Beveiliging van Operationele Technologie (OT) door gemeenten

Resultaten van een enquête onder CISO's ter voorbereiding op de NIS2 richtlijn

Lectoraten *Cybersecurity & Safety en Changing Role of Europe, juni* 2024

let's change
YOU. US. THE WORLD.

DE HAAGSE HOGESCHOOL

Beveiliging van Operationele Technologie (OT) door gemeenten

Resultaten van een enquête onder CISO's ter voorbereiding op de NIS2 richtlijn

Auteurs

Emiel Kerpershoek, Lectoraat *Cybersecurity & Safety*

Ludger Niemann, Lectoraat *Changing Role of Europe*

Kenniscentra
Cyber Security & Global and Inclusive Learning (GIL)

Datum
juni, 2024

Type project
Rapportage

Versie
1

Inleiding

Sluizen, bruggen en verkeersinstallaties zijn voorbeelden van Operationele Technologie (OT) die in Nederland ook door gemeenten wordt beheerd. Hoe is het gesteld met de digitale beveiliging van deze vitale infrastructuur?

In opdracht van de *Vereniging van Nederlandse Gemeenten* (VNG) en in samenwerking met de *Informatiebeveiligingsdienst* (IBD) hebben wij als onderzoekers van de lectoraten *Cybersecurity & Safety* en *Changing Role of Europe* van De Haagse Hogeschool een enquête uitgezet over de digitale beveiliging van Operationele Technologie (OT-) objecten van Nederlandse gemeenten.

Wij werden bij dit project geholpen door tweedejaarsstudenten van de opleiding Integrale Veiligheidskunde (IVK) die waardevolle input hebben geleverd op de vragenlijst.

De enquête werd gericht op de Chief Information Security Officers (CISO's) van Nederlandse gemeenten en had tot doel om een indruk te geven van de status van de cybersecurity van uiteenlopende OT-objecten en de stand van voorbereiding op de NIS2-richtlijn. Dit is een wettelijke verplichting van de EU die in het najaar 2024 van kracht wordt.

In totaal hebben 65 respondenten de enquête ingevuld. Gezien de vrijwilligheid van deelname kunnen we niet stellen dat de antwoorden representatief zijn voor alle gemeenten. De geanonimiseerde data geven echter belangrijke inzichten in het spectrum van meningen onder de CISO's. Gemeenten verschillen in de mate van voorbereiding op digitale dreigingen, maar geven gemiddeld slechts een "5" als rapportcijfer voor de algehele beveiliging van OT.

Dit verslag begint met een beknopte beschrijving van onze onderzoeksvraag op gebied van "gemeentelijke OT". Hierop volgt een toelichting op de onderzoeksmethode. Vervolgens presenteren we de belangrijkste enquêteresultaten die we illustreren met een selectie van ontvangen commentaren. Veel leesplezier!

Inhoudsopgave

1 Operationele Technologie en de EU richtlijn *NIS2*

Nederland monitort eens per jaar het algemene “cyberbewustzijn”: Volgens de laatste peiling in opdracht van de Rijksoverheid is de aandacht en actiebereidheid bij bedrijven en consumenten voor digitale veiligheid opnieuw iets toe genomen[1]. De meeste burgers – en waarschijnlijk ook bestuurders – denken daarbij aan risico’s als phishing, hacken en malware die zich voordoen in de informatie- en communicatietechnologie (ICT).

“Operationele technologie” (OT) daarentegen krijgt minder algemene aandacht maar is ook cruciaal voor de publieke veiligheid. OT is een verzamelnaam voor systemen die worden gebruikt voor het digitale beheer, besturing en bediening van fysieke of industriële apparatuur en ook gemeentelijke infrastructuur. Er zijn tegenwoordig nog maar weinig bruggen in Nederland die zonder enige netwerkverbinding “handmatig” geopend en gesloten worden. Gemeenten dragen specifiek de verantwoordelijkheid voor stedelijk grondwaterbeheer en staan in voor de afvoer van afvalwater en overtollige neerslag via riolering. Ze beheren ook lokale wegen, verkeersinstallaties en zwembaden. In dit hele domain doet telkens meer automatisering zijn intrede, en dat brengt kansen voor efficiëntie maar ook cyberrisico’s door menselijke fouten, hacking en malware.

