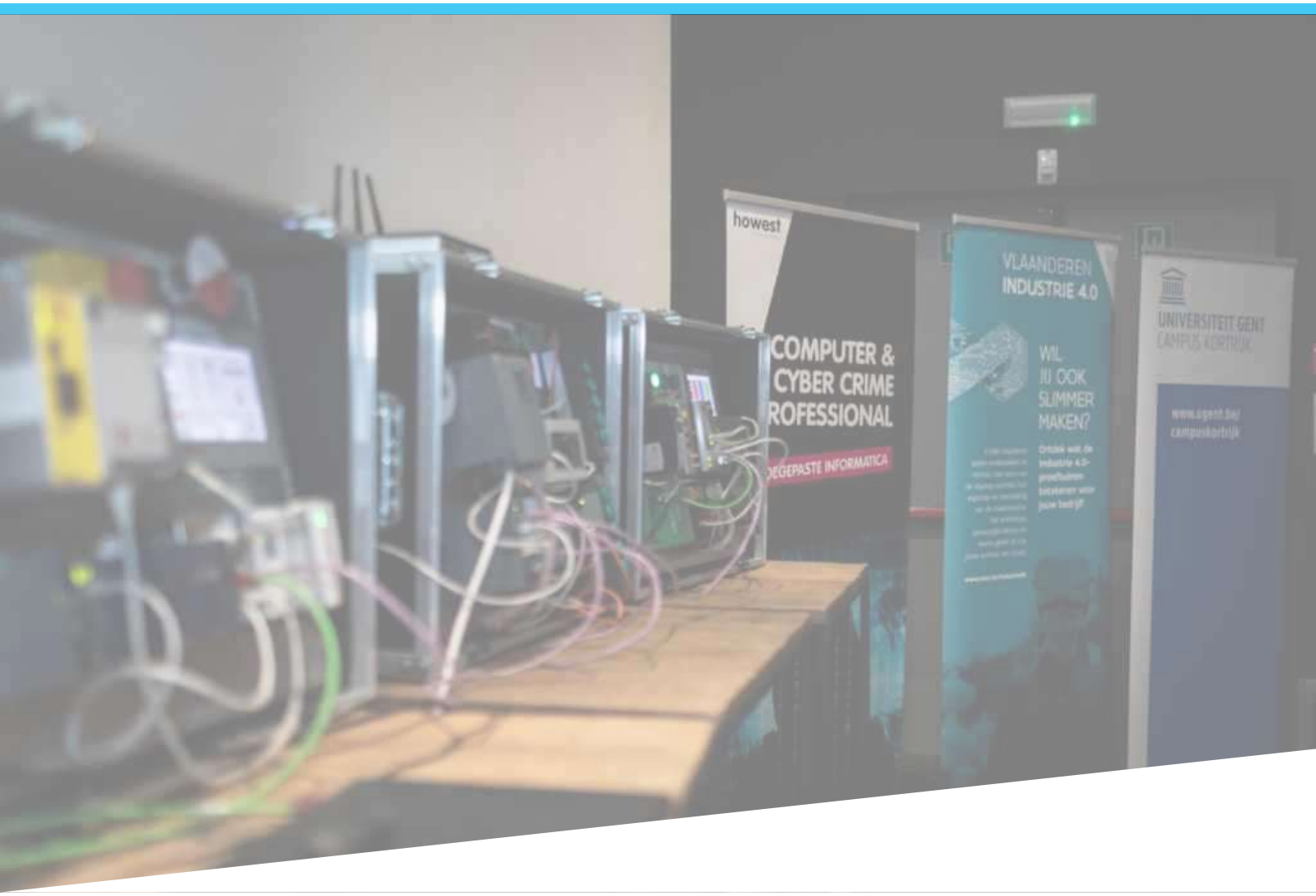
howest / cyber 3 lab



PROEFTUIN ICIL4.0

BEHOEFTEANALYSE: RAAKVLAKKEN EN VERSCHILLEN TUSSEN BEDRIJVEN

Cyber 3 Lab
Howest University of Applied Sciences research group

Table of Contents

Abstract

Deze studie presenteert een analyse van de cybersecuritymaturiteit bij zeven Vlaamse industriële organisaties uit de productie-, logistiek-, voedings- en drinkwatersector, gebaseerd op een uitgebreide enquête uitgevoerd tussen juni en juli 2025. De respondenten vertegenwoordigen een diverse mix van bedrijfsgroottes (11-250+ werknemers) met jaaromzetten tussen €10-50 miljoen en meer dan €50 miljoen, waarbij alle organisaties afhankelijk zijn van industriële controlesystemen (ICS/OT) die ouder zijn dan vijf jaar.

De bevindingen tonen een tweedeling in cybersecuritymaturiteit tussen organisaties met gevorderde beveiligingsprogramma's en bedrijven die nog worstelen met fundamentele cybersecurityuitdagingen. Slechts 14% van de organisaties beschikt over een volledig overzicht van hun ICS/OT-systemen, terwijl 43% continu hun asset-inventaris bijwerkt. Deze variatie in asset management vormt een kritieke uitdaging voor effectieve cybersecurityprogramma's.

Netwerksegmentatie is relatief goed geïmplementeerd met 43% volledig gescheiden IT/OT-netwerken en 86% firewall-implementatie, hoewel de maturiteit van firewall-regels varieert tussen basis- en strikte configuraties. Incident response-paraatheid toont echter zorgwekkende tekortkomingen: 29% heeft geen specifiek ICS/OT incident response plan en geschatte hersteltijden variëren drastisch van minder dan 4 uur tot meer dan 3 dagen.

De governance-maturiteit is gemengd, waarbij 71% directietoezicht heeft maar slechts 29% uitgebreide formele cybersecuritybeleid. Personeelstekorten vormen een kritieke bottleneck: slechts 14% heeft fulltime cybersecuritypersoneel en 71% besteedt minder dan 10% van hun IT/OT-tijd aan cybersecurity.

Dreigingsperceptie is realistisch georiënteerd op ransomware (86% van respondenten), supply chain-aanvallen (71%) en externe toegang (57%), wat overeenkomt met internationale trends. Technologie-adoptie toont universele VPN-implementatie (100%) maar beperkte geavanceerde monitoring (57% SIEM, 43% ICS/OT-antivirus).

Compliance-paraatheid voor NIS2 en andere frameworks is onvoldoende: hoewel ISO 27001 breed wordt gevolgd (57%) en ISA/IEC 62443 momentum krijgt (43%), voldoet geen enkele organisatie volledig aan alle moderne cybersecurityvereisten zonder aanvullende investeringen.

De studie identificeert drie kritieke behoeften: (1) kortetermijn-prioriteiten zoals geautomatiseerde asset discovery en incident response planontwikkeling, (2) middellange termijn-initiatieven waaronder micro-segmentatie en SOC-diensten, en (3) langetermijn-strategische behoeften zoals talent development en supply chain security management. Deze bevindingen bieden een evidence-based basis voor beleidsmakers, brancheorganisaties en cybersecurity dienstverleners om gerichte ondersteuning te ontwikkelen voor de digitale transformatie van de Vlaamse industrie.

