MAGAZINE VAN DE VERENIGING VAN
NEDERLANDSE GEMEENTEN

VNG

2024
14 JUNI

DIGITALE VEILIGHEID
SPECIALE UITGAVE

Samen digitaal *veilig*

GEMEENTEN AAN DE SLAG

DIGITALE VEILIGHEID

SPECIALE UITGAVE · 14 JUNI 2024

WEERBAARHEID VERHOGEN

Andries Kok

Kàto Vierbergen

Phishing, identiteitsfraude, ransomware-aanvallen en andere vormen van cybercrime; miljoenen inwoners en bedrijven krijgen er jaarlijks mee te maken. Omdat het vaak om grote bedragen gaat of de continuïteit van de organisatie, zijn de maatschappelijke effecten groot.
Dat geldt ook voor gemeenten. Want criminelen zijn 24 uur per dag bezig om de digitale veiligheid te ondermijnen. Wat inwoners en ondernemers raakt, raakt overheden ook. Als bij een cyberaanval de dienstverlening wordt geraakt, is de gemeente niet alleen slachtoffer, maar ook hulpverlener voor inwoners die een nieuw paspoort moeten aanvragen.
De fysieke en online wereld zijn onlosmakelijk met elkaar verbonden, ook in de aspecten die de veiligheid onder druk zetten. Daarom heeft de VNG drie jaar geleden de Agenda Digitale Veiligheid opgezet. Hiermee helpen we gemeenten bij hun rol in het verhogen van de weerbaarheid bij digitale dreigingen, bij voorbereiding op digitale incidenten en in de preventie van cybercriminaliteit bij inwoners en ondernemers. Want alleen samen kunnen we zorgen voor een digitaal veilige samenleving.
De afgelopen jaren hebben we veel gedaan om de bewustwording bij gemeenten te vergroten, bestuurders aan te spreken op hun rol en om concrete handvatten en tips te geven. Digitale veiligheid is een verantwoordelijkheid van alle medewerkers binnen de gemeente. Met bestuurders, medewerkers van gemeenten en raadsleden zorgen we vanuit de VNG voor meer bewustwording, betrokkenheid en kennisdeling. De bestuurlijke gesprekken zijn een goed voorbeeld van kennisdeling tussen gemeenten.
Ondertussen blijven de uitdagingen groot en zetten wij ons in voor meer structurele financiering, een beter cyberbeeld voor gemeenten en helpen we de uitdagingen rondom arbeidsmarktkrapte aan te pakken.
Volledige digitale veiligheid bestaat niet, maar samen kunnen we wel goede stappen maken.

Andries Kok is directeur Lokaal Bestuur en Informatiesamenleving bij VNG. Kàto Vierbergen is programmanager Agenda Digitale Veiligheid.

Bestuurlijke gesprekken
Burgemeesters Paul Depla (Breda) en Doret Tigchelaar (Wierden) blikken terug.

Opbrengst
De belangrijkste les van de gespreksronde: digitale veiligheid is 'chefsache'.

Column
'Digitale veiligheid is mensenwerk', schrijft Ester Weststeijn.

Europese richtlijn
De zeven belangrijkste vragen over de nieuwe NIS2-richtlijn.

Colofon

Speciale uitgave van de Vereniging van Nederlandse Gemeenten

Uitgever Dineke Sonderen, Sdu BV **Chef redactie** Rutger van den Dikkenberg **Medewerkers** Sanne van der Most, Michelle van der Burg, Robert van Rijssel, Nikki Nguyen, Peter van Enk
Vormgeving Monique Westenbroek, Dimitry de Bruin
Druk Senefelder Misset, Doetinchem

TEKST: SANNE VAN DER MOST

DIGITALE DREIGING

Onzichtbaar en *ongrijpbaar*

DIGITALE VEILIGHEID IS ONZICHTBAAR EN ABSTRACT. TOCH KAN EEN CYBERAANVAL OP DE GEMEENTE VERSTREKKENDE EN SOMS ZELFS **ONTWRICHTENDE GEVOLGEN** HEBBEN, ZIEN PAUL DEPLA EN DORET TIGCHELAAR. ZE NAMEN DEEL AAN DE BESTUURLIJKE PEER-TO-PEERGESPREKKEN DIE DE VNG ORGANISEERDE.

