RAPPORT INFORMATIEBEVEILIGING NEDERLANDSE GEMEENTEN 2016

Urgentie: hoog! ‘Gemeente, maak werk van informatieveiligheid’

nieuwe perspectieven

BDO

INHOUD

nieuwe inzichten

nieuwe perspectieven

Mensen, mensen

Dit is het tweede rapport van BDO over informatiebeveiliging. Vorig jaar deden we een eerste onderzoek naar de stand van zaken op dit gebied bij zorginstellingen; nu waren de gemeenten aan de beurt. Daar speelt het vraagstuk betreffende de veiligheid van digitale informatie zo mogelijk nog urgenter, gezien de enorme groei van de datastroom die gemeenten sinds enkele jaren te verwerken hebben.

De uitkomsten van beide peilingen laten zowel overeenkomsten als grote verschillen zien tussen deze twee sectoren, die door de decentralisaties in het sociaal domein steeds intensiever met elkaar te maken hebben. ICT-afdelingen hebben over het algemeen hun zaakjes aardig voor elkaar en liggen op schema om de strenge nieuwe wet- en regelgeving op het gebied van privacy- en informatiebeveiliging het hoofd te kunnen bieden.
Het grote probleem is bij gemeenten – net als bij de zorginstellingen – dat er binnen de organisatie veel te weinig is gedaan om awareness te kweken bij medewerkers. De mensen dus. Awareness-trainingen; veiligheidsprotocollen; screening van medewerkers die met privacygevoelige gegevens omgaan; gedragscodes – het is allemaal nog veel te beperkt aanwezig en dient nu echt prioriteit te krijgen, want over twee jaar kan het fataal zijn.

Een belangrijk tweede punt dat wij hier willen vermelden – en waarin zorg en gemeenten duidelijk van elkaar verschillen – is dat van de data security officer. Hoewel 75% van onze respondenten binnen gemeenten laat weten zo'n functionaris te hebben aangesteld – veel meer dan in de zorg – blijkt dat zeker de helft van die personen daarvoor niet de juiste achtergrond of papieren heeft. Dat is reden tot zorg. Dames en heren gemeentebestuurders, zonder een capabele data security officer gaat u deze slag verliezen. Slechts naar de letter voldoen aan wet- en regelgeving is niet voldoende. Serieus (samen) werken aan professionalisering van uw omgang met vertrouwelijke digitale data is dat wel.

Robert van Vianen, Rob Bouman, Julien Spronck
E-mail: lokale-overheid@bdo.nl
@BDONederland

'Slechts naar de letter voldoen aan wet- en regelgeving is niet voldoende'

Robert van Vianen

Rob Bouman

Julien Spronck

ROBERT VAN VIANEN
robert.van.vianen@bdo.nl
Specialisatie: Cybersecurity
Opvallendste uitkomst: "Nog altijd 31% van de gemeenten werkt niet samen met andere gemeenten als het gaat om IT/informatiebeveiiging"

FRANK VAN DER LEE
frank.van.der.lee@bdo.nl
Specialisatie: Advisory Publieke sector
Opvallendste uitkomst: "Slechts 57% van de gemeenten gebruikt beveiligde digitale communicatie met ketenpartners"

JULIEN SPRONCK
julien.spronck@bdo.nl
Specialisatie: Cybersecurity
Opvallendste uitkomst: "50% van de gemeenten heeft een security officer benoemd, maar in 50% van die gevallen heeft die persoon geen achtergrond in informatiebeveiliging"

ROB BOUMAN
rob.bouman@bdo.nl
Specialisatie: Audit & Assurance Publieke sector
Opvallendste uitkomst: "Slechts 40% van de gemeenten heeft aanvullende eisen aan bestuurders en raadsleden vastgelegd voor de borging van informatieveiligheid"

SANDRA KONINGS
sandra.konings@bdo.nl
Specialisatie: Cybersecurity
Opvallendste uitkomst: "Nog altijd 33% van de gemeenten heeft haar medewerkers niet bewust gemaakt hoe datalekken eenvoudig voorkomen kunnen worden."

5 STAPPEN VOOR EEN GOEDE DATA SAFETY-STRATEGIE

Informatiebeveiliging is voor gemeenten 'topprioriteit' geworden, zo blijkt uit inventarisatie door BDO. Vijf aanbevelingen voor een succesvolle data safety-strategie.

1

INFORMATIEBEVEILIGING IS EEN MENSENZAAK!

Het verhaal is zo langzamerhand klassiek: organisatie krijgt met privacygevoelige data te maken; directie geeft ICT-afdeling de opdracht daar goede en veilige systemen voor op te zetten en op een dag blijkt dat een medewerker een USB-stick met een verzameling privacygevoelige dossiers is kwijtgeraakt… Telkens weer blijkt dat organisaties onderschatten in hoeverre dataveiligheid vooral mensenwerk is, en dat awareness creëren binnen de organisatie – juist buiten de ICT-afdeling – een halszaak is. Met stip op 1.

2

BENOEM EEN CAPABELE DATA SECURITY OFFICER

Belangrijke constatering uit deze inventarisatie: 75% van de deelnemende gemeenten heeft een data security officer benoemd. Dat is uitzonderlijk hoog. Alleen blijkt bij doorvragen dat slechts de helft van hen een opleiding of arbeidsachtergrond heeft die hem/haar gekwalificeerd maakt voor die baan. Dat gaat de desbetreffende gemeenten opbreken. Een gekwalificeerde data security officer met voldoende budget en zeggenschap is cruciaal in de slag om grip te krijgen op dataveiligheid. Juist in een politiek gevoelige omgeving als een gemeente. Kleine gemeenten doen er goed aan samen zo'n specialist aan te stellen.

'Over de vraag welke gegevens je als gemeente moet opvragen om goed te kunnen registreren en controleren, is nog nauwelijks nagedacht'

3

BENOEM EEN SECURITY-COMMISSIE

Volgens de Wet meldplicht datalekken zijn organisaties die een datalek constateren verplicht om direct melding te doen bij de Autoriteit Persoonsgegevens. De vraag of dat moet gebeuren, is er niet een die door één persoon beantwoord dient te worden. Benoem een security-commissie, met daarin een bestuurder, iemand van de HR-afdeling en de data security officer, om te bepalen of er daadwerkelijk sprake is van een datalek en wat er vervolgens moet gebeuren.

'Op een dag blijkt dat een medewerker een USB-stick met een verzameling privacygevoelige dossiers is kwijtgeraakt…'

4

GEBRUIK CERTIFICERING (ISO) OM AAN HET NORMENKADER (BIG) TE VOLDOEN

De baseline informatiebeveiliging gemeenten (BIG) is het door de Rijksoverheid geformuleerde normenkader waaraan gemeenten zich voor het gebruik en de opslag van digitale gegevens over hun burgers hebben gecommitteerd. Het gaat dan over het opzetten van een langetermijnaanpak in de organisatie waarbinnen de veiligheid van die gegevens geborgd is. Belangrijke onderdelen: een veilige IT-structuur, de benoeming van een eindverantwoordelijke security officer en het creëren van awareness onder medewerkers die met de data in aanraking komen. Veel gemeenten zijn koortsachtig bezig om aan de BIG te kunnen voldoen.

