Onderzoeksopdracht OT-beveiliging binnen de kaders van NIS2

Aanleiding

In januari 2023 is de nieuwe Network and Information Systems Directive (NIS2-richtlijn) in werking getreden. De NIS-richtlijn is een wetgevingsinstrument van de Europese Unie (EU) dat initieel in 2016 is ingevoerd om de cybersecurity binnen de lidstaten te verbeteren. De herziening daarvan die begin 2023 van kracht is gegaan heeft tot doel de bestaande wetgeving te versterken door de reikwijdte van de richtlijn te vergroten, samenwerking tussen lidstaten te verbeteren en consistentie te garanderen in de gehele EU. Bovendien richt de NIS2-richtlijn zich ook op nieuwe en opkomende cybersecurity- bedreigingen, zoals het Internet of Things (IoT) en kunstmatige intelligentie (AI), en benadrukt de richtlijn naast IT-beveiliging ook de OT-beveiliging (Operational Technology). Per 17 oktober 2024 dienen alle EU-lidstaten de NIS2-richtlijn te hebben omgezet in nationale wetgeving. In Nederland wordt de implementatie bewerkstelligd middels de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni).

Context

De vernieuwde NIS2-richtlijn specificeert minimale cybersecurity maatregelen, gedetailleerd in artikel 21[1]. De richtlijn is uitgebreider en omvat nu 9 nieuwe sectoren, zoals vervoer (weg, water, spoor), afvalwaterbehandeling, drinkwatervoorziening en overheidsdiensten[2]. Gemeenten dragen de verantwoordelijkheid voor stedelijk grondwaterbeheer en staan in voor de afvoer van afvalwater en overtollige neerslag via riolering, zoals aangegeven in de Waterwet en Wet milieubeheer. Ze beheren ook lokale wegen.

De zorgplicht uit artikel 21 van de NIS2-richtlijn wordt verankerd in de Baseline Informatiebeveiliging Overheid (BIO) en heeft daarmee een wettelijke status. Voor uniformiteit tussen EU-lidstaten stimuleert de NIS2 het volgen van internationale standaarden, zoals ISO 27001 & 2 voor IT-security en IEC 62443 voor OT-beveiliging.

Hoewel gemeenten de BIO al hanteren als standaard voor IT-beveiliging, vereisen procesautomatiseringssystemen (PA-systemen) aanvullende beveiligingsnormen die de BIO niet dekt. Rijkswaterstaat heeft daarom de CSIR 2.4 (CyberSecurity Implementatie Richtlijn) gepubliceerd. Deze omvat de BIO en wordt waar nodig aangevuld met de IEC 62443. Het richt zich specifiek niet op kantoorautomatisering - waarvoor de BIO de beveiligingsstandaard is - maar op gemeentelijke processen waar PA relevant is. De CSIR is van toepassing op technische

[1] Artikel 21, p.127, NIS2-richtlijn https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022L2555&from=EN
[2] Bijlage 1, p.143, NIS2-richtlijn https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022L2555&from=EN

PA-systemen gerelateerd aan kunstwerken en objecten die meten, bedienen, beheren en monitoren.

Opdracht

Met het oog op de nieuwe wetgeving waar gemeenten tegen 17 oktober 2024 aan moeten voldoen, streeft de VNG ernaar duidelijkheid te verschaffen over de OT-beveiligingseisen voor elk object dat met een PA-systeem wordt geopereerd. Dit omvat:

- Besturing en bediening van afvalwaterinstallaties
- Besturing en bediening van bruggen en sluizen
- Besturing van gemalen
- Verkeersregelsystemen
- Gebouwbeheersingsystemen (verwarming, koeling, ventilatie, filtering, noodstroomvoorzieningen etc.)
- Als sensoren (camerasystemen, verkeerstellers en detectielussen), denk ook aan IoT
- Toegangsbeveiliging (slagbomen, elektronische hekwerken, camerasystemen)
- Parkeergarages
- Zwembaden

Werkwijze

1. **Teamformatie en focusselectie**
   Vorm koppels van twee personen, selecteer een van de bovenstaande onderzoeksdomeinen en noteer jullie namen. Kies vervolgens een gemeente om te onderzoeken welke OT-beveiligingseisen voor de betreffende objecten gelden.

Onderwerp/focus				
	Koppel-nummer	**Naam**	**Naam**	**Gemeente**
Besturing en bediening van afvalwaterinstallaties				
	Koppel 1			
	Koppel 2			
Besturing en bediening van bruggen en sluizen				
	Koppel 3			
	Koppel 4			
Besturing van gemalen				
	Koppel 5			
	Koppel 6			
Verkeersregelsystemen				
	Koppel 7			
	Koppel 8			
Gebouwbeheersingsystemen (verwarming, koeling,				
	Koppel 9			

ventilatie, filtering, noodstroomvoorzieningen etc.)	Koppel 10			
	Koppel 11			
Sensoren (camera systemen, verkeerstellers en detectielussen), inclusief IoT				
	Koppel 12			
	Koppel 13			
Toegangsbeveiliging (slagbomen, elektronische hekwerken, camera systemen)				
	Koppel 14			
	Koppel 15			
Parkeergarages				
	Koppel 16			
	Koppel 17			
Zwembaden				
	Koppel 18			
	Koppel 19			
	Koppel 20			

2. **Gemeenten contacteren**
   Alvorens met het onderzoek te beginnen, neem contact op met de gekozen gemeente om te bespreken welke specifieke objecten zij graag onderzocht willen hebben.
3. **Veldwerk en fotografie**
   Bezoek de OT-objecten persoonlijk en maak foto's van de besturingssystemen om een duidelijk beeld te krijgen van de huidige situatie. Het is essentieel om persoonlijk te ervaren en te begrijpen hoe deze systemen functioneren.
4. **Risico- en normanalyse**
   Voer een CSIR-analyse uit op de gekozen objecten om de huidige normen te identificeren en mogelijke risico's in kaart te brengen. Het doel is om een baseline veiligheidsniveau vast te stellen dat voor elk object zou moeten gelden.
5. **Interviews**
   Voer interviews uit met gemeenteambtenaren om een beeld te krijgen van de huidige en gewenste situaties, evenals de specifieke eisen voor OT-beveiliging bij nieuwe projecten. Besteed ook aandacht aan hoe bestaande systemen die al tientallen jaren in gebruik zijn, in dit plaatje passen.

Beoogde resultaten

Identificeer en rapporteer het volgende:

a. De huidige implementatiestatus van OT-beveiliging.
b. Een inschatting van de risico's geassocieerd met elk object
c. De baseline norm voor elk object en hoe ver de huidige situatie hiervan afwijkt.
d. Specifieke aanbevelingen en strategieën voor het overbruggen van eventuele kloven (wat moet er gebeuren om van de huidige situatie op de baseline veiligheidsniveau te komen?), inclusief hoe om te gaan met verouderde systemen in nieuwe projecten.