 'foto' heeft om die reden geen toegevoegde waarde.

Graag zou ik ook vanaf deze plaats alle gemeenten die wij hebben bezocht willen bedanken. We hebben veel gezien en ook veel mogen zien dankzij een open en gastvrije cultuur! Door als gemeenten onderling kennis te (blijven) delen, kunnen we het leren versnellen.

Frans Backhuijs
voorzitter visitatiecommissie Informatieveiligheid

Belangrijkste boodschappen van de visitatiecommissie

1. De beveiliging van informatie is een wereldwijde uitdaging en de wereld is tijdens de ronde van de visitatiecommissie de afgelopen twee jaar snel veranderd. Cybercriminaliteit wordt vernuftiger, de digitale infrastructuur wordt complexer, de techniek geavanceerder en IT-systemen worden meer en meer aan het internet gekoppeld. Gemeenten beschikken over een schat aan informatie van burgers en bedrijven en kunnen hierdoor een gericht doel van criminaliteit of spionage zijn. Dit besef moet bij diverse gemeenten nog dieper doordringen.
2. Informatiebeveiliging draagt bij aan de kwaliteit en continuïteit van de gemeentelijke dienstverlening, maar het conflicteert soms met gebruikersvriendelijkheid of de functionaliteit. Informatieveiligheid vergt bovendien expliciete aandacht naast privacy en integriteit. Het leggen van de verbinding tussen deze onderwerpen en perspectieven helpt om de dilemma's onder ogen te zien en bewuste keuzes te maken.
3. De commissie ziet dat alle gemeenten werken aan informatieveiligheid en constateert dat de aandacht toeneemt. Het tempo waarmee de aandacht toeneemt is vaak nog te langzaam. Zelfregulering gaat immers niet vanzelf. Het systeem van verplichtende zelfregulering kan versterkt worden als de gemeenten ook op bestuurlijk niveau aangesproken worden vanuit de VNG/IBD.
4. Actieve betrokkenheid van het bestuur is van groot belang voor prioriteitstelling binnen de gemeentelijke organisatie. In het algemeen verdient de bestuurlijke aandacht voor informatieveiligheid versterking. De introductie van de Eenduidige Normatiek Single Information Audit (ENSIA) maakt dit nóg meer noodzakelijk, ter voorkoming dat de verantwoording over informatieveiligheid alleen een papieren realiteit is.
5. Het op een hoger plan brengen van informatieveiligheid vereist dat de functie van chief information security officer (CISO) goed gepositioneerd is, wat in elk geval betekent dat de CISO een onafhankelijke positie heeft. De CISO moet midden in de organisatie staan en uitdrukkelijk ook aandacht hebben voor de harde kant van informatieveiligheid. De CISO dient daarom over voldoende technische kennis en bestuurlijke empathie te beschikken.
6. CISO's doen er goed aan om hun kennis (in regionaal verband) te delen. CISO's versterken elkaar op deze manier en kunnen voor elkaar inspringen. Ook kunnen kleinere gemeenten samen één CISO delen.
7. Naar mate het bewustzijn in de organisatie groeit, neemt ook de aandacht voor technische maatregelen weer toe. Gemeenten staan sterker als zij gezamenlijk optrekken bij het investeren in systemen en het implementeren van technische maatregelen. De commissie bemerkt in haar gesprekken een breed draagvlak voor een intensievere samenwerking en de commissie roept VNG op om in het kader van Samen organiseren ook wat betreft het onderwerp informatieveiligheid een stimulerende en coördinerende rol te vervullen.
8. Gemeenten kunnen veel van elkaar leren. Het uitwisselen van kennis in landelijke en regionale netwerken moet veel structureler worden. Te vaak vinden gemeenten nu het wiel opnieuw uit, terwijl gemeenten aangeven dat zij graag bereid zijn om elkaar te helpen. Ook is nog veel te leren van de semi-publieke sector en het bedrijfsleven. De Informatiebeveiligingsdienst voor gemeenten (IBD) dient de kennisuitwisseling nog uitdrukkelijker te faciliteren, bijvoorbeeld door een netwerk van CISO's in het leven te roepen. Het samen durven leren van gemaakte fouten is cruciaal.
9. De verantwoordelijkheid van gemeenten voor informatieveiligheid geldt over de hele linie, van inhuurkracht tot raadslid, voor leveranciers, met ketenpartners en samenwerkingsverbanden. Het vergt een enorme inspanning om deze verantwoordelijkheid waar te maken. De aandacht voor informatieveiligheid moet structureel zijn en het kan goed zijn om incidenten te benutten. Een goed ingericht en onderhouden Information Security Management Systeem (ISMS) zal daar zeker aan bijdragen.

10 Bij het onderwerp informatieveiligheid bestaat er een spanning tussen openheid, die nodig is om te kunnen leren – en geslotenheid, die nodig is om bescherming te bieden tegen bedreigingen. Wij geloven dat een meer open houding mogelijk is. Meer openheid zal leiden tot een versnelling van het leren, door het delen van kennis en het samen leren van incidenten. Een actieve communicatie over de risico's en incidenten draagt bij aan het besef dat 100% veilig niet mogelijk is.

11 Gemeenten werken in sterke mate samen met hun leveranciers. Het IT-landschap van gemeenten is over het algemeen erg complex en bevat vaak verouderde en kwetsbare IT-systemen. Het is belangrijk om bij het inkopen en inhuren van IT-diensten duidelijke afspraken te maken over de informatiebeveiliging. Daarnaast is het cruciaal om periodiek de IT-omgeving te laten onderzoeken op kwetsbaarheden. Door inzicht en controle te hebben op de kwetsbare plekken, kan informatiebeveiliging een enorme impuls krijgen.

12 Samenwerking is de crux: overheden moeten de krachten bundelen om de bedreigingen het hoofd te bieden. Dit vereist een beweging van een discussie over reguleren en controleren 'door' het Rijk naar een discussie over echte samenwerking 'met' en faciliteren door de Rijksoverheid. Gedetailleerde landelijke wet- of regelgeving is geen oplossing. Wel zien wij reden om de verantwoordelijkheid voor informatieveiligheid in bijvoorbeeld de gemeentewet te verankeren, zoals dit ook bij het onderwerp integriteit is gebeurd.

De context: een aantal belangrijke parallelle ontwikkelingen

Het centrale onderwerp van dit verslag is informatieveiligheid. Het werken aan informatieveiligheid staat echter niet op zichzelf. Informatieveiligheid is verbonden aan een groot aantal ontwikkelingen. De drie belangrijkste ontwikkelingen zijn:

ENSIA

Elk jaar moeten gemeenten zich verantwoorden over de kwaliteit van de informatieveiligheid van diverse informatiesystemen. Verantwoording houdt iedereen scherp. Het is daarbij van belang hoe deze verantwoording wordt afgelegd. Om daarin te voorzien en de administratieve lasten te beperken is het project dat zich richt op het realiseren van een Eenduidige Normatiek Single Information Audit (ENSIA) opgezet. De verticale verantwoording (aan het ministerie van BZK) kan worden gebaseerd op de integrale horizontale verantwoording (aan de gemeenteraad) over de gemeentelijke veiligheidsaanpak. De gemeenteraad heeft in dit verband een eigen rol die bovendien toeneemt in belang.