Uit onze inventarisatie blijkt echter dat de meeste gemeenten (ongeveer 80%) daar geen certificeringsprogramma bij gebruiken. Gebruik van het door de Rijksoverheid geadviseerde programma ISO (27001 en 27002) is echter wel degelijk aan te raden, omdat het organisaties dwingt planmatig te werken: plan, do, check, act. Veel projecten die niet met behulp van een dergelijke systematiek worden aangepakt, stranden en leiden zo tot negatieve energie.

5

SLUIT BEWERKINGS-OVEREENKOMSTEN MET STAKEHOLDERS

Met de decentralisaties in het sociaal domein is er een enorme extra stroom aan elektronische data richting de gemeenten op gang gekomen. Gemeenten zijn inkoper geworden van zorg en moeten dus weten wat ze moeten inkopen voor wie, wie die zorg gaat leveren en tot slot (het rechtmatigheidsprincipe indachtig) of de ingekochte zorg ook daadwerkelijk is geleverd. Maar over de vraag welke gegevens je als gemeente moet opvragen om goed te kunnen registreren en controleren, is nog nauwelijks nagedacht, met als gevolg dat her en der complete zorgdossiers zijn opgevraagd bij zorginstellingen, met alle securityrisico's van dien.

Wat moet u doen? Sluit weldoordachte bewerkingsovereenkomsten af met maatschappelijke stakeholders. Daarin beschrijven beide partijen samen het raamwerk waarbinnen zij – in redelijk vertrouwen - relevante data kunnen uitwisselen, en hoe zij omgaan met de privacy– en security-issues die daarbij spelen.

INFORMATIEBEVEILIGING GEMEENTEN: ONTWIKKELINGEN

‘EXTRA DRUK!’

Terwijl gemeenten meer en meer privacygevoelige informatie van hun burgers in beheer krijgen, wordt de wet- en regelgeving rond informatiebeveiliging in rap tempo strenger. Vier ontwikkelingen zetten daarbij extra druk.

Er is veel te doen rond de dataveiligheid in lokaal bestuur. Een greep uit het nieuws van de zomer 2016:

- Begin juni concludeert vakblad Binnenlands Bestuur dat het e-mailverkeer bij gemeenten ‘gênant slecht’ beveiligd is. Slechts bij 3 van de 50 onderzochte gemeenten voldoet de e-mail-beveiliging aan de moderne standaards.
- Half juni maakt de Autoriteit Persoonsgegevens bekend dat er tot 27 mei 2016 in totaal 147 meldingen van datalekken bij gemeenten binnen zijn gekomen. Dat is gemiddeld één melding per dag.
- Op 28 juni publiceert de Inspectie Sociale Zaken en Werkgelegenheid (SZW) een rapport over de verstrekking van persoonsgegevens uit Suwinet (database voor verstrekking uitkeringen). Dit blijkt bij 51% van de gemeenten slecht beveiligd.

Het zijn maar enkele voorbeelden uit de stapel publicaties waaruit keer op keer blijkt: Nederlandse gemeenten hebben nog te weinig grip op de aanzwellende stroom digitale persoonsgegevens om te kunnen garanderen dat die gegevens ook echt veilig zijn. Een peiling door BDO in het kader van dit rapport bevestigt dat: bij 75% van de deelnemende gemeenten is in de afgelopen twee jaar minstens één incident geweest op het gebied van informatiebeveiliging. Kortom: werk aan de winkel! Vier ontwikkelingen rond de urgentie van informatiebeveiliging:

1 STRENGERE REGELGEVING

Er is strenge regelgeving ingevoerd en er is nog strengere regelgeving op komst.

Per 1 januari 2016 is de Wet meldplicht datalekken (Wmd) ingegaan. Die houdt in dat een organisatie of bedrijf dat een datalek constateert, verplicht is een melding te doen bij de Autoriteit Persoonsgegevens (AP). De AP kan een boete opleggen van maximaal € 820.000, in geval van opzettelijke overtreding of grove nalatigheid. In minder zware gevallen legt de AP een 'bindende aanwijzing' op, die bij blijvende nalatigheid alsnog gevolgd kan worden door een boete. Vooralsnog is de Autoriteit zeer terughoudend geweest met het uitdelen van boetes, maar ze heeft aangekondigd strenger te gaan worden. De Wmd is onderdeel van de Wet bescherming persoonsgegevens (Wbp) uit 2001. Deze

'Bij 75% van de gemeenten is al minstens één incident geweest rond informatiebeveiliging'

wet bepaalt onder meer dat gegevens op een zorgvuldige manier moeten worden bewerkt, op passende wijze moeten worden beveiligd en alleen mogen worden gebruikt voor de doeleinden waarvoor ze zijn verzameld. Degene van wie de gegevens worden verwerkt, moet op de hoogte zijn wie ze gebruikt en met welk doel. Daarnaast regelt de wet de taken en bevoegdheden van de Autoriteit Persoonsgegevens.

De Wmd is de Nederlandse bewerking van de Europese richtlijn bescherming persoonsgegevens, die in 2018 wordt opgevolgd door de Europese Privacy Verordening. Organisaties moeten volgens die verordening expliciet toestemming aan burgers/klanten vragen voor big data-toepassingen; de eisen voor beveiliging van informatie worden nog strenger en de benoeming van een data protection officer wordt verplicht. De boetes onder deze verordening kunnen oplopen tot € 20 miljoen.

2 GEEN STURING VAN BOVENAF

Politiek Den Haag geeft hooguit richting, geen regie of ondersteuning.

Hoewel de centrale overheid enorme budgetverantwoordelijkheden met bijbehorende datastromen naar de gemeenten heeft gedelegeerd (waarover onder het volgende thema meer) is vanuit politiek Den Haag geen regie of ondersteuning te verwachten. In 2013 werden twee documenten gepubliceerd: de Strategische en de Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), die sindsdien door gemeenten stapsgewijs zijn aangevuld. Via de Vereniging Nederlandse Gemeenten hebben alle gemeenten zich gecommitteerd aan de implementatie van deze documenten, maar daarmee houdt de regierol op. Geen standaarden, geen protocollen voor bijvoorbeeld het samenbrengen van data die vallen onder de Wet maatschappelijke ondersteuning met data die zijn verzameld in het kader van de Participatiewet, of de omgang met gegevens van zorginstellingen. Hoewel dergelijke 'data-mismatches' leiden tot enorme en dure administratieve problemen (die de veiligheid van de betreffende gegevens compromitteren doordat er dientengevolge volop wordt geïmproviseerd) mogen gemeenten dat allemaal zelf uitzoeken. De Autoriteit Persoonsgegevens zei er dit over: 'Er is te weinig sturing vanuit Den Haag'.

Tekenend is wat dat betreft ook de reactie van minister Plasterk op Kamervragen op 18 mei 2016 over een datalek in Amersfoort. Op de vraag of dit soort incidenten bij meer gemeenten te verwachten zijn, antwoordde hij geruststellend: "Dit incident berustte op een menselijke fout, niet op een fout in techniek of procedures." Dat het doorgaans juist aan die menselijke kant van de beveiliging schort,

'Smart cities zullen een explosie aan data gaan opleveren, én een exponentiële stijging van mogelijke data safety issues'

en niet alleen bij gemeenten overigens, had de minister duidelijk even niet op het netvlies.