Methodologie en Onderzoeksopzet

ENQUÊTEOPZET EN RESPONDENTENSELECTIE

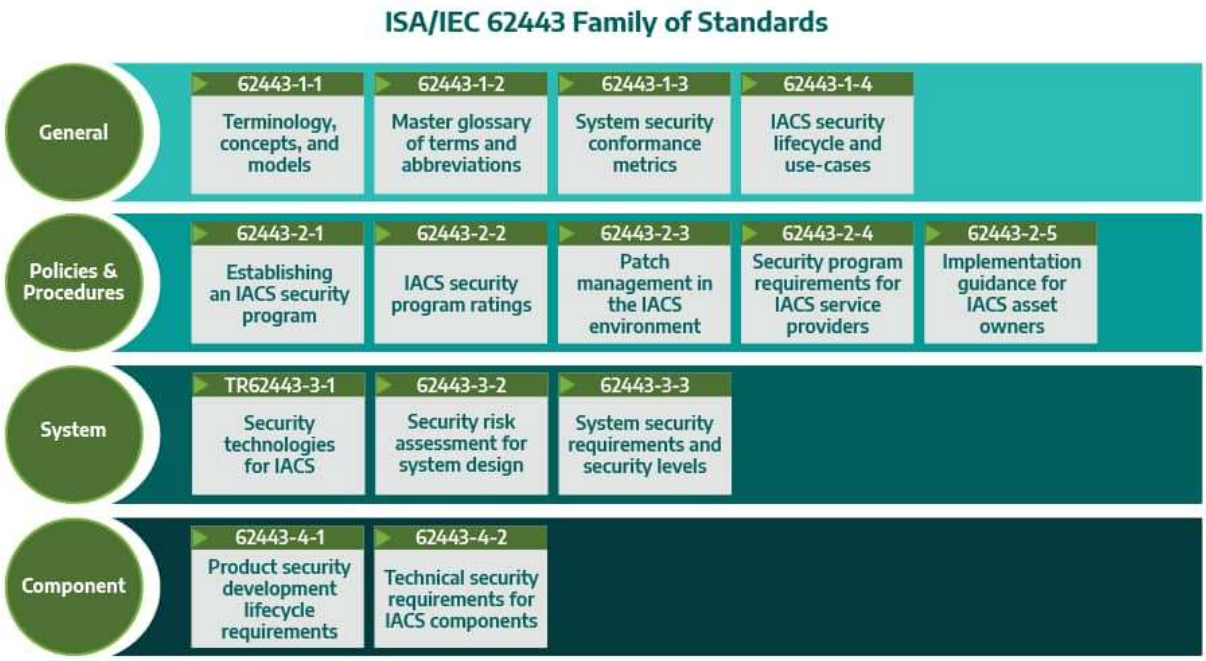
De enquête werd afgenomen bij verschillende organisaties uit verschillende industriële sectoren in Vlaanderen, waaronder productiebedrijven, logistiekondernemingen, voedingsbedrijven en een drinkwatermaatschappij. Deze diversiteit biedt een representatieve doorsnede van de Vlaamse industriële cybersecuritylandschap.

De organisaties variëren in grootte van 11-50 werknemers tot meer dan 251 werknemers, met jaaromzetten tussen €10-50 miljoen en meer dan €50 miljoen. Deze spreiding zorgt voor inzichten die relevant zijn voor zowel middelgrote als grote industriële organisaties.

ONDERZOEKSDOMEINEN

Het onderzoek evalueerde de cybersecuritymaturiteit op basis van internationale best practices en frameworks zoals ISA/IEC 62443, NIST Cybersecurity Framework en ISO 27001. De analyse richtte zich op acht kritieke domeinen:

- **Asset Management en Inventarisatie**: Volledigheid en actualiteit van ICS/OT-systeeminventarissen
- **Netwerksegmentatie en Architectuur**: Scheiding tussen IT- en OT-netwerken
- **Incident Response en Herstel**: Paraatheid voor cybersecurityincidenten
- **Governance en Risicobeheer**: Formele beleidsstructuren en toezicht
- **Personeel en Training**: Beschikbaarheid van gespecialiseerde expertise
- **Monitoring en Detectie**: Capaciteit voor continue beveiligingsbewaking
- **Dreigingslandschap**: Perceptie van primaire cybersecurityrisico's
- **Technologie-implementatie**: Adoptie van beveiligingstechnologieën



Bedrijfsprofielen en Sectorale Karakteristieken

DEMOGRAFISCHE VERDELING

De zeven respondenten vertegenwoordigen een diverse mix van industriële organisaties met verschillende niveaus van automatisering en digitale maturiteit:

Sector	Werknemers	Omzet	Locatie	Systeemleeftijd	Automatiseringsgraad
Productie	>251	>€50 mln	Zelzate	>10 jaar	>75%
Productie	51-100	€10-50 mln	Wielsbeke	>10 jaar	50-75%
Productie	51-100	€10-50 mln	Kortemark	5-10 jaar	25-50%
Logistiek	>251	>€50 mln	Antwerpen	>10 jaar	25-50%
Voeding	51-100	€10-50 mln	Izegem	>10 jaar	>75%
Productie	11-50	€10-50 mln	Breda	>10 jaar	25-50%
Drinkwater	101-250	>€50 mln	Antwerpen	>10 jaar	>75%

LEGACY SYSTEMEN EN MODERNISERINGSUITDAGINGEN

Een opvallende bevinding is dat zes van de zeven organisaties werken met systemen die ouder zijn dan tien jaar. Deze prevalentie van legacy systemen creëert aanzienlijke cybersecurityuitdagingen, aangezien deze systemen vaak werden ontworpen voordat cybersecurity een primaire ontwerpoverweging was.

Eén organisatie rapporteert systemen van 5-10 jaar oud, wat suggereert dat dit bedrijf recentelijk heeft geïnvesteerd in modernisering van hun industriële infrastructuur. Dit heeft mogelijk bijgedragen aan hun betere netwerksegmentatie (volledig gescheiden IT/OT-netwerken) ondanks beperkingen op andere gebieden.

Analyse van Cybersecuritymaturiteit per Domein

ASSET MANAGEMENT EN INVENTARISATIE

Een fundamenteel onderdeel van effectieve cybersecurity is het hebben van een volledig en actueel overzicht van alle ICS/OT-systemen. De enquêteresultaten tonen aanzienlijke variatie in asset management praktijken:

Volledigheid van Asset Overzicht:

- Volledig overzicht: 1 organisatie (14%)
- Grotendeels overzicht: 3 organisaties (43%)
- Gedeeltelijk overzicht: 3 organisaties (43%)

Update Frequentie van Asset Inventaris:

- Continu: 3 organisaties (43%)
- Elk kwartaal: 1 organisatie (14%)
- Jaarlijks: 2 organisaties (29%)
- Nooit: 1 organisatie (14%)

Eén organisatie toont best-practice met een volledig overzicht dat continu wordt bijgewerkt. Dit is consistent met de regulatoire vereisten en het kritieke karakter van water-infrastructuur. Daarentegen heeft één organisatie nog nooit hun asset-inventaris bijgewerkt, wat een aanzienlijk cybersecurityrisico vormt.

Deze bevindingen komen overeen met internationale trends waarbij asset visibility wordt erkend als de fundamentele eerste stap in cybersecurity, zoals benadrukt in recente SANS onderzoeken.