Samen organiseren

Het gevoel dat we in Nederland een te gecompliceerd landschap van per gemeente verschillende informatiearchitectuur hebben wordt steeds meer gedeeld. Er lopen al veel gezamenlijke projecten om de dienstverlening en informatievoorziening in gemeenten te verbeteren. Alleen door de samenwerking op een grotere schaal te organiseren, kunnen gemeenten werkelijk innoveren en de dienstverlening up-to-date krijgen. Het idee achter de keuze om deze zaken samen te organiseren is: wat we samen kunnen doen, moeten we ook samen doen. Samenwerking van gemeenten met elkaar en tussen de overheidslagen om zo een meer overzichtelijke en eenvoudiger I-basisarchitectuur te maken heeft een positief effect op de risico's van informatieveiligheid. En daarnaast of daarbinnen zo u wilt, passen gemeenten maatwerk toe, afgestemd op hun lokale situatie. De VNG geeft hier namens gemeenten invulling aan via de Digitale Agenda 2020.

Privacy en de Algemene Verordening Gegevensbescherming[1]

Door de (nieuwe) Europese wetgeving, de technische mogelijkheden en de decentralisaties wordt het veld rond privacy voor gemeenten steeds complexer. Privacy is niet langer een onderwerp waar alleen juristen mee bezig zijn; privacy raakt de hele gemeentelijke organisatie. Gemeenten zijn nu bezig om de brede privacy benadering te borgen in de organisatie, zoals bijvoorbeeld door het aanstellen van een functionaris gegevensbescherming.

1 De AVG is reeds in werking getreden en wordt per 25 mei 2018 ook van toepassing. De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.

1 Onze waarnemingen en indrukken

Wij zullen eerst onze waarnemingen en indrukken presenteren. In een aantal gevallen ontkomen we er niet aan om ook al een aanzet te geven tot de bijbehorende handelingsperspectieven. Onze adviezen volgen in het tweede deel van dit eindverslag

Over de hele linie boeken gemeenten vooruitgang maar het tempo moet omhoog, de verplichtende zelfregulering vereist echter om elkaar te blijven aanspreken

Over de hele linie zien we dat gemeenten werk maken van informatieveiligheid. De afgelopen twee jaar hebben wij gezien dat gemeenten een duidelijke ontwikkeling en professionalisering hebben doorgemaakt. De laatste gemeenten die wij bezochten in mei 2017 zijn al weer verder gevorderd dan de 'beste' gemeenten die wij bezochten bij onze start in de tweede helft van 2015.
De verantwoordelijkheid voor informatieveiligheid ligt bij de individuele gemeente. Maar gemeenten dragen ook een gezamenlijke verantwoordelijkheid. Het raakt gemeenten als collectief, zo hebben wij ons in toenemende mate gerealiseerd, wanneer een beperkt aantal gemeenten onvoldoende werk maakt van informatieveiligheid.

> *Het is noodzaak voor álle gemeenten om de zelfregulering, waartoe zij zichzelf hebben verplicht, ook serieus te nemen.*

Zo leiden incidenten bij de ene gemeente regelmatig tot raadsvragen bij andere gemeenten en soms zelfs ook tot Kamervragen. Het is daarom van groot belang dat gemeenten elkaar blijven aanspreken en ondersteunen, zoals in verenigingsverband.

De omvang van de gemeente is geen goede indicator voor het op orde zijn van de informatieveiligheid, maar wel bepalend voor de aanpak. De Baseline Informatiebeveiliging Gemeenten (BIG) biedt, waar het gaat om de specifieke invulling, ruimte per gemeente. Dat is ook goed want wat in de ene gemeente werkt, hoeft in de andere gemeente niet noodzakelijkerwijs ook zo te werken. Zo is bijvoorbeeld relevant wat de omvang van de gemeentelijke organisatie is. Sommige gemeenten hebben een relatief kleine organisatie en korte lijnen en daarmee zijn andere uitdagingen gemoeid dan in grote gemeentelijke organisaties, met langere lijnen. Wij constateren ook dat de professionaliteit en kwaliteit van gemeenten niet samenhangt met de omvang van de gemeente. Het beeld dat de grotere gemeenten het professioneler en kwalitatief beter doen dan de kleinere gemeenten is simpelweg niet juist. Dat gezegd hebbende, kwamen wij bij zeer kleine gemeenten wel regelmatig het probleem van onvoldoende specialisatie tegen. Daarnaast hebben wij uit de bezoeken opgemaakt dat de kwaliteit en professionaliteit van een gemeente sterk zijn verbonden met, en leunen op individuele medewerkers binnen de gemeentelijke organisatie. Regelmatig zagen we ook dat informatieveiligheid bij gemeenten nog niet voldoende bestuurlijk is ingebed en nog onvoldoende terugkomt in de organisatiestructuur en -cultuur.

De gemeenten die het verste zijn, maken zich meer zorgen dan gemeenten die minder ver zijn: die zorgen zijn terecht

Het lijkt paradoxaal, maar onze waarneming is dat gemeenten waarbij het bewustzijn groter is ook de zorgen groter zijn. Wij hebben als commissie zelf ook een dergelijke ontwikkeling doorgemaakt. Lang niet alle gemeenten beseffen dat zij interessant zijn voor bijvoorbeeld spionage en andere gerichte aanvallen. Het gaat hierbij bovendien niet alleen om de diefstal van gegevens, maar ook over de juistheid en beschikbaarheid daarvan. De realisatie dat gemeenten over een schat aan informatie van burgers én bedrijven beschikken, en om deze reden gericht aangevallen en bespioneerd kunnen

worden vanuit binnen- en buitenland, lijkt nog onvoldoende doorgedrongen. Dit zet ons ook aan het denken. De professionalisering van gemeenten gaat hard, maar ook de uitdagingen nemen in hoog tempo toe. Weten de gemeenten in deze rat race de relatieve afstand te verkleinen ten opzichte van de steeds toenemende bedreigingen? Wij hebben zorgen of de gemeenten het, gegeven de complexiteit van de uitdagingen, wel goed kúnnen doen.

Meer structuur is nodig, maar ook het gevaar van de papieren tijger dreigt

We constateren dat gemeenten nog te vaak ongestructureerd werken aan informatieveiligheid. Door de 'waan van de dag' zijn zij soms te druk met de uitvoering en komen daardoor niet toe aan het aanbrengen van structuur. Het is gewenst dat gemeenten het werken aan informatieveiligheid structureren langs een vastgesteld informatieveiligheidsbeleid, via een risicoanalyse (GAP-analyse) en impactanalyse, naar (bestuurlijk gedragen) benoemde prioriteiten in een uitvoeringsplan (PLAN) en vervolgens naar daadwerkelijke uitvoering (DO), monitoring-evaluatie (CHECK) en bijsturing (ACT). Een goed ingericht en onderhouden ISMS is daarbij van cruciaal belang. De BIG implementeren is géén eenmalige actie, maar een continue proces. Om die reden is het ook zinvol om periodiek een GAP-analyse uit te voeren.
Het beeld dat wij krijgen is echter niet eenduidig. Te vaak zagen wij dat het juist schort aan uitvoering omdat alle energie gaat zitten in de afstemming over lijvige beleidsdocumenten. Het is van belang dat de BIG ruimte toelaat voor maatwerk. Gemeenten kunnen dit nog beter benutten. De BIG is dan ook uitdrukkelijk geen 'afvinklijstje'. Op basis van het *pas toe of leg uit* principe *kiezen* gemeenten ervoor om bepaalde maatregelen uit de BIG niet of later te implementeren. Als je je dat realiseert is een goede koers te bepalen tussen de klippen van een overgestructureerde aanpak en een intuïtieve pragmatische aanpak. Het is wel zaak dat deze gekozen koers ook bestuurlijk gedragen is.