De *Vereniging van Nederlandse Gemeenten* (VNG) (www.vng.nl) is actief voor gemeentes op vlak van kennisdeling, belangenbehartiging en dienstverlening. Op gebied van informatiebeveiliging en privacy biedt de Informatiebeveiligingsdienst (IBD) van de VNG essentiële ondersteuning voor gemeenten. Veranderingen in wettelijke kaders spelen daarbij een belangrijke rol. Actueel heel relevant is de herziening van de *Europese Network and Information Security* (NIS) richtlijn die tot doel heeft de cyberbeveiliging en weerbaarheid van essentiële diensten in EU-lidstaten te verbeteren. In tegenstelling tot de oorspronkelijke NIS-richtlijn uit 2016, vallen lokale overheden nu ook onder de NIS2-richtlijn. Dit betekent dat Nederlandse gemeenten vanaf oktober 2024 moeten voldoen aan strengere eisen op het gebied van informatiebeveiliging, ook wat betreft hun OT-objecten. Zij moeten onder andere passende en evenredige maatregelen nemen om cyberbeveiligingsrisico’s te beheersen en een risicobeoordeling uitvoeren.

Volgens de VNG is er op dit moment onvoldoende zicht op de beveiliging van gemeentelijke OT[2]. Dit maakt het lastig om in te schatten wat er voor nodig is om te kunnen voldoen aan de eisen van de NIS2[3]. Dit onderzoek richt zich daarom op de vraag: **Hoe staat de beveiliging van gemeentelijke OT-objecten ervoor, en hoe ver zijn Nederlandse gemeenten met de voorbereiding op de NIS2-richtlijn?**

Ter beantwoording van deze vraag hebben wij een onderzoek ontwikkeld dat gericht is op de perspectieven van gemeenten zelf. De succesvolle ontwikkeling van cyberweerbaarheid op gemeenteniveau vergt o.a. de juiste technische kennis, geschikte werkprocessen en organisatie-brede ondersteuning van het bestuur tot de werkvloer. Deze integrale aspecten zijn daarom opgenomen in een vragenlijst die aan gemeenten werd voorgelegd. Elke gemeente heeft in principe een *Chief Information Security Officer* (CISO) in dienst, en de CISOs van alle 342 gemeenten werden daarom geïdentificeerd als de ideale ontvanger van de vragenlijst.

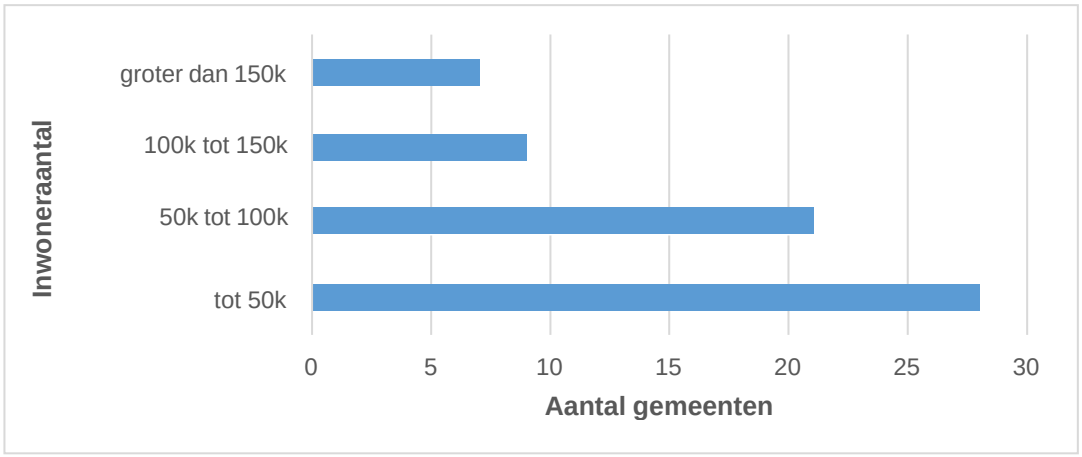
[1] https://www.rijksoverheid.nl/actueel/nieuws/2023/10/02/nederlands-bewustzijn-online-veiligheid-verbetert-maar-nog-niet-voldoende
[2] https://www.binnenlandsbestuur.nl/digitaal/hoe-gemeenten-de-security-van-sluizen-en-bruggen-kunnen-verbeteren
[3] NIS2 wordt in Nederland geïmplementeerd middels de Cyberbeveiligingswet

2 Methode en steekproef

De vragenlijst werd in een digitaal platform (Questback.com) geconstrueerd en de uitnodigingslink door de IBD verspreid onder een groep van 996 CISO's en aanverwante functionarissen die werkzaam zijn bij een van de 342 Nederlandse gemeenten of bij ambtelijke ICT-samenwerkingsverbanden. De enquêtegegevens zijn verzameld tussen 25 januari en 15 februari 2024. In totaal hebben 66 personen de enquête afgerond. Eén respondent is verwijderd uit de analyse omdat deze, naar eigen zeggen, te kort in functie was om de vragen te kunnen beantwoorden. De uiteindelijke steekproef van 65 deelnemers omvat 51 CISO's, 6 ISO's, 1 TISO, 1 manager Openbare Ruimte, 1 manager OT-security en 5 adviseurs informatiebeveiliging.