NETWERKSEGMENTATIE EN ARCHITECTUUR

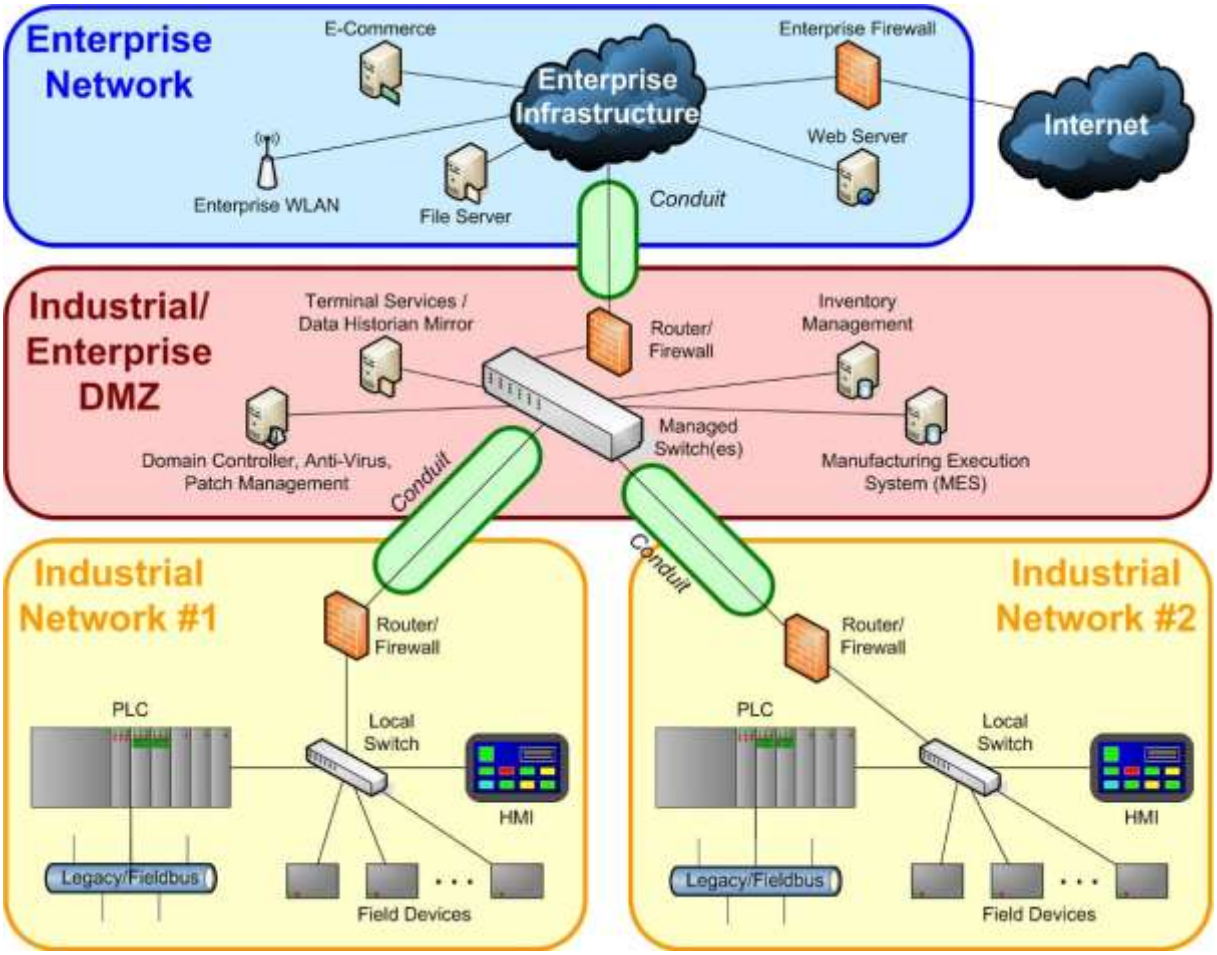
Netwerksegmentatie vormt een kritieke verdedigingslijn tegen laterale beweging van aanvallers binnen industriële netwerken. De enquêteresultaten tonen:

IT/OT Netwerk Scheiding:

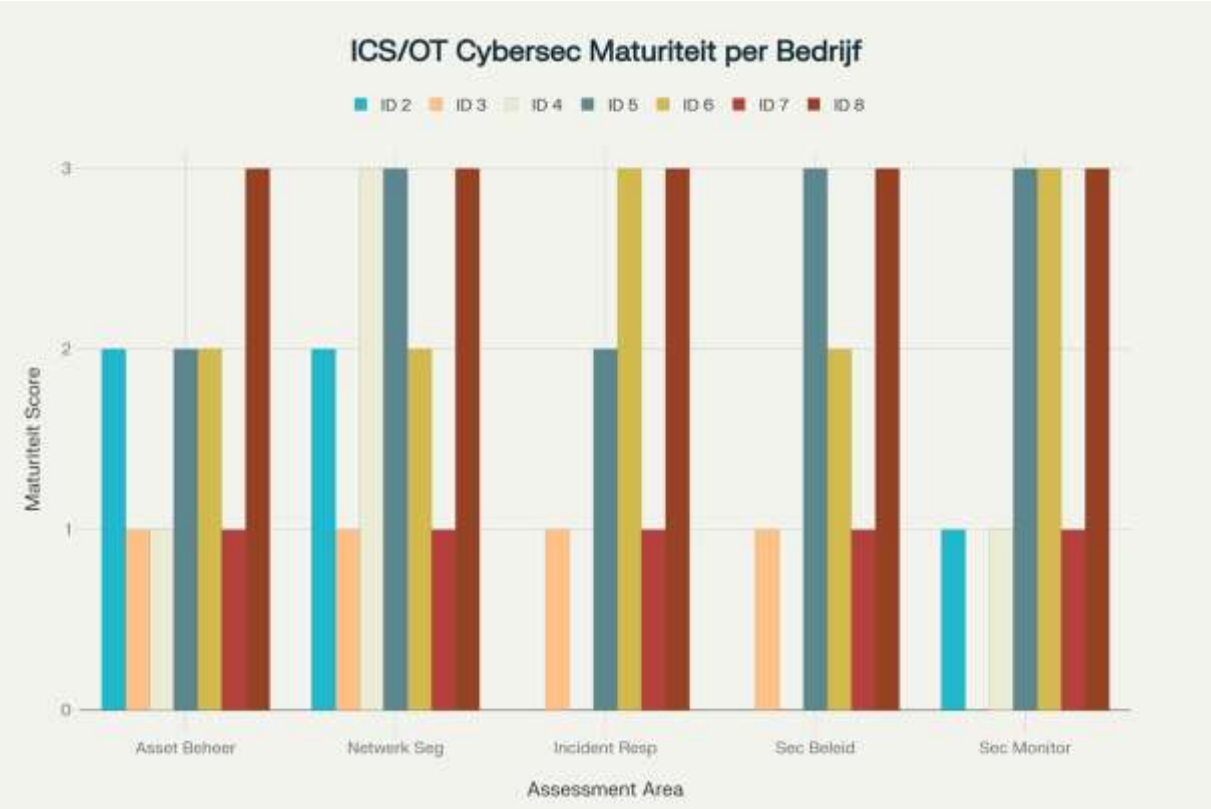
- Volledig gescheiden: 3 organisaties (43%)
- Grotendeels gescheiden: 2 organisaties (29%)
- Gedeeltelijk gescheiden: 2 organisaties (29%)

Firewall Implementatie:

- Strikte regels: 3 organisaties (43%)
- Basisregels: 3 organisaties (43%)
- Enkele firewalls: 1 organisatie (14%)



De resultaten tonen dat grotere organisaties en kritieke infrastructuur operators meer geavanceerde segmentatie hebben geïmplementeerd. Dit is consistent met internationale best practices en frameworks zoals ISA/IEC 62443 die zone-gebaseerde architecturen voorschrijven.



Cybersecurity-maturiteitsniveaus van de 7 enquêtebedrijven across verschillende kritieke veiligheidsdomeinen

INCIDENT RESPONSE EN HERSTELTIJD

INCIDENT RESPONSE PLAN MATURITEIT:

- Uitgebreid plan: 2 organisaties (29%)
- Basis plan: 1 organisatie (14%)
- Informeel plan: 2 organisaties (29%)
- Geen plan: 2 organisaties (29%)

GESCHATTE HERSTELTIJD:

- <4 uur: 1 organisatie (14%)
- 4-24 uur: 2 organisaties (29%)
- 1-3 dagen: 2 organisaties (29%)
- 3 dagen: 1 organisatie (14%)
- Geen idee: 1 organisatie (14%)

Deze resultaten zijn zorgwekkend, aangezien 28% van de organisaties geen specifiek ICS/OT incident response plan heeft. Dit is problematisch gezien de unieke eisen van OT-omgevingen waar veiligheid en continuïteit voorrang hebben op traditionele IT-security prioriteiten.