De bestuurlijke aandacht moet nog verder versterkt worden

Wij hebben een breed spectrum voorbij zien komen waar het gaat om de bestuurlijke aandacht voor informatieveiligheid. Van zeer actieve, goed ingevoerde bestuurders, tot bestuurders die het onderwerp vrijwel volledig aan de ambtelijke organisatie overlaten als een bedrijfsvoeringsvraagstuk. Informatieveiligheid is in de meeste gemeenten geen politiek onderwerp. Tenzij het misgaat. In het algemeen menen wij dat de bestuurlijke aandacht en betrokkenheid nog verder versterkt moet worden. De beperkte bestuurlijke aandacht is naar onze indruk niet het gevolg van onwil maar van een gebrek aan kennis van digitalisering en informatieveiligheid. Wij menen dat wanneer informatie over de inwoners en bedrijven in een gemeente even belangrijk wordt gevonden als de financiën,

10 In het oog springende informatieveiligheidsincidenten

1. Wankelende wethouders, http://destadamersfoort.nl/lokaal/datalek-wankelende-wethouders-en-dreigende-miljoenenboete-119074
2. Schade haven Rotterdam, https://www.nrc.nl/nieuws/2017/06/27/aanval-met-ransomware-op-containerbedrijf-haven-rotterdam-a1564693
3. Beïnvloeding presidentscampagne USA, https://informatiebeveiliging.nl/nieuws/russen-hackten-witte-huis/
4. Hack stroomnetwerk Oekraïne, https://tweakers.net/nieuws/119907/oekraiense-stroomnetwerk-is-opnieuw-getroffen-door-hackers.html
5. "Hack" Almelo, https://www.gelderlander.nl/digitaal/slachtoffers-almelo-hack-staan-compleet-machteloos~abf886fc/
6. Responsible disclosure voor 80 gemeenten, https://ibestuur.nl/podium/veiligheid-verbeteren-door-samenwerking-responsible-disclosure
7. Rekenkamer Rotterdam onderzoekt informatieveiligheid, https://nos.nl/artikel/2166818-veiligheidsrisico-voor-aboutaleb-door-zwakke-ict-beveiliging.html
8. Meer meldingen datalekken gemeenten, https://nos.nl/nieuwsuur/artikel/2172451-meer-meldingen-van-datalekken-door-gemeenten.html
9. Datalek ziekenhuizen, http://www.nu.nl/internet/4203392/datalek-ziekenhuizen-treft-ruim-200000-patienten.html
10. Hack gemeente Hellevoetsluis, http://www.ad.nl/voorne-putten/uitgelachen-joker-hackte-uit-wraak~adff46ab/

Leren van parallellen met fysieke veiligheid

Luchtvaart
Fouten worden gemaakt. Overal en door iedereen. Daar is helaas nooit een 100% garantie te geven. Dit geldt ook voor de luchtvaartsector. Desondanks is vliegen de meest veilige manier van reizen geworden. De luchtvaart is koploper als het gaat om leren van gemaakte fouten. Een werkcultuur is ontstaan waarin het maken van fouten wordt gezien als een mogelijkheid om te leren. Onderzoek naar luchtvaartincidenten richt zich dan ook niet noodzakelijk op gemaakte fouten, of door wie ze zijn gemaakt. Veel meer wordt gekeken naar wat de oorzaak van de fout is en hoe het komt dat deze fout tot dan toe onopgemerkt is gebleven.
De gemeenten kunnen voor het verstevigen van informatieveiligheid verschillende lessen van de luchtvaartsector leren:

- Creëer een werkcultuur waarbij onveilige situaties worden gemeld
- Zorg dat geaccepteerd wordt dat fouten maken inherent is aan 'normale' operationele processen
- Focus niet (enkel) op de schuldvraag wanneer een incident plaatsvindt, kijk ook naar het leren van lessen
- Deel informatie over vergissingen en incidenten

dit zich ook in bestuurlijke aandacht moet vertalen. Ook door de ontwikkeling rondom ENSIA, en de cruciale rol die de raad in deze verantwoordingssystematiek speelt, zal de bestuurlijke aandacht verder toe (moeten) gaan nemen. Het is voor raden van groot belang om de juiste kennis en expertise te verzamelen om hun controlerende rol goed in te vullen. Daarnaast hebben we bij diverse gemeenten ook zorgen opgetekend of de doelstelling om de administratieve lasten beperkt te houden, ook echt wordt bereikt. We roepen VNG op om hier goed oog voor te (blijven) houden.

Gemeenten zijn voorstander van het uitwisselen van kennis, maar kunnen elkaar nog beter opzoeken

In toenemende mate kregen wij van gemeenten de begrijpelijke vraag: "Waarom vinden we toch allemaal het wiel zelf uit?" We hebben op dit vlak een duidelijke cultuurverandering waargenomen; het gaat niet meer over de vraag 'of' er draagvlak is voor samenwerking maar echt over 'hoe' dit draagvlak te vertalen naar concrete actie.
Soms merkten wij onbekendheid met initiatieven die er al zijn. Er is een grote hoeveelheid aan informatie beschikbaar via de Informatiebeveiligingsdienst voor gemeenten (IBD) en de IBD community. Tegelijkertijd wordt beschikbare kennis onvoldoende gedeeld. Bestuurders dienen naar onze mening kennis te nemen van de maandelijkse IBD-monitor, waarin ook de NCSC-monitor is meegenomen,[1] over actuele bedreigingen. Daarnaast dienen bestuurders de actieve kennisuitwisseling te stimuleren. We hebben tijdens onze bezoeken ook zeer betrokken, creatieve bestuurders en ambtenaren gesproken.

Gemeenten staan daarbij zonder uitzondering zeer open voor het onderlinge delen van kennis.

De uitdaging ligt in hoe de beschikbare kennis een weg vindt naar andere gemeenten. We zien dat CISO's en bestuurders in de regio elkaar in toenemende mate opzoeken. We juichen die ontwikkeling toe, maar dit moet nog meer de standaardpraktijk worden. Het is van belang dat gemeenten een actieve houding aannemen; het contact met andere gemeenten is eenvoudig te leggen.

De mens is een belangrijke schakel, er zijn talloze manieren om het bewustzijn in de organisatie te stimuleren

Technische maatregelen voorkomen veel incidenten, maar de menselijke factor is eveneens cruciaal. Dit besef is inmiddels in alle gemeenten doorgedrongen. Bij alle gemeenten is bewustwording benoemd als hoge prioriteit. Juist op dit vlak kunnen gemeenten veel van elkaar leren, over effectieve

1 Nationaal Cyber Security Centrum

aanpakken en allerlei – vaak gratis te hergebruiken– materiaal gericht op bewustzijnsverhoging uitwisselen. Het is logisch dat naar mate het bewustzijn toeneemt, ook het aantal meldingen van incidenten zal toenemen. Hoewel het daardoor kan lijken alsof het *minder* goed gaat, is juist het omgekeerde het geval. Het past binnen de leercyclus: een ontwikkeling van onbewust onbekwaam naar bewust (on)bekwaam.
Het is daarbij van belang dat incidenten goed gemonitord worden. Door incidenten te registreren, te melden bij de IBD, worden de 'rode draden' en trends duidelijk. Deze rode draden kunnen op hun beurt dienen als basis en focus voor een campagne op maat met aansprekende voorbeelden, die aansluiten bij de concrete dilemma's die op de werkvloer spelen. We zien dat veel gemeenten in hun bewustzijnscampagnes nog een stap moeten maken om goed aan te sluiten bij de verschillende doelgroepen in de gemeentelijke organisatie (in de lijn, de staf en het bestuur).