Waarom is digitale veiligheid voor burgemeesters zo belangrijk?
Doret Tigchelaar: 'Een woninginbraak is heftig, maar de impact van digitale criminaliteit is voor het slachtoffer vaak groter. Bij een woninginbraak zie je meteen wat ze hebben meegenomen en welke schade is aangericht. Dan doe je aangifte bij de politie.
'Bij een cyberaanval is dat anders. Dat maakt het ongrijpbaar. Precies daarom moeten we er extra alert op zijn. Daarnaast kunnen de gevolgen van een cyberincident verstrekkend zijn. Voorzieningen, infrastructuur, ziekenhuizen; ze worden allemaal digitaal aangejaagd en daardoor zijn ze behoorlijk kwetsbaar voor een aanval. Toen Hof van Twente, onze buurgemeente, getroffen werd door een zware hack, hebben we dat met eigen ogen kunnen zien. Die lag helemaal plat.'
Paul Depla: 'Digitale veiligheid is een veelkoppig monster. Een cyberaanval gaat niet alleen over openbare orde en veiligheid, maar ook over de huishouding en de bedrijfsvoering van de gemeente zelf.
'Soms ontstaan dan tegenstrijdige belangen. Het sluiten een deal met een hacker versus de openbare orde en veiligheid bijvoorbeeld. Wat weegt zwaarder? Is dat het bedrijfsbelang van de gemeente, waardoor je snel een deal wil sluiten met een hacker, of is het vanwege het strafrechtelijk onderzoek verstandiger om het maar even te laten lopen? Dat zijn ingewikkelde kwesties waar je als burgemeester en als gemeente voor staat. Als je niet oppast, wordt alles op één grote hoop gegooid en wordt het één kluwen.'

Jullie deden beiden mee aan de peer-to-peergesprekken. Wat is blijven hangen?
Depla: 'Het is interessant om te zien waar andere gemeenten het zwaartepunt leggen. In Breda zijn we behoorlijk ver op het gebied van weerbaarheid, het maken van afspraken met vitale partners en het geven van training rond weerbaarheid van bewoners en ondernemers. Tijdens het gesprek dat ik mocht leiden tussen Haarlem en Maastricht, viel me op dat zij juist weer verder zijn in de aanpak van de risico's rond bedrijfsvoering en het alert zijn op de systemen.'

‘Je moet digitale veiligheid niet bij *één persoon* neerleggen’

Beeld: Ramon Mangold

Wie is...

Paul Depla
burgemeester van Breda

Tigchelaar: ‘Die verschillen tussen gemeenten sprongen er voor mij ook uit. Sommige gemeenten hebben het in eigen huis perfect op orde en zijn erg gefocust op risicobeheersing, maar doen weer weinig met ondernemers en burgers. Andere zijn meer op de buitenwereld gericht en zitten erg op voorlichting en preventie. Het ligt maar net waar de portefeuillehouder de focus op legt. Als gemeente Wierden zijn wij met Steenwijkerland in gesprek gegaan. Daar ligt de focus op openbare ordeverstoring. Mede gedreven door de ervaring van burgemeester Rob Bats in 2012 met ‘Project X’, hij was toen burgemeester van Haren. Digitale veiligheid stond destijds nog echt in de kinderschoenen. We zijn nu natuurlijk veel verder, maar de bevoegdheden van een burgemeester zijn nog altijd zeer beperkt.’

Wat zijn de belangrijkste lessen die uit de gesprekken werden getrokken?
Tigchelaar: ‘Dat digitale veiligheid enorm belangrijk is en blijvend prioriteit moet hebben in de gemeente. Het moet daarom onderdeel worden van het bedrijfscontinuïteitsplan en het integrale veiligheidsplan. Structureel blijven oefenen is noodzakelijk. Bespreek de dilemma’s waar je tegenaan kunt lopen. Zoals “wat doen we als we worden gehackt? Gaan we dan betalen of niet?”
‘Maar ook: wat je niet opslaat, kan ook niet lekken. Hoe ga je daar als gemeente mee om en welke afspraken maak je? Dat heeft weer alles te maken met het op orde hebben van je eigen huis.’
Depla: ‘Bij rampen en crises dachten we te lang alleen maar in termen van fysieke veiligheid. De digitale component wordt makkelijk vergeten. Bij een oefening kom je daar nog wel op, maar tijdens een