Aangezien gemeenten niet meer dan 1 CISO in dienst hebben, kan uit deze data worden opgemaakt dat tenminste 51 unieke gemeenten aan het onderzoek hebben deelgenomen. Doordat in de enquête niet is gevraagd naar de naam van de deelnemer of van de gemeente waarin deze werkzaam is, kan het aantal gemeenten in de steekproef niet nader worden gespecificeerd. Enkele respondenten schreven in commentaarvelden ongevraagd de naam van de gemeente waarvoor zij werken. In dit verslag hebben we hun citaten geanonimiseerd door alleen de provincie aan te duiden.

De omvang van de gemeenten waarvoor de deelnemers werkzaam zijn varieert van 10.000 tot inwoners. Van de 65 deelnemers is ongeveer een kwart werkzaam bij een gemeente met meer dan 100.000 inwoners – zie Figuur 1.



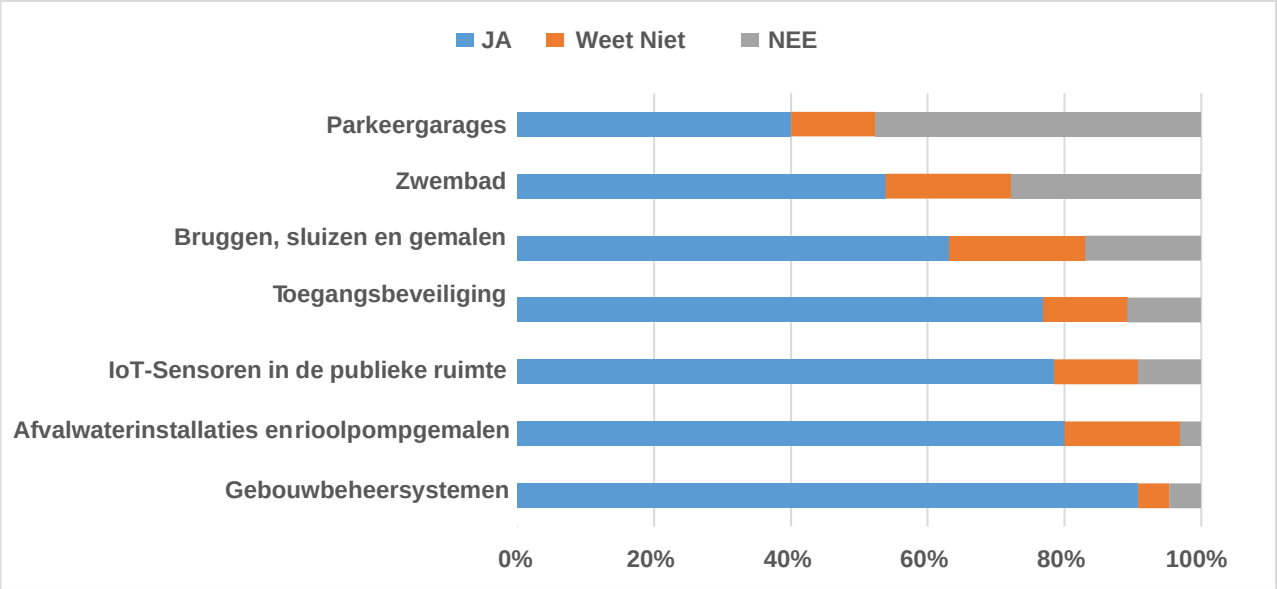
Figuur 1 - Omvang van gemeenten waar respondenten werkzaam zijn

3 Enquêteresultaten

De vragenlijst bevatte 30 vragen waaronder 5 met velden voor toelichtingen en commentaren. In deze sectie presenteren wij resultaten per onderwerp. De focus ligt op de gesloten vragen die zich lenen voor een cijfermatige analyse en grafiek. Daarbij staan enkele relevante citaten.