Informatieveiligheid in formele samenwerkingsverbanden, bij leveranciers en in ketens is een punt van aandacht, gemeenten dienen hun opdrachtgevende rol actiever in te vullen

In algemene zin is samenwerking in formele samenwerkingsverbanden, met leveranciers en in ketens een belangrijk aandachtspunt. Het sturen op informatieveiligheid is – en blijft – een eigen verantwoordelijkheid van de individuele gemeenten. Denk hierbij bijvoorbeeld aan de taakuitvoering in het sociaal domein. Deze verantwoordelijkheid voor informatieveiligheid wordt daar weliswaar in toenemende mate gevoeld, maar is nog lang niet altijd omgezet in een actieve invulling van het opdrachtgeverschap. Het groot aantal verbindingen van gemeenten in een 'lappendeken' van samenwerkingsverbanden zorgt voor onoverzichtelijkheid. Dit maakt het sturen op informatieveiligheid complex, zeker ook omdat niet alle relaties in beeld zijn, verantwoordelijkheden niet duidelijk zijn, de informatievoorziening vanuit de partners te wensen over laat of omdat 'in huis' onvoldoende kennis aanwezig over hoe als opdrachtgever actief gestuurd kan worden op informatieveiligheid.

10 Belangrijke constateringen

1. Gemeenten beschikken over een schat aan informatie van burgers en bedrijven. Er zijn aanwijzingen dat bedrijven bespioneerd worden via de informatie die over die bedrijven bij de gemeente rust.
2. Het werken aan informatieveiligheid, implementeren van de BIG en het aansluiten op stap 4 bij IBD is 'nooit af' maar een continu proces.
3. Pas toe of leg uit; de BIG laat ruimte voor lokaal maatwerk, maar dan wel op basis van bewuste en gedragen keuzes. Dit neemt niet weg dat er wel een ondergrens is!
4. Een toegenomen aantal meldingen van incidenten in uw gemeente is waarschijnlijk het gevolg van een vergroot bewustzijn in uw organisatie en daarmee een goed teken.
5. We weten niet wat we niet weten, ofwel: "There are also unknown unknowns – the ones we don't know we don't know."[1] Daarom is het van belang om structureel werk te maken van informatieveiligheid.
6. Informatie is vergelijkbaar met geld. College en raad moeten net zo actief op informatie sturen als op financiën.
7. Informatieveiligheid vraagt op drie vlakken aandacht: voor de techniek, voor een passende organisatie-inrichting en voor houding en gedrag bij alle medewerkers.
8. Het is van belang om actief te sturen op informatieveiligheid in formele samenwerkingsverbanden (denk aan: sociale dienst, belastingsamenwerking) en bij leveranciers.
9. "Never let a good crisis go to waste"2
10. Doe niet alles tegelijk: maak keuzes, stel prioriteiten en verzeker dat deze bestuurlijk gedragen zijn.

1 Secretary of Defense Donald H. Rumsfeld, February 12, 2002.
2 Winston Churchill.

2 Onze adviezen: het handelingsperspectief

Perspectieven voor de individuele gemeenten

Wees transparant over incidenten, leer ervan en realiseer dat de risico's niet geheel zijn uit te sluiten
Het leren van (elkaars) incidenten is cruciaal voor gemeenten om te professionaliseren op het gebied van informatieveiligheid. Het is van belang dat binnen de gemeenten incidenten en 'near incidents' niet in de eerste plaats aanleiding zijn om af te straffen maar vooral gebruikt worden om te leren. Dit vergt een cultuur waarin gemeenten transparant en eerlijk zijn over incidenten en hiervan willen leren. Angst voor schandalen en een afrekencultuur werken verlammend voor het leren. Het helpt om op zowel ambtelijk als bestuurlijk niveau te realiseren dat risico's niet zijn uit te sluiten en hier open over te communiceren.

Beschouw informatie als een even belangrijk onderwerp als de financiën
Gemeenten realiseren zich dat zij beschikken over zeer gevoelige en vertrouwelijke informatie over haar burgers. Dit is nog eens versterkt vanwege de drie decentralisaties in het sociale domein. Daarnaast beschikken gemeenten ook over zeer gevoelige informatie van bedrijven. Daarmee kunnen gemeenten bovendien een steeds aantrekkelijker doelwit worden voor spionage. Voor ons is dit reden om informatie over de inwoners en bedrijven als even belangrijk te kwalificeren als de gemeentelijke financiën. Bestuurders moeten zich eigenaar voelen van beide onderwerpen. Het professionaliseren van de sturing op financiën in de jaren '70-80 heeft lang geduurd. Een hoger tempo is noodzakelijk als het gaat om de professionalisering op het gebied van informatieveiligheid. In praktische zin zien wij dat het helpt om de verbinding te leggen tussen integriteit, informatieveiligheid, privacy, en continuïteit van dienstverlening. Ook moeten de controller en de CISO een vergelijkbare – onafhankelijke – rol en positie in de organisatie hebben.

Heb oog voor informatieveiligheid aan de voorkant en in relatie tot dienstverlening
Informatieveiligheid kan niet verbeterd worden zonder *security by design* en waar mogelijk het versimpelen van processen. Dit heeft een positieve uitwerking op zowel de kwaliteit van dienstverlening, efficiency en op informatieveiligheid. Dienstverlening heeft ook haar grenzen, omdat juist de toenemende verknoping van data en systemen een informatieveiligheidsrisico herbergt.

> *Stel de vragen over informatieveiligheid dus reeds bij het ontwikkelen van nieuwe initiatieven en vraag uzelf af of het ook simpeler kan.*

Versterk de bestuurlijke aandacht door het college en de raad te betrekken
In veel gemeenten kunnen de bestuurders nog beter betrokken zijn bij het onderwerp informatieveiligheid. Het verbeteren van de informatieveiligheid in gemeenten is een *chefsache*. Het gaat dan niet alleen om 'informeren', maar ook echt om het gesprek aan te gaan met bestuurders. Naast de reguliere mogelijkheden die de P&C-cyclus biedt, kan het gesprek worden gevoerd op basis van het uitvoeringsplan, door te informeren over het dreigingsbeeld, als onderdeel van politiek-urgente vraagstukken of door het organiseren van themasessies. Op structurele basis kunnen koppelingen worden gelegd met onderwerpen zoals financiën en de veranderingen in het sociaal domein, ontwikkelingen rondom Big Data, maar ook de relatie van informatieveiligheid tot privacy & integriteit. Door informatieveiligheid te benoemen als randvoorwaarde voor dienstverlening, kan eveneens een toekomstgericht gesprek worden gevoerd. Raad en college beschikken, als bestuurder, zelf ook over

10 Concrete suggesties om informatieveiligheid in uw gemeente op een hoger plan te krijgen

1. Leg de verbinding tussen informatieveiligheid en de onderwerpen privacy, integriteit en (continuïteit van) dienstverlening.
2. Werk samen in de regio, op bestuurlijk en ambtelijk vlak. Verlies geen tijd aan lastige discussies over de formele inbedding. Het onderling delen van waardevolle lessen kan ook informeel.
3. Zorg dat uw CISO beschikt over een intern (informeel) netwerk, door ambassadeurs in de organisatie aan te stellen die vanuit zichzelf al affiniteit hebben met het onderwerp informatieveiligheid. Zorg voor periodieke scholing en werk gestructureerd aan kennisontwikkeling van deze groep.
4. Neem bij alle nieuwe voorstellen een aparte paragraaf op in college- en raadsstukken over de impact van het voorstel op informatieveiligheid.
5. Schoon het applicatielandschap op en laat periodiek uw applicaties onderzoeken op kwetsbaarheden. Stel ongebruikte applicaties buiten werking en stoot deze af: dit is goedkoper én veiliger.
6. Lees (als bestuurder) de maandelijkse monitor van de IBD en het NCSC. Uw CISO kan voor u organiseren dat u deze monitors ontvangt.
7. Wijs de raadsleden op het belang van informatieveiligheid vanuit hun eigen rol en functie – ook de raad beschikt over vertrouwelijke informatie.
8. Activeer uw organisatie met een oefening rond een informatieveiligheidscrisis.
9. Organiseer een bijeenkomst (bijvoorbeeld een ontbijt) met het college en het lokale bedrijfsleven over informatieveiligheid en leer van elkaars lessen en successen.
10. Organiseer een 'week van de informatieveiligheid' en maak een ronde door het gemeentehuis en signaleer welke vertrouwelijke informatie rondslingert. Spaar de bestuurders en de gemeentesecretaris niet!

gevoelige informatie en maken gebruik van de ICT-voorziening van de gemeente. Ook dit geeft aanknopingspunten voor een toekomstgerichte dialoog over informatieveiligheid. Het werkt goed om college-en raadsleden die al affiniteit hebben met het onderwerp daarbij te benutten.