3 DATASTROOM GROEIT EXPLOSIEF

Transities in het sociaal domein brengen een tsunami aan privacygevoelige gegevens.

Met het ingaan van de transities in het sociaal domein op 1 januari 2015 hebben gemeenten er een budgettaire verantwoordelijkheid bij gekregen ter waarde van € 7,4 miljard aan jeugdhulp en maatschappelijke ondersteuning. In sommige gemeenten hebben deze transities gezorgd voor een verdubbeling van het budget en daarmee voor het verder aanzwellen van de datastroom van grotendeels vertrouwelijke gegevens die gemeenten moeten ver- en bewerken.

Op 19 april jl. publiceerde de Autoriteit Persoonsgegevens een onderzoek onder 41 gemeenten waaruit blijkt dat gemeenten onvoldoende weten welke persoonsgegevens van hun burgers ze in het sociale domein mogen verwerken en welke regels daarvoor gelden. Bovendien bleken gemeenten hun burgers niet goed te informeren over het gebruik van hun persoonsgegevens.

Bij gebrek aan helderheid hierover vragen veel gemeenten hun burgers toestemming voor het bewerken van hun gegevens. Maar ook die methode biedt geen carte blanche. Met name in het sociaal domein verkeren burgers vaak in een afhankelijkheidsrelatie met hun gemeente (beoordelaar en verstrekker van zorgdiensten en uitkeringen immers). Daardoor kan er geen sprake zijn van vrijheid om toestemming tot databewerking te geven. In dat geval is toestemming vragen door de gemeente onrechtmatig.

Volgens de Autoriteit Persoonsgegevens lopen gemeenten door dit soort werkwijzen het gevaar het vertrouwen van hun burgers te verliezen. Een serieus probleem dat kan uitmonden in een legitimiteitscrisis voor de lokale overheid.

4 ...EN GROEIT STRAKS NOG VEEL SNELLER!

Dit is nog maar het begin; de smart city komt eraan.

Terwijl gemeenten naarstig zoeken naar manieren om bovengenoemde datapuzzels doelgericht op te lossen voordat de eerste boetes volgen, wordt her en der hard nagedacht over het idee van de smart city. Die term – ooit geïntroduceerd door IT-gigant IBM – belooft een toekomstbeeld van steden die dankzij het gebruik van technologie veel efficiënter en milieuvriendelijker functioneren dan we tot nu toe kennen. Zo kunnen steden schoner, krimpgemeenten leefbaarder en kan de mobiliteit slimmer worden, terwijl met veelvuldig gebruik van sensoren – the internet of things – zaken als stedelijk beheer, verlichting, veiligheid en afval in de publieke ruimte veel beter worden geregeld.

Het is een inspirerend toekomstbeeld, dat in de komende tien jaar zomaar werkelijkheid kan worden. Maar dan wel als gemeenten in staat zijn om de datastromen die daarmee gemoeid zijn op een verantwoorde manier te accommoderen. Smart cities zullen een explosie aan data- en big data-toepassingen gaan opleveren. Maar de hoeveelheid mogelijke data safety issues die daarmee gepaard gaat, zal ook exponentieel toenemen.

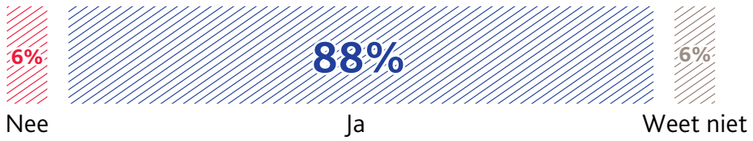
Gemeenten doen er dan ook goed aan nu serieus na te denken over (en te investeren in) kennis- en capaciteitsopbouw op het gebied van dataopslag en professionalisering van de wijze waarop hun organisaties met data omgaan. Want de ontwikkeling van smart cities is niet een zaak van de verre toekomst; die is allang begonnen op talloze innovatieplatforms en in proeftuinen her en der. Gemeenten die daarin meekunnen, hebben een grote voorsprong op de rest.

Burgerzaken

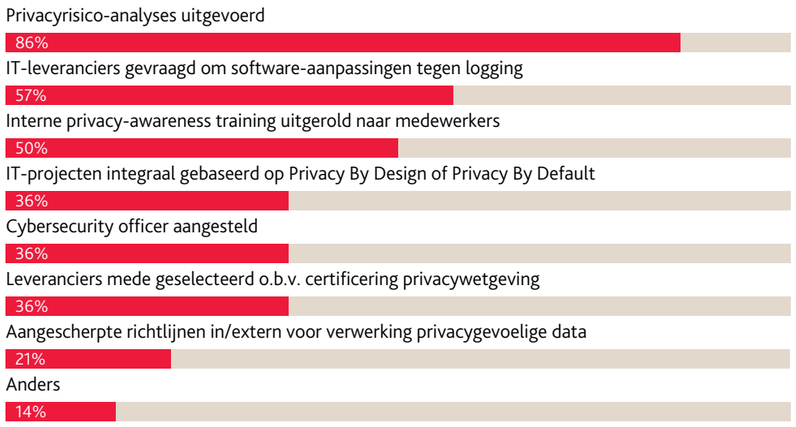
‘GEMEENTEN, MAAK WERK VAN DATAVEILIGHEID!’

Als het gaat om databeheer hebben de Nederlandse gemeenten nog veel werk te doen. Ze kennen de regels niet goed genoeg, laten vertrouwelijke informatie wegsijpelen en nemen nog onvoldoende maatregelen, blijkt uit een steekproef van BDO. De opvallendste uitkomsten.