3.1 Soort van OT-objecten per gemeente

In de enquête is deelnemers gevraagd voor welke OT-objecten hun gemeente verantwoordelijk is. Hierbij zijn 7 categorieën van OT-objecten voorgelegd. Gemiddeld rapporteren de deelnemers zo'n 5 OT-objecten voor hun gemeente. Dit levert het volgende beeld op (Figuur 2) van de OT-objecten die bij de deelnemers in beeld zijn.

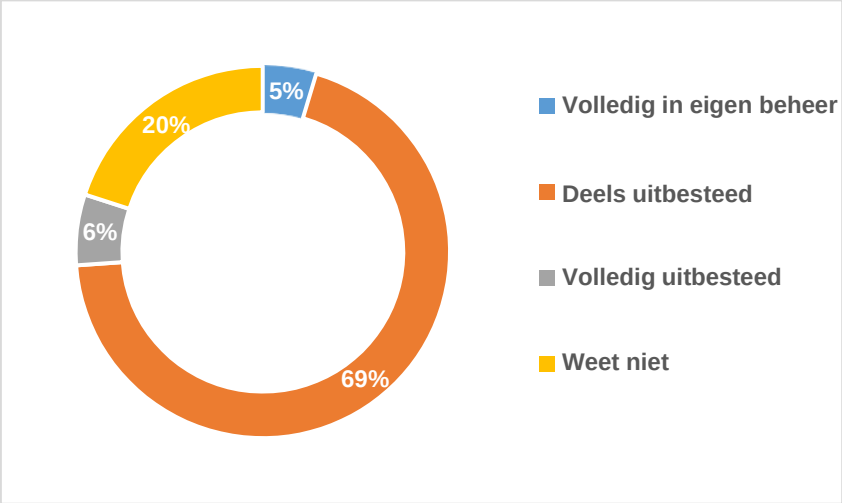


Figuur 2 – OT-objecten waar gemeenten (van respondenten) voor verantwoordelijk zijn

Naast deze 7 categorieën noemde 20% van de deelnemers nog één of meerdere andersoortige OT-objecten, waaronder verkeersregelinstallaties, parkeerautomaten, ondergrondse afvalcontainers (ORAC's), tunnels, matrixborden en gebouw-gebonden systemen als laadpalen en zonnepanelen.
Enkele respondenten gaven aan dat zij het moeilijk vonden om concreet aan te geven voor welke OT-objecten zij verantwoordelijk zijn.

3.2 Beheer van OT-objecten in gemeenten

Hoe worden gemeentelijke OT-objecten beheerd? Ruim twee derde van de deelnemers geeft aan dat het beheer van de OT-objecten deels is uitbesteed en deels wordt ingevuld door de gemeente zelf – zie Figuur 3.



Figuur 3 - Beheer van OT-objecten

Verder geeft 20% van de deelnemers aan niet goed te weten hoe het beheer van de OT-objecten is ingericht. In dit kader is de volgende opmerking tekenend die de CISO van een gemeente met 29.000 inwoners maakte:

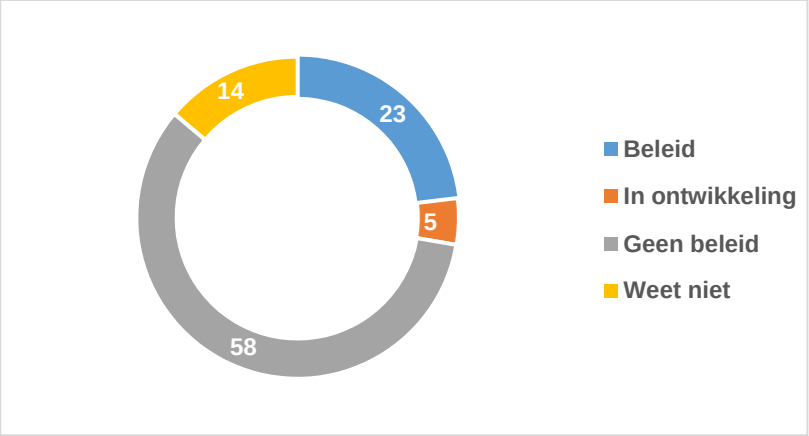
> **"Wat is uitbesteed, wordt niet door mij gecontroleerd en kan ik dus niet zeggen."**

Een andere CISO (van een gemeente met 25.000 inwoners) zegt er het volgende over:

> **"We moeten hier als Nederlandse gemeenten nog mee beginnen. Het begint met inventariseren; bijna geen gemeente in NL heeft dit beeld helder (begrepen van IBD en geverifieerd in regio)."**

3.3 Aanwezigheid van beleid, plannen en procedures

"Is er binnen uw gemeente beleid en/of zijn er procedures of plannen gericht op de cybersecurity van OT-objecten?". Op deze vraag geeft iets minder dan een kwart van de respondenten aan dat er beleid, plannen of procedures gericht op de cybersecurity van de OT in werking zijn. Zaken die hierin worden genoemd zijn een cybersecurityplan in lijn met CSIR, BIACS, BIO of andere relevante normenkaders, beheerplannen, incidentmanagement procedures of koppeling met het ISMS.
Het merendeel van de deelnemers (58%) laat weten dat er geen beleid is gericht op OT-security of dat zij hier niet van op de hoogte zijn (14%). Vergelijking toont aan dat de met name deelnemers uit wat grotere gemeenten aangeven te beschikken over beleid, plannen of procedures gericht op OT-security (gemiddeld 130.000 inwoners) dan deelnemers die aangeven daar niet over te beschikken (gemiddeld 74.000 inwoners).



Figuur 4 Aanwezigheid van beleid, procedures en plannen gericht op OT-security

Hoe maak je beleid? De CISO van een van de grootste gemeentes van Nederland geeft het volgende advies:

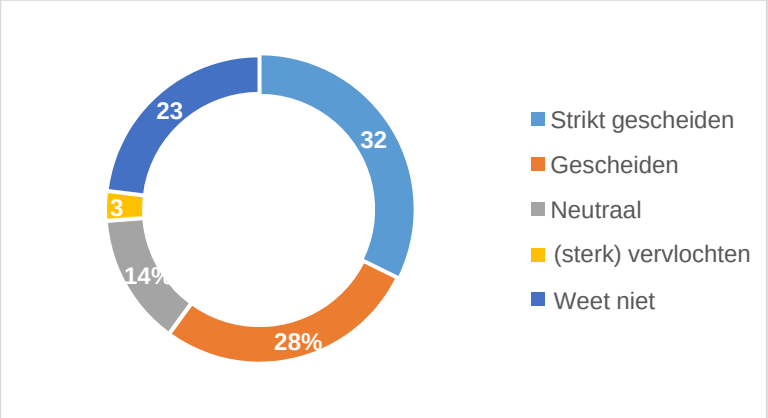
> **"OT behandelen als 'IT in de buitenruimte' en op dezelfde manier behandelen."**

3.4 Vervlechting van gemeentelijke IT- en OT-systemen

Een ruime meerderheid van de deelnemers (60%) is van mening dat de IT-systemen en OT-objecten van de gemeenten adequaat zijn gescheiden van elkaar. Voorbeelden van segmentatiemaatregelen die hierbij worden genoemd zijn fysiek gescheiden netwerken, aparte VLAN's, 4G router met simkaart of ondergebracht bij een SAAS-leverancier. Een enkele deelnemer merkt op dat de IT wel kan functioneren zonder OT, maar niet andersom. Citaat van de CISO:

> **"IT kan gescheiden draaien van OT, maar OT kan niet gescheiden draaien van IT."**

Deelnemers gaan hierbij niet in op invloed van zaken als hoe wordt omgegaan met beheer door derden of met mogelijkheden voor beheer op afstand. Verder valt op dat iets minder dan een kwart van de deelnemers aangeeft niet goed te weten in hoeverre de IT-systemen en OT-object met elkaar zijn vervlochten – zie Figuur 5.



Figuur 5 Inschatting van de mate van vervlechting van gemeentelijke IT- en OT-systemen

De mate van vervlechting is ook niet uniform voor alle soorten OT-objecten. In de woorden van de CISO van een gemeente met ruim 60,000 inwoners:

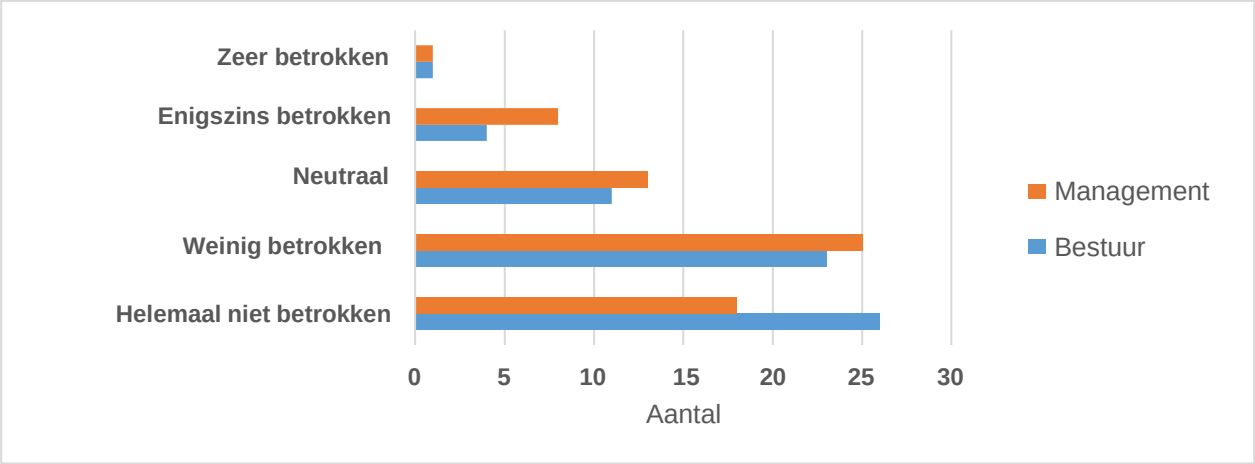
> **"Erg afhankelijk van het type object. [..]. Soms door middel van 4G-routertje met aparte simkaart voor een specifiek object, soms gescheiden met VLAN, soms volledig ontkoppeld van zowel LAN als WAN (zoals bij zonnepanelen)."**

3.5 Normenkaders voor OT-security

Van de 65 deelnemers is 39% bekend met de CSIR als normenkader voor OT-security. Iets meer dan 10% van de deelnemers geeft aan in de praktijk ook gebruik te maken van de CSIR bij het beveiligen van hun OT-objecten, in enkele gevallen aangevuld met het gebruik van andere normenkaders voor OT-security. Een additionele 5% van de deelnemers geeft aan geen gebruik te maken van CSIR, maar wel van andere normenkaders voor OT-security. Normenkaders die in dit verband worden genoemd zijn de BIO, IEC62443, BIACS (afgeleid van CSIR) NIS2, ISO 27001 en 27002 en de Handreiking PA- systemen van VNG.

3.6 Aandacht van bestuur en management voor OT-security

"In hoeverre is het bestuur van uw gemeente betrokken bij het inrichten van de cybersecurity van de OT-objecten?" Op deze vraag geeft en ruime meerderheid van de deelnemers aan dat er vanuit het bestuur (75%) en management (66%) van de eigen gemeente weinig tot geen betrokkenheid is bij het inrichten van OT-security. Zie Figuur 6. Een beperkte betrokkenheid vanuit het bestuur gaat hierbij ook vaak gepaard met een beperkte betrokkenheid vanuit het management (correlatiecoëfficiënt = 0,78).



Figuur 6 Mate van betrokkenheid van bestuurders en managers van de eigen gemeente bij het inrichten van OT-Security

Meerdere respondenten uitten hun zorgen over de betrokkenheid van gemeentelijke beslissers. In de woorden van de CISO van een gemeente in Zuid-Holland met meer dan 100.000 inwoners:

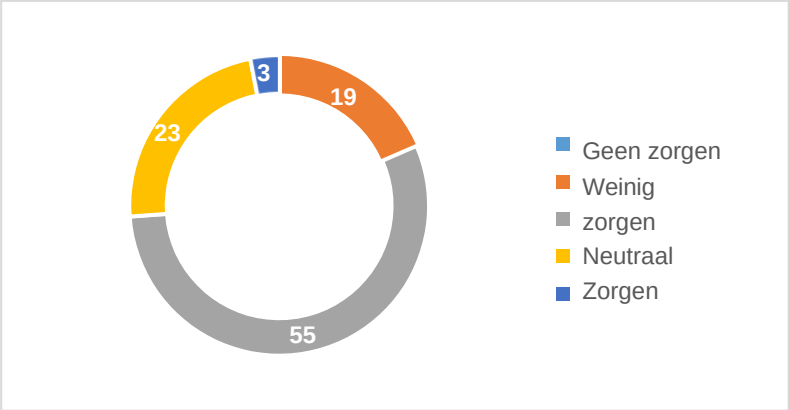
> **"Informatiebeveiliging heeft niet de interesse van bestuurders en de directie, zelfs niet na twee flinke incidenten. We hebben al 14 maanden geen CISO terwijl die wettelijk verplicht is."**