Oefen met crisissituaties

Voor bestuurders is het in het geval van een crisis van belang om te weten i) welke vragen moet ik stellen, ii) welke kwaliteiten heb ik nodig en iii) wie is aan zet om beslissingen te nemen? Alleen de ramp die al gebeurd is, kun je goed voorbereiden. Het gaat, ook bij informatieveiligheid, om een zekere routine in het onvoorspelbare en om flexibiliteit. Net als bij crisissituaties rond fysieke veiligheid is het van belang te oefenen met een crisissituatie op het gebied van informatieveiligheid. Denk daarbij bijvoorbeeld aan de door de IBD uitgebrachte crisisgame. Een ander mooi gevolg van een oefening is dat het onderwerp meer in de bestuurlijke aandacht komt te staan.

Borg een goede positionering van de CISO en zorg dat de CISO kan beschikken over een intern netwerk in de organisatie

Nog niet alle gemeenten hebben een CISO aangesteld en/of de CISO positie voldoende geborgd. In alle gevallen is het van belang dat de CISO onafhankelijk is gepositioneerd, een directe rapportagelijn heeft naar de (eindverantwoordelijke) gemeentesecretaris en de (bestuurlijk) portefeuillehouder en daarmee periodiek overleg heeft. Daarnaast dient de CISO verbonden te zijn met de ambtelijke organisatie en het primaire proces. Het is voor een CISO echter niet doenlijk (en ook niet zijn rol) om te nauw betrokken te zijn bij de specifieke werkprocessen. Het instellen van ambassadeurs in de lijn, is een goede eerste stap om de aansluiting met het primaire proces te verankeren en de verantwoordelijke lijnmanagers te ondersteunen. Hierdoor kan de CISO terugvallen op een (informeel) netwerk in de organisatie en op die manier zijn of haar slagkracht in de lijn vergroten. We roepen op om bij de werving van ambassadeurs medewerkers te benaderen die vanuit zichzelf al affiniteit en enthousiasme voor het onderwerp informatieveiligheid hebben.

Sluit aan tot en met stap 4 bij de IBD

Ongeveer tweederde van de gemeenten is inmiddels tot en met stap 4 aangesloten bij de IBD.

Leren van parallellen met fysieke veiligheid

De brandweer
Natuurlijk blust de brandweer branden. Vaak kan de brandweer erger voorkomen, maar een deel van het leed is dan al geschied. Om schade en het aantal slachtoffers te verminderen, is de brandweer 'een strategische reis' begonnen naar een nieuwe brandweerorganisatie. De brandweer zet nu meer energie in aan de voorkant van de veiligheidsketen. Een groot deel van de activiteiten van de brandweer richt zich op preventie en het maken van afspraken met allerlei partijen. Ook de inzet van de burger zelf speelt een belangrijke rol, zij hebben de meeste invloed op de brandveiligheid in hun eigen omgeving.
De gemeenten kunnen voor het verstevigen van informatieveiligheid verschillende lessen van de brandweer leren:

- Heb aandacht voor preventie én bestrijding
- Ga samenwerkingsverbanden aan met andere partijen
- Maak mensen bewust van de risico's en gevaren op het gebied van informatieveiligheid

Aansluiting tot en met stap 4 stelt de IBD in staat om gericht te kunnen waarschuwen bij concrete incidenten en bedreigingen. We benadrukken het belang dat ook de resterende gemeenten tot en met stap 4 aansluiten bij de IBD. Concreet gaat het vaak nog om het doorgeven van een lijst met IP-adressen en URL's (stap 3) en een gemeentelijke ICT-foto (stap 4). We krijgen regelmatig te horen dat een gemeente nog bezig is om 'het overzicht compleet te krijgen'. Dat is nadrukkelijk niet een doel op zich; de gemeente moet slechts nagaan over welke systemen (soft- en hardware) zij actief geïnformeerd willen worden en deze lijst up-to-date houden. Op ieder moment zijn wijzigingen in de hard- en software door te geven. Aansluiten tot en met stap 4 is dan ook géén eenmalige actie maar een (permanent) proces.

Voer periodiek een penetratietest uit
Het doel van een penetratietest is het verkrijgen van inzicht in de status en effectiviteit van de beveiligingsmaatregelen. Het resultaat geeft aan wat de aandachtsgebieden zijn en biedt concrete handvatten voor adequate maatregelen en investeringen, met als doel de beveiligingsrisico's te verkleinen. Het geeft inzicht in de gevonden inbraakmogelijkheden, de genomen maatregelen en de restrisico's en het geeft de mogelijkheid hierover aan het management te rapporteren. Een penetratietest kan ook worden ingezet als onderdeel van een bewustwordingscampagne om de bewustwording van de medewerkers te verhogen. De IBD heeft hierover een handreiking uitgebracht[1].

Perspectieven voor de gemeenten in combinatie met andere overheden en bedrijven

Versterk de positie en slagkracht van IBD
De IBD heeft een belangrijke positie bij het werken aan informatieveiligheid en heeft draagvlak bij de gemeenten vanwege haar inhoudelijke deskundigheid.

> *Het ontbreekt echter nog aan een gremium dat op bestuurlijk vlak zo nodig de noodklok kan luiden en kan interveniëren.*

Denk daarbij aan de situatie dat de CISO binnen zijn of haar eigen gemeente ziet dat het niet goed gaat, maar onvoldoende gehoor vindt bij het bestuur. De IBD werkt op basis van vertrouwelijkheid en heeft nu geen rol om toezicht te houden of gemeenten tot de orde te roepen. Het versterken van de slagkracht bij de IBD in termen van mensen en middelen is hoe dan ook wenselijk. Daarnaast zal naar een 'bovengemeentelijk' instrument gezocht moeten worden, dat ingezet kan worden bij waargenomen incidenten of structurele problemen bij gemeenten en dan ook handelingsperspectief biedt. De verplichtende zelfregulering verdient op dit vlak versterking.