‘Wat je niet opslaat, kan ook niet *lekken*’

‘Een *cyberaanval* gaat niet alleen over openbare orde en veiligheid’

echte crisis ben je er vaak helemaal niet van bewust dat je misschien wel gehackt zou kunnen zijn. Als burgemeesters moeten we ons dat veel meer gaan realiseren. Die vraag moet standaard worden. Want een digitale crisis vertaalt zich niet meteen in een echte crisis. Dat wordt niet meteen manifest.’

Hoe pakken jullie als burgemeester je eigen rol rond digitale veiligheid op?

Tigchelaar: ‘Digitale veiligheid is onzichtbaar en weinig tastbaar. Dat is ook de reden dat mensen er over het algemeen niet zo heel veel mee hebben en dat er soms zelfs een beetje weerstand is om je er echt in te verdiepen. Toch is het belangrijk om er meer over te weten, zeker als burgemeester. Digitale criminaliteit ontwikkelt zich razendsnel en wijzigt continu. Het beschermen van inwoners en ondernemers en het voorkomen van maatschappij ontwrichtende schade wordt steeds belangrijker. Precies om die reden heb ik de portefeuille digitale veiligheid in de Veiligheidsregio Twente naar me toe getrokken. Daarnaast ben ik aangesloten bij het overleg cyberburgemeesters. Dat is een landelijk platform, waar ook de VNG nauw bij betrokken is, met twee doelen: creëren van bewustzijn bij burgemeesters, bestuurders, ondernemers en inwoners, en onze problematiek in Den Haag goed voor het voetlicht brengen.’

Depla: ‘Sommige gemeenten hebben een aparte wethouder digitalisering. Je mag hopen dat die ene wethouder wel goed nadenkt over alle kansen en bedreigingen. Zelf vind ik dat je digitale veiligheid niet bij één persoon moet neerleggen. Daar is het veel te groot voor. Digitale veiligheid moet je als burgemeester altijd in samenwerking met andere partners doen, zoals de portefeuillehouder economische zaken en de wethouder wijken. De digitale veiligheid van de organisatie van de gemeente ligt bij de portefeuillehouder bedrijfsvoering. Gaat het om de veiligheid van de gemeenschap en het tegengaan van een crisis in de stad, dan ligt het eigenaarschap bij de burgemeester in zijn rol als voorzitter van het regionaal beleidsteam en soms vanuit de driehoek. Zo gaat het bij ons.’

Wie is...

Doret Tigchelaar
burgemeester van Wierden

Beeld: Studio SF ~ Sietsanne Fotografie

BESTUURLIJKE GESPREKSRONDE

De *vrijblijvendheid* voorbij

‘HET IS HEEL LEERZAAM OM IN DE KEUKEN TE KIJKEN VAN EEN ANDERE GEMEENTE.’ DE AFGELOPEN PERIODE ORGANISEERDE DE VNG EEN BESTUURLIJKE GESPREKSRONDE OVER DIGITALE VEILIGHEID. DE BELANGRIJKSTE LES: DIGITALE VEILIGHEID IS **CHEFSACHE**.

Leiderschap en professionalisering

Verken de publieke waarden, voer het gesprek met de raad

- Bestuurders beseffen dat digitale veiligheid een brede maatschappelijke opgave is.
- Digitale Veiligheid staat daarom prominent in 92% van de Integrale Veiligheidsplannen.
- Het onderwerp zat bij bedrijfsvoering en komt in de veiligheidsportefeuille.
- Het komt nu aan op concrete uitvoeringsplannen en bewust voorbeeldgedrag.
- Het gesprek met de raad helpt daarbij de publieke waarden te onderkennen.

Scan de QR-code en bekijk een praktijkvoorbeeld uit Breda

‘Digitale veiligheid krijgt bestuurlijk plek door deze op te nemen in de kadernota.’