Een andere CISO (gemeente van 40.000 inwoners) verwoorde zijn ervaring als volgt:

> **"Het is lastig het hogere management en het bestuur en of raad erbij te betrekken. Ik heb diverse keren mijn bezorgdheid uitgesproken. Ze zijn het er allemaal mee eens. Maar als je komt met concrete oplossingen kan het niet."**

3.7 Zorgen om cyberincidenten met OT-objecten van de eigen gemeente

"In hoeverre maakt u zich zorgen om cyberincidenten met OT-objecten in uw gemeente?" Volgens de antwoorden op deze vraag maken respondenten zich beperkt zorgen om eventuele cyberincidenten die de OT-objecten van hun gemeenten zouden kunnen treffen. Ongeveer een kwart geeft aan zich hier (grote) zorgen om te maken – Zie Figuur 7. Geen van de deelnemers gaf aan zich hierover geen zorgen te maken.



Figuur 7 Mate van zorgen om cyberincidenten met OT-objecten van de eigen gemeente

Desalniettemin noemen de deelnemers een breed scala aan negatieve effecten die als gevolg van een cyberincident met de OT-objecten van hun gemeente zouden kunnen optreden. Op de vraag “Wat is wat u betreft de maximale impact die een cyberincident bij de OT-objecten in uw gemeente kan veroorzaken”, schets een CISO (van een gemeente met rond 110.000 inwoners) het volgende scenario:

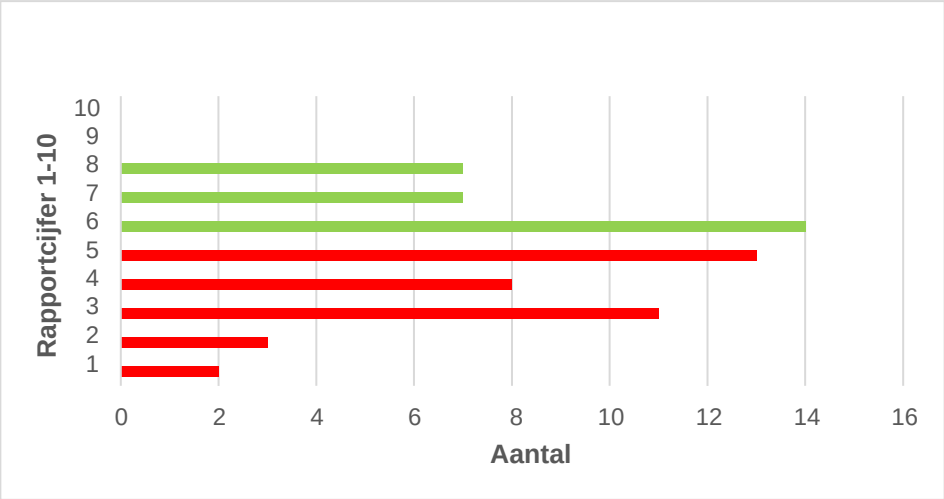
“Naast (grote) incidenten in de openbare ruimte ook datalekken. Camerabeelden die misbruikt worden; smart city componenten die overgenomen worden; brugbediening en sluisbediening; inbreuk interne netwerk; Gemaalbesturing die overgenomen wordt en tot milieuproblemen leiden of zelfs overstromingen.”

Andere respondenten zagen nog andere risico’s. Gevraagd naar de mogelijke impact van cyberincidenten met de OT-objecten zien wij grofweg de volgende categorieën terugkeren:

a) **Verstoring van rioolpompen en gemalen** kunnen weliswaar handmatig worden bediend, maar grootschalige en langduriger uitval kan leiden tot overlast door rioolafvoerproblemen, overstromingen, maar ook verontreiniging van oppervlaktewater met kans op verspreiding van ziekten of milieuschade.
b) **Verstoring van bruggen, sluizen,** maar ook ontregeling van **verkeersregelinstallaties** kan leiden tot verkeerschaos, ontwrichting van de stad en onbereikbaarheid voor hulpdiensten
c) **Hacking van gebouwbeheersystemen** kan leiden tot verstoring van de bedrijfsvoering maar belangrijker kan het ook dienen als opstap voor inbreuk op het interne IT-netwerk
d) **Schade door cyberincidenten met OT-objecten in bredere zin**. Hierbij houden deelnemers onder andere rekening met gevolgen van cyberincidenten met OT-objecten in de vorm van:
    - Schade door datalekken
    - Financiële schade door ransomware
    - Maatschappelijke ontwrichting en onrust bij inwoners en bedrijven
    - Imagoschade voor de gemeente

3.8 Rapportcijfer voor OT-security binnen de eigen gemeente

Een ruime meerderheid (57%) van de deelnemers geeft de gemeente waarvoor zij werkzaam zijn een onvoldoende rapportcijfer voor de cybersecurity van de OT-objecten – zie Figuur 8. Gemiddeld beoordelen de deelnemers hun gemeente met een 5,0 (SD = 1,82) op een schaal van 1 tot en met 10.