De variatie in hersteltijd (<4 uur tot >3 dagen) illustreert de enorme kloof tussen well-prepared en unprepared organisaties. Internationaal onderzoek toont dat organisaties met uitgebreide IR-plannen significant sneller herstellen van cyberincidenten.

GOVERNANCE EN FORMEEL CYBERSECURITYBELEID

FORMEEL CYBERSECURITYBELEID:

- Uitgebreid beleid: 2 organisaties (29%)
- Basis beleid: 1 organisatie (14%)
- Informeel beleid: 2 organisaties (29%)
- Geen beleid: 2 organisaties (29%)

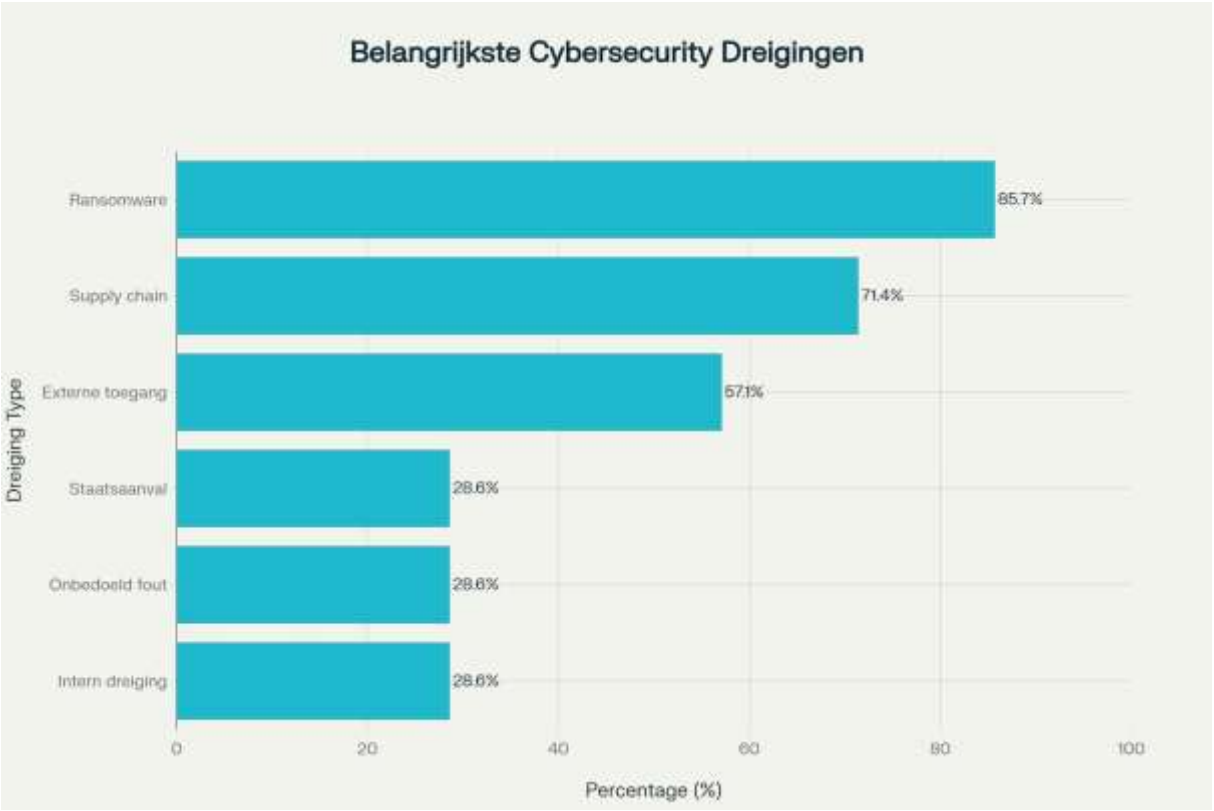
DIRECTIETOEZICHT:

- Directie/raad betrokkenheid: 5 organisaties (71%)
- Geen directietoezicht: 2 organisaties (29%)

De positieve bevinding is dat de meerderheid (71%) directietoezicht heeft op cybersecurity, wat cruciaal is voor effectieve cybersecurityprogramma's. Dit komt overeen met trends in de NIS2-implementatie waar executive accountability wordt benadrukt.

DREIGINGSPERCEPTIE EN RISICOBEWUSTZIJN

De enquête identificeerde de primaire cybersecurityzorgen van de respondenten, wat cruciale inzichten biedt in hun risicoperceptie en de werkelijke dreigingen waarmee ze geconfronteerd worden.



Top cybersecurity dreigingen die de meeste zorgen baren bij Vlaamse productie- en procesbedrijven, gerangschikt naar het percentage bedrijven dat elke dreiging identificeerde als topprioriteit

TOP CYBERSECURITY DREIGINGEN:

1. **Ransomware**: 85.7% (6/7 bedrijven)
2. **Supply chain aanvallen**: 71.4% (5/7 bedrijven)
3. **Externe toegang**: 57.1% (4/7 bedrijven)
4. **Interne dreigingen**: 28.6% (2/7 bedrijven)
5. **Onbedoelde fouten**: 28.6% (2/7 bedrijven)
6. **Staatsgesponsorde aanvallen**: 28.6% (2/7 bedrijven)

Deze prioritering komt sterk overeen met internationale trends. Onderzoek van Dragos toont dat ransomware-aanvallen op industriële organisaties in 2024 met 87% zijn toegenomen, waarbij manufacturing het zwaarst getroffen wordt. De focus op supply chain security weerspiegelt groeiend bewustzijn van deze complexe aanvalsvector.

TECHNOLOGIE-IMPLEMENTATIE EN BEVEILIGINGSTOOLS

De adoptie van cybersecuritytechnologieën toont een interessant patroon van universele en selectieve implementatie:

Implementatie van verschillende ICS/OT beveiligingstechnologieën bij Vlaamse productie- en procesbedrijven, toont universele VPN-adoptie maar variabele implementatie van andere kritieke technologieën

TECHNOLOGIE ADOPTIE:

- **VPN**: 100% (7/7 bedrijven) - Universele adoptie
- **Netwerkmonitoring**: 57.1% (4/7 bedrijven)
- **Intrusion Detection**: 57.1% (4/7 bedrijven)
- **SIEM**: 57.1% (4/7 bedrijven)

- **Industriële Firewalls**: 57.1% (4/7 bedrijven)
- **ICS/OT-antivirus**: 42.9% (3/7 bedrijven)

De universele VPN-adoptie illustreert de impact van COVID-19 op remote access behoeften. Echter, de beperkte adoptie van meer geavanceerde technologieën zoals SIEM en industriële firewalls wijst op resource- en expertisebeperkingen bij kleinere organisaties.

PERSONEEL EN EXPERTISE

TOEGEWIJD CYBERSECURITY PERSONEEL:

- **Fulltime personeel**: 1 organisatie (14%)
- **Gedeeld IT/OT team**: 2 organisaties (29%)
- **Externe expertise:** 2 organisaties (29%)
- **Geen toegewijd personeel**: 2 organisaties (29%)

TIJD BESTEED AAN CYBERSECURITY:

- **<10%:** 5 organisaties (71%)
- **10-25%:** 1 organisatie (14%)
- **25-50%:** 1 organisatie (14%)

Deze cijfers benadrukken een kritieke uitdaging: de meerderheid van organisaties besteedt minder dan 10% van hun IT/OT-tijd aan cybersecurity, wat onvoldoende is voor effectieve bescherming tegen de groeiende dreigingen.