Rian van Dam, burgemeester Hollands Kroon

De bestuurlijke peer-to-peergesprekken waren bedoeld om bewustzijn te creëren bij de burgemeesters, zegt projectleider Peter van Enk. Digitale veiligheid is *chefsache* en vraagt om een integrale benadering. Door de uitwisseling van kennis en ervaring in een bestuurlijk gesprek, konden gemeenten van elkaar leren hoe ze de digitale veiligheid kunnen vergroten.

'De integrale benadering van het maatschappelijke vraagstuk vormde de kern van het project,' zegt Van Enk. Digitale Veiligheid is meer dan 'het eigen huis op orde'. Het gaat ook om de voorbereiding op online aangejaagde ordeverstoringen en om de weerbaarheid van inwoners en bedrijven tegen cybercriminelen. Van Enk: 'Deze benadering was voor sommige gemeenten nieuw, bleek tijdens de gesprekken. De Chief Information Security Officer (CISO) en Adviseur OOV kenden elkaar vaak nog niet voor het gesprek.'

Andere gemeenten hadden de integrale aanpak al omarmd. Zo gaf burgemeester Rian van Dam van Hollands Kroon aan dat Digitale Veiligheid in het Integraal Veiligheidsplan (IVP) en daarmee uit de uit de hoek van de bedrijfsvoering was gehaald.

Prioriteit 2

Europa en digitale veiligheid

Voer een integraal veiligheidsbeleid, stuur op kansen en risico's

- Gemeenten schieten snel in de kramp door EU-regelgeving, net zoals bij AVG gebeurde.

> 'Het is zaak om te blijven zorgen dat er geen verkramping ontstaat'
>
> **Marja van Bijsterveldt,** burgemeester Delft

- Goed risicobeheer overstijgt de eigen organisatie, zeker bij essentiële entiteiten.
- Er mist echter een visie op gemeente-overkoepelend toezicht.
- Naar verwachting gaat de NIS2-richtlijn aanzienlijke impact hebben.
- Voor het borgen is menskracht en substantiële structurele financiering nodig.

Scan de QR-code en bekijk een praktijkvoorbeeld uit Haarlem en Oss

Uit de gesprekken bleek dat het 'eigen huis' er in veel gemeenten anders uitziet, voegt projectleider Robert van Rijssel toe. Veel kleinere gemeenten werken samen in een gemeenschappelijke regeling aan hun digitale veiligheid. Dit

Prioriteit 3

Eigen huis op orde

Borg de bedrijfscontinuïteit

- Digitale veiligheid wordt bestuurlijk een steeds zwaarder dossier.
- Alles is digitaal, de onderlinge afhankelijkheid en de afhankelijkheid van derden is groot.
- Voor kwaliteitstoezicht op technologie reuzen missen gemeenten slagkracht.

> 'Digitale veiligheid gaat om onze gezamenlijke dienstverlening'
>
> **Iris Meerts** burgemeester Wijk bij Duurstede

- De noodzakelijke expertise is schaars, er heerst krapte op de arbeidsmarkt.
- Van gemeentebestuurders wordt verwacht dat ze eigenaarschap nemen.

Scan de QR-code en bekijk een praktijkvoorbeeld uit Dalfsen

biedt in rustige tijden veel schaalvoordelen, maar leidt bij een cybercrisis tot bestuurlijke en organisatorische complexiteit. Van Rijssel: 'Regelmatig een cyberoefening doen helpt om deze complexiteit te reduceren.'

Ook gaven burgemeesters aan dat het lastig is om de gemeenteraad te betrekken bij een gemeenschappelijke regeling. Raadsleden ervaren vaak een grote afstand en weinig mogelijkheden om bij zo'n organisatie op afstand invloed te hebben.
Boerenprotesten en coronarellen zijn voorbeelden van online aangejaagde ordeverstoringen. Burgemeesters geven aan dat zij nog weinig instrumenten in de gereedschapskist hebben voor een effectieve aanpak. Omdat de gemeente nauwelijks bevoegdheden heeft voor online monitoring, moet de informatie vaak van de politie komen. De samenwerking met de politie kan in veel gemeenten beter. Samen optrekken met het OM in de driehoek en lobby van de VNG voor een passend wettelijk instrumentarium zijn belangrijke tips uit de bestuurlijke gesprekken, aldus de projectleiders.