1 Handreiking penetratietesten https://www.ibdgemeenten.nl/downloads/?id=2157

Investeer in landelijke en regionale kennisnetwerken

Het delen van kennis en ervaring vraagt op een viertal plekken om het verstevigen van netwerken. Ten eerste is er het overkoepelende landelijke niveau waarbij rijk, provincies, gemeenten, waterschappen, NCSC en IBD betrokken zijn. Op dit niveau is momenteel nog onvoldoende gestructureerde kennisuitwisseling. Ten tweede is kennisuitwisseling op regionaal niveau tussen CISO's en bestuurders van belang. Ondanks vele initiatieven op dit vlak, menen wij dat dergelijke samenwerkingen verdere intensivering en versterking verdienen. Het is zinvol om daarbij zoveel mogelijk bij reeds bestaande verbanden aan te knopen. Het is het onderzoeken waard of bijvoorbeeld de veiligheidsregio een meer prominente rol kan vervullen op het gebied van informatieveiligheid. Ten derde dienen de CISO's zich ook landelijk te verenigen. De IBD kan daar een rol in vervullen en ook de initiatieven hiertoe in IMG- en VIAG-verband juichen wij van harte toe. Ten slotte biedt het leggen van verbindingen met het bedrijfsleven en semipublieke instellingen waardevolle inzichten. Denk daarbij bijvoorbeeld aan ziekenhuizen, banken en andere ondernemingen waarbij informatie een belangrijke factor is en waardoor deze organisaties vaak vooruitlopen op gemeenten als het om informatiebeveiliging gaat.

Maak een gezamenlijke agenda voor de komende jaren, met name wat betreft de techniek

Gemeenten beseffen het belang van aandacht voor houding en gedrag op het gebied van informatieveiligheid. Met dit toegenomen besef, signaleren we ook een hernieuwde aandacht voor de techniek. Phishing-mails zijn tegenwoordig dermate ingenieus en geraffineerd, dat ook goed getrainde medewerkers deze niet goed herkennen. Daarom neemt de noodzaak toe om op technisch vlak maatregelen te nemen. Vanwege de kosten en technische complexiteit zien wij hierbij de noodzaak om gezamenlijk op te trekken. Een collectief investeringsprogramma om hieraan een impuls te geven, ondersteund vanuit de VNG, is wenselijk. Hiervoor zien we gelukkig een toenemend draagvlak. Bestuurders realiseren zich dat samenwerking, met name op beleidsneutraal terrein zoals op het gebied van techniek en beveiliging, niet ten koste hoeft te gaan van de gemeentelijke autonomie.

Landelijke wetgeving is geen oplossing – samenwerking is de crux

Wij verwachten niet dat gedetailleerde wet- of regelgeving de juiste oplossing is voor het versterken van informatieveiligheid. Wel zien wij reden om de verantwoordelijkheid voor informatieveiligheid in bijvoorbeeld de Gemeentewet te verankeren. Dit is ook gebeurd met het onderwerp integriteit. Een discussie over welke overheidslaag primair aan zet is, mist echter de kern. De kern is de realiteit dat we tot op bepaalde hoogte helaas altijd achter de feiten aan zullen lopen.

> *Overheden moeten daarom de krachten bundelen om de bedreigingen het hoofd te bieden.*

Wij komen tot een duidelijke conclusie: samenwerking is de crux. Dit vereist een beweging van een discussie over reguleren en controleren 'door' het Rijk naar een discussie over echte samenwerking 'met' en faciliteren door de Rijksoverheid.

Achtergrond

De visitatiecommissie Informatieveiligheid vloeit voort uit de Resolutie informatieveiligheid, zoals aangenomen op de BALV van 29 november 2013. In de resolutie dragen de gemeenten het bestuur van VNG op om te bewerkstelligen dat een externe adviserende (interbestuurlijke) visitatiecommissie wordt ingericht.[1]

Doel en opdracht

De commissie heeft tot doel gekregen om:

- De aandacht bij gemeenten voor informatieveiligheid en het handelingsperspectief van gemeenten te vergroten. Continu leren en stimuleren is de benadering waar de commissie voor staat. Door als commissie handelingsperspectieven te bieden aan gemeenten beoogt de commissie gemeenten concreet te ondersteunen.
- Bij te dragen aan het verspreiden van kennis tussen de gemeenten. Veel gemeenten hebben al een forse ontwikkeling doorgemaakt; een ontwikkeling waar andere gemeenten van kunnen leren.
- Samen met de gemeenten in kaart brengen op welke manier het systeem van verplichtende zelfregulering verder verbeterd kan worden.[2]

De commissie benadrukt overigens dat zij op grond van een gesprek van anderhalf uur en de ingevulde vragenlijst niet uitputtend en objectief kan concluderen hoe het in de betreffende gemeente is gesteld op het gebied van informatieveiligheid. De handelingsperspectieven zien op de elementen waar de commissie meent dat meer aandacht aan gegeven kan worden.

De doelgroep die de commissie bedient, is in die zin uniek dat zij, in aanvulling op diverse andere initiatieven en gremia, primair dient om gemeenten op *bestuurlijk* niveau te adviseren over informatieveiligheid. De commissie is een bestuurlijk 'leerinstrument' en geen klassieke toezichthouder.[3]

Uitgangspunten

- De werkzaamheden van de commissie zijn als project onderdeel van de Digitale Agenda 2020. Informatieveiligheid is een voorwaarde voor digitalisering. Informatieveiligheid is vanuit dit perspectief altijd een onderdeel van het succes van de digitale overheid. Hier ligt dan ook de verbinding met de andere projecten die deel uitmaken van de Digitale Agenda 2020.
- Het zelfbeeld van de gemeente, op basis van een vooraf ingevulde vragenlijst, vormt de basis van het gesprek.
- De commissie is gericht op stimuleren en bestuurlijk leren. De commissie oordeelt niet en biedt elke gemeente een handelingsperspectief op maat waarmee een volgende stap kan worden gemaakt.
- De commissie heeft vertrouwelijkheid van informatie als uitgangspunt. Individuele rapportages worden niet gedeeld met derden zonder toestemming van de gemeenten. Informatie in de openbare rapportages is niet terug te leiden naar individuele gemeenten.
- De commissie betrekt niet zelf de gemeenteraad bij haar bezoeken, maar zal iedere gemeente sterk aanbevelen het verslag van de commissie te delen met de raad.

Instrumentarium

De commissie heeft het volgende instrumentarium tot haar beschikking om uitvoering te geven aan haar opdracht:

- Gesprekken inclusief voorbereiden via vragenlijsten: het voeren van gesprekken met bestuur en hoger management over de wijze waarop informatieveiligheid aandacht krijgt, en wordt vertaald naar acties.

1 Resolutie, punt 5. Zie de bijlage bij de Ledenbrief 31 oktober 2013, nummer 13/084.
2 Toelichting bij de Resolutie, pagina 9. Zie de bijlage bij de Ledenbrief 31 oktober 2013, nummer 13/084. Zie nader de opdrachtformulering in het kader van de Digitale Agenda 2020, bijlage 2, bij Ledenbrief 6 mei 2015, nummer 15/034.
3 Toelichting bij de Resolutie, pagina 7.

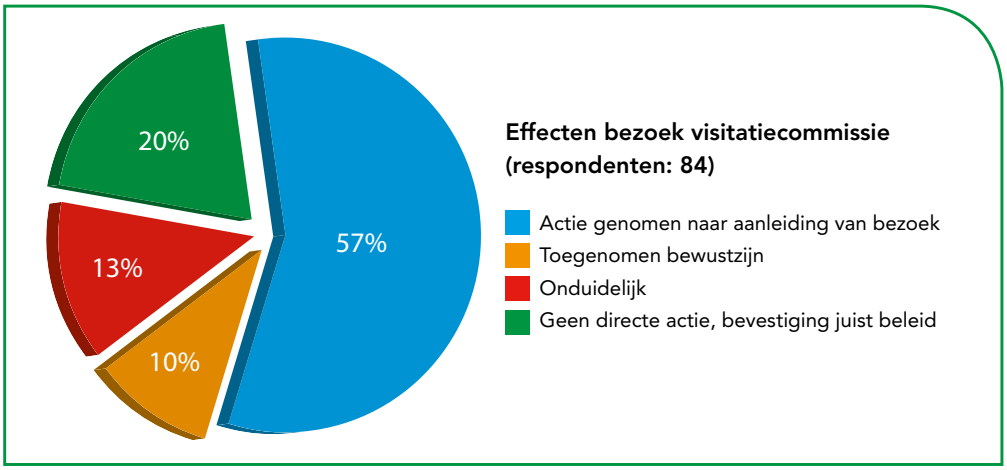
- Gespreksverslagen inclusief handelingsperspectieven: dit verscherpt het beeld van de manier waarop de gemeente werkt aan informatieveiligheid, inclusief een analyse van positieve en verbeterpunten.
- Communicatie over het werk en de werkwijze van de ommissie en de resultaten daarvan.