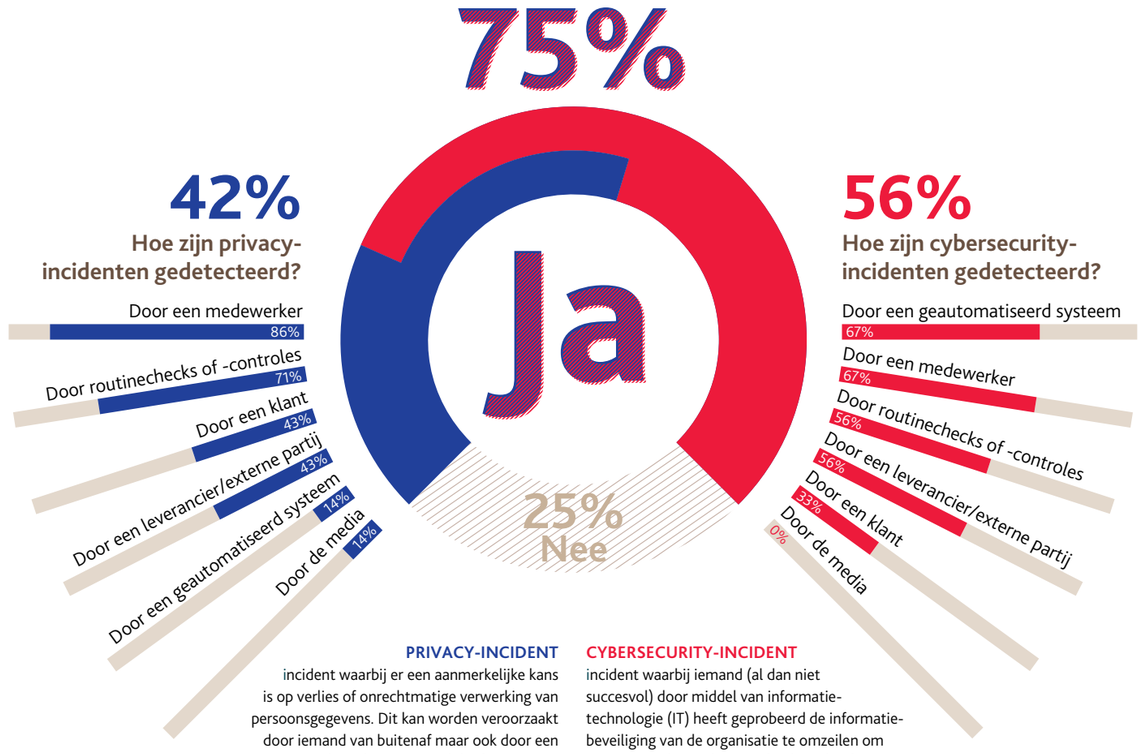
BENT U BEKEND MET DE KOMST EN DE IMPACT VAN DE EUROPESE PRIVACYVERORDENING?



WAT HEEFT U GEDAAN OM ZICH DAAROP VOOR TE BEREIDEN?



HEEFT UW ORGANISATIE IN DE AFGELOPEN 2 JAAR EEN PRIVACY- EN/OF CYBERSECURITY-INCIDENT GECONSTATEERD?



PRIVACY-INCIDENT
incident waarbij er een aanmerkelijke kans is op verlies of onrechtmatige verwerking van persoonsgegevens. Dit kan worden veroorzaakt door iemand van buitenaf maar ook door een medewerker, per ongeluk of met opzet.

CYBERSECURITY-INCIDENT
incident waarbij iemand (al dan niet succesvol) door middel van informatie-technologie (IT) heeft geprobeerd de informatie-beveiliging van de organisatie te omzeilen om gegevens te bemachtigen of te beïnvloeden.

WELKE MAATREGELEN HEEFT U IN DE AFGELOPEN 2 JAAR GETROFFEN?

100%
+ Antivirus-/malware-bescherming
+ Proxy-/firewall-bescherming
+ Back-up van belangrijkste systemen
+ Segmentatie van netwerken
+ Periodieke software-updates
+ Access control/ wachtwoordbeleid
+ Automatisch uitloggen bij standby

89%
+ Protocol voor veilig verwijderen van media (pc’s, flash drives etc.)
+ Aanstellen security officer

78%
+ Organisatiebreed informatiebeveiligings beleid communiceren
+ Softwaretests en -configuratie; change management process

67%
+ Data-encryptie op mobile devices (flash drives, laptops etc.)
+ Periodieke security audits/-reviews
+ Security awareness voor medewerkers
+ Periodieke review van userrechten

44%
+ Installatie van een Data Loss Prevention (DLP) systeem

Meer detail-uitkomsten weten? Kijk op pagina 17, 21 en 25.

‘AWARENESS MOET BOVENAAN DE TO DO-LIJST’

SANDRA KONINGS (CYBERSECURITY) EN ROB BOUMAN (PUBLIEKE SECTOR)

Informatiebeveiliging is voor een zeer belangrijk deel niet een systeem- maar een mensenkwestie. En dat besef is nog onvoldoende tot gemeenten doorgedrongen.

Laatst hoorde ik een goede anekdote over gedragsverandering, vertelt Sandra Konings, partner BDO Advisory (Cybersecurity). “Een man skiede zijn hele leven al en wist dat het veiliger was om een helm te dragen. Hij wilde wel een helm kopen, maar op de een of andere manier kwam het er maar niet van. Op een dag was hij met zijn zoontje op de piste toen het jongetje viel en botste met een snowboarder. De snowboard scheerde rakelings langs z’n hoofd. Gelukkig had zoonlief een helm op, maar zijn vader was vreselijk geschrokken. Terug in het dal kocht hij direct ook voor zichzelf een helm.” Iemand zal niet zomaar zijn gedrag veranderen nadat hij feitjes gehoord heeft over wat er mis kan gaan. Mensen zullen doorgaans hun gedrag pas veranderen als ze inzien en voelen wat de gevolgen kunnen zijn als ze dat niet doen.

Screening

Helaas is dat laatste wat massaal moet gaan gebeuren bij gemeenten. Want in de omgang van ambtenaren en inhuurkrachten met vertrouwelijke informatie gaat het regelmatig mis. En het besef dat daar een enorme opdracht ligt, is nog niet voldoende tot gemeenten doorgedrongen. Bij 35% van de respondenten in onze peiling worden medewerkers, inhuurkrachten of externe deskundigen niet gescreend voordat ze aan de slag gaan met privacygevoelige gegevens. Iets wat per definitie in 100% van de gevallen moet gebeuren. Gevraagd of aan medewerkers aanvullende eisen rond informatiebeveiliging worden gesteld, beantwoordt wederom 35% van de gemeenten negatief (55% positief, 10% weet het niet). Dezelfde vraag gesteld ten aanzien van het college van B&W en de raadsleden, levert exact dezelfde score op.

Cruciale factor

“Awareness binnen de organisatie als het gaat om de omgang met vertrouwelijke digitale informatie, moet echt een veel grotere, structurele rol krijgen. Want je medewerkers zijn hierin de cruciale factor”, zegt Rob Bouman, partner BDO Audit & Assurance Publieke sector. “Die awareness moet beginnen aan de top. Informatiebeveiliging wordt nog altijd door maar al te veel colleges van B&W netjes naar de IT-afdeling gedelegeerd, terwijl het echt bovenaan de prioriteitenlijst hoort te staan voor de gehele organisatie.”

En inderdaad: onze inventarisatie laat zien dat 40% van de gemeenten een organisatiebrede awareness-training heeft uitgerold. Bouman: “Dat betekent: 60% dus niet. En dat terwijl 75% van de respondenten laat weten dat zich bij zijn/haar gemeente cybersecurity- en/of privacy-incidenten hebben voorgedaan, waarbij nota bene de helft van die incidenten niet door de systemen werd gemeld, maar door

‘Je zult in een gemeenteraad ook niet snel een motie over het IT-securitybeleid aantreffen; dat wordt gezien als een ambtelijke aangelegenheid’

een medewerker. Daarmee is de cirkel rond. Je medewerkers zijn cruciaal op dit gebied. Awareness moet in gemeenteland de komende jaren bovenaan de to do-lijst komen te staan.”