DIGITALE WEERBAARHEID

Lang niet alle deelnemers aan de bestuurlijke gespreksronde waren ervan overtuigd dat de gemeente hier een rol heeft. En dat terwijl gemiddeld één op de zeven inwoners slachtoffer is van digitale diefstal of cybercrime. 'Als bij één op de zeven van onze inwoners een fiets gestolen werd of ingebroken zou worden, moesten we vol aan de bak', stelt een adviseur Openbare orde en Veiligheid. Veel gemeenten voeren daarom al bewustwordingsprojecten uit voor kwetsbare groepen als jonge kinderen en ouderen. Hierbij wordt samengewerkt met banken welzijnsorganisaties en onderwijsinstellingen.
Met de Europese NIS2-richtlijn in aantocht, worden voor gemeenten de wettelijke eisen aan digitale veiligheid hoger. De bestuurlijke gespreksronde is ten einde, maar aan een vervolg wordt hard gewerkt. Samen met cyberburgemeesters en de VNG-commissies is een visitatieronde in voorbereiding. De vrijblijvendheid gaat eraf, en dat is nodig om gemeenten ook in de toekomst digitaal veilig te houden.

Prioriteit 4

Versterken weerbaarheid inwoners en ondernemers

Versterk de weerbaarheid tegen cybercriminaliteit

- Cybercriminelen worden professioneler en slaan steeds vaker toe.
- Het blijft de vraag of maatregelen hiertegen lokaal of landelijk genomen moeten worden.
- Ervaringsverhalen helpen de aandacht voor weerbaarheid te bevorderen.

> 'Er is geen verschil meer tussen de fysieke en de online wereld'
>
> **Sharon Dijksma**
> burgemeester Utrecht

- Voor adequate ondersteuning is eerder zicht op potentiële dreigingen nodig.
- Dat legt beslag op politiecapaciteit en vraagt verruiming van bevoegdheden.

Scan de QR-code en bekijk een praktijkvoorbeeld uit Leeuwarden

Prioriteit 5

Voorbereiding op digitale ontwrichting, incidenten en crises

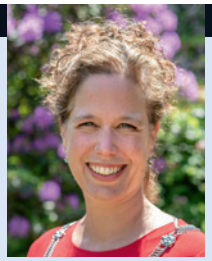
Neem de regie in regionale samenwerkingsverbanden

- Incidenten- en crisissituaties hebben steeds vaker digitaal en fysiek impact.
- Inwoners verwachten dat de gemeente ook hun digitale veiligheid garandeert.

> 'Elke gemeente zou jaarlijks moeten trainen op integrale crisissituaties'
>
> **Sjoerd Potters**
> burgemeester De Bilt

- Gemeenten kunnen digitale veiligheid uitdagingen niet alleen aan.
- Het ontbreekt bestuurders en experts aan voldoende handelingsperspectief.
- Er is verduidelijking nodig van regelgeving en opschalingsstructuren.

Scan de QR-code en bekijk een praktijkvoorbeeld uit De Bilt



Ester Weststeijn
burgemeester van Rozendaal
en lid van de VNG-commissie
Informatiesamenleving

DIGITALE VEILIGHEID IS MENSENWERK

Halverwege de zaal zit een oudere vrouw. Haren keurig gekapt, verzorgd uiterlijk, klein van stuk. Ze steekt haar hand half omhoog. Haar stem klinkt aarzelend als ze het woord krijgt. Ze vertelt hoe het ook háár overkwam: zo'n heel vriendelijke vrouw van de bank die haar belde en vertelde dat er een verdachte betaling was gedaan vanaf haar rekening. De betaalpas moest onmiddellijk vervangen worden. Nog geen half uur later stond er een man voor de deur. Keurig in pak, correct, vriendelijk. Ze gaf hem haar pinpas mee. Op dát moment kwam haar schoondochter de straat in en trok de juiste conclusie. De oh zo representatieve man nam de benen; de schoondochter rende erachteraan. De vrouw in de zaal wil het eigenlijk niet vertellen. Dat ze erin trapte! De impact was groot, al roemt ze de inzet van de politie. Ze is angstig geworden.