Figuur 8 Rapportcijfer van de cybersecurity van de OT-objecten van de eigen gemeente

Uitgesproken negatief zijn de deelnemer over het configuratiebeheer, waarvoor zij een gemiddeld rapportcijfer geven van 4,5 (SD = 2,08).
Deelnemers die de eigen gemeente een voldoende geven voor configuratiebeheer geven aan dat zij gebruikmaken van contract- en objectregistratie en management (CMDB); gebruikmaken van netwerkdiscovery en monitoring; ITIL systematiek toepassen; beheer en verantwoordelijkheden hebben belegd bij de vakafdelingen of scan en monitoring door een externe partij laten uitvoeren. Deelnemers zijn positiever over de inrichting van het toegangsbeheer, waarvoor zij een gemiddeld rapportcijfer geven van 6,6 (SD = 2,12).

3.9 Stappen om aan NIS2 te voldoen

Op de vraag om aan te geven “welke stappen u denkt dat uw gemeente moet ondernemen om aan de NIS2 richtlijn te voldoen” hebben veel respondenten een antwoord gegeven. Enkele zijn terughoudend. Een voorbeeld hiervoor is de volgende uitspraak van de CISO van een gemeente met ruim 35.000 inwoners:

“Zodra duidelijk wordt of gemeentes gezien worden als essentiële organisaties, nemen we maatregelen. Tot die tijd volgen wij de informatie van de IBN/VNG hieromtrent en volgen we seminars. Maar we lopen niet vooruit op de muziek.”

Andere respondenten zien het wel als hun taak aan om proactief te zijn. In de woorden van een andere CISO (gemeente met 61.000 inwoners):

“Zowel OT als IoT is momenteel grotendeels nog een blinde vlek. Hier werken we wel aan.”

In dit kader vragen enkele respondenten ook om ondersteuning van buiten. Zoals de respondent van een grote gemeente in Zuid-Holland schreef:

> **“Ik ben wel zeer benieuwd naar de uitslagen van dit onderzoek. Hopelijk komt er een vervolg op om vooral de kleinere gemeenten hierin te gaan ondersteunen, want die kunnen dit niet alleen.”**

4 Conclusies en aanbevelingen

Hoe staat de beveiliging van gemeentelijke OT ervoor, en hoe ver zijn Nederlandse gemeenten met de voorbereiding op de NIS2-richtlijn?

Voor de beantwoording van deze onderzoeksvraag is een enquêteonderzoek onder gemeentelijke *Chief Information Security Officers* (CISOs) uitgevoerd. Alhoewel niet alle 342 Nederlandse gemeenten hebben deelgenomen en de enquête, als zelfrapportage-instrument, geen objectieve meetgegevens biedt over cyberveiligheid, levert de enquête waardevolle inzichten op. Op basis van een grote respons (van tenminste 51 gemeenten) laten de uitkomsten van de enquête twee belangrijke trends zien. In de eerste plaats geeft het merendeel van de deelnemers de eigen gemeente een onvoldoende voor de algehele beveiliging van OT. In de tweede plaats valt op dat betrokkenheid van bestuur en management van gemeenten bij de inrichting van OT-security vaak nog erg beperkt is.

Uit veel commentaren die deelnemers aan de enquête hebben achtergelaten blijkt ook overeenstemming dat OT-security meer aandacht nodig heeft. Zoals een CISO schreef: “Op dit moment is dit bij ons zwaar onvoldoende in beeld!”

De uitkomsten van de enquête leiden tot de aanbeveling om de beveiliging van gemeentelijke OT-objecten en inbedding van OT-security vraagstukken in de organisatie nader in kaart te brengen en voortgang op dit gebied (inclusief de mate van *compliance* met de NIS2-richtlijn) regelmatig te evalueren. Tevens ligt de aanbeveling voor de hand om passende ondersteuning voor minder- en verder-gevorderde gemeenten te blijven ontwikkelen.