Zwemcomplex

Het grootste probleem bij gemeenten is volgens Bouman dat het politieke organisaties zijn. En in een politieke omgeving raken systeemgerelateerde zaken als ICT makkelijk in de verdrukking. “Een wethouder maakt zich in zijn gemeente nu eenmaal veel geliefder door een paar miljoen uit te geven aan een nieuw zwemcomplex dan door datzelfde geld uit te trekken voor een geweldig informatiebeveiligingsprogramma. Je zult in een gemeenteraad ook niet snel een motie over het IT-securitybeleid aantreffen; dat wordt gezien als een ambtelijke aangelegenheid. Bijgevolg is de budgettaire ruimte vaak niet optimaal. Wat er dan bij inschiet is juist zoiets als awareness-training, die op het eerste gezicht secundair lijkt.”

Bedrijfsleven

Wat dat betreft heeft men het in het bedrijfsleven doorgaans beter voor elkaar, vindt Sandra Konings. “Bij naar schatting driekwart van de corporates hebben de relevante medewerkers een awareness-training op het gebied van informatiebeveiliging gedaan.” Een ander punt waarin bedrijven volgens Konings beter zijn, is het werken met gedragscodes. Hiermee tekenen medewerkers voor het beschermen van de gegevens over hun bedrijf en hun klanten, en beloven ze melding te doen als ze iets waarnemen dat niet in de haak is. Bij grote bedrijven is zo’n gedragscode standaard. “En omdat de grote bedrijven dat lager in de keten ook steeds meer afdwingen, zie je die gedragscodes ook steeds vaker in het mkb.”

Twee branches die als voorbeeld zouden kunnen dienen voor hoe het moet, zijn volgens haar de bankenwereld en de chemische sector. “De banken lijken het ondertussen goed voor elkaar te hebben. Dat heeft natuurlijk te maken met de extreem privacygevoelige aard van de gegevens die ze over hun klanten beheren en de enorme externe druk van toezichthouders waarmee zij te maken hebben. Ook in de chemische wereld staat het veiligheidsdenken op een heel hoog niveau; dat zie je ook terug in de omgang met informatiebeveiliging.”

Kleine organisaties

“Belangrijk is wel om je te realiseren dat bij 80% van de gemeenten de organisatie uit niet meer dan een paar honderd mensen bestaat”, zegt Bouman. “Die missen gewoon de schaal om informatiebeveiliging professioneel op te kunnen pakken. Dat neemt echter niet weg dat ze met awareness aan de slag moeten. Want juist dat onderdeel zou ook voor die kleine organisaties goed te behappen moeten zijn. Ze moeten vooral beseffen dat het belangrijk is. Want dat is het. Razend belangrijk.”

HIGHLIGHTS

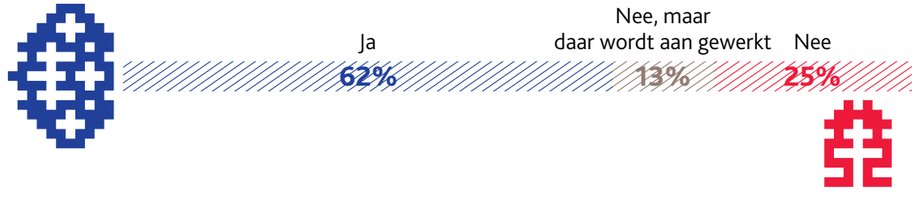
- **Mensen zijn cruciaal bij de beveiliging van gegevens.**
- **Awareness moet bij gemeenten bovenaan de agenda komen.**
- **Op het gebied van screening en gedragscodes hebben gemeenten een achterstand op het bedrijfsleven.**
- **Slechts 40% van de gemeenten heeft intern een awareness-programma uitgerold.**

OPVALLENDSTE UITKOMSTEN OP DEELTHEMA

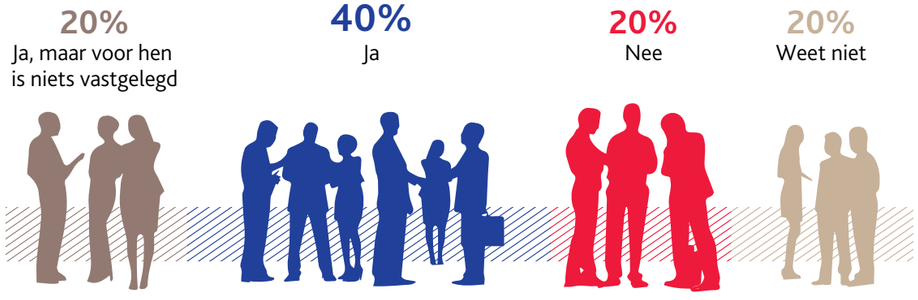
‘DE MENSELIJKE FACTOR’

HEEFT UW GEMEENTE EEN SECURITY TRAINING- EN AWARENESS-PROGRAMMA VOOR MEDEWERKERS?

STELT UW GEMEENTE AANVULLENDE EISEN AAN MEDEWERKERS VOOR DE BORGING VAN INFORMATIEVEILIGHEID?



GELDEN DIE EISEN OOK VOOR B&W EN RAADSLEDEN?



‘SAMENWERKING MAAKT REGIE MOGELIJK’

FRANK VAN DER LEE
(ADVISORY PUBLIEKE SECTOR)

Als gemeenten afspraken maken met maatschappelijke stakeholders over de uitwisseling van data, besparen ze niet alleen op bureaucratie, maar versterken ze ook hun regierol.

Overal in de samenleving groeien de hoeveelheden data die organisaties registreren en bewerken exponentieel. Maar bij de gemeenten groeien ze de afgelopen anderhalf jaar nog veel sneller. Gemeenten werken steeds meer in de keten; 85% van de respondenten in deze inventarisatie werkt samen met andere gemeenten of zorginstellingen. En dat percentage zal alleen maar verder groeien.
Dat heeft alles te maken met de transformaties in het sociaal domein. De operatie waarlangs de centrale overheid een budgetverantwoordelijkheid ter waarde van meer dan € 7 miljard bij de gemeenten heeft neergelegd. Die verantwoordelijkheid brengt een enorme schaalvergroting én een toestroom van data met zich mee. Gemeenten zijn inkoper geworden van zorg en moeten dus weten wat ze moeten inkopen voor wie, wie die zorg gaat leveren en tot slot – het rechtmatigheidsprincipe indachtig – of de ingekochte zorg ook daadwerkelijk is geleverd.

Medische dossiers

“En daar wringt het”, aldus Frank van der Lee, partner BDO Advisory en expert op het gebied van de transitie tussen gemeenten en andere maatschappelijke stakeholders. “Stel, een gezin in Ommen, Overijssel, heeft een kind dat extra zorg nodig heeft en naar een jeugdzorginstelling in Zwolle moet. Dan heeft de gemeente Ommen vanaf dat moment – krachtens het woonplaatsbeginsel - een relatie met die jeugdzorginstelling, eventueel op basis van dat ene kind. De vraag is nu: welke gegevens over die zorgcliënt ga je als gemeente opvragen om diens zorgverlening goed te kunnen registreren en controleren? Over die vraag is nog niet of nauwelijks nagedacht.” Gevolg is dat her en der gemeenten complete medische dossiers opvragen bij zorginstellingen: dan weten ze dat ze in ieder geval alles hebben.
Zulke dossiers bevatten echter uiterst privacygevoelige informatie. Niet voor niets protesteren zorginstellingen daar dan ook fel tegen. Van der Lee: “Veel van de zorginhoudelijke informatie in zo’n dossier is voor gemeenten irrelevant en brengt grote privacy issues met zich mee, die in het licht van de regelgeving ontoelaatbare risico’s geven.”