Vergelijking met Internationale Benchmarks

SANS 2024 ICS/OT CYBERSECURITY BENCHMARK

Vergelijking met het SANS 2024 onderzoek onder 530 industriële cybersecurity professionals wereldwijd toont dat Vlaamse organisaties zowel voor- als achterlopen op internationale trends:

Positieve Trends:

- **Detection Tijd**: Internationale trend toont verbetering van dagen (2019) naar uren (2024). Vlaamse respondenten tonen vergelijkbare verbeteringen bij mature organisaties
- **Multi-factor Authenticatie**: 57% van Vlaamse organisaties gebruikt MFA voor externe toegang, vergelijkbaar met internationale trends
- **Executive Oversight**: 71% heeft directietoezicht, wat hoger is dan het internationale gemiddelde

Uitdagingsgebieden:

- **Incident Response Plans**: 28% heeft geen specifiek ICS/OT IR-plan, vergelijkbaar met de internationale bevinding van 28% zonder toegewijd plan
- **Asset Visibiliteit**: Slechts 14% heeft volledig asset overzicht, wat lager is dan internationale best-performers
- **Dedicated Personnel**: Slechts 14% heeft fulltime ICS/OT cybersecurity personeel, significant lager dan internationale leaders

NIS2 COMPLIANCE PARAATHEID

Met de implementatie van NIS2 in oktober 2024 moeten veel van deze organisaties voldoen aan striktere cybersecurityvereisten. De analyse toont dat:

- Slechts 29% heeft uitgebreide formele cybersecuritybeleid
- 43% heeft adequate incident response capabilities
- Geen enkele organisatie voldoet volledig aan alle NIS2-vereisten zonder aanvullende investeringen

Dit wijst op een aanzienlijke compliance gap die urgent aandacht vereist.

IDENTIFICATIE VAN KRITIEKE BEHOEFTEN

In de snel evoluerende wereld van industriële automatisering en cyberdreigingen verschuift cybersecurity van een optioneel aandachtspunt naar een strategische noodzaak. Voor organisaties die actief zijn in industriële controlesystemen (ICS) en operationele technologie (OT) is het essentieel om een gefaseerde, structurele aanpak te hanteren die zowel kortetermijndoelen als langetermijnstrategieën omarmt. Deze aanpak moet aangepast zijn aan de grootte van de organisatie, beschikbare middelen en de complexiteit van IT/OT-integratie. In deze context worden drie belangrijke tijdshorizonten onderscheiden: kortetermijnprioriteiten (0-12 maanden), middellange termijn initiatieven (1-3 jaar) en langetermijnstrategische behoeften (3-5 jaar).

KORTETERMIJNPRIORITEITEN (0-12 MAANDEN)

De basis van elke robuuste ICS/OT cybersecuritystrategie begint bij het creëren van zichtbaarheid, het voorbereiden op incidenten en het opzetten van fundamentele monitoringmechanismen. Drie kernactiviteiten vormen de speerpunten in deze fase.

Als eerste is de inventarisatie en automatische ontdekking van IT- en OT-assets essentieel. Voor veel organisaties worden assetlijsten slechts zelden of helemaal niet bijgewerkt. Het gebruik van geautomatiseerde asset discovery tools is daarom cruciaal om een actueel overzicht te krijgen van alle verbonden systemen en apparaten. Zonder deze basis ontbreekt het inzicht om andere beveiligingsmaatregelen effectief te implementeren. Deze transparantie is een noodzakelijke bouwsteen voor risicobeoordeling, vulnerability management en netwerksegmentatie.

Een tweede prioriteit vormt de ontwikkeling van een incident response plan dat specifiek is afgestemd op OT-omgevingen. Historisch gezien zijn veel industriële organisaties slecht voorbereid op incidentmanagement, waarbij 29% aangeeft geen formeel plan te hebben. Het ontbreken van OT-specifieke procedures vergroot het risico op operationele en veiligheidsincidenten bij cyberaanvallen. Effectieve incident response vereist training van personeel, duidelijke veiligheidsprotocols, gecoördineerde respons tussen IT- en OT-teams, en uitgewerkte communicatiestrategieën voor externe stakeholders. De implementatiekosten voor een dergelijk plan worden geschat tussen €25.000 en €75.000 per organisatie.

Ten derde behoort basis netwerkmonitoring tot de onmisbare fundamenten. Organisaties zonder visibiliteit op hun OT-netwerk blijven blind voor mogelijke indringers of afwijkingen in netwerkgedrag. Passieve en non-intrusive monitoringtechnologieën die speciaal ontwikkeld zijn voor industriële omgevingen maken het mogelijk om het netwerkverkeer te volgen zonder de productieomgeving te verstoren. Ongeveer 29% van de organisaties beschikt vandaag niet over enige vorm van monitoring. De investering voor basis monitoringtechnologieën varieert doorgaans tussen €30.000 en €80.000.

MIDDELLANGE TERMIJN INITIATIEVEN (1-3 JAAR)

Na het leggen van een solide basis, verschuift de focus naar een volgend niveau van maturiteit: structurele verbetering van netwerkarchitectuur, operationele processen en detectiemogelijkheden.

Een belangrijke stap in deze fase is de implementatie van micro-segmentatie en een zero trust architectuur. In veel industriële netwerken ontbreekt voldoende netwerksegmentatie, waardoor een indringer zich zonder veel hinder binnen het netwerk kan verplaatsen. Micro-segmentatie per zone of per functie maakt het mogelijk om laterale beweging van aanvallers drastisch in te perken. De toepassing van zero trust principes verhindert toegang tenzij expliciet geverifieerd. Dit vraagt om een doordacht ontwerp dat geen impact heeft op productiecontinuïteit en dat

geschikt is voor systemen die al jaren draaien op legacy-software. De gemiddelde investering voor micro-segmentatieprojecten komt uit tussen €100.000 en €300.000 per organisatie.

Even cruciaal is de beschikbaarheid van continue monitoring via Security Operations Center (SOC)-diensten. Voor kleinere en middelgrote organisaties kan een gedeeld of gemanaged SOC een haalbare oplossing zijn die 24/7 dreigingsdetectie biedt zonder dat hiervoor een intern team nodig is. Zeker voor organisaties zonder voldoende interne expertise kan dit het verschil betekenen tussen vroege detectie of volledig verrast worden door een aanval. SOC-diensten vereisen doorgaans een jaarlijkse investering van €50.000 tot €150.000 per organisatie.

Tenslotte moet cybersecuritybeleid zich ontwikkelen tot structureel kwetsbaarheids- en patchmanagement bij industriële systemen. Vele organisaties zijn terughoudend in het doorvoeren van beveiligingsupdates uit vrees voor productieverstoringen. Hierdoor ontstaan kwetsbaarheden die jarenlang niet aangepakt worden. Het opzetten van gestructureerde processen, voorzien van offline testomgevingen en robuuste change management procedures, is geen luxe maar een noodzaak. Naar schatting heeft 43% van de organisaties op dit moment geen formeel patchproces. De implementatiekost voor dit traject bedraagt gemiddeld €75.000 tot €200.000.

LANGETERMIJNSTRATEGISCHE BEHOEFTEN (3-5 JAAR)

Op langere termijn verschuift de focus van technologieën en processen naar duurzame, structurele capaciteitsopbouw en samenwerking binnen de sector. Zonder langetermijnstrategieën blijven inspanningen gefragmenteerd.