De opzet van de werkwijze: het leren centraal

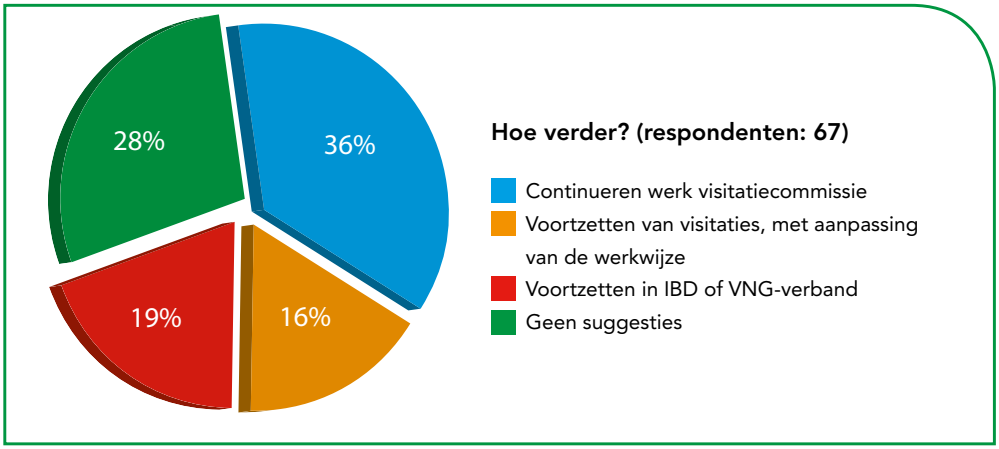
De commissie is voor 2 jaar ingesteld om 120 gemeenten te bezoeken. Initieel heeft de commissie op basis van openbare bronnen een selectie gemaakt van gemeenten die 'verder' en 'minder ver' leken te zijn op het gebied van informatieveiligheid. Voorts is gelet op spreiding tussen grotere en kleinere gemeenten en geografische spreiding. Dit laatste houdt in dat de commissie ongeveer 30% van het aantal gemeenten per provincie heeft bezocht.
De commissie heeft in haar communicatie steeds benadrukt dat het niet gaat om een 'visitatie' in klassieke zin. De commissie hecht waarde aan een op de toekomst gerichte dialoog, waarbij zij de bezochte gemeenten van een op maat gesneden en concreet handelingsperspectief voorziet.

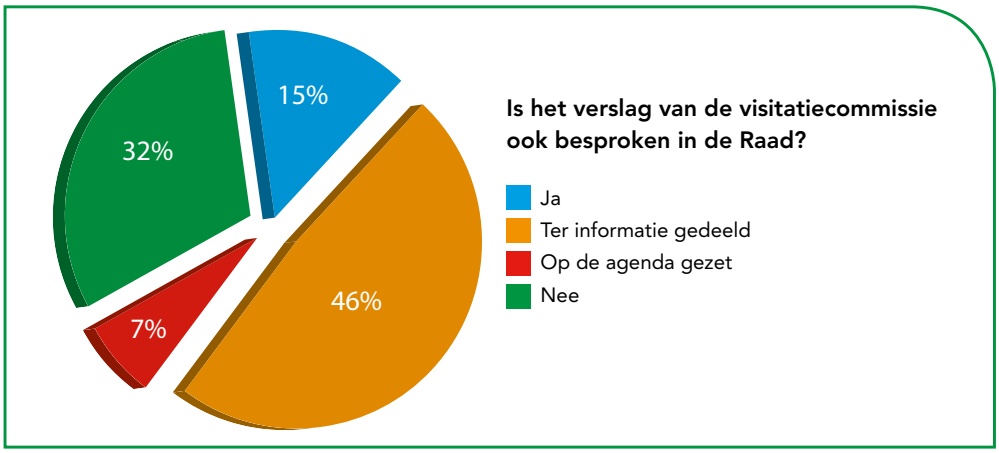
Beelden bij de effectiviteit van de commissie

De commissie heeft via de IBD reflecties ontvangen op haar functioneren. De IBD haalde haar informatie uit informele gesprekken met vertegenwoordigers van de door de commissie bezochte gemeenten. Het beeld dat de IBD heeft verkregen, is positief en sluit aan bij de ervaringen van de commissie zelf en bij de directe terugkoppeling die zij ontving vanuit gemeenten in de gesprekken en in een door de commissie via VNG afgenomen enquête (84 respondenten).

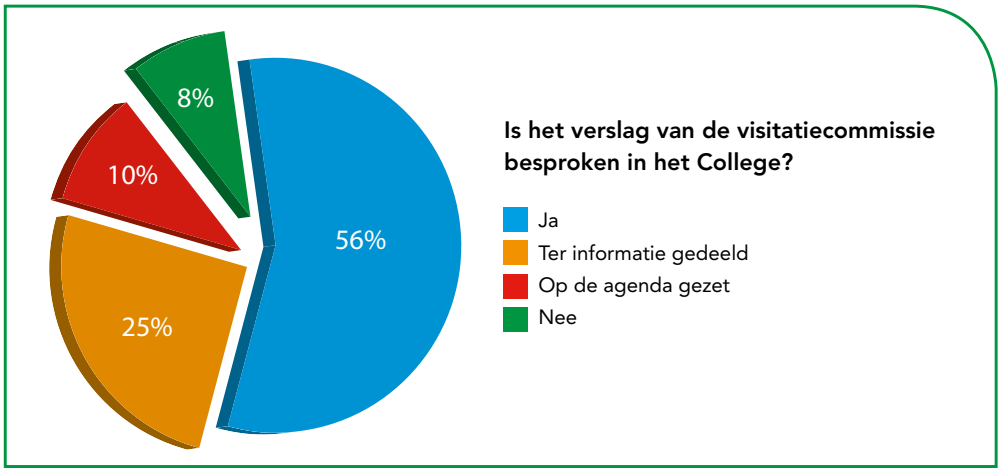


Desgevraagd bevestigde 48% van de gemeenten dat zij directe actie hebben ondernomen naar aanleiding van het bezoek van de commissie. Andere gemeenten rapporteerden een toegenomen bewustzijn. Ook waar gemeenten aangaven dat zij géén directe actie hebben ondernomen, werd regelmatig wel aangegeven dat het bezoek van de commissie een bevestiging vormde van de reeds ingezette acties en het beleid.