Vertrouwen

Hoe kan dat anders? Als gemeente wil je weten of er sprake is van rechtmatigheid van geleverde zorg/bestedingen. Zo lang gemeenteambtenaren daar complete dossiers voor nodig denken te hebben, zullen zij die opvragen. Van der Lee: “Uiteindelijk moeten we – conform de geest van de transitie – naar een systeem dat niet alleen drijft op controle, maar daarnaast ook plaats biedt voor vertrouwen. Je kunt als gemeenten proberen

‘Veel van de zorginhoudelijke informatie die in een medisch dossier staat, is voor gemeenten irrelevant en brengt grote privacy issues met zich mee’

elke zorgminuut te verantwoorden, maar je kunt ook een raamwerk opzetten waarbinnen de ketenpartners hun werk kunnen doen en waarbinnen ze – zolang de grenzen van het raamwerk niet worden overschreden – een bepaalde mate van vertrouwen krijgen, terwijl je als gemeente toch de rechtmatigheid kunt aantonen. Het denken daarover is nog maar net begonnen.”

Verzwaring

Binnen de Vereniging Nederlandse Gemeenten (VNG) wordt op dit moment wel degelijk nagedacht over een dergelijk raamwerk. Dat is echter een moeizaam proces en het zal nog even duren voordat daar een landelijk geldende oplossing uitkomt. “Sowieso is dat de makke van de hele transitie”, zegt Van der Lee. “Door de snelheid waarmee de operatie is doorgedrukt was er nooit tijd om na te denken over uniformiteit in de regelgeving. Gevolg daarvan is dat veel zorginstellingen en gemeenten met een forse verzwaring van hun administratieve lasten te maken hebben gekregen.”

Bewerkingsovereenkomst

Daarom pleit hij voor veel meer overleg en samenwerking. “Gemeenten vragen veel te veel gegevens op, en zorginstellingen verzetten zich daartegen. Hoe zou het zijn als gemeenten hun stakeholders in het sociale domein opzoeken om afspraken te maken over de vraag wie welke data waarvoor nodig heeft, en hoe ze die informatie het liefst ontvangen?” ‘Bewerkingsovereenkomsten’ noemt Van der Lee dat: afspraken waaronder data-uitwisseling tot stand komt die op maat is en waarin specifiek wordt nagedacht over de bijkomende privacy issues. “Gemeenten hoeven daarvoor echt niet op een landelijke regeling te wachten. Het belangrijkste is dat er samenwerking op gang komt in een context van vertrouwen. Op de meeste plaatsen gebeurt dat gewoon niet. Maar waar wij proberen de verschillende stakeholders aan tafel te krijgen, merk ik dat het eigenlijk heel makkelijk gaat, omdat iedereen er een groot belang bij heeft.”

Regie

Wat Van der Lee betreft zou die ‘datasamenwerking’ niet alleen tussen gemeenten en zorginstellingen moet plaatsvinden, maar zouden ook woningcorporaties daarbij moeten aanschuiven. “Wat wij zien, is dat het in die driehoek binnen een gemeente altijd over dezelfde mensen gaat. De woningcorporatie, de zorginstelling en natuurlijk de gemeente zelf - allemaal hebben ze data over die burgers/huurders/zorgvragers.”

“Wat we ook zien,” gaat hij verder, “is dat als de gemeente in zijn beleid aan een paar knoppen draait, dit vaak directe gevolgen heeft voor de andere twee. Bijvoorbeeld: als de gemeente bezuinigt op de Wmo, kan dat leiden tot verregaande bezuinigingen bij een zorginstelling, bijvoorbeeld op het gebied van vastgoed, waardoor een woningcorporatie een probleem kan krijgen. Een beslissing op het ene punt in de keten kan elders leiden tot ontslagen of zelfs faillissement. Over het algemeen heeft een gemeente daar weinig zicht op. Maar weet je de relevante data op een goede manier met elkaar te delen, dan ontstaat een ander perspectief op het transitieproces. Dan wordt regie mogelijk op geheel nieuw niveau.”

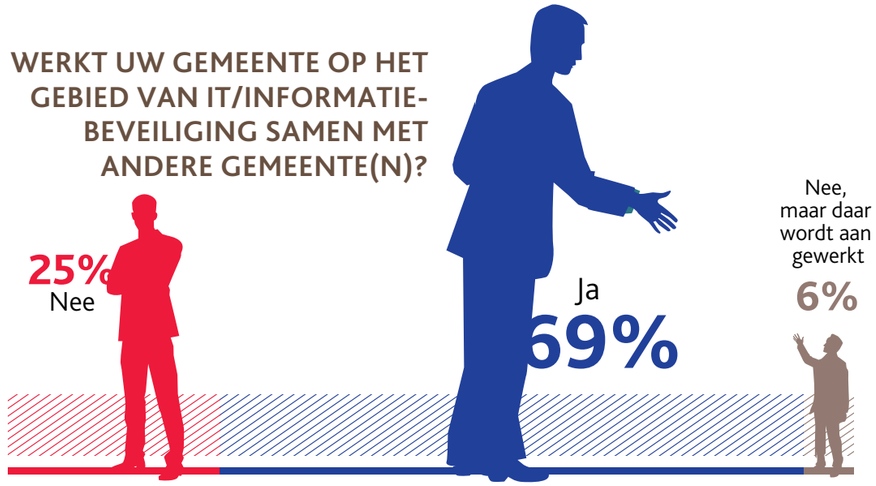
HIGHLIGHTS

- **Gemeenten zijn inkopers van zorg geworden en werken meer en meer samen met ketenpartners.**
- **Ze hebben data nodig om de rechtmatigheid van hun zorginkoop aan te kunnen tonen.**
- **Menig gemeente vraagt veel te veel data op om controle te kunnen verzekeren, met alle privacy issues van dien.**
- **Gemeenten en zorginstellingen moeten bewerkingsovereenkomsten met elkaar aangaan m.b.t. hun onderlinge datastroom.**
- **Door ‘datasamenwerking’ uit te breiden naar woningcorporaties, kunnen gemeenten regie voeren op een hoger niveau.**