Deze vrouw is mijn overbuurvrouw, 89 jaar oud. Ze is één van de velen – volgens het CBS jaarlijks 2,2 miljoen Nederlanders – die slachtoffer worden van gedigitaliseerde criminaliteit of cybercrime. Ze vertelde haar verhaal op een drukbezochte avond over allerlei vormen van digitale fraude die de gemeente samen met de politie en een bank organiseerde voor 'de wat oudere Rozendaler'.

Hoe anders zijn de gesprekken tijdens mijn portefeuillehoudersoverleg 'I-domein': het overleg waarin ik met medewerkers spreek over het digitale veld, en in het bijzonder digitale veiligheid. Over het actieplan Informatiebeveiliging. De quick scan impact NIS2. De sessie informatieveiligheid & privacy voor de gemeenteraad. Over leveranciersperikelen, risicoanalyses en audits. Overleggen die vaak technisch worden. Het lijkt een andere wereld. Een wereld waarin de openbare orde en veiligheid soms het onderspit delven in het geweld van alle inzet die nodig is om 'eigen huis op orde' te krijgen. Om zélf als gemeentelijke organisatie geen slachtoffer te worden van een hack. Mijn gemeenteraad zucht eronder: onvoldoende structureel geld, technisch complex en weer nieuwe wettelijke verplichtingen. Het verhaal van mijn overbuurvrouw helpt me om de ándere kant steeds maar weer te benoemen. Want als gemeentebestuurder kun je niet kiezen: je moet beiden aanpakken. Digitale veiligheid en 'cyber' staat ook in ons Integraal Veiligheidsbeleid. Net zoals in vele gemeenten. Nu moeten we er nog integraal naar handelen.

Wij bestuurders zijn ervoor om continu álle aspecten van digitale veiligheid te benoemen en op urgentie te drukken. Hoe kan het wél? Het gaat niet alleen over de vraag of je de ENSIA-audit op tijd hebt afgerond. Het gaat net zo goed over digitale weerbaarheid van inwoners en bedrijven, over online aangejaagde ordeverstoringen en de voorbereiding op incidenten en crises met een cybercomponent. Dat is onze taak: wij moeten als bestuurders staan voor digitale veiligheid. Voor mijn overbuurvrouw, en voor ons allemaal.

WIJ MOETEN ALS BESTUURDERS STAAN VOOR DIGITALE VEILIGHEID

ESSENTIËLE DIENSTEN

7 vragen over NIS2

ER KOMT VEEL REGELGEVING AAN OP HET GEBIED VAN **DIGITALE VEILIGHEID**, WAARONDER NIS2. WAT BETEKENT DIT ALLEMAAL VOOR GEMEENTEN? WE ZETTEN EEN AANTAL BRANDENDE VRAGEN OP EEN RIJ.

1 WAT IS DE NIS2-RICHTLIJN PRECIES?

De Europese Network and Information Security-directive, of NIS2-richtlijn, is bedoeld om de cyberbeveiliging en de weerbaarheid van essentiële diensten, waaronder lokale overheden, in EU-lidstaten te verbeteren. Betere informatiebeveiliging dus. De richtlijn geeft gemeenten een registratieplicht, een zorgplicht voor digitale veiligheid, een meldplicht voor significante (cyber)issues en het recht op hulp bij digitale incidenten. Op dit moment wordt de richtlijn naar Nederlandse wetgeving vertaald. De bepalingen worden opgenomen in Cyberbeveiligingswet.

2 HOE STAAT NIS2 IN VERHOUDING TOT BIJVOORBEELD DE BIO, DE DIGITAL DECADE EN DE CER-RICHTLIJN?

De NIS2-richtlijn is onderdeel van de EU Digital Decade. Dat is het Europese programma dat de digitale transformatie van Europa wil bevorderen. Om de fysieke, digitale en economische weerbaarheid te versterken, heeft de Europese Unie twee richtlijnen aangenomen. Naast de NIS2-richtlijn gaat het om de Critical Entities Resilience Directive (de CER-richtlijn). Die gaat over het fysieke domein. Wanneer een entiteit onder de CER-richtlijn wordt aangewezen, is deze automatisch essentieel onder NIS2.
In NIS2 worden minimale informatiebeveiligingsmaatregelen geëist, die verwerkt zijn in de Baseline Informatiebeveiliging Overheid 2.0 (BIO). De BIO 2.0 wordt dan weer wettelijk verankerd in nadere regelgeving van de NIS2-implementatiewet (Cyberbeveiligingswet). Zo komt er één basisniveau voor informatiebeveiliging voor alle overheidsorganisaties.