In diverse gevallen kreeg de commissie de indruk dat de aankondiging van haar bezoek en het verzoek om een vragenlijst in te vullen reeds aanleiding was om de gemeentelijke organisatie in beweging



te krijgen. De commissie meent dat dit anticiperende effect niet te onderschatten is en op zichzelf al resultaat oplevert.
De dialoog tijdens de bezoeken heeft de commissie als zeer waardevol ervaren. Daarbij was bovendien sprake van tweerichtingsverkeer; regelmatig werd de commissie verrast met interessante oplossingen en invalshoeken. Tegelijkertijd kon de commissie uit het gesprek opmaken dat de dialoog ook bij gemeenten tot waardevolle inzichten leidde. De commissie heeft sterk de indruk dat de samenstelling van zowel de commissie als de afvaardiging van de gemeente, die bestond uit zowel bestuurlijke áls (top) ambtelijke gesprekspartners, hieraan eveneens heeft bijgedragen.
Regelmatig kreeg de commissie als reactie op de (concept) verslagen dat de handelingsperspectieven de juiste snaar raakten en dat de gemeenten waarderen dat de commissie een opbouwende toon hanteert. De commissie ziet dit als bevestiging dat gemeenten de op het leren gerichte aanpak daadwerkelijk waarderen en tevens als indicatie dat deze aanpak effectief is.

De bezochte gemeenten

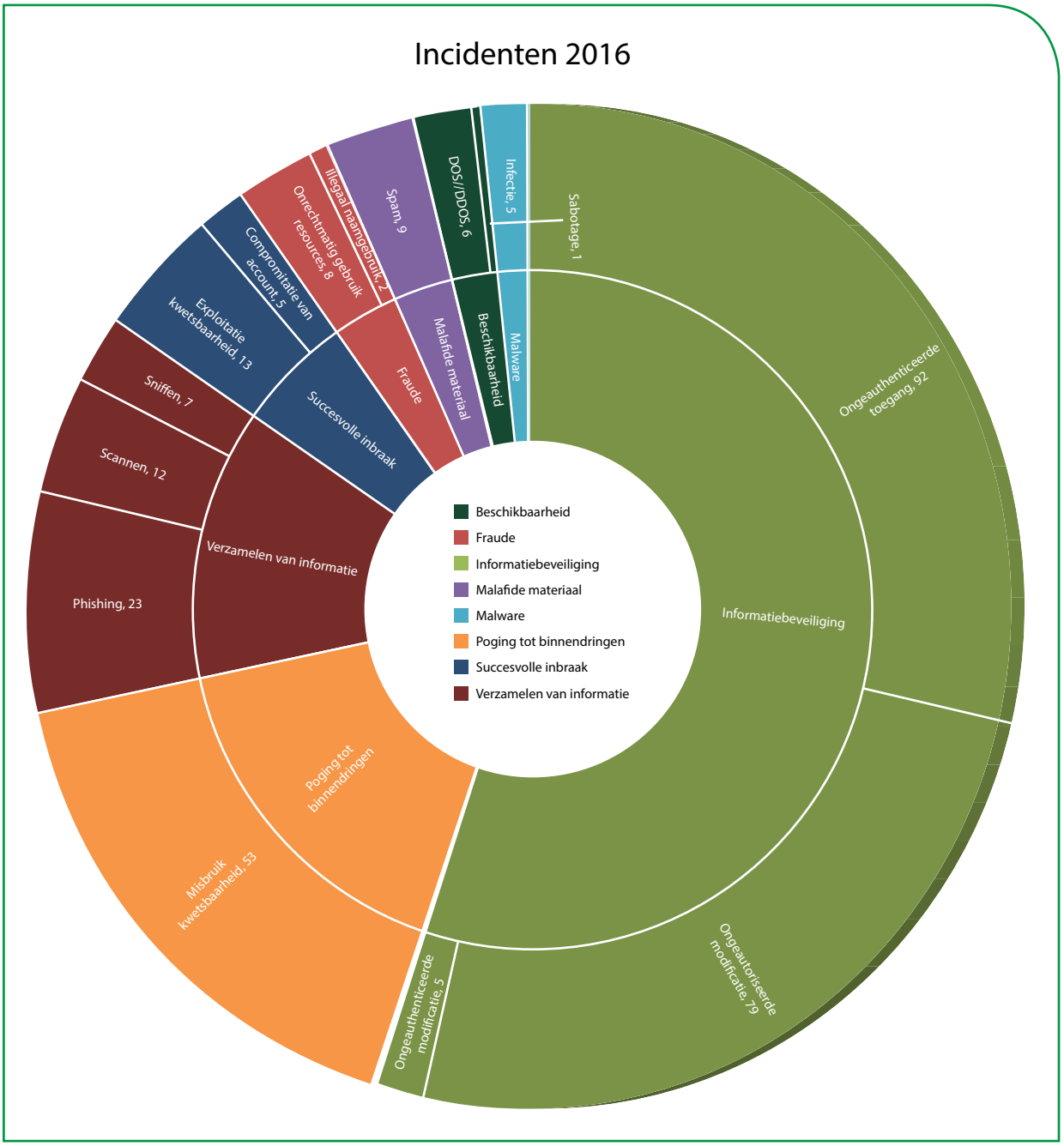
De commissie heeft 123 gemeenten bezocht, verspreid over alle 12 provincies in de periode van 26 augustus 2015 tot en met 31 mei 2017. Op alfabetische volgorde bezocht de commissie:

Aa en Hunze, Alblasserdam, Alkmaar, Alphen a/d Rijn, Amersfoort, Amstelveen, Amsterdam, Apeldoorn, Appingedam, Assen, Asten, Bellingwedde, Berg en Dal, Bergen (Lb.), Bergen op Zoom, Borne, Boxmeer, Breda, Brummen, Bunnik, Coevorden, Cuijk, Culemborg, Dalfsen, De Ronde Venen, Delft, Den Bosch, Den Haag, Diemen, Dongeradeel, Dordrecht, Druten, Edam-Volendam, Eijsden-Margraten, Eindhoven, Emmen, Enschede, Geldermalsen, Geldrop Mierlo, Gemert-Bakel, Goirle, Gooise Meren, Gouda, Grave, Haarlemmermeer, Harderwijk, Heerenveen, Heerhugowaard, Heiloo, Hendrik-Ido-Ambacht, Hoorn, Huizen, Hulst, Kampen, Krimpen a/d IJssel, Landsmeer, Langedijk, Leiden, Lelystad, Leudal, Leusden, Lochem, Loppersum, Maastricht, Meierijstad,

Meppel, Middelburg, Mill en Sint Hubert, Nijmegen, Noordenveld, Noordoostpolder, Noordwijk, Nuenen, Nunspeet, Oegstgeest, Oldambt, Oldebroek, Ooststellingwerf, Oostzaan, Oud-Beijerland, Ouder-Amstel, Papendrecht, Purmerend, Putten, Raalte, Reimerswaal, Renswoude, Roermond, Rotterdam, Schouwen-Duiveland, Sint Anthonis, Sliedrecht, Smallingerland, Son en Breugel, Stadskanaal, Steenbergen, Strijen, Ten Boer, Tholen, Tiel, Tilburg, Tynaarlo, Uitgeest, Uithoorn, Vaals, Venlo, Vianen, Vlagtwedde, Waalwijk, Waterland, West Maas en Waal, Westland, Woerden, Wormerland, Zaanstad, Zandvoort, Zederik, Zoetermeer, Zuidhorn, Zutphen, Zwartewaterland, Zwijndrecht en Zwolle.

Hoe ging het in de praktijk?

Bij de meeste bezoeken die de commissie aflegde, waren vanuit de gemeente de portefeuillehouder, gemeentesecretaris, hoofd bedrijfsvoering, de CIO en de CISO vertegenwoordigd. De commissie is zeer positief over hoe gastvrij zij in het land is ontvangen. Op een paar incidenten na is de commissie ook bij alle door haar initieel geselecteerde gemeenten welkom geweest.



Bron: Informatiebeveiligingsdienst voor gemeenten

Vereniging van Nederlandse Gemeenten
Nassaulaan 12 | 2514 JS Den Haag
info@vng.nl

vng.nl