Een van de meest urgente strategische prioriteiten is talentontwikkeling. Het structurele tekort aan ICS/OT cybersecurity-specialisten belemmert vooruitgang op alle fronten. Een regionaal programma met dual-learning trajecten, nauwe samenwerking met onderwijsinstellingen en praktijkgerichte opleidingen kan een blijvend effect genereren. De investering voor zo'n programma wordt geraamd op €2 tot €5 miljoen, verspreid over meerdere jaren en gericht op het opbouwen van capaciteit binnen de regio.

Daarnaast is supply chain security management van strategisch belang. Organisaties opereren zelden geïsoleerd – hun leveranciers en partners vormen kritieke schakels waarbij een lek zich snel door de keten kan verspreiden. Het structureel evalueren van leveranciers op security-niveau, het hanteren van contractuele verplichtingen en het inzetten van monitoringtools zorgt voor een aanzienlijk robuustere toeleveringsketen. Met 71,4% van de organisaties die de supply chain als topbedreiging aanduiden, is dit een niet te negeren uitdaging. Jaarlijkse investeringen voor deze aanpak liggen tussen €50.000 en €150.000.

Ten slotte kan proactieve verdediging slechts bereikt worden door toegang tot relevante threat intelligence. Sector-specifieke dreigingsinformatie stelt organisaties in staat om aanvallen vroegtijdig te herkennen en zich gericht voor te bereiden. Het oprichten van regionale informatie-uitwisselingsplatforms, ondersteund door dreigingsfeeds, biedt toegevoegde waarde voor alle betrokken partijen. De kosten hiervoor variëren van €100.000 tot €250.000 per organisatie per jaar, afhankelijk van de mate van deelname en de technologie die wordt ingezet.

MAATREGELEN PER ORGANISATIEGROOTTE

Afhankelijk van de schaal en complexiteit van een organisatie verschillen de prioriteiten en haalbare maatregelen.

Kleine organisaties (11-50 werknemers), vaak vertegenwoordigd door ID 7, worstelen met hun beperkte middelen, gebrek aan gespecialiseerde medewerkers en gedeelde IT/OT-verantwoordelijkheden. Voor hen ligt de focus op pragmatische, schaalbare oplossingen. Het inschakelen van managed security services, gebruikmaken van cloud-gebaseerde tools en deelname aan consortium-initiatieven bieden kostenefficiënte bescherming. Deze organisaties hebben baat bij fundamentele trainingen en awareness-programma's. De totale investering ligt tussen €75.000 en €150.000 op jaarbasis.

Middelgrote organisaties (51-250 werknemers), waaronder spelers als ID 3, ID 4 en ID 6, balanceren tussen kostefficiëntie en het bouwen van robustere processen. Ze beschikken soms over interne securitykennis, maar missen de schaal om alles zelf te doen. Een hybride aanpak waarbij kernexpertise intern wordt ontwikkeld terwijl gespecialiseerde diensten extern worden betrokken is hier aanbevolen. Gefaseerde implementaties op basis van risico-evaluatie, gekoppeld aan sectorale samenwerking, versterken structureel de weerbaarheid. Jaarlijks vraagt deze aanpak een investering tussen €150.000 en €300.000.

Grote organisaties (>250 werknemers), zoals ID 2, ID 5 en ID 8, worden geconfronteerd met complexe netwerken en hogere verwachtingen qua compliance en dreigingsweerbaarheid. Zij kunnen het zich permitteren om dedicated security-teams aan te stellen, geavanceerde technologische stacks te implementeren en zelfstandig een proactieve

houding aan te nemen via threat hunting en deelname aan internationale security overlegstructuren. Voor deze organisaties liggen de jaarlijkse investeringsniveaus tussen €300.000 en €750.000.

BELEIDSAANBEVELINGEN VOOR STAKEHOLDERS

Regionale overheden en instanties zoals VLAIO spelen een sleutelrol in het faciliteren van cybersecurity bij industriële organisaties. Allereerst wordt aanbevolen om een regionaal cybersecurity competence center op te richten dat zich specifiek richt op industriële sectoren. Zo'n centrum biedt assessments, trainingen en ondersteuning bij incidentrespons, vooral voor kleine en middelgrote ondernemingen die zelf niet over deze expertise beschikken.

Daarnaast kan gerichte subsidiëring het verschil maken. Hogere steunpercentages voor investeringen in ICS/OT-beveiligingen en nieuwe fiscale stimulansen voor training en certificering versterken de motivatie voor structurele verbetertrajecten. Co-financiering van sectorale initiatieven verlaagt de drempel voor collectieve actie.

Tot slot verdient harmonisatie van regelgeving de nadruk. Veel organisaties ervaren compliance als complex of zelfs verwarrend door overlappende normen zoals ISO 27001, NIST CSF en IEC 62443. Er is nood aan sector-specifieke richtlijnen en vereenvoudigde compliance modellen die bevattelijk en toepasbaar zijn, vooral voor kleinere bedrijven.

Brancheorganisaties hebben op hun beurt een rol in het uitdragen van best practices, het organiseren van gezamenlijke inkoop van securitydiensten, en het opzetten van sector-brede incidentresponsstructuren. Door bedreigingsinformatie op anonieme basis te delen en lessons learned na incidenten transparant te communiceren, bouwen zij mee aan het collectieve leervermogen van de sector.

Cybersecuritydienstverleners worden aangemoedigd om hun producten en diensten professioneel af te stemmen op industriële noden. Dit omvat het ontwikkelen van OT-specifieke assessments, het aanbieden van flexibele managed services, en het verzorgen van opleidingen gericht op operators en technici. Door bruggen te slaan met industriële leveranciers, internationale securityorganisaties en academische instellingen kunnen zij een sleutelpositie innemen in het ecosysteem.

Conclusie en Toekomstperspectieven

Deze enquête onder Vlaamse productie- en procesbedrijven onthult een cybersecuritylandschap in transitie, gekenmerkt door significante verschillen in maturiteit en een groeiend bewustzijn van cybersecurityrisico's. De bevindingen illustreren zowel de vooruitgang die is geboekt als de substantiële uitdagingen die nog moeten worden aangepakt.

KERNBEVINDINGEN

De kernbevindingen van de analyse van de Vlaamse industriële cybersecuritytoestand geven een gemengd beeld van positieve ontwikkelingen enerzijds en hardnekkige uitdagingen anderzijds. Aan de positieve zijde is het bemoedigend om vast te stellen dat er een universele adoptie heeft plaatsgevonden van fundamentele cybersecuritytechnologieën, zoals het gebruik van Virtual Private Networks (VPN). Dit wijst erop dat basismaatregelen breed ingeburgerd zijn geraakt, wat een eerste stap vormt in het versterken van het digitale weerstandsvermogen van organisaties.

Even belangrijk is de constatering dat er binnen een ruime meerderheid van organisaties – ongeveer 71 procent – sprake is van een duidelijke betrokkenheid van het management bij cybersecuritygovernance. Dit duidt op een groeiend strategisch bewustzijn bij de besluitvormers dat cybersecurity niet langer een operationele IT-aangelegenheid is, maar een integraal onderdeel vormt van bredere bedrijfsvoering en risicomanagement.

Bovendien laat de sector een realistisch en actueel inzicht zien in de voornaamste dreigingen. De herkenning van risico's als ransomware-aanvallen en kwetsbaarheden in de toeleveringsketen toont aan dat de perceptie van gevaar goed is afgestemd op de globale trends in het dreigingslandschap. Ten slotte valt op dat inmiddels bij meer dan de helft van de bevraagde bedrijven concrete stappen zijn gezet richting netwerksegmentatie. Dit is een belangrijke maatregel die het mogelijk maakt om indringers te isoleren en de impact van incidenten te beperken.

Tegenover deze positieve signalen staan echter nog steeds structurele tekortkomingen die de digitale weerbaarheid ernstig ondermijnen. Een van de meest prangende problemen is de grote spreiding in maturiteitsniveaus van cybersecurity tussen verschillende organisaties. Waar sommige bedrijven al geavanceerde technologieën inzetten en duidelijke beleidskaders hebben, blijft een substantiële groep achter met minimale of inconsistente beveiligingsmaatregelen.

Een tweede kloof bevindt zich in het domein van assetvisibiliteit en inventarisatie. Ondanks de centrale rol van asset management in elk modern beveiligingsraamwerk, blijkt slechts 14 procent van de organisaties hun volledige IT- en OT-infrastructuur accuraat en up-to-date in kaart te hebben gebracht. Dit betekent dat een overgrote meerderheid nog steeds in het duister tast over wat er precies op hun netwerken actief is—aangezien je niet kunt beveiligen wat je niet kent, vormt dit een fundamenteel risico.

Verder is er een merkbaar tekort aan gespecialiseerde expertise op het kruispunt van industriële controlesystemen (ICS) en cybersecurity. Veel organisaties beschikken niet over dedicated ICS/OT-beveiligingsprofessionals, waardoor ze worstelen met het toepassen van conventionele IT-beveiligingspraktijken binnen operationele omgevingen. Deze lacune in interne kennis en capaciteit leidt vaak tot suboptimale beslissingen, verlengde incidentresponstijden en een verhoogde kans op menselijke fouten.

De zwakke voorbereiding op incidenten is nog een andere kritieke tekortkoming. Ongeveer 28 procent van de bevraagde bedrijven heeft geen specifiek OT-incidentresponsplan beschikbaar. In een sector waar downtime directe economische en veiligheidsconsequenties heeft, is het ontbreken van gestandaardiseerde incidentprocedure een wezenlijk struikelblok voor effectieve respons en herstel.

Tot slot blijkt dat de inzet van meer geavanceerde detectietechnologieën, zoals anomaly detection of real-time threat intelligence feeds, voorlopig beperkt blijft. Hierdoor ontbreekt bij veel organisaties het vermogen om proactief aanvallen te detecteren, waardoor men voornamelijk op reactieve basis handelt naarmate incidenten zich voltrekken.

STRATEGISCHE IMPLICATIES

De strategische implicaties van deze bevindingen zijn aanzienlijk. De Vlaamse industriële sector bevindt zich op een keerpunt. Het momentum voor structurele investeringen in cyberveiligheid is aanwezig, maar het venster waarin deze transformatie moet plaatsvinden is smal. De cyberdreigingen evolueren snel, terwijl regelgeving zoals NIS2 ondertussen dwingende eisen oplegt aan organisaties die als essentieel of belangrijk worden aangemerkt. Wie nu niet investeert, loopt het risico zichzelf buiten spel te zetten in een steeds digitaler wordende markt.

Daarbij komt dat de groeikloof tussen de voorlopers en de achterblijvers groter wordt. Het gevolg is dat uniforme beleidsmaatregelen of technologische oplossingen waarschijnlijk niet effectief zullen zijn over de hele lijn. Differentiatie is noodzakelijk: beveiligingsinterventies moeten worden afgestemd op de grootte van een organisatie, haar sectorgebonden risico's en haar beschikbare middelen. Kleine organisaties hebben bijvoorbeeld nood aan laagdrempelige ondersteuning en gestandaardiseerde diensten, terwijl grote spelers vooruitstrevende technologieën en processen moeten inzetten om geavanceerde aanvallen af te weren.

Volgens de analyse is er een acute en groeiende behoefte aan vier structurele maatregelen. Ten eerste moet systematische capaciteitsopbouw plaatsvinden specifiek gericht op kleinere organisaties, die momenteel het meest kwetsbaar en onderbewapend zijn tegenover digitale dreigingen. Initiatieven zoals regionale competence centers, gedeelde diensten en gesubsidieerde opleidingen kunnen hen hierbij ondersteunen.

Ten tweede is er nood aan geavanceerde verdedigingscapaciteiten voor organisaties die verantwoordelijk zijn voor kritieke infrastructuur. Deze moeten in staat zijn om niet enkel goed te reageren, maar ook om proactief risico's te signaleren en indringers te detecteren voor ze schade kunnen aanrichten.

Ten derde is regionale samenwerking een noodzakelijke hefboom. Door informatie, kennis en middelen te delen, kunnen organisaties zich gezamenlijk verdedigen tegen cyberdreigingen die steeds vaker collectief en internationaal georganiseerde vormen aannemen. Sectoroverschrijdende samenwerking kan bovendien helpen bij standaardisatie, snelle respons en peer learning.

Ten vierde is structurele investering in talentontwikkeling essentieel om de huidige capaciteitstekorten op te vangen en duurzaam op te lossen. Zonder voldoende ICS/OT-specialisten zullen bedrijven niet in staat zijn om verantwoord te groeien op het vlak van cybersecurity. Het opzetten van specifieke opleidingstrajecten, nauwere samenwerking met hogescholen en universiteiten, en het aanmoedigen van herscholingstrajecten binnen bestaande personeelsbestanden kunnen hierin het verschil maken.

Samenvattend maken de bevindingen duidelijk dat Vlaamse productie- en procesbedrijven reeds enkele belangrijke stappen vooruit hebben gezet op het vlak van cybersecurity, maar ook dat de weg naar echte weerbaarheid nog lang is. Door nu een samenhangende en gedifferentieerde strategie te implementeren die zowel bedrijven als beleidsmakers, dienstverleners en opleidingsinstellingen betrekt, kan de sector zich voorbereiden op een toekomst waarin cyberdreiging de norm is, maar niet langer een struikelblok voor groei en innovatie hoeft te zijn.

AANBEVOLEN ACTIES VOOR STAKEHOLDERS

In het kader van een toekomstgerichte en risicogestuurde aanpak voor cybersecurity binnen Vlaamse productie- en procesindustrieën, is het van essentieel belang dat alle relevante stakeholders – waaronder overheden, brancheorganisaties, cybersecuritydienstverleners en de bedrijven zelf – zich actief en gecoördineerd inzetten voor de realisatie van specifieke, haalbare acties. Deze acties moeten niet alleen inspelen op de acute noden op korte termijn, maar ook uitgroeien tot structurele oplossingen op middellange en lange termijn. Enkel via gerichte, onderbouwde investeringen in mensen, processen en technologie kan de sector haar cyberweerbaarheid versterken en tegelijkertijd haar positie binnen de internationale digitale economie verstevigen.

In de komende twaalf maanden ligt de nadruk op het implementeren van fundamentele maatregelen die als hoekstenen dienen voor verdergaande ontwikkelingen. Allereerst is het absoluut noodzakelijk dat organisaties starten met de implementatie van geautomatiseerde asset discovery en inventory management. In veel gevallen blijkt dat organisaties nog steeds werken met onvolledige of sterk verouderde overzichten van hun IT- en OT-assets. Zonder een accuraat inzicht in wat er op het netwerk actief is, blijven alle andere beveiligingsmaatregelen ineffectief of onvolledig.

Tegelijkertijd dringt zich de nood op om OT-specifieke incident response plannen uit te werken. Veel van de bestaande richtlijnen zijn gefocust op klassieke IT-incidenten en houden onvoldoende rekening met de unieke

context van industriële productieomgevingen. Hierbij moeten veiligheid, continuïteit en samenwerking tussen IT- en OT-teams centraal staan. Deze plannen moeten niet alleen op papier bestaan, maar ook vertaald worden naar effectieve opleiding en oefeningen.

Een gelijktijdige prioriteit is de uitrol van passieve netwerkmonitoring bij organisaties die momenteel geen zicht hebben op het gedrag van hun OT-netwerkverkeer. Met de toenemende complexiteit en schaal van industriële netwerken is het cruciaal om anomalieën tijdig te detecteren, nog vóór deze kunnen uitgroeien tot operationele verstoringen of veiligheidsincidenten. Bij voorkeur gebeurt dit via non-intrusieve technologie, specifiek ontworpen voor de OT-context.

Tot slot moet er op korte termijn ook gestart worden met NIS2-compliance trajecten binnen organisaties die onder deze Europese regelgeving vallen. Met de inwerkingtreding van deze verordening neemt de druk toe om concrete maatregelen te nemen rond risicoanalyse, incidentrapportage, leveranciersonderzoek en structurele cybersecurity governance. Door reeds in deze fase te anticiperen op NIS2-eisen kunnen bedrijven hun compliance op kostenefficiënte wijze verankeren binnen bestaande processen.

Binnen de middellange termijn – namelijk binnen een tijdshorizon van één tot drie jaar – verschuift de focus naar opschaling, institutionalisering en samenwerking. Een cruciale stap is de operationele uitrol van een regionaal cybersecurity competence center gericht op industriële omgevingen. Dergelijk centrum kan bedrijven ondersteunen met maturity assessments, adviesdiensten, opleidingen en responsondersteuning. Zeker voor kleinere en middelgrote ondernemingen die niet over interne expertise beschikken, biedt dit centrum toegang tot harde kennis en toepasbare begeleiding.

Daarop aansluitend moet op sectorniveau een threat intelligence sharing platform worden opgezet dat industriële bedrijven toelaat om relevante dreigingsinformatie op een veilige, geanonimiseerde en operationeel bruikbare manier te delen. Dit verhoogt de paraatheid binnen de hele sector en creëert een cultuur van collectieve weerbaarheid. Idealiter wordt deze informatiedeling ondersteund door een samenwerking tussen bedrijven, onderzoekers, overheidsinstanties en technologieaanbieders.

Tegelijkertijd wordt het raadzaam om de gefaseerde implementatie van micro-segmentatie en zero-trust architecturen op te starten. Veel industriële netwerken zijn nog vlak gestructureerd, waardoor aanvallers zich vrij kunnen bewegen zodra ze toegang verkrijgen. Door segmentatie en een beleid van default-deny toe te passen, ontstaat een netwerkarchitectuur die gebaseerd is op minimale toegang en continue verificatie. Dit moet zorgvuldig gebeuren om operationele stabiliteit niet in het gedrang te brengen.

Voor kleinere organisaties biedt het collectief opzetten of afnemen van Security Operations Center-diensten een pragmatische oplossing. Deze managed diensten zorgen voor continu toezicht, incidentdetectie en ondersteuning bij respons, zonder dat hier een eigen team voor nodig is. Idealiter worden deze diensten gedeeld tussen meerdere kleinere ondernemingen via sectorale verbanden of onder leiding van het voorgenoemde competence center.

Kijkend naar de langere termijn – doorgetrokken over een periode van drie tot vijf jaar – staat structurele capaciteitsopbouw en internationale positionering centraal. Het structureel aantrekken, opleiden en behouden van talent in ICS/OT cybersecurity is één van de meest kritieke succesfactoren. Een gecoördineerd programma in samenwerking met onderwijsinstellingen is noodzakelijk, waarbij dual-learning trajecten, stages, gespecialiseerde bachelor- en masteropleidingen en praktijkgerichte certificeringen ontwikkeld worden. België, en in het bijzonder Vlaanderen, kan zich nationaal en internationaal onderscheiden door proactief te investeren in een sterke talentenpijplijn.

Een tweede strategisch element is het opbouwen van geavanceerde threat hunting- en incident response-capaciteiten. Waar organisaties in eerdere fasen vooral reactief werkten aan detectie, vereist de steeds geavanceerdere dreigingsomgeving dat organisaties zelf in staat zijn om proactief bedreigingen op te sporen voordat deze zich manifesteren. Dit vergt investering in kennis, technologie zoals machine learning en gedragsanalyse, en schaalbare processen die 24/7 operationeel kunnen zijn (eventueel vanuit een gedeeld SOC).

Daarnaast zal het ontwikkelen van supply chain security management frameworks noodzakelijk zijn, waarbij organisaties structureel leveranciers screenen op beveiligingscriteria, contractueel verantwoordelijkheden verankeren en via tooling continu zicht houden op derde partijen. De toenemende verwevenheid van industriële processen maakt dat zwakke schakels in de keten snel kunnen uitgroeien tot systeemrisico's.

Langs strategische kant krijgt Vlaanderen met deze initiatieven ook de kans om zich internationaal te positioneren als toonaangevend in industriële cybersecurity. Door tijdig en doordacht te investeren in deze domeinen kunnen

Vlaamse productiebedrijven zich onderscheiden als betrouwbare economische partners op het vlak van digitale weerbaarheid, wat hun exportpositie en aantrekkelijkheid voor internationale investeerders ten goede zal komen.

De resultaten van het enquêteonderzoek waarop dit actieplan is gebaseerd, vormen een robuuste basis voor een evidence-based aanpak. Dit geeft richting aan strategieën die aansluiten op de Belgische ambitie om tegen 2025 tot de bestbeveiligde Europese landen te behoren op het vlak van cyberveiligheid. Door de gemeten noden en prioriteiten te vertalen naar gefaseerde acties kunnen productie- en procesbedrijven hun cyberweerbaarheid niet alleen verhogen, maar ook hun concurrentiekracht versterken binnen een steeds digitaler wordende industrie.

Toch blijft het niet bij inzicht: het welslagen van deze strategie vereist dat alle belanghebbende partijen deze aanbevelingen vertalen naar concrete actie. De uitdagingen zijn niet gering, maar ook niet onoverkomelijk als de krachten gebundeld worden. Overheden, bedrijfsleven, academische wereld en dienstverleners moeten hun rol opnemen binnen een gedeeld ecosysteem waarin samenwerking en kennisdeling centraal staan.

Voor de verdere uitrol van dit plan worden meerdere vervolgstappen voorgesteld. In eerste instantie is het wenselijk de initiële enquête op grote schaal uit te breiden om de geldigheid van de bevindingen te versterken en regionale verschillen beter te begrijpen. Parallel daaraan zouden sector-specifieke maturity assessment tools ontwikkeld moeten worden waarmee bedrijven hun huidige status kunnen meten en doelgericht kunnen groeien.

Verder zouden pilootprojecten gestart kunnen worden rond prioritaire initiatieven, zoals automated asset discovery, incident response planning en netwerkmonitoring. Deze projecten kunnen als voorbeeld dienen voor bredere toepassing en sneller leertraject. Tegelijkertijd is het belangrijk om met periodieke metingen, bijvoorbeeld per kwartaal, de voortgang systematisch op te volgen, zodat succes en stagnatie tijdig herkend worden.

Tot slot is het opportuun om een internationale benchmarkingstudie te initiëren waarbij gekeken wordt waar Vlaanderen zich positioneert ten opzichte van andere industriële regio’s binnen Europa of daarbuiten. Dit laat toe om strategisch bij te sturen en vormt de basis voor bredere beleidsinitiatieven rond industriële veerkracht.

Wanneer deze aanpak gestructureerd en gecoördineerd wordt doorgevoerd, ondersteunt dit de transformatie van de Vlaamse industrie naar een toekomst waarin cybersecurity geen rem meer vormt op groei en innovatie, maar integendeel een katalysator is voor duurzaam concurrentievoordeel.