OPVALLENDSTE UITKOMSTEN OP DEELTHEMA

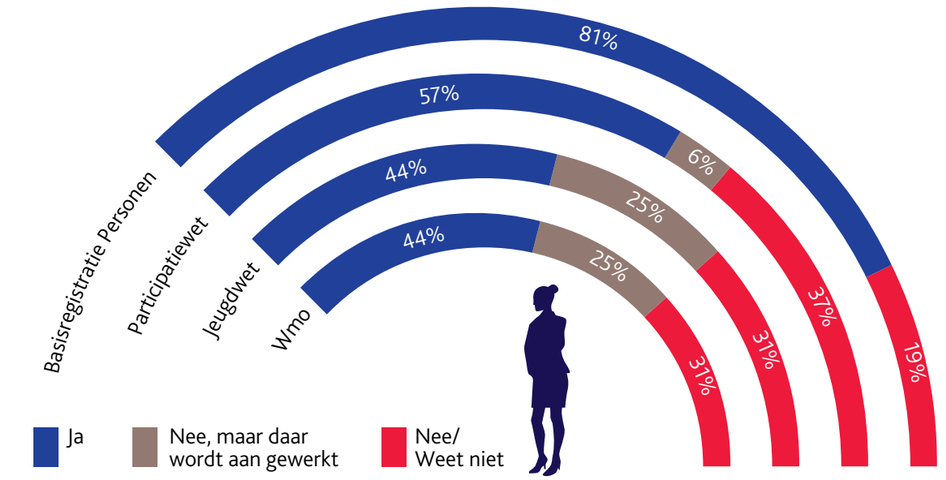
‘KETENAANSPRAKELIJKHEID’

WERKT UW GEMEENTE OP HET GEBIED VAN IT/INFORMATIE-BEVEILIGING SAMEN MET ANDERE GEMEENTE(N)?



GEBRUIKT UW GEMEENTE BEVEILIGDE DIGITALE COMMUNICATIE MET KETENPARTNERS?

HEEFT UW GEMEENTE AANVULLENDE STAPPEN GENOMEN VANWEGE KETENAANSPRAKELIJKHEID M.B.T. DE VOLGENDE WETTEN?



‘EEN GOEDE DATA SECURITY OFFICER IS CRUCIAAL’

ROBERT VAN VIANEN (CYBERSECURITY)
EN JULIEN SPRONCK (CYBERSECURITY)

Gemeenten zijn hard bezig hun omgang met data te professionaliseren. Negatieve verrassing: de helft van de benoemde data security officers blijkt daar niet voor opgeleid.

Weet je wat opvalt?, zegt Julien Spronck, manager BDO Advisory (Cybersecurity). “Maar liefst 75% van de gemeenten blijkt een data security officer te hebben aangesteld – in vergelijking met andere sectoren een ongekend hoog percentage – maar op de vervolgvraag of dat iemand is met kennis van en/of een achtergrond in informatiebeveiliging, moet echter de helft schoorvoetend ‘nee’ zeggen. Dat laatste is toch wel heel teleurstellend. Het geeft aan dat gemeenten een tokenfunctie maken van deze in onze ogen cruciale positie. Gewoon iemand benoemen, zodat aan de wet- en regelgeving is voldaan, en dan weer overgaan tot business as usual.”

Juist in een politieke omgeving als een gemeente kan een goed functionerende data security officer van grote meerwaarde zijn, vindt Sproncks collega Robert van Vianen, partner BDO Advisory (Cybersecurity): “Een goede security officer fungeert als link tussen de operatie en het management. En aangezien de koers van het management juist bij een gemeente volatiel is, door de politieke omgeving waarin het moet opereren, heb je iemand nodig die dat spel op het snijvlak tussen lokale democratie en langjarige beleidsdoelstellingen goed kan spelen. Dat geeft stabiliteit.”

Positionering

Ook het antwoord op de vraag hoe de data security officer is gepositioneerd in de organisatie is over het algemeen niet duidelijk. “Het maakt nogal wat uit”, aldus Van Vianen, “of je hem/haar een uitvoerende opdracht geeft of een meer controlerende. En het maakt zeker ook uit waar je hem in de organisatie plaatst en aan wie hij verantwoording dient af te leggen.”

Belangrijk is in ieder geval dat gemeenten deze functionaris in staat stellen succesvol te opereren. Spronck: “Gezien de zwaarte van de sancties die hen straks boven het hoofd hangen als de Europese Privacyverordening realiteit is geworden, maar ook uit het oogpunt van de betrouwbaarheid van de overheid, zou dat voor elke gemeentelijke organisatie prioriteit moeten zijn.”

Privacycommissie

Van Vianen somt enkele factoren op die dat succes dichterbij kunnen brengen: “De functionaris moet onafhankelijk kunnen opereren in de organisatie, met volledige steun van de top. Hij onderhoudt een korte lijn met B&W en legt periodiek aan hen – en alleen aan hen – verantwoording af. Daarnaast krijgt hij voldoende budget en tijd om goed zijn werk te kunnen doen. En tot slot moet duidelijk zijn dat het hier een echte functie betreft en niet een extra rol van iemand die het erbij doet, wat we helaas nogal eens aantreffen.”

‘Bij informatiebeveiliging trekt iedereen een muur op, terwijl er juist veel synergievoordeel te behalen is’

“Daarnaast”, zegt Spronck, “adviseren wij organisaties een privacycommissie op te zetten, met daarin in ieder geval een bestuurder, de security officer en iemand van de HR-afdeling. Als er incidenten zijn op het gebied van data en privacy, kan die commissie beoordelen wat er aan de hand is en wat er vervolgens gebeuren moet. Die besluitvorming kun je niet alleen juridisch bepalen en aan één enkel individu overlaten.”

Normenkader

Een tweede punt van aandacht is wat betreft Van Vianen en Spronck het normenkader met betrekking tot informatiebeveiliging. Spronck: “Als je kijkt naar de mate waarin gemeenten met het normenkader bezig zijn op het gebied van informatiebeveiliging, dan doen ze het eigenlijk best goed. Alleen vertaalt het zich nog niet in certificering.” Slechts zo’n 20% van de gemeenten in onze peiling laat weten gecertificeerd te zijn volgens de internationaal geldende standaard ISO 27001 die ook door de Rijksoverheid wordt aanbevolen, en 45% is ermee bezig. “Dat is laag,” aldus Van Vianen, “en dat is vreemd, gezien het feit dat we zien dat het denken over dat normenkader bij gemeenten veel beter ontwikkeld is dan in bijvoorbeeld de zorg.”

Langetermijn-aanpak

Het normenkader, dat is de door de Rijksoverheid geformuleerde best practice (BIG) waar gemeenten zich voor het gebruik en de opslag van digitale gegevens over hun burgers aan hebben gecommitteerd. Het gaat dan over het opzetten van een langetermijnaanpak in de organisatie waarbinnen de veiligheid van die gegevens geborgd is. Belangrijke onderdelen: een veilige IT-structuur, de benoeming van een eindverantwoordelijke privacy officer en het creëren van awareness onder medewerkers die met de data in aanraking komen.

Certificering

“In onze ogen is voldoen aan de BIG cruciaal, waarbij certificering voor ISO 27001 (en 27002) instrumenteel is”, beaamt Robert van Vianen. “ISO dwingt je planmatig te werken volgens de Plan-Do-Check-Act methode. De ervaring daarbij leert dat projecten op dit gebied die niet zo worden aangepakt, al gauw stranden en leiden tot veel negatieve energie. Maar andersom geldt ook: het feit dat je met certificering aan de slag gaat, garandeert niet dat je de juiste dingen aan het doen bent.”

Wat Van Vianen bijvoorbeeld mist bij gemeenten, is samenwerking op het gebied van gegevensbescherming. “Gaat het om IT-infrastructuur, dan wordt er volop samengewerkt. Maar bij informatiebeveiliging trekt iedereen weer een muur op, terwijl er juist op dit gebied veel synergievoordeel te behalen is.” De oorzaak daarvan is volgens hem een gebrek aan kennis. “Juist door de schaal te vergroten, ontstaat er ruimte voor serieuze professionalisering waarmee je grote progressie kunt boeken én de kosten beheersbaar kunt houden, bijvoorbeeld door het benoemen van een gezamenlijke data security officer.”

Urgentie

Beide adviseurs benadrukken dat de urgentie groot is. Van Vianen: “Elke dag die je nu nog langer wacht met het invoeren van een professionele omgang met data, loop je verder achter de feiten aan. Als over twee jaar de Europese Privacyverordening ingaat, moet je als gemeentelijke organisatie zowel transparantie als optimale veiligheid kunnen bieden als het gaat om de omgang met persoonsgegevens. Voor de meeste gemeenten schat ik in dat dat nog zo’n drie à vier jaar werk is.”

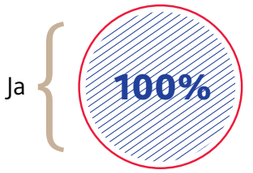
HIGHLIGHTS

- **Slechts 20% van de deelnemende gemeente is gecertificeerd volgens ISO 27001.**
- **De helft van de benoemde data security officers heeft geen achtergrond in informatiebeveiliging.**
- **Een goede data security officer met volledige steun van de organisatietop is van vitaal belang.**
- **Gemeenten dienen een privacycommissie te benoemen ter beoordeling van data-incidenten.**

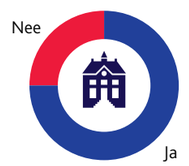
OPVALLENDSTE UITKOMSTEN OP DEELTHEMA

‘NORMENKADER & SECURITY OFFICER’

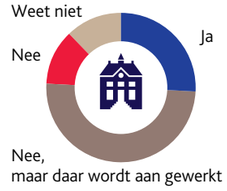
HEEFT UW GEMEENTE EEN INFORMATIEBEVEILIGINGSBELEID GEFORMULEERD/GEÏMPLEMENTEERD?



IS UW GEMEENTE INGERICHT CONFORM BIG?

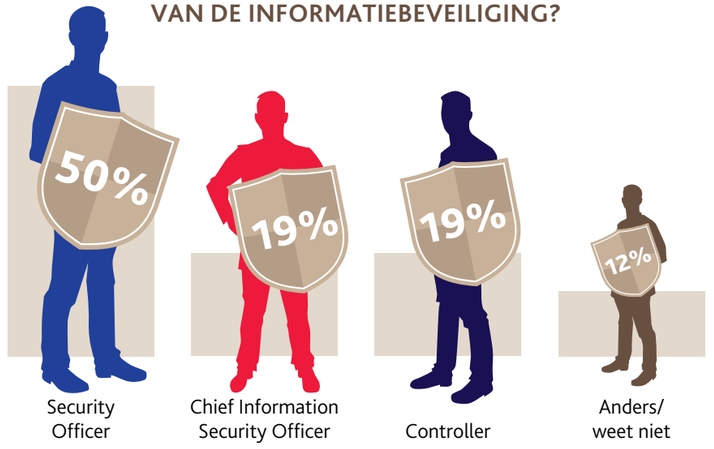


IS UW GEMEENTE INGERICHT CONFORM ISO 27001/27002?

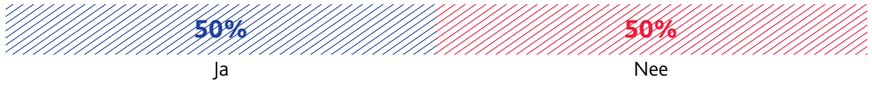


HEEFT UW GEMEENTE EEN FORMEEL PLAN HOE OM TE GAAN MET CYBERSECURITY-INCIDENTEN?

WIE IS VERANTWOORDELIJK VOOR DE IMPLEMENTATIE VAN DE INFORMATIEBEVEILIGING?



HEEFT DIE PERSOON EEN ACHTERGROND IN INFORMATIEBEVEILIGING?



BDO PUBLIEKE SECTOR BRANCHEGROEP LOKALE OVERHEID

Branchegroep Lokale overheid
Hoe zorg ik voor meer transparantie van de activiteiten van mijn gemeente met minder financiële middelen? Lokale overheden hebben met steeds meer taken en uitdagingen te maken. Bijvoorbeeld door strengere eisen aan transparantie en burgerparticipatie, een toename van ambtelijke en bestuurlijke samenwerkingsverbanden en teruglopende financiële middelen door dalende inkomsten uit gronden. De nieuwe vraagstukken waarmee lokale overheden hierdoor te maken krijgen, vragen steeds vaker om professioneel advies. De specialisten van de branchegroep Lokale overheid van BDO kennen deze vraagstukken als geen ander. Samen met collega's in andere branches van de publieke sector vertalen we actuele ontwikkelingen en inzichten naar gerichte adviezen en praktische ondersteuning voor uw organisatie.

Meer informatie
BDO branchegroep Lokale overheid
Tel: 088 - 236 48 06
E**-mail:** lokale-overheid@bdo.nl
I**nternet:** bdo.nl/lokale-overheid

Rob Bouman, partner Audit & Assurance,
voorzitter branchegroep Lokale overheid
E-mail: rob.bouman@bdo.nl
Tel: 06 2348 4550

Jeroen Cremers, partner BDO Belastingadvies,
Publieke sector
E-mail: jeroen.cremers@bdo.nl
Tel: 06 2360 2343

Frank van der Lee, partner Advisory,
Publieke sector
E-mail: frank.van.der.lee@bdo.nl
Tel: 06 1100 3117

COLOFON

Concept & realisatie
Monte Media

Tekst
Pierre de Winter

Fotografie
Sander Nagel

Infographic
Menno Mackay

Vormgeving
Tot en met ontwerpen

nieuwe perspectieven

In de nieuwe economie doen kansen zich sneller voor dan ooit. Nieuwe spelregels geven een boost aan zakelijk werken. En een nieuwe generatie staat klaar om het anders te doen. Beter, slimmer, innovatiever. Wie succesvol wil ondernemen, moet zelf ook vernieuwen. Open staan voor verandering. En met open vizier kijken naar de mogelijkheden die voor ons liggen.

Nieuwe perspectieven, dát is wat BDO u wil bieden. En kan bieden, dankzij onze unieke combinatie van lokale marktkennis en een internationaal netwerk. Persoonlijke dienstverlening en een professionele aanpak. BDO helpt u graag om vanuit een andere invalshoek naar uw business te kijken. Zodat u de juiste beslissingen neemt om uw organisatie sterker, wendbaarder en succesvoller te maken. Of u nu een mkb-bedrijf, familiebedrijf, publieke organisatie of internationale onderneming bent.

BDO kijkt graag met u vooruit. Samen komen we tot nieuwe inzichten en nieuwe kansen in uw markt. Samen creëren we nieuwe perspectieven.

bdo.nl/lokale-overheid

09/2016 – PS1623