3 WAAROM IS NIS2 BELANGRIJK VOOR GEMEENTEN?

Overheden, waaronder gemeenten, zijn essentieel verklaard onder de NIS2-wetgeving. Dit betekent dat digitale veiligheid een wettelijke plicht wordt. De vrijblijvendheid is eraf. Nieuw is dat er naast toezicht achteraf, ook vooraf audits kunnen worden uitgevoerd op de digitale beveiliging van de gemeenten. Hiervoor is de

Rijksinspectie Digitale Infrastructuur (RDI) aangewezen als toezichthouder.

4 WIE MOET ER GAAN HANDELEN?

Gemeenten krijgen een wettelijke zorgplicht voor digitale veiligheid. Voor bestuurders betekent de NIS2 dat zij voldoende budget moeten reserveren voor de implementatie van de Cyberbeveiligingswet.

5 HOE ZIT HET MET GEMEENTELIJKE SAMENWERKINGSVERBANDEN?

Nederland kent meer dan vierhonderd gemeenschappelijke regelingen. Een gemeenschappelijke regeling valt onder de NIS2, mits het voldoet aan de criteria van een overheidsinstelling van de Cyberbeveiligingswet. Samenwerkingen op het gebied van bedrijfsvoering en ICT hebben er indirect mee te maken omdat de deelnemende gemeenten zich moeten verantwoorden over de digitale veiligheid bij deze regelingen.

6 WELKE VRAGEN MOET IK ALS BESTUURDER STELLEN AAN MIJN ORGANISATIE?

Raadsleden kunnen het college vragen naar de manier waarop de gemeente omgaat met informatiebeveiliging en hoe toegankelijk en betrouwbaar de gemeente is. Een bestuurder kan aan de ambtelijke leiding vragen welke ondersteuning zij biedt aan de afdelingen om de Cyberbeveiligingswet te implementeren, wat de grootste risico's zijn voor de continuïteit van de gemeentelijke dienstverlening en hoe die worden aangepakt.

7 WAT DOET DE VNG VOOR GEMEENTEN?

Voor de VNG staan de haalbaarheid, betaalbaarheid en uitvoerbaarheid van de nieuwe wetgeving voorop. De VNG voert een lobby richting de ministeries, zodat gemeenten de wet straks kunnen uitvoeren. De wet moet duidelijk maken wat er van bestuurders, ambtenaren en raadsleden wordt verwacht. Voor een goede implementatie pleit de VNG voor structurele financiering voor gemeenten. Maar ook de implementatie is van belang. Daarom houdt de VNG via haar webpagina en forum gemeenten op de hoogte van de laatste ontwikkelingen.
Ook worden regelmatig webinars georganiseerd om gemeenten te helpen bij de voorbereiding. Vanzelfsprekend kunnen de informatiebeveiligingsfunctionarissen (CISO's) rekenen op advies en ondersteuning vanuit de Informatiebeveiligingsdienst (IBD).

Wilt u meer weten over NIS2, kijk dan op vng.nl/nis2 of mail: teamadv@vng.nl.

Gemeenten krijgen een *wettelijke zorgplicht* voor digitale veiligheid

Over de Agenda Digitale Veiligheid

De Agenda Digitale Veiligheid adviseert bestuurders, (beleids)medewerkers van gemeenten en raadsleden over digitale veiligheid. Zo ondersteunen wij gemeenten bij het voorkomen, bestrijden en oplossen van cybercriminaliteit en -incidenten. Met elkaar zorgen we voor meer (bestuurlijke) bewustwording, betrokkenheid en kennisdeling.

Meer weten? Kijk op onze website en onze Pleio pagina. Scan de QR code: